

## DATENSCHUTZERKLÄRUNG FÜR EUROPA

Willkommen bei myoncare, dem digitalen Gesundheitsportal und der mobilen App ("App") für eine effiziente und bedarfsgerechte Patientenversorgung und Unterstützung des betrieblichen Gesundheitsmanagements.

Für uns bei der Oncare GmbH (im Folgenden "**ONCARE**" oder "**wir**", "**Wir**", "**unser**"), ist der Schutz Ihrer Privatsphäre und aller personenbezogenen Daten, die sich während der Nutzung der App auf Sie beziehen, von großer Bedeutung und Wichtigkeit. Wir sind uns der Verantwortung bewusst, die sich aus Ihrem Vertrauen in die Bereitstellung und Speicherung Ihrer personenbezogenen (Gesundheits-)Daten in der myoncare App ergibt. Daher sind unsere Technologiesysteme, die für die myoncare-Dienste verwendet werden, nach höchsten Standards eingerichtet und die rechtmäßige Verarbeitung der Daten steht im Mittelpunkt unseres ethischen Verständnisses als Unternehmen.

Wir verarbeiten Ihre personenbezogenen Daten in Übereinstimmung mit den geltenden Rechtsvorschriften zum Schutz personenbezogener Daten, insbesondere der EU-Datenschutz-Grundverordnung ("**DSGVO**") und die für uns geltenden länderspezifischen Gesetzen. In dieser Datenschutzerklärung erfahren Sie, warum und wie **ONCARE** Ihre personenbezogenen (Gesundheits-) Daten verarbeitet, die wir von Ihnen erfassen oder die Sie uns zur Verfügung stellen, wenn Sie sich für die Nutzung der myoncare App entscheiden. Insbesondere finden Sie eine Beschreibung der von uns erhobenen und verarbeiteten personenbezogenen Daten sowie des Zwecks und der Grundlage, auf der wir die personenbezogenen Daten verarbeiten, und der Ihnen zustehenden Rechte.

Bitte lesen Sie die Datenschutzrichtlinie sorgfältig durch, um sicherzustellen, dass Sie jede Bestimmung verstehen. Nachdem Sie die Datenschutzrichtlinie gelesen haben, haben Sie die Möglichkeit, der Datenschutzrichtlinie zuzustimmen und der Verarbeitung Ihrer personenbezogenen (Gesundheits-)Daten, wie in der Datenschutzrichtlinie beschrieben, zuzustimmen. Wenn Sie Ihre Einwilligung geben, wird die Datenschutzerklärung Teil des Vertrages zwischen Ihnen und Oncare.

Gemäß den Nutzungsbedingungen richtet sich unser Angebot nur an Personen ab 18 Jahren. Dementsprechend werden keine personenbezogenen Daten von Kindern und Jugendlichen unter 18 Jahren gespeichert und verarbeitet.

**Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.**

## DEFINITIONEN

**"App-Nutzer"** bezeichnet jeden Nutzer der myoncare App (Patient und/oder Mitarbeiter).

**"Blockchain"** ist im myoncare-System eine weitere Datenbank, die entsprechende Daten der Anwendung speichert.

**"Unternehmen"** bezeichnet Ihren Arbeitgeber, wenn Sie und Ihr Arbeitgeber myoncare-Tools für das betriebliche Gesundheitsmanagement des Arbeitgebers einsetzen.

**"Datendienstleister"** bezeichnet jeden Beauftragten, der von der Gesellschaft beauftragt und angewiesen wird, pseudonymisierte oder anonymisierte Mitarbeiterdaten in betrieblichen Gesundheitsmanagementprogrammen auf der Grundlage einer separaten Dienstleistungsvereinbarung mit der Gesellschaft (z. B. Datenanalyst, allgemeine Gesundheitspräventionsdienste, Datenauswertungsdienste usw.) zu sammeln, zu überprüfen und zu interpretieren, und die durch ein separates Informationsblatt an die Mitarbeiter gekennzeichnet sind.

**"Leistungserbringer"** bezeichnet Ihren Arzt, Ihre Klinik, Ihre Gesundheitseinrichtung oder andere Angehörige der Gesundheitsberufe, die allein oder im Auftrag Ihres Arztes, Ihrer Klinik oder Ihrer Gesundheitseinrichtung handeln.

**"Pathway"** ist ein standardisierter Behandlungsplan, der bestehend aus mehreren, ggfs. zeitlich aneinander gereihten Caretasks, die Schritte für Diagnosen und Therapien festlegen kann. **"Caretasks"** sind spezifische Aufgaben oder Aktionen innerhalb eines Pathways, die von den beteiligten Gesundheitsdienstleistern, dem Pflegepersonal oder dem Patienten selbst durchgeführt werden müssen.

"**myoncare App**" meint die mobile myoncare Applikation zur Verwendung durch Patienten oder Mitarbeitern, die die von ONCARE angebotenen Dienste nutzen möchten.

"**myoncare Portal**" ist das myoncare-Webportal, das für die professionelle Nutzung durch Portalnutzer bestimmt ist und als Schnittstelle zwischen Portal-Nutzern und App-Nutzer dient.

"**myoncare Tools**" meint die myoncare App und das myoncare Portal gemeinsam.

"**myoncare PWA**" bezeichnet die myoncare Progressive Web App Anwendung für Patienten, die die von ONCARE angebotenen Dienste über die PWA und nicht über die myoncare App nutzen möchten.

"**myoncare Services**" bezeichnet die Dienste, Funktionalitäten und sonstigen Angebote, die den Portalnutzern über das myoncare Portal und/oder den App-Nutzern über die myoncare App angeboten werden oder angeboten werden können.

"**ONCARE**" bedeutet ONCARE GmbH, Deutschland.

"**Portal-Benutzer**" bezeichnet jeden Gesundheitsdienstleister, jedes Unternehmen oder jeden Datendienstleister, der das webbasierte myoncare Portal nutzt.

"**Datenschutzerklärung**" meint diese Erklärung, die Ihnen als Patient und Nutzer der myoncare App gegenüber abgegeben wird und die beschreibt, wie wir Ihre personenbezogenen Informationen erfassen, nutzen und aufbewahren und die Sie über Ihre umfassenden Rechte informiert.

"**Nutzungsbedingungen**" bezeichnet die Nutzungsbedingungen für die Nutzung der myoncare App.

## VERARBEITUNG VON (BEHANDLUNGS-)DATEN

Die Oncare GmbH, ein beim Amtsgericht München unter der Registernummer 219909 eingetragenes Unternehmen mit Sitz in der Balanstraße 71a, 81541 München, Deutschland, bietet die mobile Anwendung an **myoncare App** und betreibt diese als Zugang zu den **myoncare Services**. Diese **Datenschutzerklärung** gilt für alle personenbezogenen Daten, die von ONCARE im Zusammenhang mit der Nutzung der **myoncare App** verarbeitet werden.

## WAS SIND PERSONENBEZOGENE DATEN

"**personenbezogene Daten**" bezeichnet alle Informationen, die es ermöglichen, eine natürliche Person zu identifizieren. Insbesondere beinhaltet dies Ihren Namen, Ihren Geburtstag, Ihre Adresse, Ihre Telefonnummer, Ihre E-Mail-Adresse und Ihre IP-Adresse.

"**Gesundheitsdaten**" sind personenbezogene Daten, die sich auf die physische und psychische Gesundheit einer natürlichen Person beziehen, einschließlich der Bereitstellung von Gesundheitsdiensten, die Informationen über ihren Gesundheitszustand offenbaren.

Daten sind als "**anonym**" anzusehen, wenn kein persönlicher Bezug zu der Person/dem Nutzer hergestellt werden kann.

Im Gegensatz dazu sind "**pseudonymisiert**" Daten, aus denen ein persönlicher Bezug oder persönlich identifizierbare Informationen durch einen oder mehrere künstliche Identifikatoren oder Pseudonyme ersetzt werden, die aber im Allgemeinen durch den Identifikatorschlüssel re-identifiziert werden können.

## myoncare PWA

Eine Progressive Web App (PWA) ist eine Website, die aussieht und die Funktionalität einer mobilen App hat. PWAs sind so aufgebaut, dass sie die Vorteile der nativen Funktionen von Mobilgeräten nutzen, ohne dass der Nutzer einen App-Store benötigt. Das Ziel von PWAs ist es, den Unterschied zwischen Apps und dem traditionellen Web zu kombinieren, indem die Vorteile nativer mobiler Apps in den Browser gebracht werden. Die PWA basiert auf der Technologie von "React". "React" ist eine Open-Source-Software für PWA-Anwendungen.

Um die Funktion **myoncare PWA** nutzen zu können benötigen Patienten einen Computer oder ein Smartphone und eine aktive Internetverbindung. Es ist nicht erforderlich, eine App herunterzuladen.

Einige der myoncare App-Dienste können nicht innerhalb der **myoncare PWA** genutzt werden, Details dazu siehe die Beschreibung unten. Dabei handelt es sich um die folgenden Dienstleistungen oder Spezifikationen:

- Chatten mit **Leistungserbringern**;
- Videoanrufe;

- Sicherheits-PIN-Codes;
- Tracking von Aktivitätsdaten (z.B. über AppleHealth, GoogleFit, Withings).

Die folgenden Informationen über die **myoncare App** gilt auch für die **myoncare PWA**, sofern in diesem Abschnitt nichts anderes beschrieben ist.

## WELCHE PERSONENBEZOGENEN DATEN WERDEN BEI DER NUTZUNG DER MYONCARE APP VERWENDET

Wir können die folgenden Datenkategorien über Sie bei der Nutzung der **myoncare App** verarbeiten:

**Operative Daten:** Personenbezogene Daten, die Sie uns bei der Registrierung in unserer **myoncare App**, bei der Kontaktaufnahme zu Problemen mit der App oder bei sonstigen Interaktionen mit uns zum Zweck der Nutzung der App zur Verfügung stellen.

**Daten zur Behandlung:** Sie oder Ihr Gesundheitsdienstleister stellen uns Ihre personenbezogenen Daten wie Name, Alter, Größe, Gewicht, Indikation, Krankheitssymptome und andere Informationen im Zusammenhang mit Ihrer Behandlung (z. B. in einem Pflegeplan) zur Verfügung. Zu den Informationen im Zusammenhang mit Ihrer Behandlung gehören insbesondere: Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien, die von Ihrem **Leistungserbringer**, bereitgestellt wurden, geplante und erledigte Aufgaben.

**Aktivitätsdaten:** Personenbezogene Daten, welche von uns verarbeitet werden, falls Sie die **myoncare App** mit einer Gesundheitsapplikation verbinden (z.B. GoogleFit, AppleHealth, Withings). Ihre Aktivitätsdaten werden an Ihre verbundenen **Leistungserbringer** als **Portalnutzer** transferiert.

## Kommerzielle und nicht-kommerzielle Forschungsdaten:

Wir verarbeiten Ihre personenbezogenen Daten in anonymisierter/pseudonymisierter Form, um zusammenfassende wissenschaftliche Berichte zu analysieren und zu erstellen, um Produkte, Behandlungen und wissenschaftliche Ergebnisse zu verbessern.

**Produktsicherheitsdaten** Personenbezogene Daten, die zur Erfüllung unserer gesetzlichen Verpflichtungen als Hersteller der **myoncare App** als Medizinprodukt verarbeitet werden. Darüber hinaus können Ihre personenbezogenen Daten zur Erfüllung der gesetzlichen Sicherheits- oder Vigilanzzwecke von Medizinprodukte- oder Pharmaunternehmen verarbeitet werden.

**Kostenerstattungsdaten:** Personenbezogene Daten, die für den Kostenerstattungsprozess zwischen Ihrem Leistungserbringer und Ihrer Krankenkasse erforderlich sind.

**Daten zum betrieblichen Gesundheitsmanagement:** Persönliche oder aggregierte Daten, die in konkreten Projekten und Fragebögen auf Anfrage Ihrer **Firma** (entweder direkt oder durch einen von Ihrem Unternehmen beauftragten Datendienstleister) erhoben werden. Die Daten können sich auf bestimmte Gesundheitsinformationen, Ihre Meinung über Ihr persönliches Wohlbefinden, Ihre Meinung als Mitarbeiter zu einer bestimmten internen oder externen Situation oder Daten über Pflege oder Gesundheit im Allgemeinen beziehen.

## BLOCKCHAIN-TECHNOLOGIE

Die **Blockchain Technologie** ("**Blockchain**") (Europäisches Patent Nr. 4 002 787) ist ein optionaler Dienst, der nicht verpflichtend buchbar ist. Es ist Ihr **Leistungserbringer**, der sich für die Verwendung der Blockchain-Lösung entscheidet. Die **Blockchain** basiert auf der Technologie von Hyperledger Fabric. Hyperledger Fabric ist eine Open-Source-Software für Blockchain-Implementierungen auf Unternehmensebene. Sie bietet eine skalierbare und sichere Plattform, die Blockchain-Projekte unterstützt.

Die Blockchain im myoncare-System ist eine zusätzliche Datenbank, in der Daten aus der Anwendung gespeichert werden. Alle Daten der **Blockchain** werden in der Bundesrepublik Deutschland gespeichert. Es handelt sich um ein private **Blockchain** ("**Private Blockchain**"), es erlaubt nur die Eingabe ausgewählter verifizierter Teilnehmer und es ist möglich, Einträge nach Bedarf zu überschreiben, zu bearbeiten oder zu löschen.

Im Allgemeinen besteht die **Blockchain** aus digitalen Daten in einer Kette von Paketen, die als "Blöcke" bezeichnet werden und die entsprechenden Transaktionen speichern. Die Art und Weise, wie diese Blöcke miteinander verbunden sind, ist chronologisch. Der erste Block, der erstellt wird, wird als Genesis-Block bezeichnet, und jeder danach hinzugefügte Block hat einen kryptografischen Hash, der sich auf den vorherigen Block bezieht, sodass Transaktionen und Informationsänderungen auf den Genesis-Block zurückgeführt werden können. Alle Transaktionen innerhalb der Blöcke werden durch einen Blockchain-Konsensmechanismus validiert und verifiziert, um sicherzustellen, dass jede Transaktion unverändert bleibt.

Jeder Block enthält die Liste der Transaktionen, einen Zeitstempel, einen eigenen Hash und den Hash des vorherigen Blocks. Ein Hash ist eine Funktion, die digitale Daten in eine alphanumerische Kette umwandelt. Wenn eine unbefugte Person versucht, die Daten eines einzelnen Blocks zu ändern, ändert sich auch der Hash des Blocks und die Verknüpfung zu diesem Block geht verloren. In diesem Fall kann der Block nicht mehr mit den anderen synchronisiert werden. Dieser technische Prozess verhindert, dass Unbefugte die Inhalte der **Blockchain** Kette manipulieren können. Wenn alle Nodes (Netzwerkknoten) versuchen, ihre Kopien zu synchronisieren, wird erkannt, dass eine Kopie geändert wurde, und das Netzwerk betrachtet diesen Node als fehlerhaft.

Unser **Blockchain** ist eine private **Blockchain**. Eine private **Blockchain** ist dezentralisiert. Dabei handelt es sich um ein sogenanntes Distributed-Ledger-System (digitales System zur Erfassung von Transaktionen), das als geschlossene Datenbank fungiert. Im Gegensatz zu öffentlichen **Blockchains**, die "nicht autorisiert" sind, sind privat **Blockchains** "autorisiert", da eine Autorisierung erforderlich ist, um Benutzer zu werden. Im Gegensatz zu öffentlichen **Blockchains**, die für jedermann öffentlich zugänglich sind, ist der Zugang zu privaten **Blockchains** abhängig von der Berechtigung, um Benutzer zu werden. Diese Struktur ermöglicht es, die Sicherheit und Unveränderlichkeit der Blockchain-Technologie zu nutzen und gleichzeitig datenschutzkonform zu sein und insbesondere die Vorschriften der Datenschutz-Grundverordnung (DSGVO) einzuhalten. Private Blockchain-Datensätze

können bearbeitet, geändert oder gelöscht werden. Eine Löschung bedeutet in diesem Zusammenhang, dass der Referenzwert auf die UUID (Universally Unique Identifier) in der Datenbank des **Leistungserbringers** gelöscht wird. Darüber hinaus wird der Hash in der Blockchain-Datenbank anonymisiert, so dass dieser Gesamtprozess konform mit der Datenschutz-Grundverordnung ist und die Rechte einer betroffenen Person gewährleistet sind (Recht auf Löschung/ "Recht auf Vergessenwerden", Art. 17 DSGVO).

#### Art der Daten, die in der Blockchain gespeichert und verarbeitet werden:

- Institutionen/Leistungserbinger UUID
  - Patienten-UUID
  - Asset-UUID
  - Hash von Caretask- und Asset-Daten.
- (UUID: Universell eindeutiger Identifikator).

Die in der **Blockchain** gespeicherten Datei sind pseudo-anonymisiert.

Unser **Blockchain** soll den Datenschutz gewährleisten, und zwar in Bezug auf die Integrität der Daten, das Patientenprofil, die Assets und die zugewiesenen **Caretask** und Medikationen. Um mit der **Blockchain** zu kommunizieren, muss der Benutzer eine Reihe von öffentlich-privaten Schlüsseln registrieren. Um mit der **Blockchain** zu kommunizieren, benötigt der Nutzer mehrere public-private Keys; der Registrierungsprozess erzeugt Zertifikate, die in einer separaten Datenbank des **Leistungserbringers** und auf dem Handy des Patienten gespeichert werden. Eine Sicherungskopie des Patienten Keys wird verschlüsselt und in der Datenbank des **Leistungserbringers**, gespeichert, auf die nur der Patient seinerseits zugreifen kann.

Bei der Überprüfung der Einwilligung zum Datenschutz überprüft das System, im Falle, dass der **Leistungserbringer** mit dem Patienten kommunizieren will, ob der Patient seine Zustimmung zu den Datenschutzrichtlinien des **Leistungserbringers** erteilt hat. Die **Blockchain** dient daher, die Integrität und Accountability des Datensatzes zu gewährleisten, um sicherzugehen, dass der Patient die Datenschutzrichtlinie akzeptiert hat.

Wenn ein **Leistungserbringer** eine neue Version einer Datenschutzerklärung hochlädt, wird der Hash der Datei in der **Blockchain** gespeichert und nachdem der Patient seine Einwilligung erteilt hat, wird diese Interaktion in der **Blockchain** gespeichert. Bei jeder Kommunikation mit dem Patienten antwortet die **Blockchain** durch den Vergleich des Hashs mit einer Flag (Markierung), die Auskunft darüber gibt, ob die Einwilligung des Patienten für die aktuelle Datenschutzrichtlinie noch gültig ist.

Auch bei der Patientensynchronisierung wird die Integrität des Patientenprofils durch die **Blockchain** gewährleistet. Der **Leistungserbringer** erkennt sofort, wenn das Patientenprofil mit dem Profil auf dem Handy nicht synchronisiert bzw. übereinstimmt, indem der Hash des Patientenprofils in der **Blockchain** verglichen wird. Auf diese Weise erreicht der **Leistungserbringer** eine hinreichende Aktualität in Bezug auf das Patientenprofil.

#### myoncare Portal:

Wenn sich der **Leistungserbringer** für die Blockchain-Lösung entscheidet, implementiert ONCARE ein zusätzliches Tool, genannt "Adapter Service", dass für die Kommunikation mit der **Blockchain** verwendet wird. Die Blockchain-Instanz wird von ONCARE gehostet.

#### myoncare App:

Die Patienten können sich mit der gleichen Blockchain-Instanz verbinden, und zwar mit Hilfe des Phone Manager Tools, welches ebenfalls von ONCARE gehostet wird. Dieser Service wird ebenfalls von ONCARE gehostet.

**Rechtsgrundlage für die Datenverarbeitung:** Die Datenverarbeitung durch ONCARE für den **Leistungserbringer** erfolgt auf der Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

## VERARBEITUNG VON OPERATIVEN DATEN

### Anwendbar für alle App-Nutzer

Sie können uns bestimmte personenbezogene Daten zur Verfügung stellen, wenn Sie sich mit uns in Verbindung setzen, um die Funktionen und die Nutzung der **myoncare App** zu verstehen, im Falle einer Serviceanforderung Ihrerseits oder im Falle von

unsererseits initiierten (telefonischen) Unterstützungsangebot.

#### Service-Mitarbeiter

Im Auftrag des Datenverantwortlichen (bspw. Leistungserbringers) bieten wir Ihnen an, Sie beim Ausfüllen von Fragebögen telefonisch zu unterstützen (Outbound Calls), um Ihre digitale Patientenbegleitung zu optimieren. Sollten Sie dieses Angebot nicht nutzen wollen, steht es Ihnen frei, dieses nicht anzunehmen und der telefonischen Unterstützung zu widersprechen.

Im Falle einer Serviceanfrage sowie einem Outbound Call können auch folgende personenbezogene Daten von autorisierten ONCARE-Mitarbeitern eingesehen werden:

- Die personenbezogenen Daten, die Sie über unsere App Ihrem **Leistungserbringer** zur Verfügung gestellt haben (z. B. Name, Geburtsdatum, Profilbild, Kontaktdaten).
- Die Gesundheitsdaten, die Sie Ihrem **Gesundheitsdienstleister**, dem **Datendienstleister** oder dem **Arbeitgeber** über unsere **myoncare App** zur Verfügung gestellt haben (z. B. Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien von medizinischem Fachpersonal, geplante und erledigte Aufgaben).

Autorisierte ONCARE-Mitarbeiter, die zum Zweck der Bearbeitung einer Serviceanfrage oder eines Outbound Calls auf die Datenbank Ihres **Leistungserbringers**, **Datendienstleister** oder **Arbeitgeber** zugreifen können, sind vertraglich verpflichtet, alle personenbezogenen Daten streng vertraulich zu behandeln.

#### Push-Benachrichtigungen und E-Mails

Im Rahmen Ihrer Unterstützung durch myoncare möchten wir Sie darüber informieren, wie wir mit Benachrichtigungen und wichtige Informationen umgehen, die wir Ihnen zukommen lassen.

##### 1. Push-Benachrichtigungen:

- Wir senden Ihnen Push-Benachrichtigungen über unsere **myoncare-PWA** (Progressive WebApp)



und die **myoncare-App**, um Sie über Aufgaben, Termine und wichtige Updates zu informieren.

- Sie haben die Möglichkeit, diese Push-Benachrichtigungen in den Einstellungen Ihrer App zu deaktivieren.

## 2. E-Mail-Benachrichtigungen:

- Unabhängig davon, ob Sie Push-Benachrichtigungen aktiviert oder deaktiviert haben, senden wir Ihnen weiterhin wichtige Informationen und Erinnerungen per E-Mail.
- Dies stellt sicher, dass Sie keine wichtigen Benachrichtigungen verpassen und Ihre Betreuung reibungslos verläuft.

### Warum wir dies tun:

- Unser Ziel ist es, Sie über Ihre Aufgaben und wichtige Updates auf dem Laufenden zu halten, um Ihre Gesundheit bestmöglich zu unterstützen.
- E-Mails sind ein zuverlässiger Weg, um sicherzustellen, dass wichtige Informationen Sie erreichen, auch wenn Push-Benachrichtigungen deaktiviert sind.

### Ihre Handlungsmöglichkeiten:

- Wenn Sie keine Push-Benachrichtigungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare App** deaktivieren.
- Bitte stellen Sie sicher, dass Ihre E-Mail-Adresse korrekt und aktuell ist, um einen reibungslosen Empfang unserer Nachrichten zu gewährleisten.
- Wenn Sie keine E-Mail Erinnerungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare App** deaktivieren.

### Speicherdauer

Die Daten, die Sie uns zum Empfang von E-Mails zur Verfügung stellen, werden von uns gespeichert, bis Sie sich von unseren Diensten abmelden, und nach Ihrer Abmeldung sowohl von unseren Servern als auch von den Servern von Sendgrid gelöscht.

Bei der Verarbeitung von operativen Daten fungiert ONCARE als Datenverantwortlicher, der für die rechtmäßige Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist.

**Arten von Daten:** Ihr Name, Ihre E-Mail-Adresse, Ihre Telefonnummer, Ihr Geburtsdatum, das Datum der Registrierung, die von der App generierten Pseudoschlüssel; Geräte-Token zur Identifizierung Ihres Geräts, Ihre Pseudo-Identifikationsnummer, Ihre IP-Adresse, Typ und Version des von Ihrem Gerät verwendeten Betriebssystems.

Wenn die **myoncare App** heruntergeladen wird, werden die notwendigen Informationen an den App-Store-Anbieter übermittelt. Wir haben keinen Einfluss auf diese Datenerhebung und sind dafür auch nicht verantwortlich. Wir verarbeiten die uns vom Anbieter des App-Stores im Rahmen unseres Vertragsverhältnisses zur Verfügung gestellten personenbezogenen Daten zum Zwecke der Weiterentwicklung unserer **myoncare Apps** und Services.

Die App verwendet die Google Maps API, um geografische Informationen zu verwenden. Bei der Nutzung von Google Maps werden von Google auch Daten über die Nutzung der Kartenfunktionen erhoben, verarbeitet und genutzt. Nähere Informationen über den Umfang, die Rechtsgrundlage und den Zweck der Datenverarbeitung durch Google sowie die Speicherdauer finden Sie in der Datenschutzerklärung von Google.

**Zwecke der Verarbeitung von operativen Daten:** Wir verwenden die operativen Daten, um die Funktionalitäten der **myoncare App** aufrechtzuerhalten und um bei Bedarf oder von Ihnen initiiert direkt mit Ihnen in Kontakt zu treten (z. B. bei Änderung der Allgemeinen Geschäftsbedingungen, notwendigem Support, technischen Problemen, Hilfestellung beim Ausfüllen der Fragebögen, usw.).

**Rechtfertigung der Verarbeitung:** Die Verarbeitung von Betriebsdaten ist auf der Grundlage von Art. 6 Abs. 1 lit. b DSGVO für die Erfüllung des Vertrages, den Sie mit ONCARE zum Zwecke der Nutzung der **myoncare App** abschließen, gerechtfertigt.

### IP GEOLOKALISIERUNG

Wir verwenden für unsere Dienste eine Geolokalisierungsanwendung. Wir verwenden ipapi

(bereitgestellt von apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Wien, Österreich) und Geoapify (zur Verfügung gestellt von Keptago Ltd., N. Nikolaidi und T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Zypern), um den Standort von Patientenbenutzern zu identifizieren. Wir verwenden sie, um unsere Anwendungen zu sichern und den Standort des Patientenbenutzers zu überprüfen, um sicherzustellen, dass die Nutzung unserer Dienste konform ist. Wir kombinieren die von uns gesammelten Informationen nicht mit anderen Informationen über den Benutzer, die ihn identifizieren könnten. Zu den von apilayer verarbeiteten Daten gehören die IP-Adresse des Patienten und weitere Angaben zum Standort. Rechtsgrundlage für die Nutzung ist Art. 6 Abs. 1 lit. f DSGVO. Die Daten werden gelöscht, wenn der mit ihr verbundene Zweck, für den sie erhoben wurden, nicht mehr besteht und keine gesetzliche Aufbewahrungspflicht mehr besteht. Weitere Informationen zu deren Datenschutzrichtlinien finden Sie unter <https://ipapi.com/privacy/>

## VERARBEITUNG VON (BEHANDLUNGS-)DATEN

### *Anwendbar für App-Nutzer, die die App mit ihrem Leistungserbringer nutzen*

Während der Nutzung der **myoncare-App** kann Ihr **Leistungserbringer** Ihre persönlichen Daten in das **myoncare-Portal** eingeben, um die **myoncare-Dienste** zu starten (z. B. Sie als Patient anlegen, Bereitstellung einer individuellen Aufgabe, Erinnerung zur Medikamenteneinnahme usw.). Zusätzlich können Sie und Ihr **Leistungserbringer** Dokumente und Dateien in die **myoncare-App** und das **myoncare-Portal** hochladen und miteinander teilen. Ihr **Leistungserbringer** kann eine **Datenschutzrichtlinie** zu Ihrer Information hochladen und weitere Zustimmungserfordernisse für Sie als Patient festlegen, für die Ihre Zustimmung erforderlich ist. Die Dateien werden in einer Cloud-Datenbank in Deutschland gespeichert. Ihr **Leistungserbringer** kann die Freigabe solcher Dateien mit anderen **Portalnutzern** innerhalb seiner Einrichtung oder anderen **Leistungserbringern** außerhalb seiner Einrichtung (Konsiliarärzte) für medizinische Zwecke ermöglichen.

Andere Portalbenutzer haben ohne diese Freigabe keinen Zugriff auf diese Dateien. Ferner kann Ihr **Leistungserbringer** uns beauftragen, Sie telefonisch beim Ausfüllen von Fragebögen zu unterstützen (Outbound Calls). Dies erfolgt nur nach Anweisung Ihres Leistungserbringers und wird ausschließlich von autorisierten ONCARE Mitarbeitern durchgeführt.

Wir werden Ihre Daten in Übereinstimmung mit den in dieser **Datenschutzrichtlinie** festgelegten Bestimmungen verwenden und verarbeiten, vorausgesetzt Sie erteilen uns Ihre Zustimmung, soweit erforderlich.

Wir verarbeiten diese personenbezogenen Daten, einschließlich Ihrer Gesundheitsdaten, im Rahmen einer Vereinbarung mit und in Übereinstimmung mit den Anweisungen Ihres **Leistungserbringers**. Für diese Verarbeitungszwecke ist der **Leistungserbringer** im Sinne der geltenden Datenschutzgesetze als Datenverantwortlicher für die Verarbeitung Ihrer personenbezogenen Daten und Gesundheitsdaten verantwortlich, und ONCARE ist der Datenverarbeiter dieser personenbezogenen (Gesundheits-) Daten. Das bedeutet, dass ONCARE personenbezogene Daten nur nach den Weisungen des **Leistungserbringers** verarbeitet. Wenn Sie Fragen oder Bedenken bezüglich der Verarbeitung Ihrer personenbezogenen Daten oder Gesundheitsdaten haben, sollten Sie sich in erster Linie an Ihren **Leistungserbringer** wenden.

**Arten von Daten:** Name, Geburtsdatum, Profilinformationen, Kontaktdaten und auch Gesundheitsdaten, wie z.B. Symptome, Fotos, Informationen über eingenommene Medikamente, Fragebogenantworten einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien von medizinischem Fachpersonal, geplante und erledigte Aufgaben.

**Zwecke der Datenverarbeitung:** Wir verarbeiten Ihre Behandlungsdaten, um unseren **myoncare-Dienst** für Ihren **Leistungserbringer** und für Sie bereitzustellen. Ihre Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden von Ihrem **Leistungserbringer** zur Beratung und Unterstützung für Sie verwendet. Wir verarbeiten diese personenbezogenen Daten im Rahmen einer Vereinbarung mit und in Übereinstimmung mit den Anweisungen Ihres

**Leistungserbringers.** Die Übertragung dieser Behandlungsdaten erfolgt pseudonymisiert und verschlüsselt. Zur Ausübung Ihrer Betroffenenrechte wenden Sie sich bitte an Ihre **Leistungserbringer**.

**Rechtfertigung der Verarbeitung von Behandlungsdaten:** Ihre personenbezogenen (Behandlungs-) Daten werden von Ihrem **Leistungserbringer** gemäß den Bestimmungen der **DSGVO** und aller anderen geltenden Datenschutzvorschriften verarbeitet. Rechtsgrundlagen für die Datenverarbeitung ergeben sich insbesondere aus Art. 9 Abs. 2 lit. h DSGVO für Gesundheitsdaten als besonders schützenswerte Daten sowie Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a und 9 Abs. 2 lit. a DSGVO. Die Verarbeitung von Daten durch ONCARE für Ihre **Leistungserbringer** erfolgt darüber hinaus auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

Ihr **Leistungserbringer** ist als Datenbeauftragter für die Einholung Ihrer Einwilligung verantwortlich. Auch wenn Sie die **myoncare App** ohne eine solche Einwilligung nutzen können, funktionieren die meisten Funktionen nicht mehr (z. B. die Weitergabe von Daten an Ihren Gesundheitsdienstleister). Die Verweigerung oder der Widerruf der Einwilligung in die Verarbeitung von Behandlungsdaten führt daher zu einer starken Einschränkung der Funktionalität der App-Dienste und Ihre **Leistungserbringer** kann Sie nicht mehr über die **myoncare App** unterstützen.

## VERARBEITUNG VON AKTIVITÄTSDATEN

*Nur anwendbar, wenn Sie der Aktivitätsdatenübertragung über myoncare Tools zustimmen und diese aktivieren*

**myoncare Tools** bieten Ihnen die Möglichkeit, die **myoncare App** mit bestimmten Gesundheits-Apps (z. B. AppleHealth, GoogleFit, Withings), zu verbinden, die Sie nutzen ("**Health App**"). Um die Verarbeitung von Aktivitätsdaten zu ermöglichen, holen wir vorab Ihre Einwilligung in die Verarbeitung ein. Wenn die Verbindung nach Ihrer Einwilligung hergestellt wird, werden die von der **Health-App** gesammelten Aktivitätsdaten Ihren **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen. Bitte beachten Sie, dass Aktivitätsdaten nicht von **myoncare Tools** validiert

werden und von Ihrem **Leistungserbringer** nicht für diagnostische Zwecke als Basis der medizinischen Entscheidungsfindung genutzt werden sollen. Bitte beachten Sie auch, dass Ihre **Leistungserbringer** nicht verpflichtet sind, Ihre Aktivitätsdaten zu überprüfen und Ihnen keine Rückmeldung zu Ihren Aktivitätsdaten geben müssen.

Aktivitätsdaten werden jedes Mal, wenn die **myoncare-App** aufgerufen wird, mit Ihren angeschlossenen **Leistungserbringern** geteilt. Sie können Ihre Einwilligung zur Weitergabe von Aktivitätsdaten jederzeit in den Einstellungen der **myoncare App** widerrufen. Bitte beachten Sie, dass Ihre Aktivitätsdaten ab diesem Zeitpunkt nicht mehr weitergegeben werden. Aktivitätsdaten, die bereits geteilt wurden, werden nicht aus dem **myoncare-Portal** Ihrer angeschlossenen **Leistungserbringer** gelöscht.

Die Verarbeitung von Aktivitätsdaten liegt in Ihrer eigenen Datenverantwortung.

**Arten von Daten:** Der Typ und Umfang der übertragenen Daten hängen von Ihrer Entscheidung und der Verfügbarkeit dieser Daten innerhalb der **Health-App** ab. Zu den Daten können unter anderem Gewicht, Größe, zurückgelegte Schritte, verbrannte Kalorien, Schlafstunden, Herzfrequenz und Blutdruck gehören.

**Zweck der Verarbeitung von Aktivitätsdaten:** Ihre Aktivitätsdaten werden Ihren verbundenen **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen.

**Rechtfertigung der Verarbeitung:** Die Verarbeitung von Aktivitätsdaten unterliegt Ihrer eigenen Verantwortung.

## VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

*Anwendbar für App-Nutzer, deren Leistungserbringer die Medizinproduktvariante der myoncare Tools verwendet*

Das **myoncare App** ist als Medizinprodukt gemäß den europäischen Medizinprodukteverordnungen klassifiziert und vermarktet. Als Hersteller der App müssen wir bestimmte gesetzliche Verpflichtungen einhalten (z.B. Überwachung der Funktionalität der App,



Auswertung von Vorfallmeldungen, die mit der Nutzung der App in Verbindung stehen könnten, Tracking von Nutzern etc.). Zusätzlich ermöglicht die **myoncare-App** Ihnen und Ihrem **Leistungserbringer**, zu kommunizieren und persönliche Daten über bestimmte medizinische Geräte oder Medikamente, die in Ihrer Behandlung verwendet werden, zu erfassen. Die Hersteller solcher Medizinprodukte oder Arzneimittel haben auch gesetzliche Verpflichtungen hinsichtlich der Marktüberwachung (z.B. Sammlung und Bewertung von Nebenwirkungsmeldungen).

ONCARE ist der Datenverantwortliche für die Verarbeitung von Produktsicherheitsdaten.

**Arten von Daten:** Fallberichte, personenbezogene Daten, die in einem Vorfallbericht bereitgestellt wurden, und Ergebnisse der Auswertung.

**Verarbeitung von Produktsicherheitsdaten:** Wir speichern und werten alle personenbezogenen Daten im Zusammenhang mit unseren gesetzlichen Verpflichtungen als Hersteller eines Medizinprodukts aus und übermitteln diese personenbezogenen Daten (soweit möglich nach Pseudonymisierung) an zuständige Behörden, Benannte Stellen oder andere Datenbeauftragte mit Aufsichtspflichten. Zusätzlich speichern und übertragen wir personenbezogene Daten im Zusammenhang mit medizinischen Geräten und/oder Medikamenten, wenn wir Mitteilungen von Ihrem **Leistungserbringer**, von Ihnen als Patient oder von Dritten (z. B. unseren Vertriebspartnern oder Importeuren der **myoncare-Tools** in Ihrem Land) erhalten, die dem Hersteller des Produkts gemeldet werden müssen, damit dieser seinen gesetzlichen Verpflichtungen zur Produktsicherheit nachkommen kann.

**Rechtfertigung der Verarbeitung von Produktsicherheitsdaten:** Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung rechtlicher Verpflichtungen als Medizinprodukte- oder Arzneimittelhersteller ist Art. 6 Abs. 1 lit. c, Art. 9 Abs. 2 lit. i DSGVO in Verbindung mit den Pflichten zur Überwachung nach dem Inverkehrbringen nach dem Medizinproduktegesetz und der Medizinprodukterichtlinie (geregelt ab dem 26. Mai 2021 in Kapitel VII der neuen

Medizinprodukteverordnung (EU) 2017/745) und/oder dem Arzneimittelgesetz.

## VERARBEITUNG VON GESUNDHEITS- bzw. BEHANDLUNGSDATEN

**Anwendbar für App-Nutzer, die die App mit ihrem Leistungserbringer für Kostenerstattungszwecke verwenden**

Die **myoncare-App** unterstützt Ihren **Leistungserbringer** bei der Einleitung standardmäßiger Verfahren zur Kostenerstattung für die Gesundheitsleistungen, die Ihnen über die **myoncare-App** bereitgestellt werden. Um den Erstattungsprozess zu ermöglichen, unterstützt die **myoncare-App** die Erfassung Ihrer personenbezogenen (Gesundheits-) Daten durch Ihren **Leistungserbringer** zur Übermittlung dieser Daten an Ihre zahlende Stelle (entweder die Kassenärztliche Vereinigung und/oder Ihre Krankenversicherung). Diese Datenverarbeitung ist nur eine initiale Datenübermittlung für den **Leistungserbringer**, um eine Kostenerstattung von Ihrer Krankenversicherung zu erhalten. Die Art und Menge der verarbeiteten personenbezogenen Daten unterscheidet sich nicht von anderen ErstattungsROUTINEN des **Leistungserbringers**. Ihr Leistungserbringer ist der Datenbeauftragte für Erstattungsdaten. ONCARE agiert als Datenverarbeiter auf der Grundlage der Datenverarbeitungsvereinbarung mit Ihrem **Leistungserbringer**.

**Arten von Daten:** Name, Diagnose, Indikationen, Behandlung, Behandlungsdauer, andere Daten, die für die Verwaltung der Erstattung erforderlich sind.

**Verarbeitung von Erstattungsdaten:** Ihr **Leistungserbringer** übermittelt die für die Erstattung erforderlichen Behandlungsdaten an den Kostenträger (entweder seine gesetzliche Krankenversicherungseinrichtung und/oder Ihre Krankenversicherung), und der Kostenträger verarbeitet die Erstattungsdaten, um die Erstattung an Ihren **Leistungserbringer** zu leisten.

**Rechtfertigung der Verarbeitung von Erstattungsdaten:** Die Erstattungsdaten werden auf Grundlage der §§ 295, 301 SGB V, Art. 9 Abs. 2 lit. b DSGVO verarbeitet. Die Datenverarbeitung durch ONCARE für Ihren

**Leistungserbringer** erfolgt ebenfalls auf Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

## VERARBEITUNG VON DATEN DES BETRIEBLICHEN GESUNDHEITSMANAGEMENTS

*Anwendbar für Nutzer der App, die die App mit dem betrieblichen Gesundheitsmanagement der Firma verwenden*

Während der Nutzung der **myoncare-App** im **betrieblichen Gesundheitsmanagement** des Unternehmens werden bestimmte personenbezogene (Gesundheits-)Daten in aggregierter Form als Daten für das betriebliche Gesundheitsmanagement an das **Unternehmen** und die von dem **Unternehmen** beauftragten **Datenanbieter** (z. B. Datenanalysten oder Forschungsunternehmen) weitergegeben. Weder das **Unternehmen** noch ein **Datendienstleister** können solche Daten Ihrer Identität zuordnen. ONCARE empfiehlt, während der Nutzung der **myoncare-Dienste** im Rahmen des betrieblichen Gesundheitsmanagements keine persönlichen Daten zu teilen.

Das bedeutet, dass ONCARE und alle **Datenanbieter** die Daten für das betriebliche Gesundheitsmanagement nur gemäß den Anweisungen des **Unternehmens** verarbeiten werden. Wir verarbeiten solche Daten für das betriebliche Gesundheitsmanagement, einschließlich Ihrer Gesundheitsdaten, auf der Grundlage einer Vereinbarung mit Ihrem **Unternehmen** und/oder einem **Datenanbieter** und gemäß deren Anweisungen. Für die Zwecke dieser Vereinbarung ist das **Unternehmen** oder der **Datenanbieter** der Datenverantwortliche für die Verarbeitung Ihrer Daten zu Zwecken des betrieblichen Gesundheitsmanagements, und ONCARE sowie alle vom **Unternehmen** beauftragten **Datenanbieter** sind die Datenverarbeiter dieser Daten. Wenn Sie Fragen oder Bedenken hinsichtlich der Verarbeitung Ihrer Daten für das betriebliche Gesundheitsmanagement haben, sollten Sie sich in erster Linie an das **Unternehmen** wenden.

**Zwecke der Datenverarbeitung im betrieblichen Gesundheitsmanagement:** Wir verarbeiten Ihre Daten für das betriebliche Gesundheitsmanagement, um Ihnen und dem **Unternehmen** unsere **myoncare-Dienste**

anbieten zu können. Ihre Daten zum betrieblichen Gesundheitsmanagement, die Sie in unsere **myoncare-App** eingeben, werden vom **Unternehmen** (entweder direkt oder über einen **Datenanbieter**) im Rahmen des betrieblichen Gesundheitsmanagements verwendet. Wir verarbeiten diese Daten für das betriebliche Gesundheitsmanagement im Rahmen einer Vereinbarung mit und gemäß den Anweisungen des **Unternehmens** und/oder eines **Datenanbieters** für dessen betriebliches Gesundheitsmanagement. Die Übertragung dieser Daten für das betriebliche Gesundheitsmanagement erfolgt pseudonymisiert und verschlüsselt. Zur Ausübung Ihrer Betroffenenrechte wenden Sie sich bitte an das **Unternehmen**.

**Rechtfertigung der Verarbeitung von Daten zum betrieblichen Gesundheitsmanagement:** Ihre Daten zum betrieblichen Gesundheitsmanagement werden vom **Unternehmen** gemäß den Bestimmungen der **DSGVO** und aller anderen geltenden Datenschutzvorschriften verarbeitet. Rechtsgrundlage für die Datenverarbeitung ist insbesondere Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. eine DSGVO oder eine andere für das **Unternehmen** geltende rechtliche Grundlage. Die Verarbeitung von Daten durch ONCARE für das **Unternehmen** (entweder direkt oder über einen von Ihrem Unternehmen beauftragten **Dienstleister**) basiert ebenfalls auf Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

Das **Unternehmen** ist als Datenverantwortlicher dafür verantwortlich, Ihre Einwilligung einzuholen, wenn dies durch Datenschutzvorschriften erforderlich ist, und die Daten für Zwecke des betrieblichen Gesundheitsmanagements gemäß den geltenden Datenschutzgesetzen zu verarbeiten.

## WELCHE TECHNOLOGIE WIRD VON DER MYONCARE APP VERWENDET?

### E-Mail-Dienst

Wir verwenden Brevo (bereitgestellt von der Sendinblue GmbH, mit Sitz in der Köpenicker Straße 126, 10179 Berlin) und Sendgrid (bereitgestellt von Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Diese E-Mail-Dienste können verwendet werden, um den Versand von E-Mails zu organisieren. Sendgrid wird verwendet, um Bestätigungs-E-Mails,

Transaktionsbestätigungen und E-Mails mit wichtigen Informationen zu Anfragen zu senden. Die von Ihnen zum Zwecke des Empfangs von E-Mails eingegebenen Daten werden auf den Servern von Sendgrid gespeichert. Wenn wir in Ihrem Namen E-Mails über SendGrid versenden, verwenden wir eine SSL-gesicherte Verbindung.

Die E-Mail-Kommunikation wird für die folgenden Aufgaben verwendet:

- Erstmaliges Einloggen in die Webanwendung;
- Zurücksetzen des Passworts für die Webanwendung;
- Erstellen Sie ein Konto für die Patientenanwendung;
- Zurücksetzen des Passworts für die Patientenanwendung;
- Erstellung und Versand eines Berichts;
- Ersetzen von Push-Benachrichtigungen durch E-Mails für **PWA** (Progressive Web App) in den folgenden Fällen:
  - (i) wenn ein Careplan in einer Stunde endet;
  - (ii) wenn Medikamente zugewiesen wurden;
  - (iii) wenn die Datenschutzrichtlinie aktualisiert wurde;
  - (iv) wenn ein Termin an Patienten und Ärzte gesendet wird, insbesondere für die Terminart "Videoanruf";
  - (v) Alle Informationen, die sich auf eine **Caretask** beziehen oder wenn ein **Leistungserbringer** eine **Caretask** zugewiesen hat.

#### Brevo (Datenschutzerklärung):

Datenschutzerklärung - Schutz personenbezogener Daten | Brevo

#### SendGrid (englisch) (Datenschutzerklärung):

<https://sendgrid.com/resource/general-data-protection-regulation-2/>

#### Matomo

Dabei handelt es sich um ein Open-Source-Web-Analyse-Tool. Matomo (bereitgestellt von InnoCraft Ltd., Neuseeland) überträgt keine Daten an Server, die außerhalb der Kontrolle von ONCARE liegen. Matomo ist zunächst deaktiviert, wenn Sie unsere Dienste nutzen. Nur wenn Sie damit einverstanden sind, wird Ihr Nutzerverhalten anonymisiert erfasst. Wenn diese deaktiviert ist, wird ein "permanenter Cookie" gespeichert, sofern Ihre Browsereinstellungen dies

zulassen. Dieses Cookie signalisiert Matomo, dass Sie nicht möchten, dass Ihr Browser aufgezeichnet wird.

Die durch den Cookie gesammelten Nutzungsinformationen werden an unsere Server übertragen und dort gespeichert, damit wir das Nutzerverhalten analysieren können.

Die vom Cookie erzeugten Informationen über Ihre Nutzung sind:

- Benutzerrolle;
- Geolokalisierung des Benutzers;
- Benutzer-Betriebssystem;
- Zeit, zu der der Nutzer Inhalte verwendet hat;
- IP-Adresse;
- Websites, die über das Web / besucht werden **PWA** (Weitere Informationen finden Sie im Abschnitt über PWA in dieser Datenschutzrichtlinie);
- Schaltflächen, die der Benutzer im **myoncare-Portal**, der **myoncare-App** und der **myoncare-PWA** anklickt.

Die durch den Cookie erzeugten Informationen werden nicht an Dritte weitergegeben.

Sie können die Verwendung von Cookies ablehnen, indem Sie die entsprechenden Einstellungen in Ihrem Browser vornehmen. Bitte beachten Sie jedoch, dass Sie in diesem Fall möglicherweise nicht alle Funktionen nutzen können. Weitere Informationen finden Sie unter: <https://matomo.org/privacy-policy/>.

Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Nutzer ist Art. 6 Abs. 1 Satz 1 lit. a DSGVO. Die Verarbeitung personenbezogener Daten der Nutzer ermöglicht es uns, das Nutzungsverhalten zu analysieren. Durch die Auswertung der gewonnenen Daten sind wir in der Lage, Informationen über die Nutzung der einzelnen Komponenten unserer Dienste zusammenzustellen. Dies hilft uns, unsere Dienste und deren Usability kontinuierlich zu verbessern.

Wir verarbeiten und speichern personenbezogene Daten nur so lange, wie es zur Erfüllung des beabsichtigten Zwecks erforderlich ist.

#### SICHERE ÜBERTRAGUNG PERSONENBEZOGENER DATEN

Wir setzen angemessene technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre

bei uns gespeicherten personenbezogenen Daten optimal gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Die Sicherheitsstufen werden in Zusammenarbeit mit Sicherheitsexperten kontinuierlich überprüft und an neue Sicherheitsstandards angepasst.

Der Datenaustausch zur und von der App erfolgt verschlüsselt. Wir verwenden TLS und SSL als Verschlüsselungsprotokolle für eine sichere Datenübertragung. Auch der Datenaustausch ist durchgehend verschlüsselt und erfolgt mit Pseudoschlüsseln.

## DATENÜBERTRAGUNGEN / OFFENLEGUNG AN DRITTE

Wir werden Ihre personenbezogenen Daten nur im Rahmen der gesetzlichen Bestimmungen oder aufgrund Ihrer Einwilligung an Dritte weitergeben. In allen anderen Fällen werden die Informationen nicht an Dritte weitergegeben, es sei denn, wir sind aufgrund zwingender gesetzlicher Vorschriften dazu verpflichtet (Weitergabe an externe Stellen, einschließlich Aufsichts- oder Strafverfolgungsbehörden).

Jede Übertragung personenbezogener Daten wird während der Übertragung verschlüsselt.

## ALLGEMEINE INFORMATIONEN ZUR EINWILLIGUNG IN DIE DATENVERARBEITUNG

Ihre Einwilligung stellt auch eine Einwilligung in die datenschutzrechtliche Datenverarbeitung dar. Bevor Sie Ihre Einwilligung erteilen, informieren wir Sie über den Zweck der Datenverarbeitung und Ihr Widerspruchsrecht.

Wenn sich die Einwilligung auch auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht, wird die **myoncare-App** Sie im Rahmen des Einwilligungsverfahrens ausdrücklich darüber informieren.

Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darf nur erfolgen, wenn dies gesetzlich vorgeschrieben ist und kein Grund zur Annahme besteht, dass Ihre berechtigten Interessen der Verarbeitung dieser personenbezogenen Daten entgegenstehen oder Sie

Ihre Einwilligung in die Verarbeitung dieser personenbezogenen Daten gemäß Art. 9 Abs. 2 DSGVO gegeben haben.

Für die Datenverarbeitung, für die Ihre Einwilligung erforderlich ist (wie in dieser **Datenschutzerklärung** erläutert), wird die Einwilligung im Rahmen des Registrierungsprozesses eingeholt. Nach erfolgreicher Registrierung können die Einwilligungen in den Kontoeinstellungen der **myoncare App** verwaltet werden.

## DATENEMPFÄNGER / KATEGORIEN VON EMPFÄNGERN

In unserer Organisation stellen wir sicher, dass nur diejenigen Personen berechtigt sind, personenbezogene Daten zu verarbeiten, die zur Erfüllung ihrer vertraglichen und gesetzlichen Pflichten erforderlich sind. Ihre persönlichen Daten und Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden entweder direkt oder über einen **Datenanbieter** Ihrem **Leistungserbringer** und/oder Ihrem **Unternehmen** zur Verfügung gestellt (abhängig von der Art der Nutzung der **myoncare-Tools**).

In bestimmten Fällen unterstützen Dienstleister unsere Fachabteilungen bei der Erfüllung ihrer Aufgaben. Mit allen Dienstleistern, die Auftragsverarbeiter für personenbezogene Daten sind, wurden die erforderlichen Datenschutzvereinbarungen abgeschlossen. Diese Dienstleister sind Google (Google Firebase), Anbieter von Cloud-Speichern und Support-Dienstleistern.

Google Firebase ist eine "NoSQL-Datenbank", die die Synchronisation zwischen dem **myoncare-Portal** Ihres **Leistungserbringers** und der **myoncare-App** ermöglicht. NoSQL definiert einen Mechanismus zum Speichern von Daten, der nicht nur in tabellarischen Beziehungen modelliert wird, indem es eine einfachere "horizontale" Skalierung im Vergleich zu tabellarischen/relationalen Datenbankmanagementsystemen in einem Cluster von Maschinen ermöglicht.

Zu diesem Zweck wird ein Pseudokey der **myoncare-App** zusammen mit dem entsprechenden **Medikationsplan** in Google Firebase gespeichert. Die Datenübertragung erfolgt für ONCARE und seine Dienstleister pseudonymisiert, was bedeutet, dass ONCARE und seine Dienstleister keine Beziehung zu Ihnen als betroffene Person aufbauen können. Dies wird erreicht, indem die



Daten während der Übertragung zwischen Ihnen und Ihrem **Dienstleister** oder **Unternehmen** (entweder direkt oder an einen **Datenanbieter**) verschlüsselt und Pseudokeys anstelle persönlicher Kennungen wie Name oder E-Mail-Adresse zur Nachverfolgung dieser Übertragungen verwendet werden. Die Re-Identifizierung erfolgt, sobald die personenbezogenen Daten das Konto Ihres **Leistungserbringers** oder Unternehmens im **myoncare-Portal** oder Ihr Konto in der **myoncare-App** erreicht haben, nachdem sie durch spezielle Tokens verifiziert wurden.

Unsere Cloud-Speicheranbieter bieten Cloud-Speicher an, in dem der Firebase-Manager, der die Firebase-URLs für das **myoncare-Portal** verwaltet, gespeichert wird. Darüber hinaus stellen diese Dienstleister die isolierte Serverdomäne des **myoncare-Portals** bereit, in der Ihre persönlichen Daten gespeichert werden. Es hostet auch die Video- und Dateiverwaltungsdienste von myoncare, die verschlüsselte Videokonferenzen zwischen Ihnen und Ihrem **Leistungserbringer** sowie den Austausch von Dateien ermöglichen. Der Zugriff auf Ihre persönlichen Daten durch Sie und Ihren **Leistungserbringer** wird durch das Senden spezifischer Tokens gewährleistet. Diese personenbezogenen Daten werden während der Übertragung und im Ruhezustand verschlüsselt und für ONCARE und seine Dienstleister pseudonymisiert. Die Leistungserbringer von ONCARE haben zu keinem Zeitpunkt Zugriff auf diese personenbezogenen Daten.

Des Weiteren setzen wir Dienstleister ein, um Serviceanfragen (Support-Dienstleister) bezüglich der Nutzung des Accounts zu bearbeiten, z.B. wenn Sie Ihr Passwort vergessen haben, Ihre gespeicherte E-Mail-Adresse ändern möchten etc. Mit diesen Dienstleistern wurden die erforderlichen Auftragsverarbeitungsverträge abgeschlossen; Darüber hinaus wurden die mit der Bearbeitung von Serviceanfragen betrauten Mitarbeiter entsprechend geschult. Nach Erhalt Ihrer Serviceanfrage wird ihr eine Ticketnummer zugewiesen.

Handelt es sich um eine Serviceanfrage bezüglich Ihrer Account-Nutzung, werden die relevanten Informationen, die Sie uns bei der Kontaktaufnahme zur Verfügung gestellt haben, an einen der autorisierten Mitarbeiter des externen Dienstes weitergeleitet. Er wird sich dann mit Ihnen in Verbindung setzen.

Andernfalls werden sie weiterhin von speziell zugelassenen ONCARE-Mitarbeitern verarbeitet, wie unter "VERARBEITUNG VON OPERATIVEN DATEN" beschrieben.

Über unsere Support-Dienstleister verwenden wir das RepairCode-Tool, auch bekannt als Digital Twin Code, eine Customer-Experience-Plattform für den Umgang mit externem Feedback mit der Möglichkeit, Support-Tickets zu erstellen. Hier finden Sie die Datenschutzerklärung:

<https://app.repaircode.de/?main=main-client-Rechtliches/privacy>.

Schlussendlich zeigen wir Ihnen Inhalte von Instagram (Anbieter: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland) ein (z. B. Bilder, Videos oder Beiträge). Wenn Sie auf einen verlinkten Instagrambeitrag klicken, werden Sie auf Instagram weitergeleitet. Dabei können von Instagram Cookies gesetzt und Nutzerdaten verarbeitet werden.

Wenn Sie eine Seite mit verlinkten Instagram-Beitrag aufrufen, kann Ihr Browser automatisch eine Verbindung zu den Servern von Instagram herstellen. Instagram erhält dadurch die Information, dass Sie unsere Website besucht haben, selbst wenn Sie kein Instagram-Konto besitzen oder nicht eingeloggt sind. Falls Sie eingeloggt sind, kann Instagram den Besuch Ihrem Benutzerkonto zuordnen.

Datenschutzerklärung:

<https://privacycenter.instagram.com/policy>

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Zur Erbringung unserer Dienste können wir Dienstleister in Anspruch nehmen, die außerhalb der Europäischen Union ansässig sind. Wenn die Daten in ein Drittland übertragen werden, in welchem der Schutz für personenbezogene Daten als nicht angemessen beurteilt wurde, stellen wir sicher, dass angemessene Maßnahmen in Übereinstimmung mit nationalem und europäischem Recht getroffen werden und das – falls erforderlich – entsprechende Standardvertragsklauseln zwischen den verarbeitenden Parteien vereinbart wurden.

Die persönlichen Daten, die von dieser **myoncare-App** erfasst werden, werden nicht in den App-Stores gespeichert. Eine Übermittlung personenbezogener Daten in Drittländer (außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums) erfolgt nur, wenn dies zur Erfüllung der vertraglichen Verpflichtung erforderlich ist, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben.

Die Synchronisierung der **myoncare-App** und des **myoncare-Portals** erfolgt über Google Firebase. Der Google Firebase-Server wird in der Europäischen Union gehostet. Wie in den Nutzungsbedingungen von Google Firebase beschrieben, sind jedoch kurzfristige Datenübermittlungen in Länder möglich, in denen Google oder seine Dienstanbieter ansässig sind; Bei bestimmten Google Firebase-Diensten erfolgt eine Datenübermittlung nur in die USA, es sei denn, die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Unrechtmäßiger Zugriff auf Ihre Daten wird mit Ende-zu-Ende-Verschlüsselung und sicheren Zugriffstoken verhindert. Unsere Server werden in Deutschland gehostet. Zu Analysezwecken enthalten die mit SendGrid versendeten E-Mails ein sogenanntes "Zählpixel", das sich beim Öffnen der E-Mail mit den Servern von Sendgrid verbindet. Damit kann festgestellt werden, ob eine E-Mail-Nachricht geöffnet wurde.

Wir binden Inhalte von Instagram ein, die von der Meta Platforms Ireland Ltd. bereitgestellt werden. Wenn Sie einen verlinkten Instagram-Beitrag anklicken, kann es sein, dass personenbezogene Daten (z. B. IP-Adresse, Browser-Informationen, Interaktionen) an Meta Platforms Inc. in die USA oder andere Drittländer übermittelt werden.

Meta ist unter dem EU-U.S. Data Privacy Framework (DPF) zertifiziert, wodurch für die Übermittlung in die USA ein angemessenes Datenschutzniveau anerkannt ist. Dennoch können auch Daten in Länder übertragen werden, für die kein Angemessenheitsbeschluss der Europäischen Kommission besteht. In solchen Fällen können zusätzliche Schutzmaßnahmen erforderlich sein, deren Wirksamkeit jedoch nicht immer garantiert werden kann.

## Rechtsgrundlage

Die Datenverarbeitung erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Diese

Einwilligung können Sie jederzeit widerrufen. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitungsvorgänge bleibt vom Widerruf unberührt.

Bitte beachten Sie, dass Ihre Daten in der Regel von uns an einen Server von SendGrid in den USA übermittelt und dort gespeichert werden. Wir haben mit Sendgrid einen Vertrag abgeschlossen, der die EU-Standardvertragsklauseln enthält. Dadurch wird sichergestellt, dass ein Schutzniveau besteht, das mit dem der EU vergleichbar ist.

Zur Verarbeitung von Aktivitätsdaten werden auf dem mobilen Gerät des **App-Benutzers** Schnittstellen zu Google Cloud-Diensten (im Fall von GoogleFit) oder zu AppleHealth oder Withings verwendet. **myoncare-Tools** verwenden diese Schnittstellen, die von Google, Apple und Withings bereitgestellt werden, um Aktivitätsdaten von verbundenen Gesundheits-Apps anzufordern. Die von den **myoncare-Tools** gesendete Anfrage enthält keine personenbezogenen Daten. Personenbezogene Daten werden den **myoncare Tools** über diese Schnittstellen zur Verfügung gestellt.

## DAUER DER SPEICHERUNG PERSONENBEZOGENER DATEN

Wir bewahren Ihre personenbezogenen Daten so lange auf, wie sie für den Zweck, für den sie verarbeitet werden, erforderlich sind. Bitte beachten Sie, dass zahlreiche Aufbewahrungsfristen die weitere Speicherung personenbezogener Daten erfordern. Dies gilt insbesondere, aber nicht ausschließlich, für handels- oder steuerrechtliche Aufbewahrungspflichten (z.B. Handelsgesetzbuch, Steuergesetz, etc.). Darüber hinaus muss Ihr **Leistungserbringer** auch die Aufbewahrung Ihrer medizinischen Unterlagen sicherstellen (je nach Art der Dokumente zwischen 1 und 30 Jahren).

Bitte beachten Sie, dass ONCARE auch Aufbewahrungspflichten unterliegt, die mit Ihrem **Leistungserbringer** aufgrund der gesetzlichen Bestimmungen vertraglich vereinbart werden. Darüber hinaus, und nur wenn Ihr **Leistungserbringer** die Medizinproduktvariante der **myoncare-Tools** verwendet, gelten aufgrund der Einstufung der **myoncare-App** als Medizinprodukt bestimmte Aufbewahrungsfristen, die sich aus dem

Medizinproduktgesetz ergeben. Sofern keine anderweitigen Aufbewahrungspflichten bestehen, werden die personenbezogenen Daten routinemäßig gelöscht, sobald der Zweck erreicht ist.

Darüber hinaus können wir personenbezogene Daten aufbewahren, wenn Sie uns Ihre Einwilligung dazu erteilt haben oder wenn es zu einem Rechtsstreit kommt und wir innerhalb der gesetzlichen Verjährungsfristen, die bis zu 30 Jahre betragen können, Beweismittel verwenden; Die regelmäßige Verjährungsfrist beträgt drei Jahre.

## VERPFLICHTUNG ZUR ANGABE PERSONENBEZOGENER DATEN

Für die Begründung, Durchführung und Beendigung des Vertragsverhältnisses und die Erfüllung der damit verbundenen vertraglichen und gesetzlichen Pflichten sind verschiedene personenbezogene Daten erforderlich. Das Gleiche gilt für die Nutzung unserer **myoncare-App** und die verschiedenen Funktionen, die sie bietet.

Die Details haben wir für Sie unter den oben genannten Punkten zusammengefasst. In bestimmten Fällen müssen personenbezogene Daten auch gemäß den gesetzlichen Bestimmungen erhoben oder zur Verfügung gestellt werden. Bitte beachten Sie, dass es ohne die Bereitstellung dieser personenbezogenen Daten nicht möglich ist, Ihre Anfrage zu bearbeiten oder die zugrundeliegende vertragliche Verpflichtung zu erfüllen.

## ZUGRIFFSRECHTE

Für alle Geräte, unabhängig vom verwendeten Betriebssystem, ist es notwendig, der App bestimmte Berechtigungen zu erteilen, die wir als "grundlegende Zugriffsrechte" bezeichnen. Abhängig vom Betriebssystem des Geräts, das Sie verwenden, verfügt es möglicherweise über zusätzliche Funktionen, die zusätzliche Berechtigungen erfordern, damit die App funktioniert. Damit die **myoncare-App** auf Ihrem Gerät funktioniert, muss der App verschiedene Berechtigungen erteilt werden, um auf bestimmte Funktionen des Geräts zuzugreifen. Gegebenenfalls werden wir sie in der Reihenfolge des Betriebssystems (Android oder iOS) gemäß den "Rahmenbedingungen" auflisten.

Die grundlegenden Zugriffsrechte (Android und iOS) sind:

### WLAN-Verbindungen abrufen

Erforderlich, um die Funktionalität des Dokumentendownloads in Verbindung mit Wi-Fi-Verbindungen sicherzustellen.

### Netzwerk-Verbindung abrufen

Erforderlich, um die Funktionalität des Dokumentendownloads in Verbindung mit Netzwerkverbindungen sicherzustellen, bei denen es sich nicht um Wi-Fi-Verbindungen handelt.

### Bildschirmsperre deaktivieren (Stand-by-Modus verhindern)

Erforderlich, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne durch eine Bildschirmsperre unterbrochen zu werden.

### Zugang zu allen Netzwerken

Zum Herunterladen von Dokumenten ist der Zugang zu allen Netzwerken erforderlich.

### Deaktivieren des Schlafmodus

Dies ist notwendig, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne dass die Wiedergabe durch das Auftreten des Ruhezustands unterbrochen wird.

### Mobile Daten / Zugriff auf mobile Daten

Möchte der Nutzer Dokumente ausschließlich über WLAN herunterladen, kann er im Menü der App die entsprechende Einstellung vornehmen und die Nutzung mobiler Daten deaktivieren. Der Zugriff auf mobile Daten ist erforderlich, um die Funktionalität der Deaktivierung von Dokumentendownloads über mobile Daten sicherzustellen.

### Zugriff auf die Kamera

Sowohl für das Scannen von QR-Codes als auch für Videokonsultationen ist ein Kamerazugang erforderlich

### Zugriff auf das Mikrofon

Für Videosprechstunden ist ein Mikrofonzugang erforderlich

### Zugriff auf Dateien und Fotos

Dies ist für den Austausch von Dateien zwischen Ihnen und Ihren verbundenen Portalbenutzern erforderlich.

### Zugriff auf den Webbrowser

Dies ist erforderlich, um empfangene Dateien von Benutzern des verbundenen Portals anzuzeigen.

Wir verwenden Push-Benachrichtigungen, bei denen es sich um Nachrichten handelt, die als Service der **myoncare-App** über Dienste wie den Apple Push Notification Service oder den Google Cloud Messaging Service an Ihr mobiles Gerät gesendet werden. Diese Dienste sind Standardfunktionen von Mobilgeräten. Die Datenschutzrichtlinie des Diensteanbieters regelt den Zugriff, die Verwendung und die Offenlegung personenbezogener Daten infolge Ihrer Nutzung dieser Dienste.

### AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL

Wir verwenden keine rein automatisierte Verarbeitung, um Entscheidungen zu treffen.

### IHRE RECHTE ALS BETROFFENE PERSON

Wir möchten Sie über Ihre Rechte als betroffene Person informieren. Diese Rechte sind in den Artikeln 15 bis 22 DSGVO festgelegt und umfassen:

**Auskunftsrecht (Art. 15 DSGVO):** Sie haben das Recht, Auskunft darüber zu verlangen, ob und wie Ihre personenbezogenen Daten verarbeitet werden, einschließlich Informationen über die Verarbeitungszwecke, Empfänger, Speicherdauer sowie Ihre Rechte auf Berichtigung, Löschung und Widerspruch. Sie haben auch das Recht, eine Kopie aller personenbezogenen Daten zu erhalten, die wir über Sie gespeichert haben.

**Recht auf Löschung / Recht auf Vergessenwerden (Art. 17 DSGVO):** Sie können von uns verlangen, dass Ihre von uns erhobenen und verarbeiteten personenbezogenen Daten unverzüglich gelöscht werden. In diesem Fall werden wir Sie bitten, die **myoncare-App** einschließlich Ihrer UID (Unique Identification Number) von Ihrem Smartphone/Handy zu löschen. Bitte beachten Sie jedoch, dass wir Ihre personenbezogenen Daten erst nach Ablauf der gesetzlichen Aufbewahrungsfristen löschen können.

**Recht auf Berichtigung (Art. 16 DSGVO):** Sie können uns auffordern, unrichtige personenbezogene Daten zu aktualisieren oder zu korrigieren oder unvollständige personenbezogene Daten zu vervollständigen.

**Recht auf Datenübertragbarkeit (Art. 20 DSGVO):** Grundsätzlich können Sie von uns verlangen, dass wir Ihnen personenbezogene Daten, die Sie uns zur Verfügung gestellt haben und die auf Grundlage Ihrer Einwilligung oder der Durchführung eines Vertrages mit Ihnen automatisiert verarbeitet werden, in maschinenlesbarer Form zur Verfügung stellen, damit diese zu einem Ersatzdienstleister "portiert" werden können.

**Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO):** Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn die Richtigkeit der Daten bestritten wird, die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden oder ein Widerspruch gegen die Verarbeitung geprüft wird.

**Widerspruchsrecht gegen die Datenverarbeitung (Art. 21 DSGVO):** Sie haben das Recht, der Verwendung Ihrer personenbezogenen Daten durch uns zu widersprechen und Ihre Einwilligung jederzeit zu widerrufen, wenn wir Ihre personenbezogenen Daten auf der Grundlage Ihrer Einwilligung verarbeiten. Wir werden unsere Dienstleistungen auch dann weiterhin erbringen, wenn sie nicht von einer widerrufenen Einwilligung abhängig sind.

Um diese Rechte auszuüben, wenden Sie sich bitte zunächst an Ihren **Leistungserbringer** oder Ihr **Unternehmen** oder kontaktieren Sie uns unter: [privacy@myoncare.com](mailto:privacy@myoncare.com). Widerspruch und Widerruf der Einwilligung müssen in Textform an [privacy@myoncare.com](mailto:privacy@myoncare.com) erklärt werden.

Wir verlangen von Ihnen einen ausreichenden Nachweis Ihrer Identität, um sicherzustellen, dass Ihre Rechte geschützt sind und dass Ihre personenbezogenen Daten nur an Sie und nicht an Dritte weitergegeben werden.

Bitte kontaktieren Sie uns auch jederzeit unter [privacy@myoncare.com](mailto:privacy@myoncare.com) wenn Sie Fragen zur Datenverarbeitung in unserem Unternehmen haben



## MYONCARE PATIENTEN APP – DATENSCHUTZERKLÄRUNG (EUROPA)

Stand: Februar 2025

oder wenn Sie Ihre Einwilligung widerrufen möchten. Sie haben auch das Recht, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

[privacy@myoncare.com](mailto:privacy@myoncare.com)

Zuletzt aktualisiert am 20. Februar 2025.

### DATENSCHUTZBEAUFTRAGTER

\* \* \* \*

Unseren Datenschutzbeauftragten für alle Fragen zum Datenschutz erreichen Sie unter [privacy@myoncare.com](mailto:privacy@myoncare.com).

### ALTERSBESCHRÄNKUNG DER ANWENDUNG

Ein Mindestalter von 18 Jahren ist erforderlich, um die **myoncare-App** zu nutzen.

### ÄNDERUNGEN DER DATENSCHUTZERKLÄRUNG

Wir behalten uns ausdrücklich das Recht vor, diese **Datenschutzerklärung** in Zukunft nach unserem alleinigen Ermessen zu ändern. Änderungen oder Ergänzungen können beispielsweise notwendig sein, um gesetzlichen Anforderungen zu entsprechen, technische und wirtschaftliche Entwicklungen zu berücksichtigen oder den Interessen der **App-** oder **Portal-Nutzer** gerecht zu werden.

Änderungen sind jederzeit möglich und werden Ihnen in geeigneter Weise und in einem angemessenen Zeitrahmen mitgeteilt, bevor sie in Kraft treten (z. B. durch Veröffentlichung einer überarbeiteten Datenschutzerklärung beim Login oder durch Vorankündigung wesentlicher Änderungen).

***Bei Auslegungsfragen oder Streitigkeiten ist ausschließlich die deutsche Fassung der Datenschutzerklärung verbindlich und maßgeblich.***

ONCARE GmbH

Postanschrift

Balanstraße 71a

81541 München, Deutschland

T | +49 (0) 89 4445 1156

E | [privacy@myoncare.com](mailto:privacy@myoncare.com)

Kontaktdaten des Datenschutzbeauftragten

## U.S. DATENSCHUTZRICHTLINIE

Willkommen bei myoncare, dem digitalen Gesundheitsportal und der mobilen App ("App") für eine effiziente und bedarfsorientierte Patientenversorgung sowie Unterstützung von Programmen zum betrieblichen Gesundheitsmanagement.

Diese Datenschutzrichtlinie beschreibt, wie Ihre persönlichen und medizinischen Daten verwendet und weitergegeben werden können und wie Sie auf diese Informationen zugreifen können. Bitte lesen Sie diese Datenschutzrichtlinie sorgfältig durch. In dieser Datenschutzerklärung erfahren Sie, warum und wie ONCARE Ihre uns zur Verfügung gestellten personenbezogenen Gesundheitsdaten verarbeitet, wenn Sie sich für die Nutzung der myoncare App entscheiden.

Für uns bei der Oncare GmbH (im Folgenden "**Oncare (ONCARE)**" oder "**wir**", "**uns**", "**unser**") ist der Schutz Ihrer Privatsphäre und der Sie betreffenden personenbezogenen Daten bei der Nutzung der myoncare-App von großer Relevanz und Bedeutung. Wir sind uns der Verantwortung bewusst, die sich aus Ihrem Vertrauen in die Bereitstellung und Speicherung Ihrer personenbezogenen (Gesundheits-)Daten in der myoncare App ergibt. Daher sind unsere Technologiesysteme, die für die myoncare-Dienste verwendet werden, nach höchsten Standards eingerichtet und die rechtmäßige Verarbeitung der Daten steht im Mittelpunkt unseres ethischen Verständnisses als Unternehmen.

Alle Informationen, die wir besitzen und die von Ihren Leistungserbringern bereitgestellt werden, sind **geschützte Gesundheitsinformationen (PHI)** und/oder andere medizinische Informationen. Diese sind durch bestimmte Gesetze geschützt, wie z. B. dem U.S. Gesetz Health Insurance Portability and Accountability Act (**HIPAA**). Wir sind gesetzlich verpflichtet, die Privatsphäre und Sicherheit geschützter Gesundheitsinformationen zu schützen. Wir sind ständig bestrebt, Gesundheitsinformationen durch administrative, physische und technische Mittel zu schützen und ansonsten die geltenden Bundes- und Landesgesetze einzuhalten.

Die Nutzung und Offenlegung solcher **PHIs** erfolgt in Übereinstimmung mit den geltenden Datenschutzrichtlinien und den anwendbaren Gesetzen. Um genauer zu verstehen, wie wir diese **PHIs** verarbeiten und teilen, sollten Sie diese **Datenschutzerklärung** sorgfältig lesen.

Bitte lesen Sie die Datenschutzrichtlinie sorgfältig durch, um sicherzustellen, dass Sie jede Bestimmung verstehen. Nachdem Sie die Datenschutzrichtlinie gelesen haben, haben Sie die Möglichkeit, der Datenschutzrichtlinie zuzustimmen und der Verarbeitung Ihrer personenbezogenen (Gesundheits-)Daten, wie in der Datenschutzrichtlinie beschrieben, zuzustimmen. Wenn Sie Ihre Einwilligung erteilen, wird die Datenschutzerklärung Bestandteil des Vertrags zwischen Ihnen und ONCARE. Wir halten uns an die in dieser Datenschutzerklärung beschriebenen Rechte und Pflichten. Wir verwenden und verarbeiten Ihre Daten in Übereinstimmung mit den Bestimmungen dieser Datenschutzerklärung.

Unser Angebot richtet sich laut Nutzungsbedingungen nur an Personen ab 18 Jahren. Dementsprechend werden keine personenbezogenen Daten von Kindern und Jugendlichen unter 18 Jahren gespeichert und verarbeitet.

## DEFINITIONEN

**„App-Nutzer“** bezeichnet jeden Benutzer der myoncare-App (Patient und/oder Mitarbeiter).

**„Blockchain-Technologie“** Das myoncare-System enthält eine zusätzliche Datenbank, in der die Daten aller Installationen gespeichert werden.

**„Firma“** bezeichnet Ihren Arbeitgeber, wenn Sie und Ihr Arbeitgeber die myoncare-Tools für das betriebliche Gesundheitsmanagement des Arbeitgebers nutzen.

**„Betroffene Entität“** bezeichnet einen Gesundheitsplan, eine Clearingstelle für das Gesundheitswesen oder einen Leistungserbringer, der Gesundheitsinformationen in elektronischer Form im Zusammenhang mit einer Transaktion übermittelt, die unter HIPAA fällt.

**„Datendienstleister“** bezeichnet jeden Beauftragten, der von der Firma beauftragt und angewiesen wird, pseudonymisierte oder anonymisierte Mitarbeiterdaten

in Programmen zum betrieblichen Gesundheitsmanagement auf der Grundlage einer separaten Dienstleistungsvereinbarung mit der Firma zu sammeln, zu überprüfen und zu interpretieren (z. B. Datenanalyst, allgemeine Gesundheitspräventionsdienste, Datenauswertungsdienste usw.), die durch ein separates Informationsblatt an die Mitarbeiter gekennzeichnet sind.

**"EU-Datenschutz-Grundverordnung"**. Die Datenschutz-Grundverordnung (DSGVO) ist ein europäisches Datenschutzgesetz. Die Verordnung trat am 25. Mai 2018 in Kraft und zielt darauf ab, den Datenschutz in allen Mitgliedstaaten zu harmonisieren und den Bürgerinnen und Bürgern mehr Kontrolle über ihre personenbezogenen Daten zu geben. Die DSGVO gilt für alle Unternehmen und Organisationen, die in der EU tätig sind oder personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig davon, ob das Unternehmen innerhalb oder außerhalb der EU ansässig ist. Die DSGVO gilt auch für Sie als US-Bürger, da Oncare seinen Sitz in Deutschland hat.

**„Leistungserbringer“** bezeichnet Ihren Arzt, Ihre Klinik, Ihre Gesundheitseinrichtung oder einen anderen Angehörigen der Gesundheitsberufe, der allein oder im Auftrag Ihres Arztes, Ihrer Klinik oder Ihrer Gesundheitseinrichtung handelt.

**„Care Pathway“** ist ein standardisierter Behandlungsplan, der die Schritte für Diagnosen und Therapien festlegen kann. **„Caretasks“** sind spezifische Aufgaben oder Handlungen innerhalb eines Pathways, die von den beteiligten Leistungserbringern, dem Pflegepersonal oder dem Patienten selbst durchgeführt werden müssen.

**„Gesundheitsinformationen“** bezeichnet alle Informationen, einschließlich genetischer Informationen, unabhängig davon, ob sie mündlich oder in irgendeiner Form oder auf einem Medium aufgezeichnet wurden, und die

- von einem Gesundheitsdienstleister, einer Krankenkasse, einer Gesundheitsbehörde, einem Arbeitgeber, einem Lebensversicherer, einer Schule oder Universität oder einer Clearingstelle für das Gesundheitswesen verarbeitet oder übertragen werden; und

- sich auf die vergangene, gegenwärtige oder zukünftige körperliche oder geistige Gesundheit einer Person oder auf einen Gesundheitszustand im Zusammenhang mit der medizinischen Behandlung der Person bezieht, je nach Fall;

- die vergangene, gegenwärtige oder zukünftige Honorarvergütung für die Gesundheitsversorgung einer Person. **„Geschützte Gesundheitsinformationen“** oder **„PHI“** bezeichnet individuell identifizierbare Gesundheitsinformationen, die

i) über elektronische Medien übermittelt werden;

(ii) in elektronischen Medien gepflegt werden; oder

(iii) in einer anderen Form oder einem anderen Medium übertragen oder aufrechterhalten werden.

**„Gesetz zur Übertragbarkeit und Verantwortlichkeit der Krankenversicherung“**, das Health Insurance Portability and Accountability Act von 1996 (**HIPAA**) ist ein US-amerikanisches Bundesgesetz, das die Schaffung nationaler Standards vorsieht, um die sensiblen Gesundheitsdaten der Patienten vor unbefugter Offenlegung ohne deren Zustimmung oder Wissen zu schützen. Die HIPAA-Anforderungen gelten für die Verwendung und Offenlegung von Gesundheitsinformationen von Einzelpersonen durch Institutionen, die dem HIPAA-Gesetz unterliegen. Diese Personen und Organisationen werden als "Covered Entities" bezeichnet.

**„myoncare PWA“** bezeichnet die myoncare Progressive Web App für Patienten, die die von ONCARE angebotenen Dienste über die PWA und nicht über die myoncare-App nutzen möchten.

**„myoncare-Portal“** ist das myoncare-Webportal, das für die professionelle Nutzung durch Portalnutzer bestimmt ist und als Schnittstelle zwischen Portalnutzern und App-Nutzern dient.

**„myoncare-Dienste“** bezeichnet die Dienste, Funktionalitäten und sonstigen Angebote, die den Portalnutzern über das myoncare-Portal und/oder den App-Nutzern über die myoncare-App angeboten werden oder angeboten werden können.

„**myoncare-Tools**“ meint die myoncare-App und das myoncare-Portal zusammen.

„**ONCARE**“ oder „**wir**“ meint die ONCARE GmbH mit Sitz in Deutschland.

„**Portalnutzer**“ bezeichnet jeden Leistungserbringer, jede Firma oder jeden Datendienstleister, der das webbasierte myoncare-Portal nutzt.

„**Datenschutzerklärung**“ meint diese Erklärung, die Ihnen als Patient oder Mitarbeiter und Nutzer der myoncare-App gegenüber abgegeben wird und beschreibt, wie wir Ihre personenbezogenen Daten erfassen, nutzen und speichern, und Sie über Ihre Rechte informiert.

„**myoncare-App**“ meint die mobile myoncare-App zur Nutzung durch Patienten oder Mitarbeiter, die die von ONCARE angebotenen Dienste in Anspruch nehmen möchten.

„**Nutzungsbedingungen**“ bezeichnet die Nutzungsbedingungen für die Nutzung der myoncare App.

## EINHALTUNG GESETZEN

Die Oncare GmbH, ein beim Amtsgericht München unter der Registernummer 219909 eingetragenes Unternehmen mit Sitz in der Balanstraße 71a, 81541 München, Deutschland, bietet die mobile Anwendung **myoncare-App** an und betreibt diese als Zugang zu den **myoncare-Diensten**. Diese Datenschutzerklärung gilt für alle personenbezogenen Daten, die von ONCARE im Zusammenhang mit der Nutzung der **myoncare App**.

ONCARE ist ein „Geschäftspartner“ im Sinne von **HIPAA**, der Dienstleistungen und Gesundheitspläne für Leistungserbringer erbringt, die im Sinne von **HIPAA** als „erfasste Einheiten“ bezeichnet werden; ONCARE schließt mit diesen erfassten Unternehmen Geschäftspartnervereinbarungen ab. ONCARE wird die **PHIs** nur unter den Bedingungen der Vereinbarungen und gemäß **HIPAA** verarbeiten und weitergeben.

Wir sind gemäß den U.S. Gesetz verpflichtet, den Datenschutz und die Sicherheit Ihrer geschützten Gesundheitsdaten zu wahren.

Wir sind gemäß den U.S. Gesetzen verpflichtet, die Gesetze zum Schutz der Privatsphäre und Sicherheit geschützter Gesundheitsinformationen zu folgen. Wir werden Sie unverzüglich informieren, wenn es zu einer Verletzung (sog. Datenschutzverletzung) kommt, die die Privatsphäre oder Sicherheit von (Gesundheits-) Informationen gefährdet haben könnte.

Wir müssen die in dieser Datenschutzrichtlinie beschriebenen Verpflichtungen und Inhalte einhalten und Ihnen auf Anfrage eine Kopie der Datenschutzrichtlinie zur Verfügung stellen.

Es werden keine identifizierbaren persönlichen (Gesundheits-)Informationen verkauft.

Wir werden Ihre Daten nicht anders als hier beschrieben verwenden oder weitergeben, es sei denn, Sie teilen uns mit, dass wir dazu berechtigt sind.

U.S. Datenschutzerklärung, U.S. Bundes- und Landesgesetze können zusätzliche Einschränkungen für die Weitergabe Ihrer Gesundheitsdaten im Zusammenhang mit der medizinischen Behandlung von Drogen- oder Alkoholmissbrauch, sexuell übertragbaren Krankheiten, genetischen Informationen oder Behandlungsprogrammen für psychische Gesundheit, vorsehen. Falls entsprechende Gesetze einschlägig sind, holen wir Ihre Genehmigung ein, bevor wir diese Daten weitergeben bzw. verarbeiten.

## WAS SIND PERSONENBEZOGENE DATEN IM SINNE DER DSGVO?

Wir verarbeiten Ihre personenbezogenen Daten in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen zum Schutz personenbezogener Daten, insbesondere der EU-Datenschutz-Grundverordnung und den für uns geltenden landesspezifischen Gesetzen. Sie finden eine Beschreibung der von uns erhobenen und verarbeiteten personenbezogenen Daten sowie des Zwecks und der Grundlage, auf der wir die personenbezogenen Daten verarbeiten, und der Ihnen zustehenden Rechte.



**"Personenbezogene Daten"** bezeichnet alle Informationen, die es ermöglichen, eine natürliche Person zu identifizieren. Insbesondere beinhaltet dies Ihren Namen, Ihren Geburtstag, Ihre Adresse, Ihre Telefonnummer, Ihre E-Mail-Adresse und Ihre IP-Adresse.

**"Gesundheitsdaten"** sind personenbezogene Daten, die sich auf die physische und psychische Gesundheit einer natürlichen Person beziehen, einschließlich der Bereitstellung von Gesundheitsdiensten, die Informationen über ihren Gesundheitszustand offenbaren.

Daten sind als **"anonym"** anzusehen, wenn kein persönlicher Bezug zu der Person/dem Nutzer hergestellt werden kann. Im Gegensatz dazu sind **„pseudonymisierte“** Daten Daten, bei denen der Personenbezug oder personenbezogene Daten durch einen oder mehrere künstliche Identifikatoren oder Pseudonyme ersetzt werden, die jedoch im Allgemeinen durch den Identifikatorschlüssel wieder reidentifiziert werden können (im Sinne von Art. 4 Nr. 5 DSGVO).

### myoncare PWA

Eine Progressive Web App (PWA) ist eine Website, die aussieht und die Funktionalität einer mobilen App hat. PWAs wurden entwickelt, um die nativen Funktionen mobiler Geräte zu nutzen, ohne dass ein App Store erforderlich ist. Das Ziel von PWAs ist es, den Unterschied zwischen Apps und dem traditionellen Web zu kombinieren, indem die Vorteile nativer mobiler Apps in den Browser gebracht werden. Die PWA basiert auf der Technologie von "React ". "React " ist eine Open-Source-Software für PWA-Anwendungen.

Um die Funktion **myoncare PWA** nutzen zu können benötigen Patienten einen Computer oder ein Smartphone und eine aktive Internetverbindung. Es ist nicht erforderlich, eine App herunterzuladen.

Einige Dienste der **myoncare-App** können innerhalb der **myoncare PWA** nicht genutzt werden, siehe die Beschreibung unten für Details. Dabei handelt es sich um die folgenden Dienstleistungen oder Spezifikationen:

- Chatten mit **Leistungserbringern**;
- Videoanrufe;

- Sicherheits-PIN-Codes;
- Tracking von Aktivitätsdaten (z.B. über AppleHealth, GoogleFit, Withings).

Die folgenden Informationen über die **myoncare App** gilt auch für die **myoncare PWA**, sofern in diesem Abschnitt nichts anderes beschrieben ist

### WELCHE PERSONENBEZOGENEN DATEN WERDEN BEI DER NUTZUNG DER MYONCARE APP VERWENDET

Wir verwenden und geben Ihre Gesundheitsdaten für übliche Geschäftsaktivitäten weiter, die gesetzlich in die Kategorien Behandlung und Gesundheitsversorgung fallen. Wir können die folgenden Datenkategorien über Sie bei der Nutzung der **myoncare App** verarbeiten:

**Operative Daten:** Personenbezogene Daten, die Sie uns bei der Registrierung in unserer **myoncare App**, bei der Kontaktaufnahme zu Problemen mit der App oder bei sonstigen Interaktionen mit uns zum Zweck der Nutzung der App zur Verfügung stellen.

**Behandlungsdaten:** Sie oder Ihr **Leistungserbringer** geben personenbezogene Daten wie Name, Alter, Größe, Gewicht, Indikation, Krankheitssymptome und weitere Informationen im Zusammenhang mit Ihrer Behandlung (z. B. in einem Behandlungsplan) mit Unterstützung der **myoncare-App** ein. Zu den Informationen im Zusammenhang mit Ihrer Behandlung gehören unter anderem: Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien, die von Ihrem **Leistungserbringer** bereitgestellt wurden, sowie geplante und erledigte Aufgaben.

**Aktivitätsdaten:** Personenbezogene Daten, die von uns verarbeitet werden, wenn Sie die **myoncare-App** mit einer Gesundheits-App (z. B. GoogleFit, AppleHealth, Withings) verbinden. Ihre Aktivitätsdaten werden an Ihre angeschlossenen **Leistungserbringer** als Portalnutzer übertragen.

<b>Kommerzielle</b>	<b>und</b>	<b>nicht-kommerzielle</b>
<b>Forschungsdaten:</b>	Wir	verarbeiten Ihre
	personenbezogenen	Daten in
	anonymisierter/pseudonymisierter	Form, um

zusammenfassende wissenschaftliche Berichte zu analysieren und zu erstellen, um Produkte, Behandlungen und wissenschaftliche Ergebnisse zu verbessern.

**Produktsicherheitsdaten:** Personenbezogene Daten, die verarbeitet werden, um unseren gesetzlichen Verpflichtungen als Hersteller der **myoncare-App** als Medizinprodukt nachzukommen. Darüber hinaus können Ihre personenbezogenen Daten von Medizinprodukte- oder Pharmaunternehmen verarbeitet werden, um Ziele der Rechtssicherheit oder der Vigilanz zu erfüllen.

**Informationen zur Rückerstattung:** Personenbezogene Daten, die für den Erstattungsprozess zwischen Ihrem myoncare **Leistungserbringer** und Ihrer Krankenkasse erforderlich sind.

**Daten zum betrieblichen Gesundheitsmanagement:** Persönliche oder aggregierte Daten, die in spezifischen Projekten und Fragebögen auf Anfrage der **Firma** (entweder direkt oder durch einen von der **Firma** beauftragten **Datendienstleister**) erhoben werden. Die Daten können sich auf bestimmte Gesundheitsinformationen, Ihre Meinung über Ihr persönliches Wohlbefinden, Ihre Meinung als Mitarbeiter zu einer bestimmten internen oder externen Situation oder Daten über Pflege oder Gesundheit im Allgemeinen beziehen.

## BLOCKCHAIN-TECHNOLOGIE

**Blockchain-Technologie** („**Blockchain**“) (Europäisches Patent Nr. 4 002 787) ist ein optionaler Dienst, der nicht verpflichtend ist. Es liegt an Ihrem **Leistungserbringer**, sich für die Nutzung der Blockchain-Lösung zu entscheiden. Das **Blockchain** basiert auf der Technologie von Hyperledger Fabric. Hyperledger Fabric ist eine Open-Source-Software für Blockchain-Implementierungen auf Unternehmensebene. Es bietet eine skalierbare und sichere Plattform, die Blockchain-Projekte unterstützt.

Die **Blockchain** im myoncare-System ist eine zusätzliche Datenbank, die Daten aus der Anwendung speichert. Alle Blockchain-Daten werden in der Bundesrepublik Deutschland gespeichert. Es handelt sich um eine private **Blockchain** („**Private Blockchain**“), die nur den Input

ausgewählter, verifizierter Teilnehmer zulässt, und es ist möglich, Einträge bei Bedarf zu überschreiben, zu bearbeiten oder zu löschen.

Die **Blockchain** besteht im Allgemeinen aus digitalen Daten in einer Kette von Paketen, die „Blöcke“ genannt werden und die entsprechenden Transaktionen speichern. Die Art und Weise, wie diese Blöcke miteinander verbunden sind, ist chronologisch. Der erste Block, der erstellt wird, wird als Genesis-Block bezeichnet, und jeder danach hinzugefügte Block hat einen kryptografischen Hash, der sich auf den vorherigen Block bezieht, sodass Transaktionen und Informationsänderungen auf den Genesis-Block zurückgeführt werden können. Alle Transaktionen innerhalb der Blöcke werden durch einen Blockchain-Konsensmechanismus validiert und verifiziert, um sicherzustellen, dass jede Transaktion unverändert bleibt.

Jeder Block enthält die Liste der Transaktionen, einen Zeitstempel, einen eigenen Hash und den Hash des vorherigen Blocks. Ein Hash ist eine Funktion, die digitale Daten in eine alphanumerische Kette umwandelt. In diesem Fall kann der Block nicht mehr mit den anderen synchronisiert werden. Wenn eine unbefugte Person versucht, die Daten eines einzelnen Blocks zu ändern, ändert sich auch der Hash des Blocks und die Verknüpfung zu diesem Block geht verloren. Wenn alle Knoten (Netzwerkknoten) versuchen, ihre Kopien zu synchronisieren, wird erkannt, dass eine Kopie geändert wurde, und das Netzwerk betrachtet diesen Knoten als fehlerhaft. Dieser technische Prozess verhindert, dass Unbefugte den Inhalt der Blockchain-Kette **manipulieren**.

Unsere **Blockchain** ist eine **private Blockchain**. Eine **private Blockchain** ist dezentralisiert. Dabei handelt es sich um ein sogenanntes Distributed-Ledger-System (digitales System zur Erfassung von Transaktionen), das als geschlossene Datenbank fungiert. Im Gegensatz zu öffentlichen **Blockchains**, die „unauthorisiert“ sind, sind private **Blockchains** „autorisiert“, da eine Autorisierung erforderlich ist, um Nutzer zu werden. Im Gegensatz zu öffentlichen **Blockchains**, die für jeden öffentlich zugänglich sind, ist der Zugang zu privaten **Blockchains** von einer Autorisierung abhängig, um Nutzer zu werden. Diese Struktur ermöglicht es, die Sicherheit und Unveränderlichkeit der **Blockchain-Technologie** zu

nutzen und gleichzeitig datenschutzkonform zu bleiben, insbesondere die Vorschriften der Datenschutz-Grundverordnung (**DSGVO**) einzuhalten. Private Blockchain-Einträge können bearbeitet, geändert oder gelöscht werden; Löschen bedeutet in diesem Zusammenhang, dass der Referenzwert zur UUID (Universally Unique Identifier) in der Datenbank des **Leistungserbringers** gelöscht wird. Darüber hinaus wird der Hash in der Blockchain-Datenbank anonymisiert, so dass dieser Gesamtprozess konform mit der Datenschutz-Grundverordnung ist und die Rechte einer betroffenen Person gewährleistet sind (Recht auf Löschung "Recht auf Vergessenwerden", Art. 17 DSGVO).

#### Art der Daten, die in der Blockchain gespeichert und verarbeitet werden:

- Patienten-UUID
- Institutionen/Leistungserbringer UUID
- Asset-UUID
- Hash von **caretask** und Asset-Daten.  
(UUID: *Universeller eindeutiger Identifikator*).

Die in der **Blockchain** gespeicherten Daten sind pseudonymisiert.

Unsere **Blockchain** ist darauf ausgelegt, den Datenschutz in Bezug auf Datenintegrität, Patientenprofile, Vermögenswerte sowie zugewiesene **Care Tasks** und Medikamente zu gewährleisten. Um mit der **Blockchain** zu kommunizieren, muss der Benutzer eine Reihe von öffentlichen und privaten Schlüsseln registrieren. Um mit der **Blockchain** zu kommunizieren, benötigt der Benutzer mehrere öffentliche und private Schlüssel; der Registrierungsprozess generiert Zertifikate, die in einer separaten Datenbank des **Leistungserbringers** und auf dem Mobiltelefon des Patienten gespeichert werden. Eine Sicherungskopie des Patientenschlüssels wird verschlüsselt in der Datenbank des **Leistungserbringers** gespeichert, auf die nur der Patient zugreifen kann.

Bei der Überprüfung der Zustimmung zum Datenschutz, falls der **Leistungserbringer** mit dem Patienten kommunizieren möchte, überprüft das System, ob der Patient der Datenschutzrichtlinie des **Leistungserbringers** zugestimmt hat. Die **Blockchain** dient somit dazu, die Integrität und Verantwortlichkeit des Protokolls sicherzustellen, um zu gewährleisten, dass der Patient die Datenschutzrichtlinie akzeptiert hat.

Wenn ein **Leistungserbringer** eine neue Version einer Datenschutzrichtlinie hochlädt, wird der Hash der Datei auf der **Blockchain** gespeichert, und nachdem der Patient der Datenschutzrichtlinie zugestimmt hat, wird diese Interaktion auf der **Blockchain** gespeichert. Jedes Mal, wenn eine Kommunikation mit dem Patienten erfolgt, antwortet die **Blockchain**, indem sie den Hash mit einer Markierung vergleicht, die anzeigt, ob die Zustimmung des Patienten für die aktuelle Datenschutzrichtlinie noch gültig ist.

Die Integrität des Patientenprofils wird auch durch die Blockchain bei der Patientensynchronisation sichergestellt. Der **Leistungserbringer** erkennt sofort, wenn das Patientenprofil nicht synchronisiert oder nicht mit dem Profil auf dem Mobiltelefon übereinstimmt, indem er den Hash des Patientenprofils in der **Blockchain** vergleicht. Auf diese Weise erreicht der **Leistungserbringer** eine ausreichende Aktualität in Bezug auf das Patientenprofil.

#### myoncare Portal:

Falls der **Leistungserbringer** sich für die Nutzung der Blockchain-Lösung entscheidet, implementiert ONCARE ein zusätzliches Tool namens „Adapter Service“, das zur Kommunikation mit der **Blockchain** verwendet wird. Die Blockchain-Instanz wird von ONCARE gehostet.

#### myoncare App:

Patienten können sich mit dem Phone Manager-Tool, das ebenfalls von ONCARE gehostet wird, mit derselben Blockchain-Instanz verbinden. Dieser Service wird ebenfalls von ONCARE gehostet.

**Rechtfertigung der Verarbeitung:** Die Verarbeitung von Daten durch ONCARE im Auftrag des **Leistungserbringers** erfolgt auf der Grundlage von Art. 28 DSGVO (Auftragsverarbeitungsvertrag).

#### VERARBEITUNG VON OPERATIVEN DATEN

##### Anwendbar für alle App-Nutzer

Sie können uns bestimmte personenbezogene Daten zur Verfügung stellen, wenn Sie sich mit uns in Verbindung setzen, um die Funktionen und die Nutzung der App zu verstehen oder zu besprechen, im Falle einer Serviceanfrage Ihrerseits oder im Falle von unsererseits initiierten (telefonischen) Unterstützungsangebot.

## Service-Mitarbeiter

Im Auftrag des Datenverantwortlichen (bspw. Leistungserbringers) bieten wir Ihnen an, Sie beim Ausfüllen von Fragebögen telefonisch zu unterstützen (Outbound Calls), um Ihre digitale Patientenbegleitung zu optimieren. Sollten Sie dieses Angebot nicht nutzen wollen, steht es Ihnen frei, dieses nicht anzunehmen und der telefonischen Unterstützung zu widersprechen.

Im Falle einer Serviceanfrage sowie einem Outbound Call können auch folgende personenbezogene Daten von autorisierten ONCARE-Mitarbeitern eingesehen werden:

- die personenbezogenen Daten, die Sie Ihrem **Leistungserbringer** über unsere App zur Verfügung gestellt haben (z. B. Name, Geburtsdatum, Profilbild, Kontaktdaten);
- die Gesundheitsinformationen, die Sie Ihrem **Leistungserbringer**, dem **Datendienstleister** oder der Firma über unsere **myoncare-App** zur Verfügung gestellt haben (z. B. Informationen über eingenommene Medikamente, Antworten auf Fragebögen einschließlich krankheits- oder zustandsbezogener Informationen, Diagnosen und Therapien von medizinischen Fachkräften, geplante und erledigte Aufgaben).

Autorisierte ONCARE-Mitarbeiter, die zum Zwecke der Bearbeitung einer Serviceanfrage oder eines Outbound Calls auf die Datenbank Ihres **Leistungserbringers**, **Datendienstleisters** oder **Unternehmens** zugreifen dürfen, sind vertraglich verpflichtet, alle personenbezogenen Daten streng vertraulich zu behandeln.

## Push-Benachrichtigungen und E-Mails

Im Rahmen Ihrer Unterstützung durch myoncare möchten wir Sie darüber informieren, wie wir mit Benachrichtigungen und wichtige Informationen umgehen, die wir Ihnen zukommen lassen.

### 1. Push-Benachrichtigungen:

- o Wir senden Ihnen Push-Benachrichtigungen über unsere **myoncare-PWA** (Progressive Web App) und die **myoncare-App**, um Sie über Aufgaben, Termine und wichtige Updates zu informieren.
- o Sie haben die Möglichkeit, diese Push-Benachrichtigungen in den Einstellungen Ihrer App zu deaktivieren.

### 2. E-Mail-Benachrichtigungen:

- o Unabhängig davon, ob Sie Push-Benachrichtigungen aktiviert oder deaktiviert haben, senden wir Ihnen weiterhin wichtige Informationen und Erinnerungen per E-Mail.
- o Dies stellt sicher, dass Sie keine wichtigen Benachrichtigungen verpassen und Ihre Betreuung reibungslos verläuft.

### Warum wir dies tun:

- Unser Ziel ist es, Sie über Ihre Aufgaben und wichtige Updates auf dem Laufenden zu halten, um Ihre Gesundheit bestmöglich zu unterstützen.
- E-Mails sind ein zuverlässiger Weg, um sicherzustellen, dass wichtige Informationen Sie erreichen, auch wenn Push-Benachrichtigungen deaktiviert sind.

### Ihre Handlungsmöglichkeiten:

- Wenn Sie keine Push-Benachrichtigungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare App** deaktivieren.
- Bitte stellen Sie sicher, dass Ihre E-Mail-Adresse korrekt und aktuell ist, um einen reibungslosen Empfang unserer Nachrichten zu gewährleisten.
- Wenn Sie keine E-Mail Erinnerungen erhalten möchten, können Sie diese in den Einstellungen der **myoncare App** deaktivieren.

### Speicherdauer

Die Daten, die Sie uns zum Empfang von E-Mails zur Verfügung stellen, werden von uns gespeichert, bis Sie sich von unseren Diensten abmelden, und nach Ihrer Abmeldung sowohl von unseren Servern als auch von den Servern von Sendgrid gelöscht.

Beim Herunterladen der **myoncare-App** werden die notwendigen Informationen an den App-Store-Anbieter übermittelt. Wir haben keinen Einfluss auf diese Datenerhebung und sind dafür auch nicht verantwortlich. Wir verarbeiten die uns vom Anbieter des App-Stores bereitgestellten personenbezogenen Daten im Rahmen unserer Vertragsbeziehung zum Zweck der Weiterentwicklung unserer **myoncare-Apps** und **Dienste**.



Bei der Verarbeitung von Betriebsdaten fungiert ONCARE als Datenverantwortlicher, der für die rechtmäßige Verarbeitung Ihrer personenbezogenen Daten verantwortlich ist.

**Arten von Daten:** Ihr Name, E-Mail-Adresse, Ihre Telefonnummer, Geburtsdatum, Registrierungsdatum, von der App generierte Pseudokeys; Gerätetokens zur Identifizierung Ihres Geräts, Ihre Pseudo-Identifikationsnummer, Ihre IP-Adresse, Typ und Version des von Ihrem Gerät verwendeten Betriebssystems.

Die App verwendet die Google Maps API, um geografische Informationen zu verwenden. Bei der Nutzung von Google Maps werden von Google auch Daten über die Nutzung der Kartenfunktionen erhoben, verarbeitet und genutzt. Nähere Informationen über den Umfang, die Rechtsgrundlage und den Zweck der Datenverarbeitung durch Google sowie die Speicherdauer finden Sie in der Datenschutzerklärung von Google.

In unserer Organisation stellen wir sicher, dass nur diejenigen Personen berechtigt sind, personenbezogene Daten zu verarbeiten, die zur Erfüllung ihrer vertraglichen und gesetzlichen Pflichten dazu verpflichtet sind. Die persönlichen Daten und Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden entweder direkt oder über einen Datendienstleister Ihrem **Dienstleister** und/oder Ihrer **Firma** zur Verfügung gestellt (abhängig von der Art der Nutzung der **myoncare-Tools**).

**DSGVO-Regeln:** Die Verarbeitung von Unternehmensdaten ist auf der Grundlage von Art. 6 Abs. 1 lit. b DSGVO für die Erfüllung des Vertrages, den Sie mit ONCARE zum Zwecke der Nutzung der **myoncare App** abschließen, gerechtfertigt.

## IP GEOLOKALISIERUNG

**IP-Geolokalisierung:** Wir verwenden eine Geolokalisierungsanwendung für unsere Dienste. Wir verwenden ipapi (bereitgestellt von apilayer Data Products GmbH, Elisabethstraße 15/5, 1010 Wien, Österreich) und Geoapify (zur Verfügung gestellt von Keptago Ltd., N. Nikolaidi und T. Kolokotroni ONISIFOROU CENTER 8011 Paphos, Zypern), um den

Standort von Patientenbenutzern zu identifizieren. Wir verwenden sie, um unsere Anwendungen zu sichern und den Standort des Patientenbenutzers zu überprüfen, um sicherzustellen, dass die Nutzung unserer Dienste konform ist. Wir kombinieren die von uns gesammelten Informationen nicht mit anderen Informationen über den Benutzer, die ihn identifizieren könnten. Zu den von apilayer verarbeiteten Daten gehören die IP-Adresse des Patienten und weitere Angaben zum Standort. Rechtsgrundlage für ihre Nutzung ist Art. 6 Abs. 1 lit. f DSGVO. Die Daten werden gelöscht, wenn der mit ihr verbundene Zweck, für den sie erhoben wurden, nicht mehr besteht und keine gesetzliche Aufbewahrungspflicht mehr besteht. Weitere Informationen zu deren Datenschutzrichtlinien finden Sie unter <https://ipapi.com/privacy/> und [Datenschutzerklärung](#) | [Geoapify Standortplattform](#).

## VERARBEITUNG VON (BEHANDLUNGS-)DATEN

**Gilt für App-Nutzer, die die App mit ihrem Leistungserbringer nutzen**

Während der Nutzung der **myoncare-App** gibt Ihr **Leistungserbringer** Ihre persönlichen Daten in das **myoncare-Portal** ein, um **myoncare-Dienste** zu starten (z. B. Sie als Patient anlegen, Bereitstellung eines individuellen Behandlungsplans, Erinnerung zur Medikamenteneinnahme usw.). Zusätzlich können Sie und Ihr **Leistungserbringer** Dokumente und Dateien in die **myoncare-App** und das **myoncare-Portal** hochladen und miteinander teilen. Ihr **Leistungserbringer** kann eine Datenschutzrichtlinie zu Ihrer Information hochladen und weitere Zustimmungserfordernisse für Sie als Patient festlegen, für die Ihre Zustimmung erforderlich ist. Die Dateien werden in einer Cloud-Datenbank in Deutschland gespeichert. Ihr **Leistungserbringer** kann die Freigabe solcher Dateien mit anderen Portalnutzern innerhalb seiner Einrichtung oder anderen **Leistungserbringern** außerhalb seiner Einrichtung (Konsiliarärzte) für medizinische Zwecke ermöglichen. Andere Portalbenutzer haben ohne diese Freigabe keinen Zugriff auf diese Dateien. Ferner kann Ihr **Leistungserbringer** uns beauftragen, Sie telefonisch beim Ausfüllen von Fragebögen zu unterstützen

(Outbound Calls). Dies erfolgt nur nach Anweisung Ihres **Leistungserbringers** und wird ausschließlich von autorisierten ONCARE Mitarbeitern durchgeführt.

Wir verwenden und verarbeiten Ihre Gesundheitsdaten nur für die betrieblichen Aktivitäten, die nach HIPAA und anderen Bundesgesetzen zulässig sind.

Wir verarbeiten solche personenbezogenen Daten, einschließlich Ihrer Gesundheitsdaten, im Rahmen einer Vereinbarung mit und gemäß den Anweisungen Ihres **Leistungserbringers**. Für die Verarbeitungszwecke ist der **Leistungserbringer** im Sinne der geltenden Datenschutzgesetze als Datenverantwortlicher für die Verarbeitung Ihrer persönlichen Daten und Gesundheitsdaten verantwortlich, und ONCARE ist der Datenverarbeiter dieser personenbezogenen (Gesundheits-) Daten. Das bedeutet, dass ONCARE personenbezogene Daten nur gemäß den Anweisungen des **Leistungserbringers** verarbeitet. Wenn Sie Fragen oder Bedenken bezüglich der Verarbeitung Ihrer personenbezogenen Daten oder Gesundheitsdaten haben, sollten Sie sich in erster Linie an Ihren Gesundheitsdienstleister wenden.

## VERARBEITUNG VON AKTIVITÄTSDATEN

***Nur zutreffend, wenn Sie dem Aktivitätsdatentransfer über myoncare Tools zustimmen und diesen aktivieren***

Die **myoncare-Tools** bieten Ihnen die Möglichkeit, die **myoncare-App** mit bestimmten Gesundheits-Apps (z. B. AppleHealth, GoogleFit, Withings), die Sie verwenden („**Gesundheits-App**“), zu verbinden. Wenn die Verbindung nach Ihrer Einwilligung hergestellt wird, werden die von der Gesundheitsanwendung gesammelten Aktivitätsdaten Ihren **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen. Um die Verarbeitung von Aktivitätsdaten zu ermöglichen, holen wir vorab Ihre Einwilligung in die Verarbeitung ein. Bitte beachten Sie, dass Aktivitätsdaten nicht von den **myoncare-Tools** validiert werden und von Ihrem **Leistungserbringer** nicht für diagnostische Zwecke oder als Grundlage für medizinische Entscheidungen verwendet werden sollten. Bitte beachten Sie auch, dass Ihre **Leistungserbringer** nicht verpflichtet sind, Ihre

Aktivitätsdaten zu überprüfen und Ihnen kein Feedback zu Ihren Aktivitätsdaten geben müssen.

Aktivitätsdaten werden jedes Mal, wenn die **myoncare-App** aufgerufen wird, mit Ihren angeschlossenen **Leistungserbringern** geteilt. Sie können Ihre Einwilligung zur Weitergabe von Aktivitätsdaten jederzeit in den Einstellungen der **myoncare App** widerrufen. Bitte beachten Sie, dass Ihre Aktivitätsdaten ab diesem Zeitpunkt nicht mehr weitergegeben werden. Aktivitätsdaten, die bereits geteilt wurden, werden nicht aus dem **myoncare-Portal** Ihrer angeschlossenen **Leistungserbringer** gelöscht.

Die Verarbeitung von Aktivitätsdaten liegt in Ihrer eigenen Datenverantwortung.

**Arten von Daten:** Die Art und Menge der übertragenen Daten hängen von Ihrer Entscheidung und den in Ihrer verbundenen Health-App verfügbaren Daten ab. Zu den Daten gehören unter anderem Gewicht, Größe, zurückgelegte Schritte, verbrannte Kalorien, Schlafstunden, Herzfrequenz und Blutdruck.

**Zweck der Verarbeitung von Aktivitätsdaten:** Ihre Aktivitätsdaten werden Ihren verbundenen **Leistungserbringern** zur Verfügung gestellt, um zusätzliche kontextuelle Informationen zu Ihrer Aktivität bereitzustellen.

**Rechtfertigung der Verarbeitung:** Die Verarbeitung von Tätigkeitsdaten unterliegt Ihrer eigenen Verantwortung.

## VERARBEITUNG VON PRODUKTSICHERHEITSDATEN

***Anwendbar für App-Nutzer, deren Leistungserbringer die Medizinproduktvariante der myoncare Tools verwendet***

Die **myoncare-App** ist gemäß den europäischen Medizinprodukteverordnungen als Medizinprodukt klassifiziert und wird vermarktet. Als Hersteller der App müssen wir bestimmte gesetzliche Verpflichtungen einhalten (z.B. Überwachung der Funktionalität der App, Auswertung von Vorfalleinsendungen, die mit der Nutzung der App in Verbindung stehen könnten, Tracking von Nutzern etc.). Zusätzlich ermöglicht die **myoncare-App** Ihnen und Ihrem **Leistungserbringer**, zu kommunizieren und persönliche Daten über bestimmte medizinische

Geräte oder Medikamente, die in Ihrer Behandlung verwendet werden, zu erfassen. Die Hersteller solcher Medizinprodukte oder Arzneimittel haben auch gesetzliche Verpflichtungen hinsichtlich der Marktüberwachung (z.B. Sammlung und Bewertung von Nebenwirkungsmeldungen).

**Arten von Daten:** Fallberichte, in einem Vorfalbericht bereitgestellte personenbezogene Daten und Ergebnisse der Auswertung.

**Verarbeitung von Produktsicherheitsdaten:** Wir speichern und bewerten alle personenbezogenen Daten im Zusammenhang mit unseren gesetzlichen Verpflichtungen als Hersteller eines Medizinprodukts und übermitteln solche personenbezogenen Daten (wenn möglich nach Pseudonymisierung) an zuständige Behörden, benannte Stellen oder andere Datenverantwortliche mit Überwachungspflichten. Zusätzlich speichern und übertragen wir personenbezogene Daten im Zusammenhang mit medizinischen Geräten und/oder Medikamenten, wenn wir Mitteilungen von Ihrem **Leistungserbringer**, von Ihnen als Patient oder von Dritten (z. B. unseren Vertriebspartnern oder Importeuren der **myoncare-Tools** in Ihrem Land) erhalten, die dem Hersteller des Produkts gemeldet werden müssen, damit dieser seinen gesetzlichen Verpflichtungen zur Produktsicherheit nachkommen kann.

## DSGVO-Regeln

ONCARE ist der Datenverantwortliche für die Verarbeitung von Produktsicherheitsdaten.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten zur Erfüllung rechtlicher Verpflichtungen als Hersteller von Medizinprodukten oder Arzneimitteln ist Art. 9 Abs. 2 lit. i DSGVO in Verbindung mit den nach dem Inverkehrbringen bestehenden Überwachungspflichten nach dem Medizinproduktegesetz und der Medizinprodukte-Richtlinie (ab 26. Mai 2021 geregelt in Kapitel VII der neuen Medizinprodukteverordnung (EU) 2017/745) und/oder dem Arzneimittelgesetz.

## VERARBEITUNG VON DATEN DES BETRIEBLICHEN GESUNDHEITSMANAGEMENTS

### **Anwendbar für Nutzer der App, die die App mit dem betrieblichen Gesundheitsmanagement des Unternehmens nutzen**

Während der Nutzung der **myoncare-App** im betrieblichen Gesundheitsmanagement der **Firma** werden bestimmte persönliche (Gesundheits-)Daten in aggregierter Form als Daten für das betriebliche Gesundheitsmanagement an die Firma und die von der Firma beauftragten Datendienstleister (z. B. Datenanalysten oder Forschungsunternehmen) weitergegeben. Weder die **Firma** noch ein **Datendienstleister** können solche Daten Ihrer Identität zuordnen. ONCARE empfiehlt, während der Nutzung der **myoncare-Dienste** im Rahmen des betrieblichen Gesundheitsmanagements keine persönlichen Daten zu teilen.

Das bedeutet, dass ONCARE und alle **Datendienstleister** die Daten für das betriebliche Gesundheitsmanagement nur gemäß den Anweisungen der **Firma** verarbeiten werden. Wir verarbeiten solche Daten für das betriebliche Gesundheitsmanagement, einschließlich Ihrer Gesundheitsdaten, auf der Grundlage einer Vereinbarung mit der **Firma** und/oder einem **Datendienstleister** und gemäß deren Anweisungen. Für die Zwecke dieser Vereinbarung ist die Firma der Datenverantwortliche für die Verarbeitung Ihrer Daten zum betrieblichen Gesundheitsmanagement, und ONCARE sowie alle von Ihrer **Firma** beauftragten **Datendienstleister** sind die Datenverarbeiter dieser Daten. Wenn Sie Fragen oder Bedenken zur Verarbeitung Ihrer Daten für das betriebliche Gesundheitsmanagement haben, sollten Sie sich zunächst an das Unternehmen wenden.

**Datenverarbeitung:** Wir verarbeiten Ihre Daten zum betrieblichen Gesundheitsmanagement, um unsere **myoncare-Dienste** für die **Firma** und für Sie bereitzustellen. Ihre Daten zum betrieblichen Gesundheitsmanagement, die Sie in unsere **myoncare-App** eingeben, werden von der **Firma** (entweder direkt oder über einen **Datendienstleister**) im Rahmen des betrieblichen Gesundheitsmanagements verwendet. Wir verarbeiten diese personenbezogenen Daten im Rahmen einer Vereinbarung mit und gemäß den Anweisungen Ihres **Leistungserbringers**. Die Übertragung dieser Behandlungsdaten erfolgt pseudonymisiert und verschlüsselt. Zur Ausübung Ihrer

Betroffenenrechte wenden Sie sich bitte an Ihren **Leistungserbringer**.

### DSGVO-Regeln

Ihre Daten für das betriebliche Gesundheitsmanagement werden von der **Firma** gemäß den Bestimmungen der **DSGVO** und allen anderen geltenden Datenschutzvorschriften verarbeitet. Rechtsgrundlage für die Datenverarbeitung ist insbesondere Ihre Einwilligung gemäß Art. 6 Abs. 1 lit. a und Art. 9 Abs. 2 lit. **DSGVO** oder ein andere für die **Firma** geltende Normen. Die Verarbeitung von Daten durch ONCARE für die **Firma** (entweder direkt oder über einen von der **Firma** beauftragten **Dienstleister**) basiert ebenfalls auf Art. 28 **DSGVO** (Vereinbarung zur Auftragsverarbeitung).

Das **Firma** ist als Datenbeauftragter dafür verantwortlich, Ihre Einwilligung einzuholen, wenn dies nach den datenschutzrechtlichen Vorschriften erforderlich ist, und die Daten für Zwecke des betrieblichen Gesundheitsmanagements gemäß den geltenden Datenschutzgesetzen zu verarbeiten.

### WELCHE TECHNOLOGIE WIRD VOM MYONCARE PORTAL UND DER MYONCARE APP VERWENDET?

Das **myoncare-Portal** funktioniert als webbasiertes Tool, für das Sie eine funktionierende Internetverbindung und eine aktuelle Version des Internetbrowsers Chrome, Firefox oder Safari benötigen.

### E-Mail-Dienst

Wir verwenden Brevo (bereitgestellt von der Sendinblue GmbH, mit Sitz in der Köpenicker Straße 126, 10179 Berlin) und Sendgrid (bereitgestellt von Twilio Inc., 1801 California Street Suite 500, Denver, CO 80202, USA). Diese E-Mail-Dienste können verwendet werden, um den Versand von E-Mails zu organisieren. Sendgrid wird verwendet, um Bestätigungs-E-Mails, Transaktionsbestätigungen und E-Mails mit wichtigen Informationen zu Anfragen zu senden. Die von Ihnen zum Zwecke des Empfangs von E-Mails eingegebenen Daten werden auf den Servern von Sendgrid gespeichert. Wenn wir in Ihrem Namen E-Mails über SendGrid versenden, verwenden wir eine SSL-gesicherte Verbindung.

Die E-Mail-Kommunikation wird für die folgenden Aufgaben verwendet:

- Erstmaliges Einloggen in die Webanwendung;
- Workflow zum Zurücksetzen des Passworts für die Webanwendung;
- Erstellen Sie ein Konto für die Patientenanwendung;
- Zurücksetzen des Passworts für die Patientenanwendung;
- Erstellung und Versand eines Berichts;
- Ersetzen Sie Push-Benachrichtigungen durch E-Mails für PWA (Progressive Webapp) in den folgenden Fällen:
  - (i) Wenn ein Careplan innerhalb eines Tages endet;
  - (ii) wenn Medikamente zugewiesen wurden;
  - (ii) wenn die Datenschutzrichtlinie aktualisiert wurde;
  - (iv) wenn ein Termin an Patienten und Ärzte gesendet wird, insbesondere für die Terminart "Videoanruf";
  - (v) Alle Informationen, die sich auf eine **Caretask** beziehen oder wenn ein **Leistungserbringer** eine Caretask zugewiesen hat.

### Brevo (Datenschutzerklärung):

Datenschutzerklärung - Schutz personenbezogener Daten | Brevo

**SendGrid** (Privacy Policy):  
<https://sendgrid.com/resource/general-data-protection-regulation-2/>.

### Matomo

Dabei handelt es sich um ein Open-Source-Web-Analyse-Tool. Matomo (bereitgestellt von InnoCraft Ltd., Neuseeland) überträgt keine Daten an Server, die außerhalb der Kontrolle von ONCARE liegen. Matomo ist zunächst deaktiviert, wenn Sie unsere Dienste nutzen. Nur wenn Sie damit einverstanden sind, wird Ihr Nutzerverhalten anonymisiert erfasst. Bei Deaktivierung wird ein "persistentes Cookie" gespeichert, sofern Ihre Browsereinstellungen dies zulassen. Dieses Cookie signalisiert Matomo, dass Sie nicht möchten, dass Ihr Browser aufgezeichnet wird.

Die durch den Cookie gesammelten Nutzungsinformationen werden an unsere Server übertragen und dort gespeichert, damit wir das Nutzerverhalten analysieren können.

Die vom Cookie erzeugten Informationen über Ihre Nutzung sind:

- Benutzerrolle;

- Geolokalisierung des Benutzers;
- Browser;
- Benutzer-Betriebssystem;
- IP-Adresse;
- Websites, die über das Web / PWA besucht werden (weitere Informationen finden Sie im Abschnitt über PWA in dieser Datenschutzrichtlinie);
- Schaltflächen, die der Benutzer im **myoncare-Portal**, in der **myoncare-App** und in der **myoncare-PWA** anklickt;
- Zeit, in der der Nutzer Inhalte verwendet hat.

Die durch den Cookie erzeugten Informationen werden nicht an Dritte weitergegeben.

Sie können die Verwendung von Cookies ablehnen, indem Sie die entsprechenden Einstellungen in Ihrem Browser vornehmen. Bitte beachten Sie jedoch, dass Sie in diesem Fall möglicherweise nicht alle Funktionen nutzen können. Weitere Informationen finden Sie unter: <https://matomo.org/privacy-policy/>.

Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Nutzer ist Art. 6 Abs. 1 Satz 1 lit. a DSGVO. Die Verarbeitung personenbezogener Daten der Nutzer ermöglicht es uns, das Nutzungsverhalten zu analysieren. Durch die Auswertung der gewonnenen Daten sind wir in der Lage, Informationen über die Nutzung der einzelnen Komponenten unserer Dienste zusammenzustellen. Dies hilft uns, unsere Dienste und deren Usability kontinuierlich zu verbessern.

Wir verarbeiten und speichern personenbezogene Daten nur so lange, wie es zur Erfüllung des beabsichtigten Zwecks erforderlich ist.

## SICHERE ÜBERTRAGUNG PERSONENBEZOGENER DATEN

Wir setzen angemessene technische und organisatorische Sicherheitsmaßnahmen ein, um Ihre bei uns gespeicherten personenbezogenen Daten optimal gegen zufällige oder vorsätzliche Manipulationen, Verlust, Zerstörung oder gegen den Zugriff unberechtigter Personen zu schützen. Die Sicherheitsstufen werden in Zusammenarbeit mit Sicherheitsexperten kontinuierlich überprüft und an neue Sicherheitsstandards angepasst.

Der Datenaustausch zur und von der App erfolgt verschlüsselt. Wir verwenden TLS und SSL als Verschlüsselungsprotokolle für eine sichere Datenübertragung. Auch der Datenaustausch ist durchgehend verschlüsselt und erfolgt mit Pseudoschlüsseln.

## DATENÜBERTRAGUNGEN / OFFENLEGUNG AN DRITTE

Eine Weitergabe Ihrer personenbezogenen Daten an Dritte erfolgt nur im Rahmen der gesetzlichen Bestimmungen oder auf Grundlage Ihrer Einwilligung. In allen anderen Fällen werden die Informationen nicht an Dritte weitergegeben, es sei denn, wir sind aufgrund zwingender gesetzlicher Vorschriften dazu verpflichtet (Weitergabe an externe Stellen, einschließlich Aufsichts- oder Strafverfolgungsbehörden). Jede Übertragung personenbezogener Daten wird während der Übertragung verschlüsselt.

Wir geben Informationen und Daten über Sie nur weiter, wenn Gesetze einzelner Bundesstaaten oder U.S. Bundesgesetze dies verlangen; dies schließt Anfragen des Department of Health and Human Services mit ein, wenn die Behörde die Einhaltung von U.S. Bundesgesetzen überprüfen möchte. Wir dürfen Ihre Gesundheitsdaten auch verarbeiten und weiterleiten, und zwar um:

- Einhaltung von Bundes-, Landes- oder lokalen Gesetzen;
- Unterstützung von Aktivitäten im Bereich der öffentlichen Gesundheit, wie z. B. bei Krankheiten oder der Verwendung medizinischer Geräte;
- den Behörden Informationen zur Verfügung zu stellen, um Opfer von Missbrauch oder Vernachlässigung zu schützen;
- Einhaltung von Gesundheitsaufsichtsaktivitäten auf Bundes- und Landesebene, wie z. B. Betrugsermittlungen;
- Zur Vollstreckung von Strafverfolgungs- oder Gerichtsbeschlüssen, Vorladungen oder anderen damit verbundenen hoheitlichen Maßnahmen;
- Durchführung von Recherchen zu internen Überprüfungsprotokollen, um ein Gleichgewicht zwischen Datenschutz und Forschungsbedürfnissen zu gewährleisten;
- Abwendung einer ernsthaften Gefahr für Gesundheit oder Sicherheit.



## ALLGEMEINE INFORMATIONEN ZUR EINWILLIGUNG IN DIE DATENVERARBEITUNG

Ihre Einwilligung stellt auch eine Einwilligung in die datenschutzrechtliche Datenverarbeitung dar. Bevor wir Ihre Einwilligung erteilen, informieren wir Sie über den Zweck der Datenverarbeitung und Ihr Widerspruchsrecht. Wenn sich die Einwilligung auch auf die Verarbeitung besonderer Kategorien personenbezogener Daten bezieht, wird die **myoncare-App** Sie im Rahmen des Einwilligungsverfahrens ausdrücklich darüber informieren.

Für die Datenverarbeitung, für die Ihre Einwilligung erforderlich ist (wie in dieser **Datenschutzerklärung** erläutert), wird die Einwilligung im Rahmen des Registrierungsprozesses eingeholt. Nach erfolgreicher Registrierung können die Einwilligungen in den Kontoeinstellungen der **myoncare-App** verwaltet werden.

### DSGVO-Regeln

Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO darf nur erfolgen, wenn dies aufgrund gesetzlicher Vorschriften erforderlich ist und kein Grund zur Annahme besteht, dass Ihre berechtigten Interessen die Verarbeitung dieser personenbezogenen Daten ausschließen oder Sie Ihre Einwilligung zur Verarbeitung dieser personenbezogenen Daten gemäß Art. 9 Abs. 2 DSGVO gegeben haben.

### DATENEMPFÄNGER / KATEGORIEN VON EMPFÄNGERN

In unserer Organisation stellen wir sicher, dass nur diejenigen Personen berechtigt sind, personenbezogene Daten zu verarbeiten, die zur Erfüllung ihrer vertraglichen und gesetzlichen Pflichten erforderlich sind. Ihre persönlichen Daten und Gesundheitsdaten, die Sie in unsere **myoncare-App** eingeben, werden entweder direkt oder über einen **Datendienstleister** Ihrem **Leistungserbringer** und/oder Ihrer **Firma** zur Verfügung gestellt (abhängig von der Art der Nutzung der **myoncare-Tools**).

In bestimmten Fällen unterstützen Dienstleister unsere Fachabteilungen bei der Erfüllung ihrer Aufgaben. Mit allen Dienstleistern, die Auftragsverarbeiter für die

personenbezogenen Daten sind, wurden die erforderlichen Datenschutzvereinbarungen abgeschlossen. Diese Dienstleister sind Google (Google Firebase), Anbieter von Cloud-Speichern und Support-Dienstleistern.

Google Firebase ist eine „NoSQL-Datenbank“, die die Synchronisation zwischen dem **myoncare-Portal** Ihres **Leistungserbringers** und der **myoncare-App** ermöglicht. NoSQL definiert einen Mechanismus zum Speichern von Daten, der nicht nur in tabellarischen Beziehungen modelliert wird, indem es eine einfachere "horizontale" Skalierung im Vergleich zu tabellarischen/relationalen Datenbankmanagementsystemen in einem Cluster von Maschinen ermöglicht.

Zu diesem Zweck wird ein Pseudokey der **myoncare-App** zusammen mit dem entsprechenden Behandlungsplan in Google Firebase gespeichert. Die Datenübertragung erfolgt für ONCARE und seine Dienstleister pseudonymisiert, was bedeutet, dass ONCARE und seine Dienstleister keine Beziehung zu Ihnen als betroffene Person aufbauen können. Dies wird erreicht, indem die Daten während der Übertragung zwischen Ihnen und Ihrem **Leistungserbringer** oder **Unternehmen** (entweder direkt oder an einen **Datendienstleister**) verschlüsselt und Pseudokeys anstelle persönlicher Kennungen wie Name oder E-Mail-Adresse zur Nachverfolgung dieser Übertragungen verwendet werden. Die Re-Identifizierung erfolgt, sobald die personenbezogenen Daten das Konto Ihres **Leistungserbringers** oder **Unternehmens** im **myoncare-Portal** oder Ihr Konto in der **myoncare-App** erreicht haben, nachdem sie durch spezifische Tokens verifiziert wurden.

Unsere Cloud-Speicheranbieter bieten eine Reihe von Cloud-Speicherdiensten an, in denen der Firebase-Manager, der die Firebase-URLs für das **myoncare-Portal** verwaltet, gespeichert wird. Darüber hinaus stellen diese Dienstanbieter die isolierte Serverdomäne des **myoncare-Portals** bereit, in der Ihre persönlichen Daten gespeichert werden. Es hostet auch die Video- und Dateiverwaltungsdienste von myoncare, die verschlüsselte Videokonferenzen zwischen Ihnen und Ihrem **Leistungserbringer** sowie den Austausch von Dateien ermöglichen. Der Zugriff auf Ihre persönlichen Daten durch Sie und Ihren **Leistungserbringer** wird durch das Senden spezifischer Tokens gewährleistet. Diese

personenbezogenen Daten werden während der Übertragung und im Ruhezustand verschlüsselt und für ONCARE und seine Dienstleister pseudonymisiert. Die Leistungserbringer von ONCARE haben zu keinem Zeitpunkt Zugriff auf diese personenbezogenen Daten.

Des Weiteren setzen wir Dienstleister ein, um Serviceanfragen (Support-Dienstleister) bezüglich der Nutzung des Accounts zu bearbeiten, z.B. wenn Sie Ihr Passwort vergessen haben, Ihre gespeicherte E-Mail-Adresse ändern möchten etc. Mit diesen Dienstleistern wurden die erforderlichen Auftragsverarbeitungsverträge abgeschlossen; darüber hinaus wurden die mit der Bearbeitung von Serviceanfragen betrauten Mitarbeiter entsprechend geschult. Nach Erhalt Ihrer Serviceanfrage wird ihr eine Ticketnummer zugewiesen.

Handelt es sich um eine Serviceanfrage bezüglich Ihrer Account-Nutzung, werden die relevanten Informationen, die Sie uns bei der Kontaktaufnahme zur Verfügung gestellt haben, an einen der autorisierten Mitarbeiter des externen Dienstes weitergeleitet. Er wird sich dann mit Ihnen in Verbindung setzen.

Andernfalls bleiben sie weiterhin von speziell zugelassenen ONCARE-Mitarbeitern verarbeitet, wie unter "VERARBEITUNG VON OPERATIVEN DATEN" beschrieben.

Über unsere Support-Dienstleister verwenden wir das Tool RepairCode, auch bekannt als Digital Twin Code, eine Customer-Experience-Plattform für den Umgang mit externem Feedback mit der Möglichkeit, Support-Tickets zu erstellen. Hier finden Sie die Datenschutzrichtlinie:

<https://app.repaircode.de/?main=main-client> – [Rechtliches/privacy](#).

Schlussendlich zeigen wir Ihnen Inhalte von Instagram (Anbieter: Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland) ein (z. B. Bilder, Videos oder Beiträge). Wenn Sie auf einen verlinkten Instagrambeitrag klicken, werden Sie auf Instagram weitergeleitet. Dabei können von Instagram Cookies gesetzt und Nutzerdaten verarbeitet werden.

Wenn Sie eine Seite mit verlinkten Instagram-Beitrag aufrufen, kann Ihr Browser automatisch eine Verbindung zu den Servern von Instagram herstellen. Instagram erhält dadurch die Information, dass Sie unsere Website

besucht haben, selbst wenn Sie kein Instagram-Konto besitzen oder nicht eingeloggt sind. Falls Sie eingeloggt sind, kann Instagram den Besuch Ihrem Benutzerkonto zuordnen.

Datenschutzerklärung:

<https://privacycenter.instagram.com/policy>

## ÜBERMITTLUNG PERSONENBEZOGENER DATEN IN DRITTLÄNDER

Zur Erbringung unserer Dienste können wir Dienstleister in Anspruch nehmen, die außerhalb der Europäischen Union ansässig sind. Wenn die Daten in ein Drittland übertragen werden, in welchem der Schutz für personenbezogene Daten als nicht angemessen beurteilt wurde, stellen wir sicher, dass angemessene Maßnahmen in Übereinstimmung mit nationalem und europäischem Recht getroffen werden und das – falls erforderlich – entsprechende Standardvertragsklauseln zwischen den verarbeitenden Parteien vereinbart wurden.

Eine Übermittlung personenbezogener Daten in Drittländer erfolgt nur, wenn dies zur Erfüllung der vertraglichen Verpflichtung erforderlich ist, gesetzlich vorgeschrieben ist oder Sie uns Ihre Einwilligung erteilt haben.

Die Synchronisierung der **myoncare-App** und des **myoncare-Portals** erfolgt über Google Firebase. Der Google Firebase-Server wird in der Europäischen Union gehostet. Wie in den Nutzungsbedingungen von Google Firebase beschrieben, sind jedoch kurzfristige Datenübermittlungen in Länder möglich, in denen Google oder seine Dienstleister ansässig sind; Bei bestimmten Google Firebase-Diensten erfolgt eine Datenübermittlung nur in die USA, es sei denn, die Verarbeitung findet in der Europäischen Union oder im Europäischen Wirtschaftsraum statt. Unrechtmäßiger Zugriff auf Ihre Daten wird durch Ende-zu-Ende-Verschlüsselung und sichere Zugriffstoken verhindert. Unsere Server werden in Deutschland gehostet. Zu Analysezwecken enthalten die mit SendGrid versendeten E-Mails ein sogenanntes "Zählpixel", das sich beim Öffnen der E-Mail mit den Servern von Sendgrid verbindet. Damit kann festgestellt werden, ob eine E-Mail-Nachricht geöffnet wurde.

Wir binden Inhalte von Instagram ein, die von der Meta Platforms Ireland Ltd. bereitgestellt werden. Wenn Sie einen verlinkten Instagram-Beitrag anklicken, kann es sein, dass personenbezogene Daten (z. B. IP-Adresse, Browser-Informationen, Interaktionen) an Meta Platforms Inc. in die USA oder andere Drittländer übermittelt werden.

Meta ist unter dem EU-U.S. Data Privacy Framework (DPF) zertifiziert, wodurch für die Übermittlung in die USA ein angemessenes Datenschutzniveau anerkannt ist. Dennoch können auch Daten in Länder übertragen werden, für die kein Angemessenheitsbeschluss der Europäischen Kommission besteht. In solchen Fällen können zusätzliche Schutzmaßnahmen erforderlich sein, deren Wirksamkeit jedoch nicht immer garantiert werden kann.

### DSGVO-Regeln

Die Datenverarbeitung erfolgt auf Grundlage Ihrer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO). Diese Einwilligung können Sie jederzeit widerrufen. Die Rechtmäßigkeit der bereits erfolgten Datenverarbeitungsvorgänge bleibt vom Widerruf unberührt.

Bitte beachten Sie, dass Ihre Daten in der Regel von uns an einen Server von SendGrid in den USA übermittelt und dort gespeichert werden. Wir haben mit Sendgrid einen Vertrag abgeschlossen, der die EU-Standardvertragsklauseln enthält. Dadurch wird sichergestellt, dass ein Schutzniveau besteht, das mit dem der EU vergleichbar ist.

Zur Verarbeitung von Aktivitätsdaten werden auf dem mobilen Gerät des **App-Nutzers** Schnittstellen zu Google Cloud-Diensten (im Fall von GoogleFit) oder zu AppleHealth oder Withings verwendet. Die **myoncare-Tools** nutzen diese Schnittstellen, die von Google, Apple und Withings bereitgestellt werden, um Aktivitätsdaten von den verbundenen Gesundheits-Apps anzufordern. Die von den **myoncare-Tools** gesendete Anfrage enthält keine personenbezogenen Daten. Personenbezogene Daten werden den **myoncare-Tools** über diese Schnittstellen zur Verfügung gestellt.

### DAUER DER SPEICHERUNG PERSONENBEZOGENER DATEN GEMÄSS DER DSGVO

Wir bewahren Ihre personenbezogenen Daten so lange auf, wie sie für den Zweck, für den sie verarbeitet

werden, erforderlich sind. Bitte beachten Sie, dass zahlreiche Aufbewahrungsfristen die weitere Speicherung personenbezogener Daten erfordern. Dies gilt insbesondere für handels- oder steuerrechtliche Aufbewahrungspflichten (z.B. Handelsgesetzbuch, Steuergesetz, etc.). Darüber hinaus muss Ihr **Leistungserbringer** auch die Aufbewahrung Ihrer medizinischen Unterlagen sicherstellen (je nach Art der Dokumente zwischen 1 und 30 Jahren).

Darüber hinaus, und nur wenn Ihr **Leistungserbringer** die Medizinproduktvariante der **myoncare-Tools** verwendet, gelten bestimmte Aufbewahrungsfristen, die sich aus dem Medizinproduktegesetz ergeben, aufgrund der Einstufung der **myoncare-App** als Medizinprodukt. Bitte beachten Sie, dass ONCARE ebenfalls Aufbewahrungspflichten unterliegt, die vertraglich mit Ihrem **Leistungserbringer** auf der Grundlage der gesetzlichen Bestimmungen vereinbart sind. Sofern keine anderweitigen Aufbewahrungspflichten bestehen, werden die personenbezogenen Daten routinemäßig gelöscht, sobald der Zweck erreicht ist.

Darüber hinaus können wir personenbezogene Daten aufbewahren, wenn Sie uns Ihre Einwilligung dazu erteilt haben oder wenn es zu einem Rechtsstreit kommt und wir innerhalb der gesetzlichen Verjährungsfristen, die bis zu 30 Jahre betragen können, Beweismittel verwenden; Die regelmäßige Verjährungsfrist beträgt drei Jahre.

### ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Für die Begründung, Durchführung und Beendigung des Vertragsverhältnisses und die Erfüllung der damit verbundenen vertraglichen und gesetzlichen Pflichten sind verschiedene personenbezogene Daten erforderlich. Das Gleiche gilt für die Nutzung unserer **myoncare-App** und die verschiedenen Funktionen, die sie bietet.

Die Details haben wir für Sie unter dem obigen Punkt zusammengefasst. In bestimmten Fällen müssen personenbezogene Daten auch gemäß den gesetzlichen Bestimmungen erhoben oder zur Verfügung gestellt werden. Bitte beachten Sie, dass es ohne die Bereitstellung dieser personenbezogenen Daten nicht möglich ist, Ihre Anfrage zu bearbeiten oder die zugrundeliegende vertragliche Verpflichtung zu erfüllen.

## ZUGRIFFSRECHTE

Damit die **myoncare-App** auf Ihrem Gerät funktioniert, muss der App verschiedene Berechtigungen erteilt werden, um auf bestimmte Funktionen des Geräts zuzugreifen. Für alle Geräte, unabhängig vom verwendeten Betriebssystem, ist es notwendig, der App bestimmte Berechtigungen zu erteilen, die wir als "grundlegende Zugriffsrechte" bezeichnen. Gegebenenfalls werden wir sie in der Reihenfolge des Betriebssystems (Android oder iOS) gemäß den "Rahmenbedingungen" auflisten. Abhängig vom Betriebssystem des Geräts, das Sie verwenden, verfügt es möglicherweise über zusätzliche Funktionen, die zusätzliche Berechtigungen erfordern, damit die App funktioniert.

Die grundlegenden Zugriffsrechte (Android und iOS) sind:

### Abrufen von Wi-Fi-Verbindungen

Erforderlich, um die Funktionalität des Dokumentendownloads in Verbindung mit Wi-Fi-Verbindungen sicherzustellen.

### Netzwerk-Verbindung abrufen

Erforderlich, um die Funktionalität des Dokumentendownloads in Verbindung mit Netzwerkverbindungen sicherzustellen, bei denen es sich nicht um Wi-Fi-Verbindungen handelt.

### Bildschirmsperre deaktivieren (Stand-by-Modus verhindern)

Erforderlich, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne durch eine Bildschirmsperre unterbrochen zu werden.

### Zugang zu allen Netzwerken

Zum Herunterladen von Dokumenten ist der Zugang zu allen Netzwerken erforderlich.

### Deaktivieren des Schlafmodus

Dies ist notwendig, damit die Videos, die zu den bereitgestellten Dokumenten gehören, direkt in der App abgespielt werden können, ohne dass die Wiedergabe durch das Auftreten des Ruhezustands unterbrochen wird.

## Mobile Daten / Zugriff auf mobile Daten

Möchte der Nutzer Dokumente ausschließlich über WLAN herunterladen, kann er im Menü der App die entsprechende Einstellung vornehmen und die Nutzung mobiler Daten deaktivieren. Der Zugriff auf mobile Daten ist erforderlich, um die Funktionalität der Deaktivierung von Dokumentendownloads über mobile Daten sicherzustellen.

### Zugriff auf die Kamera

Sowohl für das Scannen von QR-Codes als auch für Videokonsultationen ist ein Kamerazugang erforderlich.

### Zugriff auf das Mikrofon

Für Videosprechstunden ist ein Mikrofonzugang erforderlich.

### Zugriff auf Dateien und Fotos

Dies ist für den Austausch von Dateien zwischen Ihnen und Ihren verbundenen Portalbenutzern erforderlich.

### Zugriff auf Webbrowser

Dies ist erforderlich, um empfangene Dateien von Benutzern des verbundenen Portals anzuzeigen.

Wir verwenden Push-Benachrichtigungen, bei denen es sich um Nachrichten handelt, die als Service der **myoncare-App** über Dienste wie den Apple Push Notification Service oder den Google Cloud Messaging Service an Ihr mobiles Gerät gesendet werden. Diese Dienste sind Standardfunktionen von Mobilgeräten. Die Datenschutzrichtlinie des Diensteanbieters regelt den Zugriff, die Verwendung und die Offenlegung personenbezogener Daten infolge Ihrer Nutzung dieser Dienste.

## AUTOMATISIERTE ENTSCHEIDUNGEN IM EINZELFALL ENTSPRECHEND DER DSGVO

Wir verwenden keine rein automatisierte Verarbeitung, um Entscheidungen zu treffen.

## IHRE HIPAA-RECHTE

Gemäß **HIPAA** stehen Ihnen folgende Rechte zu:

- Anzeigen und Kopieren bestimmter Teile Ihrer Gesundheitsinformationen. Sie können verlangen, dass Ihnen Ihre Gesundheitsdaten in elektronischer Form zur

Verfügung gestellt werden. Eine Kopie oder Zusammenfassung Ihrer Gesundheitsinformationen wird Ihnen in der Regel innerhalb von 30 Tagen nach Ihrer Anfrage zur Verfügung gestellt. Es kann eine angemessene Bearbeitungsgebühr erhoben werden.

- Sie können verlangen, dass der Inhalt Ihrer Gesundheitsinformationen geändert wird, wenn Sie der Meinung sind, dass die Gesundheitsinformationen falsch oder unvollständig sind. Sie können die Korrektur von Gesundheitsinformationen verlangen, wenn Sie der Meinung sind, dass diese ungenau oder unvollständig sind.

- Aufstellung von zwingenden Offenlegungen Ihrer Gesundheitsinformationen für die zurückliegenden sechs Jahre, mit der Einschränkung in Bezug auf Behandlungen, Honorarvergütungen und Behandlungsmaßnahmen. Es kann eine angemessene Bearbeitungsgebühr erhoben werden.

- Sie können verlangen, dass bestimmte Gesundheitsinformationen, einschließlich Behandlung, Lizenzzahlungen oder andere medizinische Themen, nicht verwendet oder weitergegeben werden dürfen.

- Sie können jederzeit eine Papierkopie der Datenschutzrichtlinie anfordern, auch wenn Sie zugestimmt haben, die Mitteilung nur auf elektronischem Wege zu erhalten.

- Reichen Sie eine Beschwerde bei der zuständigen Behörde ein, wenn Sie der Ansicht sind, dass Ihre Datenschutzrechte verletzt wurden. Sie können eine Beschwerde bei den U.S. Ministerium für Gesundheit und Soziale Dienste einreichen indem Sie einen Brief an 200 Independence Avenue, S.W., Washington, D.C. 20201 senden, telefonisch unter 1-800-368-1019 (gebührenfrei) oder 1-800-537-7697 (TTD) oder besuchen Sie <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>.

Viele U.S. Bundesstaaten haben eigene Gesetze für den Schutz von Patientenrechten erlassen, die bei Patienten von Ärzten und/oder Krankenhäusern und anderen Einrichtungen des Gesundheitswesens Anwendung finden. Einige dieser U.S. Bundesstaaten verlangen, dass die Ärzte ihren Patienten ein Exemplar dieser Patientenrechte zur Verfügung stellen.

## IHRE RECHTE ALS BETROFFENE PERSON NACH DER DSGVO

Wir möchten Sie über Ihre Rechte als betroffene Person informieren. Diese Rechte sind in den Artikeln 15 bis 22 DSGVO festgelegt und umfassen:

**Recht auf Auskunft (Art. 15 DSGVO):** Sie haben das Recht, Auskunft darüber zu verlangen, ob und wie Ihre personenbezogenen Daten verarbeitet werden, einschließlich Informationen über die Verarbeitungszwecke, Empfänger, Speicherdauer und Ihre Rechte auf Berichtigung, Löschung und Widerspruch. Sie haben auch das Recht, eine Kopie aller personenbezogenen Daten zu erhalten, die wir über Sie gespeichert haben.

**Recht auf Löschung / Recht auf Vergessenwerden (Art. 17 DSGVO):** Sie können von uns verlangen, dass Ihre von uns erhobenen und verarbeiteten personenbezogenen Daten unverzüglich gelöscht werden. In diesem Fall werden wir Sie bitten, die **myoncare-App** einschließlich Ihrer UID (Unique Identification Number) von Ihrem Smartphone/Handy zu löschen.

**Recht auf Berichtigung (Art. 16 DSGVO):** Sie können uns auffordern, unrichtige personenbezogene Daten zu aktualisieren oder zu korrigieren oder unvollständige personenbezogene Daten zu vervollständigen.

**Recht auf Datenübertragbarkeit (Art. 20 DSGVO):** Grundsätzlich können Sie von uns verlangen, dass wir Ihnen personenbezogene Daten, die Sie uns zur Verfügung gestellt haben und die auf Grundlage Ihrer Einwilligung oder der Durchführung eines Vertrages mit Ihnen automatisiert verarbeitet werden, in maschinenlesbarer Form zur Verfügung stellen, damit diese zu einem Ersatzdienstleister "portiert" werden können.

**Recht auf Einschränkung der Datenverarbeitung (Art. 18 DSGVO):** Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, wenn die Richtigkeit der Daten bestritten wird, die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden oder ein Widerspruch gegen die Verarbeitung geprüft wird.



**Recht auf Widerspruch gegen die Datenverarbeitung (Art. 21 DSGVO):** Sie haben das Recht, der Verwendung Ihrer personenbezogenen Daten durch uns zu widersprechen und Ihre Einwilligung jederzeit zu widerrufen, wenn wir Ihre personenbezogenen Daten auf der Grundlage Ihrer Einwilligung verarbeiten. Wir werden unsere Dienstleistungen auch dann weiterhin erbringen, wenn sie nicht von einer widerrufenen Einwilligung abhängig sind.

Um diese Rechte auszuüben, wenden Sie sich bitte in erster Linie an Ihren **Leistungserbringer** oder Ihr Unternehmen oder kontaktieren Sie uns unter: [privacy@myoncare.com](mailto:privacy@myoncare.com). Wir verlangen von Ihnen einen ausreichenden Nachweis Ihrer Identität, um sicherzustellen, dass Ihre Rechte geschützt sind und dass Ihre personenbezogenen Daten nur an Sie und nicht an Dritte weitergegeben werden.

Bitte wenden Sie sich auch jederzeit unter [privacy@myoncare.com](mailto:privacy@myoncare.com) an uns, wenn Sie Fragen zur Datenverarbeitung in unserem Unternehmen haben oder Ihre Einwilligung widerrufen möchten. Sie haben auch das Recht, sich an die zuständige Datenschutzaufsichtsbehörde zu wenden.

#### BESCHWERDE EINREICHEN

Wenn Sie der Meinung sind, dass Ihre Privatsphäre von ONCARE verletzt wurde, können Sie eine Beschwerde bei uns und dem U.S. Behörde Secretary of Health and Human Services in Washington, D.C. einreichen. Für Sie entstehen keine Nachteile bei der Einreichung einer Beschwerde. Um eine Beschwerde einzureichen oder weitere Informationen zu erhalten, nutzen Sie bitte die folgenden Kontaktmöglichkeiten:

Telefon: +49 (0) 89 4445 1156

E-Mail: [privacy@myoncare.com](mailto:privacy@myoncare.com)

Adresse: Balanstraße 71a  
81541 München, Deutschland

Betr: Complaint

Um eine Beschwerde bei dem U.S. Ministerium für Gesundheit und Soziale Dienste einzureichen, schreiben Sie an 200 Independence Ave., S.W., Washington, D.C. 20201 oder rufen Sie 1-800-368-1019 an (gebührenfreier

Anruf) oder 1-800-537-7697 (TTD) oder reichen Sie eine Online-Beschwerde ein unter <https://ocrportal.hhs.gov/ocr/smartscreen/main.jsf>

#### DATENSCHUTZBEAUFTRAGTER NACH DSGVO

Unser Datenschutzbeauftragter steht Ihnen bei [privacy@myoncare.com](mailto:privacy@myoncare.com) für alle Fragen zum Datenschutz zur Verfügung.

#### ALTERSBESCHRÄNKUNG DER ANWENDUNG

Ein Mindestalter von 18 Jahren ist erforderlich, um die **myoncare App** zu nutzen. Wenn Sie unter 18 Jahre alt sind, müssen Ihre Eltern oder Erziehungsberechtigten, die für die Nutzung der App erforderliche Zustimmung zum Datenschutz erteilen.

#### ÄNDERUNGEN DER DATENSCHUTZRICHTLINIE

Wir behalten uns ausdrücklich das Recht vor, diese Datenschutzerklärung in Zukunft nach eigenem Ermessen zu ändern. Änderungen oder Ergänzungen können z. B. erforderlich sein, um gesetzlichen Anforderungen zu entsprechen, um technischen und wirtschaftlichen Entwicklungen Rechnung zu tragen oder um den Interessen von **App** oder **Portal-Benutzer** gerecht zu werden.

Änderungen sind jederzeit möglich und werden Ihnen in geeigneter Weise und in einem angemessenen Zeitrahmen mitgeteilt, bevor sie in Kraft treten (z. B. durch Veröffentlichung einer überarbeiteten Datenschutzerklärung beim Login oder durch Vorankündigung wesentlicher Änderungen).

ONCARE GmbH

Postanschrift

Balanstraße 71a  
81541 München, Deutschland

T | +49 (0) 89 4445 1156

E | [privacy@myoncare.com](mailto:privacy@myoncare.com)

Kontaktdaten des Datenschutzbeauftragten  
[privacy@myoncare.com](mailto:privacy@myoncare.com)

*Zuletzt aktualisiert am 20. Februar 2025.*

\* \* \* \*