Datenschutzhinweise KKH-Gesundheitsberatung: 3
myCoach-Software 3
Begriffsbestimmungen 3
1. Allgemeines – Information nach Art. 13 + 14 DSGVO 5
2. Zweck und Rechtsgrundlage der Verarbeitung 6
3. Arten der verarbeiteten Daten 6
3.2. Registrierung und Anmeldung für telemedizinisch Verantwortliche 7
(Login) 7
3.3. Gesundheitsdaten 8
3.4 Videosprechstunde 9
3.4.1 Erfassung von allgemeinen Daten und Informationen 10
3.4.2 Zweck der Datenverarbeitung für myCoach Videosprechstunde 10
3.4.3 Nutzung der Videosprechstunde für Teilnehmende (Patienten) 10
3.4.4 Nutzung der Videosprechstunde für telemedizinisch Verantwortliche 11
3.5 Kontaktmöglichkeit auf der Internetseite 12
3.6 Versandinformationen 12
4. Datenaufbewahrung und -Löschung 13
5. Datenweitergabe 15
6. Sicherheit 16
7. Ihre Rechte 16
8. Kontakt 20
9. Änderungen der Datenschutzerklärung 20
Datenschutzhinweise KKH-Gesundheitsberatung: 22
myCoach-App 22
1. Allgemeines – Information nach Art. 13 + 14 DSGVO 22
2. Rechtsgrundlage der Verarbeitung 24
3. Allgemeines 24
4. Nutzung der App 29
5. Widerruf, Berichtigung, Sperrung & Löschung 31
6. Auskunftsrecht 32
7. Fragen, Anregungen, Beschwerden 32
8. Links 32
9. Änderung der Datenschutzerklärung 32
Datenschutzhinweise KKH-Gesundheitsberatung: 33
myCoach-Löschkonzept 33
1.Pflicht zur Datenlöschung (Grundsatz) 33
2.Löschfristen in Abhängigkeit von eigenen Zwecken und gesetzlichen Vorschriften 33
3.Übergangsfrist zur endgültigen Löschung 34
4.Durchführung der Löschung 34
5. Prozessuales Vorgehen zur Umsetzung der Löschung 34

6. Protokollierung ..... 35
7. Interne Vorgaben ..... 35
8. Verantwortlichkeit ..... 36
9.Gesetzliche Aufbewahrungsfristen ..... 36
10.Aufbewahrungsformen ..... 37
11. Recht auf Löschung durch Betroffenen ..... 38
12. Aufbau eines datenschutzkonformen Löschkonzepts ..... 39
13. Ermittlung des Schutzbedarfs und Zuordnung der Schutzklasse ..... 39
14. Sicherheitsstufen für Datenträger ..... 40
15. Zuordnung von Schutzklassen und Sicherheitsstufen ..... 41
16. Wann müssen Daten vernichtet werden? ..... 41
17. Geltungsbereich ..... 42
Anlage 1 ..... 43
Anlage 2 ..... 44

# Datenschutzhinweise KKH-Gesundheitsberatung: myCoach-Software

**Dokumentinformation**

- ID: DOC-PRIVACY-4
- Version: 1
- gültig ab: 26.04.2024
- gültig bis: /
- Geltungsbereich: Diese Datenschutzerklärung erstreckt sich auf sämtliche Nutzer der Webanwendung myCoach-Software. Des Weiteren findet diese Datenschutzerklärung Anwendung auf sämtliche von myCoach –Software bereitgestellten Konfigurationen, einschließlich, jedoch nicht beschränkt auf die myCoach Videosprechstunde, sowie auf die Nutzer dieser Konfigurationen.

**Autorinformation**

- Name: Artur Schens
- Funktion: Geschäftsführer – OU Operations
- Freigabe durch: Artur Schens

**Historie**

- Version: 1
- Datum: 25.10.204
- Änderung: Erstellung und Überführung in ein gelenktes
- Autor: Artur Schens

- Version: 2
- Datum: 26.04.2024
- Änderung: Angabe von Versandinformationen und
- Lieferanschrift vom Patienten.
- Autor: Artur Schens

## Begriffsbestimmungen

Die Datenschutzerklärung der Qurasoft GmbH für myCoach –Software beruht auf den Begrifflichkeiten, die durch den Europäischen Richtlinien- und Verordnungsgeber beim Erlass der Datenschutz-Grundverordnung (DSGVO) verwendet wurden. Unsere Datenschutzerklärung soll sowohl für die Öffentlichkeit als auch für unsere Kunden und Geschäftspartner einfach lesbar und verständlich sein. Um dies zu gewährleisten, möchten wir vorab die verwendeten Begrifflichkeiten erläutern.

Wir verwenden in dieser Datenschutzerklärung unter anderem die folgenden Begriffe:

### Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere

mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Betroffene Person

Betroffene Person ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten, von dem für die Verarbeitung Verantwortlichen verarbeitet werden.

Verarbeitung

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Verantwortlicher oder für die Verarbeitung Verantwortlicher

Verantwortlicher oder für die Verarbeitung Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden. Im Kontext dieser Datenschutzerklärung ist der für die Verarbeitung Verantwortliche in der Regel die Qurasoft GmbH.

Auftragsverarbeiter

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Dritter

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Einwilligung

Einwilligung ist jede von der betroffenen Person freiwillig für den bestimmten Fall in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Telemedizinisch Verantwortlicher

Der Begriff "telemedizinisch Verantwortlicher" bezieht sich auf eine Person oder eine Institution, die die Verantwortung für die Planung, Umsetzung und Bereitstellung von telemedizinischen Dienstleistungen trägt. Telemedizin bezieht sich auf die Bereitstellung von medizinischen Dienstleistungen, Diagnosen, Beratungen oder Behandlungen über digitale Kommunikations- und Informations-Technologien, wie zum Beispiel Videoanrufe, Telefonate, E-Mail oder andere Online-Plattformen.

Die telemedizinisch Verantwortliche ist eine qualifizierte medizinische Fachkraft, wie ein Arzt, eine Krankenschwester oder ein Gesundheitscoach.

## 1. Allgemeines – Information nach Art. 13 + 14 DSGVO

Die Qurasoft GmbH (nachfolgend Qurasoft oder wir) als Betreiberin und datenschutzrechtlich Verantwortliche der myCoach Plattform für die Webanwendung myCoach –Software („Webapp“) ist der Schutz und die Vertraulichkeit Ihrer Daten von besonderer Bedeutung. In den nachstehenden Hinweisen zum Datenschutz möchten wir Sie darüber informieren, welche Arten von Daten wir zu welchen Zwecken erheben, verarbeiten und nutzen und welche Rechte Ihnen zustehen. Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt, es sind jedoch immer alle Geschlechter gemeint.

Zweckbestimmung von myCoach –Software

Die Telemonitoring-Webanwendung myCoach –Software ist ausschließlich für Ärzte und medizinisches Fachpersonal konzipiert. Ihr Zweck besteht darin, eine hochsichere Plattform bereitzustellen, über die medizinische Fachkräfte in der Lage sind, Gesundheitsdaten und -informationen in Echtzeit zu übertragen, zu analysieren und zu verwalten. Die Anwendung ermöglicht eine kontinuierliche Fernüberwachung von Patienten und deren Gesundheitszuständen, um medizinische Entscheidungsprozesse zu optimieren, Frühwarnsignale zu erkennen und dadurch die Qualität der Gesundheitsversorgung zu erhöhen. myCoach –Software bietet Ärzten die Möglichkeit, Gesundheitsdaten sicher zu speichern, medizinische Bewertungen vorzunehmen und relevante Informationen in Echtzeit, in strukturierter Form oder als Audio- und Videosignal auszutauschen.

Verantwortlicher im Sinne des Datenschutzes und Datenschutzbeauftragter

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten ist

Qurasoft GmbH

Im Metternicher Feld 30c

D-56072 Koblenz am Rhein

Telefon: (+49) 261 – 134 986 0

E-Mail: kontakt@qurasoft.de

Geschäftsführer:

Tobias Hastenteufel, Erwin Junker & Artur Schens

Handelsregister Amtsgericht Koblenz

HRB 24744

USt.-IdNr.: DE301340994

Unseren externen Datenschutzbeauftragten erreichen Sie unter:

TÜV Technische Überwachung Hessen GmbH

E-Mail: datenschutz@qurasoft.de

## 2. Zweck und Rechtsgrundlage der Verarbeitung

Wir verarbeiten Ihre personenbezogenen Daten ausschließlich für folgende Zwecke:

- die Bereitstellung von Remote-Patientenüberwachungsdiensten,
- die Verarbeitung und Übertragung von Gesundheitsdaten an medizinisches Fachpersonal,
- die Kommunikation zwischen Patienten und medizinischem Fachpersonal,
- die Versendung von Hardware und Material
- die Verbesserung und Anpassung unserer Software, sowie
- zur Abrechnung von medizinischen Dienstleistungen (falls zutreffend).

Die Verarbeitung Ihrer personenbezogenen Daten erfolgt auf Grundlage Ihrer freiwillig erteilten Einwilligung gemäß Art. 6 Abs. 1lit. a DSGVO.

Eine von Ihnen erteilte Einwilligung ist jederzeit uns gegenüber widerruflich. Es sei jedoch darauf hingewiesen, dass die Übermittlung von Patientendaten an Ihren jeweiligen telemedizinischen Unterstützer auf der Grundlage erfolgt, dass die betreffenden Patienten ihre ausdrückliche Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für einen oder mehrere der zuvor bestimmten Zwecke erteilen. Weiterführende Informationen bezüglich der Patienten finden sich in der Datenschutzerklärung der myCoach-App.

## 3. Arten der verarbeiteten Daten

Wir erheben und verarbeiten möglicherweise folgende Arten von personenbezogenen Daten in unserer Telemonitoring Softwarelösung myCoach –Software:

### 3.1. Zugriffsdaten

Die Nutzung der myCoach –Software Webplattform der Qurasoft GmbH erfasst mit jedem Aufruf der Internetseite durch eine betroffene Person oder ein automatisiertes System eine Reihe von allgemeinen Daten und Informationen. Diese allgemeinen Daten und Informationen werden in den Logfiles des Servers gespeichert.

Diese Daten dienen ausschließlich zu statistischen Zwecken und werden zur Verbesserung und Sicherheit der Webapp verwendet. Eine Verknüpfung dieser Daten mit anderen Datenquellen wird nicht vorgenommen.

- IP-Adresse des Nutzers, gekürzt auf die letzten beiden Oktette
- Datum und Uhrzeit des Zugriffs
- Browsertyp und -version
- Betriebssystem des Nutzers
- Referrer-URL

• Hostname des zugreifenden Rechners

• Menge der übertragenen Daten

• Statusmeldungen (z.B., ob der Zugriff erfolgreich war)

Bei der Nutzung dieser allgemeinen Daten und Informationen zieht die Qurasoft GmbH keine Rückschlüsse auf die betroffene Person. Diese Informationen werden vielmehr benötigt, um (1) die Inhalte unserer Internetseite korrekt auszuliefern, (2) die dauerhafte Funktionsfähigkeit unserer informationstechnologischen Systeme und (3) der Technik unserer Internetseite zu gewährleisten sowie (4) um Strafverfolgungsbehörden im Falle eines Cyberangriffes die zur Strafverfolgung notwendigen Informationen bereitzustellen. Diese erhobenen Daten und Informationen werden durch die Qurasoft GmbH daher einerseits statistisch und ferner mit dem Ziel ausgewertet, den Datenschutz und die Datensicherheit in unserem Unternehmen zu erhöhen, um letztlich ein optimales Schutzniveau für die von uns verarbeiteten personenbezogenen Daten sicherzustellen. Die Daten der Server-Logfiles werden getrennt von allen durch eine betroffene Person angegebenen personenbezogenen Daten gespeichert.

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. b DSGVO zur Erfüllung vertraglicher Maßnahmen.

## 3.2. Registrierung und Anmeldung für telemedizinisch Verantwortliche (Login)

Um die Webanwendung vollumfänglich nutzen zu können, ist eine Registrierung eines telemedizinisch Verantwortlichen oder einer in Verbindung stehenden Organisation erforderlich. Die Registrierung kann entweder selbständig auf der Webseite https://register.saniq.org durchgeführt werden, oder von Qurasoft vorkonfiguriert erfolgen. Bei der Registrierung werden folgende personenbezogene Daten erfasst:

• Anrede, ggf. Akademischer Titel, Vor- und Nachname

• Anschrift durch Straße, Hausnummer, Postleitzahl und Ort

• E-Mail-Adresse

• Telefonnummer

• Name ihrer Institution

• Betriebsstättennummer

• Passwort

• IP-Adresse

Durch eine Registrierung auf der Internetseite des für die Verarbeitung Verantwortlichen wird ferner die vom Internet-Service-Provider (ISP) der betroffenen Person vergebene IP-Adresse, das Datum sowie die Uhrzeit der Registrierung gespeichert. Die IP-Adresse wird sofort auf die letzten beiden Oktette gekürzt. Die Speicherung dieser Daten erfolgt vor dem Hintergrund, dass nur so der Missbrauch unserer Dienste verhindert werden kann, und diese Daten im Bedarfsfall ermöglichen, begangene Straftaten aufzuklären. Insofern ist die Speicherung dieser Daten zur Absicherung des für die Verarbeitung Verantwortlichen erforderlich. Eine Weitergabe dieser Daten an Dritte erfolgt grundsätzlich nicht, sofern keine gesetzliche Pflicht zur Weitergabe besteht oder die Weitergabe der Strafverfolgung dient. Die Löschung der gekürzten IP-Adresse erfolgt nach 7 Tagen.

Die Registrierung der betroffenen Person unter freiwilliger Angabe personenbezogener Daten dient dem für die Verarbeitung Verantwortlichen dazu, der betroffenen Person Inhalte oder

Leistungen anzubieten, die aufgrund der Natur der Sache nur registrierten Benutzern angeboten werden können. Registrierten Personen steht die Möglichkeit frei, die bei der Registrierung angegebenen personenbezogenen Daten jederzeit abzuändern oder vollständig aus dem Datenbestand des für die Verarbeitung Verantwortlichen zu löschen.

Die Daten werden verwendet, um die Authentifizierung zu ermöglichen und um die Funktionen der Webapp bereitzustellen. Der Login erfolgt auf der Webseite https://login.saniq.org. Diese Daten werden nicht ohne Ihre ausdrückliche Zustimmung an Dritte weitergegeben. Bei der Anmeldung werden folgende Daten verarbeitet:

• E-Mail-Adresse

• Passwort

• Zugangstoken

• IP-Adresse

Der für die Verarbeitung Verantwortliche erteilt jeder betroffenen Person jederzeit auf Anfrage Auskunft darüber, welche personenbezogenen Daten über die betroffene Person gespeichert sind. Ferner berichtigt oder löscht der für die Verarbeitung Verantwortliche personenbezogene Daten auf Wunsch oder Hinweis der betroffenen Person, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Unser Datenschutzbeauftragte (Anschrift siehe oben) steht diesem Zusammenhang als Ansprechpartner zur Verfügung.

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. b,f DSGVO zur Erfüllung vorvertraglicher Maßnahmen und zur Wahrung berechtigter Interessen.

## 3.3. Gesundheitsdaten

Die Webanwendung ermöglicht die Erfassung und Speicherung von Gesundheitsdaten und medizinische Informationen von Versicherten. Der Zugriff auf diese Daten erfolgt ausschließlich durch die KKH. Diese Daten werden vertraulich behandelt und gemäß den geltenden Datenschutzbestimmungen verarbeitet.

Patienteninformationen

• Vorname, Nachname

• Geburtsdatum

• Geschlecht

• E-Mail-Adresse

• Telefonnummer• Größe

• Gewicht

• ICD10-Diagnosen

Behandlungsdaten

• Medikationsplan und getätigte Medikationseinnahmen

• Gesundheitsrelevante Dokumente und Dateien

• Vitalparameter:

  - o Körpertemperatur
  - o Gewicht
  - o Schritte
  - o Sauerstoffsättigung
  - o Tragedauer von Wearables
  - o Peak-Flow-Expiratory-Flow (PEF)
  - o Einsekundenkapaztität (FEV1)
  - o Forcierte Vitalkapazität (FVC)
  - o Atemfrequenz
  - o Fraktioniertes exhaliertes Stickstoffmonoxid (FeNO)
  - o Blutdruck
  - o EKG / Elektrokardiogramm
  - o RR-Intervall (Frequenz)
  - o RR-Intervall (Zeit)
  - o Puls
  - o Glukose

• Beantwortete Fragebögen

• Teilnahme an Studien und Studienparameter

Kommunikationsdaten

• Chatnachrichten. Hierbei wird Ihr Name und der Chatverlauf mit dem Patienten verarbeitet.

• Audio- und Videosignal. Weitere Hinweise finden Sie im nächsten Abschnitt 3.4 Videosprechstunde.

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. a, b und f DSGVO erfolgt auf Grundlage Ihrer freiwillig erteilten Einwilligung, zur Erfüllung von vertraglichen Maßnahmen und zur Wahrung berechtigter Interessen.

## 3.4 Videosprechstunde

myCoach –Software hat in der Plattformkonfiguration „Videosprechstunde“ (myCoach-VSS) die Möglichkeit Audio- und Videosignale zum Zweck einer Videosprechstunde zu

verarbeiten. In dieser Konfiguration werden in der Regel keine Behandlungsdaten (siehe 3.3 Gesundheitsdaten) vom Patienten verarbeitet.

Die von der betroffenen Person eingegebenen personenbezogenen Daten (siehe 3.3 Gesundheitsdaten: Patienteninformationen und Kommunikationsdaten) werden für die Verwaltung und Durchführung der Videosprechstunde und für interne Zwecke erhoben und gespeichert. Der für die Verarbeitung Verantwortliche kann die Weitergabe an einen oder mehrere Auftragsverarbeiter, beispielsweise einen Postdienstleister oder Steuerberater veranlassen, der die personenbezogenen Daten ebenfalls ausschließlich für eine interne Verwendung, die dem für die Verarbeitung Verantwortlichen zuzurechnen ist, nutzt.

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. b, f DSGVO zur Erfüllung vertraglicher Maßnahmen und zur Wahrung berechtigter Interessen.

### 3.4.1 Erfassung von allgemeinen Daten und Informationen

Der telemedizinisch Verantwortliche erfasst in myCoach-VSS personenbezogene Teilnehmerdaten zur Durchführung der Videosprechstunde. Folgende Teilnehmerdaten werden vom telemedizinischen Verantwortlichen erfasst und durch den für Verarbeitung Verantwortlichen verarbeitet:

- Vorname, Nachname
- Geburtsdatum
- Geschlecht
- E-Mail-Adresse
- Telefonnummer

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. a DSGVO auf Grundlage der freiwillig erteilten Einwilligung des Teilnehmenden.

### 3.4.2 Zweck der Datenverarbeitung für myCoach Videosprechstunde

Wir verarbeiten Ihre personenbezogenen Daten ausschließlich für folgende Zwecke:

- Zur Durchführung der Videosprechstunde und medizinischen Beratung.
- Zur Terminvereinbarung und -bestätigung.
- Zur Abrechnung von medizinischen Dienstleistungen (falls zutreffend).
- Zur Verbesserung und Wartung unserer Videosprechstundenplattform.

### 3.4.3 Nutzung der Videosprechstunde für Teilnehmende (Patienten)

Qurasoft GmbH erbringt mit der Videosprechstunde selbst keine ärztlichen und/oder therapeutischen Leistungen. Ein Behandlungsvertrag kommt ausschließlich zwischen Versicherten und der KKH zustande. Die vorliegende Datenschutzerklärung informiert daher auch nicht über Datenverarbeitungsvorgänge, die die KKH eigenverantwortlich durchführt. Sämtliche an der Videosprechstunde beteiligten Ärzte sind aber

selbstverständlich gesetzlich verpflichtet, personenbezogene Daten nach den jeweils geltenden datenschutz- und berufsrechtlichen Vorschriften zu behandeln. Für die sich an die Videosprechstunde anschließende Weiterverarbeitung Ihrer Daten (einschließlich der Abrechnung) ist allein der Sie behandelnde Leistungserbringer verantwortlich.

Die Anmeldung (Login) für Teilnehmende erfolgt direkt auf unserer Plattform unter https://meeting.saniq.org und ist nur mit vorher übermittelten Zugangsdaten nutzbar.

Bei der Nutzung der myCoach-VSS werden vom Teilnehmenden folgende personenbezogenen Daten verarbeitet:

• E-Mail-Adresse

• Zugangs-TAN

• Videosprechstunden-Token

• IP-Adresse des Nutzers, gekürzt auf die letzten beiden Oktette

• Datum und Uhrzeit des Zugriffs

• Browsertyp und -version

• Betriebssystem des Nutzers

• Referrer-URL

• Hostname des zugreifenden Rechners

• Menge der übertragenen Daten

• Statusmeldungen (z.B., ob der Zugriff erfolgreich war)

• Audio- / Videosignale

Diese Datenverarbeitung erfolgt gemäß Art. 6 Abs. 1 lit. b DSGVO zur Durchführung und Erfüllung von vertraglichen Maßnahmen, die auf Anfrage der betroffenen Person erfolgen.

### 3.4.4 Nutzung der Videosprechstunde für telemedizinisch Verantwortliche

Im Verhältnis zu Leistungserbringern ist Qurasoft GmbH die verantwortliche Stelle im Sinne des Datenschutzrechts.

Die Erfassung und Verarbeitung dieser Informationen ist für die Erfüllung des Vertrages mit uns erforderlich (Art. 6 Abs. 1 S. 1 lit. b DSGVO). Die von Ihnen bei der Registrierung angegeben Daten werden von uns grundsätzlich nur so lange verarbeitet, wie dies zur Erreichung des Zwecks der Verarbeitung erforderlich ist. Sollten Sie Ihren Benutzeraccount widerrufen, wird Ihr Benutzerkonto sowie Ihre Daten unverzüglich nach Eingang Ihres Widerrufs innerhalb von 10 Werktagen gelöscht, sofern dem keine rechtliche Verpflichtungen gegenüberstehen.

Sofern Sie über die Plattform an einer Videosprechstunde teilnehmen, wird Ihre IP-Adresse für einen begrenzten Zeitraum erhoben und gespeichert, um die Videoübertragung zu ermöglichen und zu dokumentieren, Fehler bei der Videoübertragung zu beseitigen und die Videoqualität zu analysieren. Zudem verarbeiten wir Ihre Authentifizierungsdaten sowie das Datum und die Uhrzeit (Beginn und Ende der Videoübertragung). Letzteres ist erforderlich, um zu dokumentieren, dass

die Videosprechstunde ordnungsgemäß durchgeführt wurde. Für die Videoübertragung werden Audio- und Videodaten verschlüsselt über eine sichere Peer-to-Peer-Verbindung zwischen Patienten und Ihnen übertragen. Sollte eine Peer-to-Peer-Verbindung aus technischen Gründen nicht aufgebaut werden können, wird von uns ein Proxyserver bereitgestellt. Die Audio- und Videosignale können zu keinem Zeitpunkt von uns und/oder

sonstigen Personen eingesehen werden. Lediglich der Patient kann die Audio- und Videosignale live betrachten. Die Audio- und Videodaten werden zu keinem Zeitpunkt gespeichert. Die Übermittlung dieser Daten ist für die Durchführung der Videosprechstunde und damit für die Erfüllung des Vertrages erforderlich (Art. 6 Abs. 1 S. 1 lit. b DSGVO).

Sämtliche Daten, die für die technische Durchführung der Videosprechstunde erforderlich sind, werden von unseren Systemen unmittelbar nach Beendigung der Videosprechstunde gelöscht. Der Name des Patienten, Datum und Uhrzeit des Termins sowie die Dauer der Videosprechstunde werden für das Gesprächsprotokoll gespeichert.

Die Anmeldung (Login) erfolgt direkt auf unserer Plattform unter https://login.saniq.org und ist nur nutzbar nach vorheriger Registrierung der KKH oder Institution bei der Qurasoft GmbH.

Wichtig: Die Registrierung für die Videosprechstunde erfolgt nicht über https://register.saniq.org, sondern gesondert über den Direktkontakt zum Vertrieb.

## 3.5 Kontaktmöglichkeit auf der Internetseite

Soweit Sie mit uns über das Kontaktformular, via E-Mail oder einen anderen Kanal kommunizieren, verarbeiten wir Ihre personenbezogenen Daten zur Bearbeitung Ihrer Anfrage, insbesondere Kontaktdaten, z.B. Name, E-Mail-Adresse, Telefonnummer, sowie Inhaltsdaten der Kommunikation.

Sie können folgende Kontaktmöglichkeiten nutzen:

• über unser Kontaktformular auf unserer Webseite. Diese ist unter

https://qurasoft.de/kontakt erreichbar,

• über die E-Mail-Adresse kontakt@qurasoft.de, sowie

• über unseren Support-Webseite: Diese ist unter https://support.qurasoft.de erreichbar.

Die Verarbeitung Ihrer personenbezogenen Daten erfolgt auf Grundlage Ihrer freiwillig erteilten Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

## 3.6 Versandinformationen

Zur Abwicklung des Versands erheben wir folgende Informationen von Ihnen:

• Name,

• Lieferadresse,

• E-Mail-Adresse

• und Telefonnummer (optional).

Diese Daten werden benötigt, um Ihnen Ihre Bestellung zuzustellen und Sie über den Lieferstatus zu informieren. Ihre Daten werden ausschließlich zur Abwicklung und Durchführung des Versands verwendet. Dies beinhaltet die Weitergabe Ihrer Daten an den beauftragten Logistikpartner zur Zustellung Ihrer Bestellung.

Die Verarbeitung Ihrer personenbezogenen Daten erfolgt auf Grundlage Ihrer freiwillig erteilten Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

## 4. Datenaufbewahrung und -Löschung

Im Rahmen unserer Datenschutzerklärung möchten wir Sie darüber informieren, wie wir personenbezogene Daten aufbewahren und löschen.

### 4.1 Aufbewahrungsfristen

Wir speichern Ihre personenbezogenen Daten nur so lange, wie dies für die Erfüllung der Zwecke, für die sie erhoben wurden, erforderlich ist. Dies bedeutet, dass wir Daten so lange aufbewahren, wie es gesetzlich vorgeschrieben ist oder wie es zur Erfüllung unserer vertraglichen Verpflichtungen oder berechtigten Geschäftszwecke notwendig ist. Die genaue Aufbewahrungsdauer kann je nach Art der Daten und Zweck der Verarbeitung variieren. Sofern nicht anders angegeben ist das Kriterium für die Dauer der Speicherung von personenbezogenen Daten, die jeweilige gesetzliche Aufbewahrungsfrist. Nach Ablauf der Frist werden die entsprechenden Daten routinemäßig gelöscht, sofern sie nicht mehr zur Vertragserfüllung oder Vertragsanbahnung erforderlich sind.

### 4.2 Löschung von personenbezogenen Daten

Die Löschung Ihrer Daten aus dem myCoach-System kann von den telemedizinischen Verantwortlichen durchgeführt werden. Bitte beachten Sie, dass diese Aufforderung zur Löschung an die telemedizinisch Unterstützenden gerichtet werden muss und dort im Rahmen berufsrechtlicher Vorgaben durchgeführt wird. Bitte beachten Sie weiterhin, dass einer Löschung rechtliche Aufbewahrungspflichten entgegenstehen können.

Sobald die Zwecke, für die Ihre Daten erhoben wurden, erfüllt sind und keine rechtlichen oder vertraglichen Verpflichtungen mehr bestehen, werden wir Ihre personenbezogenen Daten routinemäßig und entsprechend den gesetzlichen Vorschriften sperren oder sicher und dauerhaft löschen. Dies kann bedeuten, dass Ihre Daten nach Ablauf der gesetzlichen Aufbewahrungsfristen oder nach Vertragsende gelöscht werden. Wir treffen angemessene technische und organisatorische Maßnahmen, um sicherzustellen, dass Ihre Daten sicher und unwiederbringlich gelöscht werden.

Sofern vorherige Zustimmungen zur Übertragung in Drittsysteme erfolgt sind, sind wir nicht in der Lage, die Löschfristen dieser Drittsysteme zu kontrollieren oder zu beeinflussen.

Die Löschfristen sind wie folgt für die folgenden Arten von Daten definiert:

### 3.1. Zugriffsdaten

Zugriffsdaten werden nach 10 Tagen routinemäßig gelöscht, indem die Server-Logfiles gelöscht werden. IP-Adressen werden anonymisiert gespeichert und auf die letzten beiden Oktette direkt gekürzt.

### 3.2. Registrierung und Anmeldung für telemedizinisch Verantwortliche (Login)

Die Löschung Ihrer Daten wird innerhalb von 10 Tagen routinemäßig nach dem Datum der Vertragsbeendigung erfolgen. Wir werden sicherstellen, dass sämtliche personenbezogenen Daten, die in unserer Obhut sind, dauerhaft gelöscht werden.

Es ist uns wichtig, darauf hinzuweisen, dass bestimmte gesetzliche Aufbewahrungspflichten oder berechtigte Interessen es erforderlich machen könnten, bestimmte Informationen über einen bestimmten Zeitraum aufzubewahren. Diese Daten werden jedoch nur für gesetzlich vorgeschriebene Zwecke verwendet und sind nicht mehr in unserem alltäglichen Betrieb zugänglich.

3.3. Gesundheitsdaten

Gemäß den geltenden gesetzlichen Anforderungen und Aufbewahrungsfristen werden Gesundheitsdaten nach einem festgelegten Zeitrahmen gelöscht. Diese gesetzlichen Fristen können je nach Art der Daten und den regionalen Gesetzen variieren, reichen jedoch oft von 10 bis 30 Jahren.

Es ist wichtig zu beachten, dass die Aufbewahrungsfristen für Gesundheitsdaten von den entsprechenden medizinischen Behörden und Gesundheitseinrichtungen festgelegt werden und darauf abzielen, den rechtlichen und medizinischen Anforderungen gerecht zu werden. Diese Aufbewahrungsfristen können je nach der Art der Gesundheitsdaten, den individuellen Patientenakten und den gesundheitlichen Bedürfnissen variieren.

Wir respektieren und unterstützen die Einhaltung dieser gesetzlichen Vorschriften und stehen im Einklang mit den bewährten medizinischen Praktiken. Sollten Sie weitere Informationen zur Löschung Ihrer Gesundheitsdaten benötigen oder Fragen zu diesem Prozess haben, stehen Ihnen die telemedizinisch Verantwortlichen Fachkräfte und unser Datenschutzbeauftragte gerne zur Verfügung.

3.4.1 Erfassung von allgemeinen Daten und Informationen

Die Löschung Ihrer Daten wird innerhalb von 10 Tagen nach dem Datum der Vertragsbeendigung erfolgen. Wir werden sicherstellen, dass sämtliche personenbezogenen Daten, die in unserer Obhut sind, dauerhaft gelöscht werden.

3.4.3 Nutzung der Videosprechstunde für Teilnehmende (Patienten)

Die Löschung Ihrer personenbezogenen Daten erfolgt innerhalb von 10 Tagen nach dem Datum der Vertragsbeendigung, sofern keine gesetzlichen, buchhalterischen oder medizinischen Aufbewahrungspflichten dem Entgegenstehen.

Entsprechende Zugriffsdateien, die in Logdateien erfasst wurden, werden nach 30 Tagen routinemäßig gelöscht.

3.5 Kontaktmöglichkeit auf der Internetseite

Die Löschung Ihrer personenbezogenen Daten erfolgt in der Regel spätestens 10 Tage nach dem Abschluss der vorvertraglichen oder vertraglichen Maßnahmen. Dieser Zeitrahmen kann je nach den spezifischen Umständen und den geltenden gesetzlichen Anforderungen variieren.

Bitte beachten Sie, dass bestimmte gesetzliche Aufbewahrungspflichten oder berechtigte Interessen es erforderlich machen könnten, bestimmte Informationen über einen längeren Zeitraum aufzubewahren. In solchen Fällen werden wir sicherstellen, dass Ihre Daten nur für die jeweils vorgeschriebenen Zwecke verwendet werden und dennoch angemessen geschützt sind.

3.6 Versandinformationen

Ihre Daten werden nach Abschluss des Versandservice gemäß den gesetzlichen Aufbewahrungsfristen gelöscht, sofern keine gesetzlichen oder vertraglichen Aufbewahrungspflichten bestehen.

Backups

Nach der Löschung Ihrer personenbezogenen Daten im Rahmen unserer Datenschutzrichtlinien werden auch die Daten in unseren Backups sorgfältig behandelt. Diese Backups unterliegen ebenfalls den gleichen Datenschutzstandards und Sicherheitsvorkehrungen. Die personenbezogenen Daten, die gelöscht wurden, werden spätestens innerhalb von 7 Tagen nach der Löschung in den Backups ebenfalls gelöscht.

Unsere Verpflichtung zur Gewährleistung Ihrer Privatsphäre und der Schutz Ihrer Daten endet nicht mit der Löschung Ihrer Daten aus unserer aktiven Datenbank. Wir setzen alles daran, sicherzustellen, dass Ihre Daten auch in unseren Backups ordnungsgemäß und zeitnah entfernt werden.

## 5. Datenweitergabe

In einigen Fällen kann es notwendig sein, personenbezogene Daten an Dritte weiterzugeben, um die oben genannten Zwecke zu erfüllen. Diese Weitergaben erfolgen ausschließlich unter Berücksichtigung der geltenden Datenschutzbestimmungen. Dritte, an die wir Daten weitergeben können, sind unter anderem:

• Versanddienstleister für die Zustellung von Waren

• Service Provider und IT-Dienstleister

• Zahlungsdienstleister zur Abwicklung von Zahlungen

• Steuerberater und Wirtschaftsprüfer zur Erfüllung gesetzlicher Pflichten

• Behörden und Gerichte zur Einhaltung rechtlicher Verpflichtungen

Wir geben Ihre personenbezogenen Daten nur dann an Dritte weiter, wenn:

• Sie ausdrücklich eingewilligt haben,

• die Weitergabe zur Abwicklung von Vertragsverhältnissen erforderlich ist,

• eine gesetzliche Verpflichtung zur Weitergabe besteht, oder

• die Weitergabe zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Wir übermitteln personenbezogene Daten nicht an Drittstaaten außerhalb der EU/EWR. Wir setzen teilweise (in Deutschland ansässige) Service Provider ein, die Daten in unserem Auftrag verarbeiten (z.B. bei Hosting/E-Mail-Marketing). In den hier beschriebenen Fällen werden die Informationen an diese dritten Stellen weitergegeben, um die weitere Bearbeitung zu ermöglichen. Die externen Service Provider werden von uns sorgfältig ausgewählt und regelmäßig überprüft, um sicherzugehen, dass Ihre Privatsphäre gewahrt bleibt.

Die Service Provider sind weisungsgebundene Dienstleister / Auftragsverarbeiter und werden dementsprechend von uns u.a. verpflichtet, Ihre Daten ausschließlich entsprechend unseren Weisungen sowie den jeweils geltenden Datenschutzgesetzen zu behandeln. Insbesondere werden sie verpflichtet, Ihre Daten streng vertraulich zu behandeln. Es ist Ihnen auch untersagt, die Daten für andere Zwecke als vereinbart zu verarbeiten.

Die Weitergabe von Daten an Auftragsverarbeiter erfolgt auf Grundlage von Art. 28 Abs. 1 DSGVO.

Wir verkaufen Ihre Daten nicht an Dritte, noch vermarkten wir sie anderweitig.

## 6. Sicherheit

Qurasoft setzt technische und organisatorische Sicherungsmaßnahmen ein, um Ihre zur Verfügung gestellten Daten vor zufälligen oder vorsätzlichen Manipulationen, Verlust, Zerstörung oder dem Zugriff unberechtigter Personen zu schützen. Dies gilt auch, wenn externe Dienstleistungen bezogen werden. Die Wirksamkeit unserer Sicherheitsmaßnahmen wird überprüft und die Maßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

## 7. Ihre Rechte

Sie haben bestimmte Rechte in Bezug auf Ihre personenbezogenen Daten. Folgend werden die bestimmten Rechte ausgeführt.

7.1 Recht auf Bestätigung

Jede betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber eingeräumte Recht, von dem für die Verarbeitung Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Möchte eine betroffene Person dieses Bestätigungsrecht in Anspruch nehmen, kann sie sich hierzu jederzeit an den Datenschutzbeauftragten des die Verarbeitung Verantwortlichen wenden (Anschrift siehe oben).

7.2 Auskunftsrecht

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, jederzeit von dem für die Verarbeitung Verantwortlichen unentgeltliche Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten und eine Kopie dieser Auskunft zu erhalten. Ferner hat der Europäische Richtlinien- und Verordnungsgeber der betroffenen Person Auskunft über folgende Informationen zugestanden:

• die Verarbeitungszwecke

• die Kategorien personenbezogener Daten, die verarbeitet werden

• die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen

• falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer

• das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde

• wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden:

Alle verfügbaren Informationen über die Herkunft der Daten

• das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Abs.1 und 4 DSGVO und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Ferner steht der betroffenen Person ein Auskunftsrecht darüber zu, ob personenbezogene Daten an ein Drittland oder an eine internationale Organisation

übermittelt wurden. Sofern dies der Fall ist, so steht der betroffenen Person im Übrigen das Recht zu, Auskunft über die geeigneten Garantien im Zusammenhang mit der Übermittlung zu erhalten.

### 7.3 Recht zur Berichtigung unrichtiger Daten

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Ferner steht der betroffenen Person das Recht zu, unter Berücksichtigung der Zwecke der Verarbeitung, die Vervollständigung unvollständiger personenbezogener Daten — auch mittels einer ergänzenden Erklärung — zu verlangen.

### 7.4 Recht auf Löschung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, sofern einer der folgenden Gründe zutrifft und soweit die Verarbeitung nicht erforderlich ist:

• Die personenbezogenen Daten wurden für solche Zwecke erhoben oder auf sonstige Weise verarbeitet, für welche sie nicht mehr notwendig sind.

• Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Art. 6 Abs. 1 lit. a DSGVO oder Art. 9 Abs. 2 lit. a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

• Die betroffene Person legt gemäß Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein, und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein.

• Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

• Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

• Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Sofern einer der oben genannten Gründe zutrifft und eine betroffene Person die Löschung von personenbezogenen Daten, die bei der Qurasoft GmbH gespeichert sind, veranlassen möchte, kann sie sich hierzu jederzeit an den Datenschutzbeauftragens des für die Verarbeitung Verantwortlichen wenden (Anschrift siehe oben). Der Datenschutzbeauftragte wird veranlassen, dass dem Löschverlangen unverzüglich nachgekommen wird.

Wurden die personenbezogenen Daten von der Qurasoft GmbH öffentlich gemacht und ist unser Unternehmen als Verantwortlicher gemäß Art. 17 Abs. 1 DSGVO zur Löschung der personenbezogenen Daten verpflichtet, so trifft die Qurasoft GmbH unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um andere für die Datenverarbeitung Verantwortliche, welche die veröffentlichten personenbezogenen Daten verarbeiten, darüber in Kenntnis zu setzen, dass die betroffene Person von diesen anderen für die Datenverarbeitung Verantwortlichen die Löschung sämtlicher Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser

personenbezogenen Daten verlangt hat, soweit die Verarbeitung nicht erforderlich ist. Der Datenschutzbeauftrage der Qurasoft GmbH wird im Einzelfall das Notwendige veranlassen.

### 7.5 Recht auf Einschränkung der Verarbeitung

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

• Die Richtigkeit der personenbezogenen Daten wird von der betroffenen Person bestritten, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.

• Die Verarbeitung ist unrechtmäßig, die betroffene Person lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung der personenbezogenen Daten.

• Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

• Die betroffene Person hat Widerspruch gegen die Verarbeitung gem. Art. 21 Abs. 1 DSGVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Sofern eine der oben genannten Voraussetzungen gegeben ist und eine betroffene Person die Einschränkung von personenbezogenen Daten, die bei der Qurasoft GmbH gespeichert sind, verlangen möchte, kann sie sich hierzu jederzeit an den Datenschutzbeauftragten des für die Verarbeitung Verantwortlichen wenden (Anschrift siehe oben). Der Datenschutzbeauftrage der Qurasoft GmbH wird die Einschränkung der Verarbeitung veranlassen.

### 7.6 Recht auf Datenübertragbarkeit

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, die sie betreffenden personenbezogenen Daten, welche durch die betroffene Person einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat außerdem das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf der Einwilligung gemäß Art. 6 Abs. 1 Buchstabe a DSGVO oder Art. 9 Abs. 2 Buchstabe a DSGVO oder auf einem Vertrag gemäß Art. 6 Abs. 1 Buchstabe b DSGVO beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt, sofern die Verarbeitung nicht für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, welche dem Verantwortlichen übertragen wurde.

Ferner hat die betroffene Person bei der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Art. 20 Abs. 1 DSGVO das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen an einen anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist und sofern hiervon nicht die Rechte und Freiheiten anderer Personen beeinträchtigt werden.

Zur Geltendmachung des Rechts auf Datenübertragbarkeit kann sich die betroffene Person jederzeit an den Datenschutzbeauftragen der Qurasoft GmbH wenden (Anschrift siehe oben).

### 7.7 Widerspruchsrecht

Jede von der Verarbeitung personenbezogener Daten betroffene Person hat das vom Europäischen Richtlinien- und Verordnungsgeber gewährte Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 lit. e oder f DSGVO erfolgt, Widerspruch einzulegen. Dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.

Die Qurasoft GmbH verarbeitet die personenbezogenen Daten im Falle des Widerspruchs nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die den Interessen, Rechten und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Verarbeitet die Qurasoft GmbH personenbezogene Daten, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung der personenbezogenen Daten zum Zwecke derartiger Werbung einzulegen. Dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widerspricht die betroffene Person gegenüber der Qurasoft GmbH der Verarbeitung für Zwecke der Direktwerbung, so wird die Qurasoft GmbH die personenbezogenen Daten nicht mehr für diese Zwecke verarbeiten.

Zudem hat die betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die sie betreffende Verarbeitung personenbezogener Daten, die bei der Qurasoft GmbH zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken gemäß Art. 89 Abs. 1 DSGVO erfolgen, Widerspruch einzulegen, es sei denn, eine solche Verarbeitung ist zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich.

Zur Ausübung des Rechts auf Widerspruch kann sich die betroffene Person direkt den Datenschutzbeauftragen der Qurasoft GmbH wenden (Anschrift siehe oben). Der betroffenen Person steht es ferner frei, im Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft, ungeachtet der Richtlinie 2002/58/EG, ihr Widerspruchsrecht mittels automatisierter Verfahren auszuüben, bei denen technische Spezifikationen verwendet werden.

### 7.8 Recht zur Beschwerde bei einer Aufsichtsbehörde

Gemäß den geltenden Datenschutzgesetzen haben Sie das Recht, eine Beschwerde bei der zuständigen Datenschutzaufsichtsbehörde einzureichen, wenn Sie der Ansicht sind, dass Ihre personenbezogenen Daten in Bezug auf unsere Dienstleistungen unrechtmäßig verarbeitet wurden oder gegen datenschutzrechtliche Bestimmungen verstoßen wurde. Die Aufsichtsbehörde, bei der Sie Ihre Beschwerde einreichen können, hängt von Ihrem Wohnsitzland und der Art der behaupteten Verletzung ab.

In Deutschland ist die für uns zuständige Aufsichtsbehörde:

Name der Behörde:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Adresse: Hintere Bleiche 34, 55116 Mainz

Telefon: +49 6131 89200 | Website: www.datenschutz.rlp.de

Formular:

https://www.datenschutz.rlp.de/de/themenfelder-themen/online-services/beschwerdeformular

Bitte beachten Sie, dass Sie dieses Recht zur Beschwerde unbeschadet anderweitiger verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe ausüben können.

## 8. Kontakt

Für alle Anfragen, Anliegen oder Informationen bezüglich Ihrer personenbezogenen Daten und unserer Datenschutzpraktiken stehen wir Ihnen gerne zur Verfügung. Sie können uns wie folgt kontaktieren:

Kontaktadresse:

Qurasoft GmbH

Im Metternicher Feld 30c

D-56072 Koblenz am Rhein

Rheinland-Pfalz / Deutschland

Kontakt E-Mail

kontakt@qurasoft.de

Kontakt-Telefon

+49 261 1349860

Unsere externen Datenschutzbeauftragte steht Ihnen ebenfalls zur Verfügung und kann wie folgt

erreicht werden:

Datenschutzbeauftragter

TüV Technische Überwachung Hessen GmbH

Robert-Bosch-Str. 16

64293 Darmstadt

nicolas.kurze@tuevhessen.de / datenschutz@qurasoft.de

Telefon +49 6151 - 6001403

## 9. Änderungen der Datenschutzerklärung

Wir behalten uns das Recht vor, unsere Datenschutzerklärung in regelmäßigen Abständen zu aktualisieren, um sicherzustellen, dass sie den aktuellen gesetzlichen Anforderungen und unseren eigenen Datenschutzpraktiken entspricht. Änderungen dieser Datenschutzerklärung treten in Kraft, sobald sie auf unserer Website veröffentlicht werden. Daher empfehlen wir Ihnen, diese Seite regelmäßig zu überprüfen, um sich über Aktualisierungen und Änderungen zu informieren.

Im Falle von wesentlichen Änderungen, die sich auf die Verarbeitung Ihrer personenbezogenen Daten auswirken könnten, werden wir Sie über die Änderungen in

angemessener Weise informieren. Dies kann beispielsweise durch eine Benachrichtigung per E-Mail oder durch eine deutlich sichtbare Mitteilung auf unserer Website geschehen.

Bitte beachten Sie, dass Ihre fortgesetzte Nutzung unserer Dienstleistungen nach Veröffentlichung von Änderungen in dieser Datenschutzerklärung als Annahme dieser Änderungen betrachtet wird. Sollten Sie mit den Änderungen nicht einverstanden sein, haben Sie das Recht, die Nutzung unserer Dienste einzustellen und uns gegebenenfalls zu kontaktieren, um Ihre Bedenken zu besprechen.

Wir sind bestrebt, Transparenz in Bezug auf unsere Datenschutzpraktiken zu wahren und sicherzustellen, dass Sie stets darüber informiert sind, wie wir Ihre personenbezogenen Daten verwenden. Wenn Sie Fragen oder Bedenken bezüglich dieser Datenschutzerklärung oder etwaiger Änderungen haben, zögern Sie bitte nicht, uns über die in unserer Kontaktinformation angegebenen Kanäle zu kontaktieren. Wir stehen Ihnen gerne zur Verfügung, um Ihre Anliegen zu klären und Ihnen bei Datenschutzfragen behilflich zu sein.

# Datenschutzhinweise KKH-Gesundheitsberatung: myCoach-App

**Dokumentinformation**

- ID: DOC-PRIVACY-2
- Version: 1
- gültig ab: 24.10.2023
- gültig bis: /
- Geltungsbereich: Anwender der mobilen Anwendung myCoach für die Plattformen von Apple iOS und Android.

**Autorinformation**

- Name: Artur Schens
- Funktion: Geschäftsführer – OU Operations
- Freigabe durch: Artur Schens

**Historie**

- Version: 1
- Datum: 24.10.2023
- Änderung: Überführung in ein gelenktes Dokument
- Autor: Artur Schens

## 1. Allgemeines – Information nach Art. 13 + 14 DSGVO

Der Qurasoft GmbH (nachfolgend Qurasoft oder wir) als Betreiberin und datenschutzrechtlich Verantwortliche der myCoach -App für mobile Endgeräte („App“) ist der Schutz und die Vertraulichkeit Ihrer Daten von besonderer Bedeutung. In den nachstehenden Hinweisen zum Datenschutz möchten wir Sie darüber informieren, welche Arten von Daten wir zu welchen Zwecken erheben, verarbeiten und nutzen und welche Rechte Ihnen zustehen. Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt, es sind jedoch immer alle Geschlechtergemeint.

Zweckbestimmung der myCoach -App

Die App richtet sich an Menschen, die an chronischen Krankheiten leiden. Sie sollen, während der akuten/chronischen Krankheitsphase beziehungsweise in der Nachsorge unterstützt werden. myCoach soll ein fundiertes Eigenmonitoring sowie ein Monitoring durch Angehörige von Gesundheitsberufen ermöglichen.

Die App kann - nach einer dafür notwendigen Kopplung - zur telemedizinischen Kontrolle durch Unterstützende (z.B. der Coach) dienen.

Nachfolgend werden diese Personen oder Institutionen telemedizinisch Unterstützende genannt. Die entsprechende Software-Lösung wird myCoach-Software genannt. Den Anwender der myCoach -App bezeichnen wir im Folgenden als Anwender.

Die App kann vom Anwender eigenständig aus einem App-Store bezogen und zum ausschließlichen Eigenmonitoring verwendet werden. Dabei kann der Anwender für sein

Krankheitsbild relevante Messdaten protokollieren und Unterstützung (z.B. Messerinnerungen) im Umgang mit seiner Gesundheit erhalten. Sie ist somit ein Instrument zur Auseinandersetzung und Kontrolle der eigenen Gesundheit.

*Sofern der Nutzer von telemedizinisch Unterstützenden einen Aktivierungscode für* myCoach-Software *erhalten hat, kann er diesen innerhalb der App eingeben.*

***Nach dieser Eingabe und Abgleich des Geburtsdatums des Anwenders werden sämtliche erfassten Daten -sofern nicht anders in der App kommuniziert an die*** myCoach***-Analysesoftware für telemedizinisch Unterstützende online übersandt.*** Auf diese Daten kann von telemedizinisch Unterstützenden zugegriffen werden. Telemedizinisch Unterstützende können die übertragenen Werte einsehen und den Anwender unterstützen.

Die Nutzung von myCoach ersetzt ausdrücklich keinen notwendigen physischen Arztbesuch.

Anwender haben innerhalb der myCoach -App die Möglichkeit, alle Messdaten in einer PDF-Datei aufzubereiten und zu exportieren. Die myCoach -App darf ausschließlich von Personen verwendet werden, die mindestens 16 Jahre alt sind. Eine Erhebung oder Verarbeitung von personenbezogenen Daten von Personen, die jünger als 16 Jahre alt sind, erfolgt ausdrücklich gegen unseren Willen und ohne unsere Kenntnis. Außerdem stellt dies einen Verstoß gegen unsere Allgemeinen Geschäftsbedingungen dar.

Im Folgenden umfasst der Begriff „myCoach -App im Eigenmonitoring“ die Standard-Ausprägung myCoach ohne Anbindung an myCoach. Der Begriff „myCoach -App im Telemedizin-Modus“ umfasst die Ausprägung mit der telemedizinischen Anbindung an myCoach-Software.

Verantwortlicher im Sinne des Datenschutzes und Datenschutzbeauftragter

Verantwortlich für die Verarbeitung Ihrer personenbezogenen Daten ist

Qurasoft GmbH

Im Metternicher Feld 30c

D-56072 Koblenz am Rhein

Telefon: (+49) 261 – 134 986 0

E-Mail: kontakt@qurasoft.de

Geschäftsführer:

Tobias Hastenteufel, Erwin Junker & Artur Schens

Handelsregister Amtsgericht Koblenz

HRB 24744

USt.-IdNr.: DE301340994

Unseren externen Datenschutzbeauftragten erreichen Sie unter:

TÜV Technische Überwachung Hessen GmbH

Nicolas Kurze

E-Mail: datenschutz@qurasoft.de oder Nicolas.Kurze@tuevhessen.de

## 2. Rechtsgrundlage der Verarbeitung

Wenn Sie die myCoach -App im Eigenmonitoring nutzen, werden zunächst Ihre personenbezogenen Daten nur auf Ihrem Endgerät gespeichert. Dementsprechend werden keine Gesundheitsdaten übermittelt. Wir erhalten nur Ihre E-Mail-Adresse (Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO –vertragliche Maßnahme), um zu überprüfen, ob Sie auch tatsächlich der Inhaber der E-Mail-Adresse sind. Zudem benötigen wir Ihre Mobilfunknummer, um Ihnen den Einmalcode per SMS zu zusenden. Sollten Sie in die Verarbeitung Ihrer Standortdaten einwilligen (Art. 6 Abs.1 lit. a DSGVO), um z.B. den Pollenflug in Ihrer Umgebung zu bestimmen, wird ihr Standort sowie Ihre IP-Adresse an unsere Server übertragen. Sie haben hier jederzeit das Recht Ihre Einwilligung durch Klicken des Buttons „Verbindung trennen“ zu widerrufen.

Wenn Sie die myCoach -App im Telemedizin-Modus verwenden, werden Ihre personenbezogenen Daten an Ihren jeweiligen telemedizinischen Unterstützenden zum Zweck der Behandlung übermittelt. Die Übermittlung erfolgt nur, wenn Sie darin eingewilligt haben (Art. 9 Abs. 2 lit. a DSGVO). Sie haben jederzeit die Möglichkeit Ihre Einwilligung durch Klicken des Buttons „Verbindung trennen“ zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Nach der Datenübermittlung an Ihren jeweiligen telemedizinischen Unterstützenden ist dieser für die weitere Datenverarbeitung verantwortlich.

Wir möchten Sie nochmals darauf hinweisen, dass die Übermittlung Ihrer Daten an Ihren jeweiligen telemedizinisch Unterstützenden auf der Grundlage erfolgt, dass Sie Ihre ausdrückliche Einwilligung zu der Verarbeitung der Sie betreffenden personenbezogenen Daten für einen oder mehrere der soeben bestimmten Zwecke geben.

Eine von Ihnen erteilte Einwilligung ist jederzeit uns gegenüber widerruflich. Der Widerruf der Einwilligung führt allerdings nicht dazu, dass die Verarbeitung Ihrer personenbezogenen Daten aufgrund anderer Rechtfertigungsgründe, bspw. aufgrund bestehender Vertragsverhältnisse mit Ihren telemedizinisch Unterstützenden, unzulässig wird.

**Vorgegebenes Mindestalter**

Unsere myCoach -App darf ausschließlich von Personen verwendet werden, die mindestens 16 Jahre alt sind. Eine Erhebung oder Verarbeitung von personenbezogenen Daten von Personen, die jünger als 16 Jahre alt sind, erfolgt ausdrücklich gegen unseren Willen und ohne unsere Kenntnis. Außerdem stellt dies einen Verstoß gegen unsere Allgemeinen Geschäftsbedingungen dar.

## 3. Allgemeines

1. Verarbeitung personenbezogener Daten

Wir erheben, verarbeiten und nutzen Ihre personenbezogenen und besonderen personenbezogenen Daten (zusammen: „Persönliche Daten“) ausschließlich im Rahmen der deutschen und europäischen Datenschutzregelungen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. (Art. 4 Nr. 1 Datenschutzgrundverordnung – „DSGVO“). Als personenbezogene Daten gelten daher z.B. Ihr Name, Ihre Adresse und Ihre Mobilfunknummer.

Sogenannte besondere Kategorien personenbezogener Daten sind besonders sensible Daten, die besonders schutzbedürftig sind, u.a. Angaben über Ihre Gesundheit (Art. 9 Abs. 1DSGVO).

Die Verwendung der myCoach -App und die Erfassung persönlicher Daten erfolgt grundsätzlich freiwillig. Von Ihnen in der App erfasste persönliche Daten werden wir nur dazu verwenden, Ihnen die gewünschten Dienstleistungen bereitzustellen, oder aber zu anderen Zwecken, für die Sie Ihre Einwilligung erteilt haben, sofern keine anders lautenden gesetzlichen Verpflichtungen bestehen.

Sofern in unserer App die Möglichkeit der Eingabe persönlicher Daten besteht, machen wir Sie darauf aufmerksam, dass nur die besonders gekennzeichneten Pflichtfelder zur Bereitstellung unserer Dienste oder zur Vertragsabwicklung benötigt werden. Sollten darüber hinaus weitere Angaben von Daten möglich sein, so ist deren Eingabe freiwillig.

Eine sonstige Weitergabe Ihrer persönlichen Daten an weitere Dritte, z.B. Ihren telemedizinisch Unterstützenden, findet nur statt, sofern Sie in die Weiterleitung Ihrer personenbezogenen Daten eingewilligt haben. Innerhalb der myCoach -App erhalten Sie von uns keine Werbung. Die Erhebung beziehungsweise Übermittlung persönlicher Daten an staatliche Einrichtungen und Behörden erfolgt nur im Rahmen zwingender Rechtsvorschriften.

Sämtliche von uns getroffenen Voreinstellungen sind so gewählt, dass grundsätzlich nur persönliche Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszwecke erforderlich ist, verarbeitet werden.

Unsere App ist von vornherein auf die Minimierung anfallender Daten angelegt.

## 2. Verwendung der myCoach -App

Es gibt zwei Möglichkeiten, die myCoach -App einzusetzen. Sie lässt sich als Unterstützung bei einem Eigenmonitoring verwenden. Dabei erfassen Sie selbst Vitalparameter und führen ein Gesundheitstagebuch.

Koppeln Sie die myCoach -App über einen Telemedizin-Modus (d.h. über eine Verbindung zur Software myCoach) mit telemedizinisch Unterstützenden, die die zugehörige Analysesoftware einsetzen, werden Ihre Messdaten an das myCoach -Software-Onlinesystem übertragen, von wo aus Ihre telemedizinisch Unterstützenden darauf zugreifen können.

**Dies wird im Folgenden genauer dargelegt:**

### 2.1. Nutzung der myCoach -App im Eigenmonitoring

Mit „myCoach-App“ (nachfolgend auch „App“ genannt) bieten wir Ihnen eine spezielle App für Ihr Mobilfunkgerät, Ihr Smartphone oder Ihr Tablet (Nachfolgend: Gerät) zur Kontrolle Ihrer Gesundheit. Zur Durchführung der Krankheitskontrolle ist es erforderlich, dass Sie bei der Einrichtung der App bestimmte Daten (Pflichtangaben) angeben müssen:

- Ihre E-Mail-Adresse,
- Ihre Mobilfunknummer
- Ihr Geburtsdatum,
- Ihr Geschlecht,
- Ihre Körpergröße

Diese Daten dienen lediglich der für Sie einfacheren Einschätzung von Messwerten, da die App Ihnen Richtwerte anzeigt. Diese Werte dienen jedoch nur als Hinweis und haben keine Aussagekraft über die tatsächliche Schwere Ihrer Erkrankung. Eine vollständige Namensangabe durch Sie ist freiwillig.

Durch die Kopplung eines Messgerätes über die Bluetooth-Verbindung oder durch Ihre manuelle Eingabe können die entsprechenden Messwerte

• der Peak Expiratory Flow (PEF)

• der Forced Expiratory Value (FEV1)

• die Forced vital capacity (FVC)

• die Sauerstoffsättigung (Sp02)

• die Schrittzahl (Bewegung)

• Körpertemperatur

• Atemfrequenz

• Puls

• Blutdruck

• Glukose

• EKG (Elektrokardiogramm)

nebst entsprechenden Begleitnotizen verarbeitet werden.

Bei den erhobenen Daten handelt es sich u.a. um besonders sensible, schutzbedürftige sog. „besondere Kategorien personenbezogener Daten“: So stellt z.B. der Peak Flow-Wert eine Angabe über die Gesundheit des Anwenders dar. Wir nutzen die gespeicherten personenbezogenen Daten unter Beachtung der datenschutzrechtlichen Bestimmungen ausschließlich für die Bereitstellung zur Nutzung innerhalb der myCoach -App.

Sofern Sie die App zum Eigenmonitoring verwenden, werden keine Gesundheitsdaten auf unseren Servern gespeichert. Sie können Ihre Daten selbst einsehen und durch Löschung der App vernichten. Einzelne Betriebssysteme sind so eingestellt, dass die Anwenderdaten lokal auf dem Gerät gespeichert bleiben.

Auf diese Einstellungen haben wir keinen Einfluss, sodass Sie sich beim Hersteller erkundigen müssen, wie die Daten manuell gelöscht werden können.

2.2. Nutzung der myCoach -App im Telemedizin-Modus (Verbindung mit myCoach -Software)

Sofern Sie der Nutzung der direkten KKH-verbindung zustimmen, die von Ihren telemedizinisch Unterstützenden initiiert wurde, ändert sich das Datenübertragungsverhalten der App.

Haben Sie den Telemedizin-Modus aktiviert, werden in der App erhobene Daten auf einen unserer Server in Deutschland verschlüsselt übertragen, über den Ihre telemedizinisch Unterstützenden darauf zugreifen können. Eine Datenübertragung in Drittstaaten, an weitere Dritte oder an internationale Organisationen seitens Qurasoft erfolgt nicht.

Sie erteilen Ihre ausdrückliche EINWILLIGUNG zur Inanspruchnahme von Telemedizin (d.h., zur Herstellung einer Verbindung zur myCoach –Software innerhalb der Anwendung), indem Sie entweder den Ihnen von den telemedizinisch tätigen Fachkräften zur Verfügung gestellten Aktivierungscode in Verbindung mit Ihrem Geburtsdatum eingeben oder alternativ einen Ihnen von den telemedizinisch tätigen Fachkräften ausgehändigten QR-Code verwenden. Eine einmal erteilte Einwilligung ist jederzeit uns gegenüber widerruflich durch Klicken des Buttons „Verbindung trennen“.

Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung, nicht berührt. Zudem hat der Widerruf keinen

Einfluss auf andere Rechtfertigungsgründe zur Datenverarbeitung, insbesondere zur Erfüllung des Vertrages mit den telemedizinisch Unterstützenden.

Nach Ihrer Einwilligung zur Nutzung von Telemedizin ist Ihre App mit der myCoach -Analysesoftware gekoppelt, mit der Ihre telemedizinisch Unterstützenden auf die von Ihnen übermittelten Daten zugreifen können. Bei der Aktivierung von Telemedizin erfolgt - sofern erfasst - die Verarbeitung folgender persönlicher Daten:

• Ihr Name,

• Ihr Geburtsdatum,

• Ihr Geschlecht,

• Ihre Körpergröße und

• Ihr derzeitiges Gewicht,

• Messwerte (Peak Flow, FEV1, Schritte, Gewicht, FVC, Sauerstoffsättigung, Körpertemperatur,

Atemfrequenz, Blutdruck, Puls, Glukose, EKG / Elektrokardiogramm) und Begleitnotizen,

• Umgebungsdaten während der Messung am Ort der Messung (Pollenflug,

Wetterinformationen und Luftbelastung)

• Medikation (eigenständige Eingabe möglich) und Medikationseinnahmen

• Beantwortungen von Fragebögen,

• Dokumente (z.B. Befunde)

Mitteilungen von telemedizinisch Unterstützenden können empfangen werden. Zudem können eigene Mitteilungen an telemedizinisch Unterstützende geschickt werden. Name, Geschlecht, Geburtsdatum können von den telemedizinisch Unterstützenden gegebenenfalls korrigiert werden, sofern z.B. ein Rechtschreibfehler vorliegt.

Fragebögen können von telemedizinisch Unterstützenden bezogen werden. Sie haben die Möglichkeit, diese innerhalb der App zu beantworten und die Antworten über eine verschlüsselte Verbindung an telemedizinisch Unterstützende zu übertragen. Die von Ihnen innerhalb der Fragebögen eingegebenen personenbezogenen Daten werden ebenfalls verschlüsselt auf Ihrem Gerät sowie auf unserem Server gespeichert. Dies gilt gleichfalls für Meldungen und Informationen über die Medikation/-en sowie Dokumente.

Bei den verarbeiteten Daten handelt es sich auch um besonders sensible, schutzbedürftige sog. „besondere Kategorien personenbezogener Daten“: So stellt z.B. der Peak Flow-Wert eine Angabe über die Gesundheit des Anwenders dar. Wir nutzen die gespeicherten personenbezogenen Daten unter Beachtung der datenschutzrechtlichen Bestimmungen ausschließlich für die Bereitstellung zur Nutzung innerhalb der myCoach -App und der myCoach -Analysesoftware für telemedizinisch Unterstützende; eine Übermittlung an weitere Dritte seitens Qurasoft erfolgt nicht.

Die Gesundheitsanwendung ist in diesem Fall nicht auf das private IT-System des Nutzers beschränkt. Dies kann mit möglichen Sicherheitsrisiken einhergehen, die Qurasoft nicht vollständig adressieren kann.

Sie können die Telemedizin-Verbindung jederzeit beenden, indem Sie in den Einstellungen der App die direkte Verbindung abschalten. Dann ist die App nicht mehr mit dem myCoach -Analysesystem von Qurasoft verbunden und stattdessen wieder zum reinen Eigenmonitoring konfiguriert. Die Daten werden dann wieder ausschließlich auf Ihrem Gerät gespeichert (siehe 3.2.1).

Bereits übertragene Daten an telemedizinisch Unterstützende bleiben weiterhin in der Analysesoftware der telemedizinisch Unterstützenden bestehen.

Sofern der Anwender seine personenbezogenen Daten von unserem System löschen möchte, ist dies nur über und durch die telemedizinisch Unterstützenden möglich. Eine Löschung der personenbezogenen Daten des Anwenders vom Server von Qurasoft ist also ohne vorherige Kontaktaufnahme mit den telemedizinisch Unterstützenden ausdrücklich nicht möglich, um gegebenenfalls einen Verstoß gegen Aufbewahrungspflichten zu verhindern.

Sofern telemedizinisch Unterstützende personenbezogene Daten des Anwenders löschen möchte, ist dies nur mit ausdrücklicher Zustimmung des Anwenders möglich. Um über die Verarbeitung Ihrer persönlichen Daten innerhalb der myCoach -Analysesoftware für telemedizinisch Unterstützende Auskünfte und Löschaufträge erteilen zu können, wenden Sie sich also bitte an Ihre telemedizinisch Unterstützenden. Diese werden Ihnen im Rahmen ihrer berufsrechtlichen Befugnisse weiterhelfen.

## 2.3. Nutzung der myCoach -App im Eigenmonitoring

Zur Nutzung der App muss zu Beginn ein Benutzerkonto angelegt werden. Bei der Angabe des Nutzerkontosmüssen folgende Daten eingegeben werden:

- E-Mail-Adresse
- (Wunsch-) Passwort
- Mindestens 8 Zeichen / einen Kleinbuchstaben / einen Großbuchstaben / Spezialzeichen bzw. Zahl
- Einen Lizenz- oder Gerätecode

Dieser Code wird zu Lizenz- und Abrechnungszwecken benötigt und dient der Abrechnung, z.B. über die Krankenkassen.

Zur Fertigstellung des Registrierungsprozesses wird eine Kurznachricht (SMS) an die angegebene Mobilfunknummer gesandt. Nur wenn hier eine Bestätigung stattfindet, kann die App verwendet werden (2-Faktor-Authentifizierung). Anmeldungen geschehen künftig immer über die Kombination aus Benutzernamen, Passwort und dem neu zugesendeten Einmalcode.

## 2.4. PDF-Export Ihres Gesundheitstagebuches

Sowohl im Eigenmonitoring-, als auch im Telemedizin-Modus können Sie Ihre Messdaten in eine PDF-Datei exportieren und z.B. für einen Ausdruck verwenden. Erst wenn Sie Ihre Messungen als PDF-Datei auswerten und exportieren, werden für die Erzeugung der PDF notwendige Daten verschlüsselt an einen unserer in Deutschland befindlichen Server übertragen, dort die PDF erstellt und anschließend verschlüsselt zurück auf Ihr Gerät übertragen. Es werden keine (bzw. im Telemedizin-Modus: keine zusätzlichen) Daten auf den Servern gespeichert. Die PDF und alle im Bezug stehenden Daten werden direkt nach der Erstellung von den Servern der Qurasoft gelöscht.

Die Gesundheitsanwendung ist in diesem Fall nicht auf das private IT-System des Nutzers beschränkt. Dies kann mit möglichen Sicherheitsrisiken einhergehen, die Qurasoft nicht vollständig adressieren kann. Rechtsgrundlage der Übermittlung Ihrer personenbezogenen

Daten an unsere Server zum Zweck der Erstellung eines PDF-Gesundheitstagebuchs ist Ihre Einwilligung (Art. 9 Abs. 2 lit. a DSGVO).

2.5. Online-Backup

Sie haben die Möglichkeit ein Online-Backup durchzuführen. Dies erfolgt nur, wenn Sie darin eingewilligt haben (Art. 9 Abs.2 lit.a DSGVO). Das Backup wird mit einem von Ihnen erstellten Passwort verschlüsselt und dann auf unseren Servern gespeichert. Möchten Sie auf das Backup zurückgreifen, weil Sie z.B. Ihr Handy gewechselt haben, erhalten Sie das Backup durch die Eingabe Ihres Passworts.

2.6. Videosprechstunde

Sie haben die Möglichkeit eine Videosprechstunde mit Ihrem Coach durchzuführen. Dazu erhalten Sie per E-Mail den Zugangslink zur Videosprechstunde. Die Rechtsgrundlage für die notwendige Datenverarbeitung ist Ihre Teilnahmeerklärung (Art. 6 Abs.1 lit.b DSGVO). Die Datenschutzerklärung der SaniQ Videosprechstunde stellt ein eigenständiges Dokument dar. In der Datenschutzerklärung der Videosprechstunde werden ausführlich die Vorgänge der Datenverarbeitung im Kontext der myCoach Videosprechstunde erörtert.

2.7 Kontaktformular

Sofern Sie eine Frage an uns haben, können Sie eine Anfrage mittels des Kontaktformulars auf unserer Website stellen (https://qurasoft.de/kontakt). Die erforderlichen Daten werden dabei als Pflichtfelder gekennzeichnet. Bei Ihrer Kontaktaufnahme werden die von Ihnen mitgeteilten Daten (insbesondere Ihr Vor- und Nachname, Ihre E-Mail-Adresse und der Text Ihrer Anfrage sowie ggf. weitere Angaben) von uns gespeichert. Bei weitergehenden Angaben handelt es sich um eine freiwillige Auskunft. Die Verarbeitung erfolgt zwecks Bearbeitung der Anfragen auf Grundlage von Art. 6 Abs. 1 lit. b, f DSGVO.

Die im Rahmen Ihrer Kontaktaufnahme anfallenden Daten werden gelöscht, sobald diese für die Bearbeitung Ihrer Anfrage nicht mehr erforderlich sind.

## 4. Nutzung der App

1. Installation der App

Um die App herunterladen bzw. installieren zu können, müssen Sie gegebenenfalls zuvor mit einem Drittanbieter (derzeit Google und Apple) eine Nutzungsvereinbarung über den Zugang zu einem Portal oder Online-Shop des jeweiligen Drittanbieters (nachfolgend: „App-Store“ genannt) abschließen. Wir sind nicht Partei einer derartigen Vereinbarung und haben keinen Einfluss auf die Datenverarbeitung durch den Drittanbieter. Welche Daten auf welche Art und Weise und zu welchem Zweck der Drittanbieter im Rahmen der Registrierung im App-Store verarbeitet, entnehmen Sie bitte den Datenschutzerklärungen des jeweiligen Drittanbieters.

2. Protokollierung und Analyse der App-Verbindungen

2.1. Allgemeines

Wir protokollieren jede Verbindung der App und des myCoach -Analysesystems zu unseren Servern für statistische Zwecke, zu Sicherungszwecken sowie zur Fehlerbehebung. Zu diesem Zweck werden

Ihre

• IP-Adresse (gekürzt auf die letzten beiden Oktette, ohne Rückschlussmöglichkeit auf Ihre

Person),

• das Datum und die Uhrzeit Ihres Abrufs,

• die aufgerufenen App-Funktionen,

• die übertragene Datenmenge sowie

• der erfolgreiche Abruf in Protokolldateien (sog. Logfiles)

von uns jeweils für maximal 10 Wochen gespeichert. Es werden keine Gesundheitsdaten protokolliert. Rechtsgrundlage hier ist Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse). Unser berechtigtes Interesse an der Datenverarbeitung liegt dabei darin, das ordnungsgemäße Funktionieren unserer App sicherzustellen.

2.2. Token

Wir verwenden in der App sogenannte Token. Bei diesen handelt es sich in technischer Sicht um ein Äquivalent zu den bei Internetbrowsern üblichen Cookies; sie ermöglichen uns eine technische Zuordnung der Zugriffe der App. Diese Tokens setzen wir zu dem Zweck ein, Ihre Berechtigung zur Kommunikation mit unseren Servern zu überprüfen (z.B. bei der Erstellung des PDF-Datenexportes oder beim Abruf des Pollenfluges). Ihre IP-Adresse wird übertragen, aber direkt danach anonymisiert, indem die letzten beiden Oktette der IP-Adresse gekürzt werden. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO.

3. Weitere Funktionalitäten

3.1. Umgebungsinformationen

Wenn Sie der App über die Systemeinstellungen Ihres Geräts für bestimmte Angebote der App den Zugriff auf den Standort Ihres Endgeräts erlauben, verarbeiten wir sowohl beim Eigenmonitoring als auch im Telemedizin-Modus Ihre aktuellen Standortdaten (über GPS). Dies erfolgt nur mit Ihrer ausdrücklichen Einwilligung.

Auch diese Einwilligung kann widerrufen werden, in dem Sie die Einstellungen Ihres Smartphones entsprechend anpassen.

Daten zu Ihrem Standort werden ausschließlich für die Bearbeitung Ihrer Anfrage genutzt, etwa die Ermittlung des an Ihrem Standort vorhandenen Pollenflugs. Ein Bewegungsprofil wird nicht erstellt. Insgesamt ist der Bezug folgender Informationen am Standort zum Zeitpunkt der Messung möglich:

Pollenflug, Wetterinformationen und Luftbelastung. Soweit Sie den Standort-Zugriff verweigern, sind bestimmte Funktionen der App (z.B. der Pollenflug) nicht nutzbar. Dies wird auch innerhalb der App deutlich kommuniziert und kann jederzeit geändert werden. Ihr Standort wird nicht an Dritte weitergegeben.

3.2. Apple Health Kit

Sofern Sie die myCoach -App auf einem Smartphone der Marke Apple verwenden, können Sie auf Vitaldaten und persönliche Daten aus Apple Health Kit zugreifen. Dies erleichtert die Einrichtung von myCoach, da Sie bereits zuvor erfasste Daten (z.B. Name, Geburtsdatum, aber auch Messwerte) nicht erneut eingeben müssen bzw. direkt zur Verfügung stehen haben. Mit dem Zugriff auf Apple Health Kit werden nur die personenbezogenen Daten verarbeitet, die auch bei der Nutzung der myCoach -App von uns verarbeitet werden. Dies bedeutet, dass wir uns, nachdem Sie die Berechtigung dazu erteilt haben, vorhandener Daten zum Import in Ihre myCoach -App bedienen.

Rechtsgrundlage für diese Datenverarbeitung ist Ihre Einwilligung (Art. 9 Abs. 2 lit. a DSGVO). Die Einwilligung dieser Datenverarbeitung können Sie jederzeit in der Health-App von Apple widerrufen.

3.3. Benachrichtigungen

Sie haben die Möglichkeit, sich innerhalb der myCoach -App z.B. an notwendige Messungen, aber auch an die Beantwortung von Fragebögen oder Medikationseinnahmen erinnern zu lassen.

Im Eigenmonitoring-Modus werden die zur Benachrichtigung notwendigen Informationen auf Ihrem Gerät generiert und verlassen das Gerät zu keinem Zeitpunkt.

Im Telemedizin-Modus können Informationen, wie z.B. zu einem zu beantwortenden, neuen Fragebogen, nur vom myCoach -Analysesystem der telemedizinisch Unterstützenden ausgelöst werden. In diesem Falle werden keine personen- und krankheitsspezifischen Informationen übertragen, sondern lediglich der Hinweis, dass Sie eine neue Nachricht erhalten haben. Um den tatsächlichen Inhalt zu erfahren, ist es dann notwendig, die myCoach -App zu öffnen. Diese erhält dann die angefallene Information (z.B. einen neuen Fragebogen zur notwendigen Beantwortung), die auf Ihrem Gerät gespeichert und mittels einer gesicherten Verbindung mit dem myCoach Analysesystem für telemedizinisch Unterstützende ausgetauscht wird.

3.4. Datenverschlüsselung

Die von Ihnen erfassten Messwerte und Eingaben werden verschlüsselt auf Ihrem Gerät gespeichert und verlassen das Gerät im Eigenmonitoring nicht. Sofern eine telemedizinische Kopplung (an myCoach-Software) durchgeführt wurde, werden die Daten, nach vorheriger Zustimmung, verschlüsselt an den telemedizinisch Unterstützenden gesendet. Die Verschlüsselung erfolgt unter Einsatz eines anerkannten Verschlüsselungsverfahrens.

Erhobene Messdaten werden in der myCoach -App lokal und inhaltsverschlüsselt abgespeichert (es besteht eine sogenannte Content-Verschlüsselung). Die verwendete symmetrische Verschlüsselungsmethodik basiert auf dem Standard AES-256 und zeichnet sich durch hohe technische Sicherheit aus. In der App wird ein Zufallsschlüssel generiert und angezeigt, der die Grundlage sowohl für die lokale als auch für die Sicherungsverschlüsselung ist. Der Schlüssel ist einmalig. Eine Wiederherstellung einer Datensicherung, z.B. nach dem Wechsel des Smartphones, ist nur damit möglich. Zugang zu den Daten erfolgt nur über die entsprechende myCoach -App.

Bei der Datenübertragung zum Server wird folgende Transportverschlüsselung angewandt: TLS 1.2 unter Verwendung von SHA256 mit RSA als Signieralgorithmus. Zudem liegen die Daten auch inhaltsverschlüsselt in der Datenbank ab.

Das verwendete Protokoll basiert auf einer Ende-zu-Ende-Verschlüsselung, bei der die Informationen bereits vor dem Versenden verschlüsselt und erst beim Empfänger entschlüsselt werden. Somit authentifiziert das Protokoll den Kommunikationspartner und stellt die Integrität der transportierten Daten sicher. Die Authentifizierung geschieht mittels digitalen Zertifikats, das alle benötigten Informationen, zur Prüfung der Authentizität und Sicherstellung der Integrität, enthält.

## 5. Widerruf, Berichtigung, Sperrung & Löschung

Uns gegenüber erteilten Einwilligungen können jederzeit mit Wirkung für die Zukunft widerrufen werden.

Möchten Sie die App löschen aber Ihre Messdaten behalten, dann speichern Sie sich diese bitte mit einem PDF-Export ab.

Der Widerruf einer Einwilligung im Telemedizin-Modus ist für Qurasoft der Auftrag, keine personenbezogenen Daten mehr an Ihren telemedizinisch Unterstützenden zu übertragen und Ihre Kopplung zum myCoach -Analysesystem der telemedizinisch Unterstützenden zu lösen.

Die Löschung Ihrer Daten aus dem myCoach -Analysesystem kann nur von den telemedizinisch Unterstützenden durchgeführt werden. Bitte beachten Sie, dass diese Aufforderung zur Löschung an die telemedizinisch Unterstützenden gerichtet werden muss und dort im Rahmen berufsrechtlicher Vorgaben durchgeführt wird. Bitte beachten Sie weiterhin, dass einer Löschung rechtliche Aufbewahrungspflichten entgegenstehen können.

Außerdem haben Sie bei Vorliegen der rechtlichen Voraussetzungen die Möglichkeit zum Widerspruch gegen die Datenverarbeitung, und das Recht auf Berichtigung und Sperrung/Einschränkung der Verarbeitung der von Ihnen erhobenen und verarbeiteten persönlichen Daten sowie das Recht auf Datenübertragbarkeit (derzeit: PDF-Format, s.o.). Wie soeben ausgeführt, müssen Sie sich bei Nutzung des myCoach -Software-Analysesystems aber mit einer Löschaufforderung in jedem Fall an die telemedizinisch Unterstützenden wenden.

Wir weisen darauf hin, dass die Datenübertragung im Internet (z.B. bei der Kommunikation per E-Mail oder über das Mobilfunknetz) sowie mittels Bluetooth Sicherheitslücken aufweisen kann. Ein lückenloser Schutz der Daten vor dem Zugriff durch Dritte ist nicht möglich. Im Falle der Nutzung unserer App beachten Sie bitte zusätzlich die Datenschutzhinweise des jeweiligen App-Stores, vgl. Ziff. 2.1.

## 6. Auskunftsrecht

Sie können jederzeit unentgeltlich Auskunft über die von uns über Sie gespeicherten personenbezogenen Daten, deren Herkunft und Empfänger sowie den Zweck der Datenverarbeitung verlangen. Dazu können Sie sich insbesondere per E-Mail an datenschutz@qurasoft.de wenden.

## 7. Fragen, Anregungen, Beschwerden

Sie können die Datenschutzerklärung innerhalb der App jederzeit aufrufen unter dem Hauptmenü „Mehr“-> „Datenschutzinformationen anzeigen“.

Wenn Sie weitergehende Fragen, Anregungen oder Beschwerden zu unseren Hinweisen zum Datenschutz und zur Verarbeitung Ihrer persönlichen Daten haben, können Sie sich direkt an uns unter datenschutz@qurasoft.de wenden.

Sie haben außerdem unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer (Datenschutz-) Aufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen deutsches oder europäisches Datenschutzrecht verstößt.

## 8. Links

Unsere Angebote können Links zu Internetseiten anderer Anbieter enthalten, auf die sich diese Hinweise zum Datenschutz nicht erstrecken. Wenn Sie diese Links anklicken, haben wir keinen Einfluss darauf, welche Daten durch diese Drittanbieter erhoben und verarbeitet werden.

## 9. Änderung der Datenschutzerklärung

Wir behalten uns das Recht vor, unsere Sicherheits- und Datenschutzmaßnahmen zu verändern, soweit dies wegen der technischen Entwicklung erforderlich wird. In diesen Fällen werden wir –soweit erforderlich – auch unsere Datenschutzerklärung anpassen und Sie hierüber umgehend innerhalb der myCoach -App informieren.

# Datenschutzhinweise KKH-Gesundheitsberatung: myCoach-Löschkonzept

**Dokumentinformation**

- ID: DOC-PRIVACY-2
- Version: 1
- gültig ab: 01.10.2023
- gültig bis: /
- Geltungsbereich: Qurasoft

**Autorinformation**

- Name: Artur Schens
- Funktion: Geschäftsführer – OU Operations
- Freigabe durch: Artur Schens

**Historie**

- Version: 1
- Datum: 03.11.2023
- Änderung: Überführung in ein gelenktes Dokument. Harmonisierung mit dem ITP-Löschkonzept
- Autor: Tina Conrad

## 1.Pflicht zur Datenlöschung (Grundsatz)

Personenbezogene Daten dürfen nur so lange gespeichert und verarbeitet werden, wie sie für den jeweils definierten Zweck benötigt werden. Wenn der Zweck nicht (mehr) besteht, müssen sie gelöscht werden, sofern dieser Löschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. Eine unbegrenzte Aufbewahrung ist nichtzulässig. Im Übrigen gilt:

• Für alle Kategorien von personenbezogenen Daten sind Aufbewahrungsfristen von vorneherein von uns festzulegen (gem. Art. 30 Abs. 1 Buchst. f DSGVO).

• Wenn ein Gesetz eine Aufbewahrungsfrist definiert, darf erst nach deren Ablauf gelöscht werden.

## 2.Löschfristen in Abhängigkeit von eigenen Zwecken und gesetzlichen Vorschriften

Wir löschen personenbezogene Daten, wenn wir sie für unsere eigenen Zwecke nicht mehr benötigen und keine gesetzlichen Vorgaben entgegenstehen (vgl. unten Nr. 9). Unsere konkreten Löschfristen dokumentieren wir in der Übersicht der Verarbeitungstätigkeiten (s. Anlage).

## 3.Übergangsfrist zur endgültigen Löschung

Nach Ablauf der Löschfrist bis zur Durchführung der Löschung dürfen in der Regel nicht mehr als 6 Monate vergehen. (Beispiele: Wirtschaftsprüfer sind am Jahresanfang da; in der Aktenvernichtung ist gerade in den ersten Monaten eines neuen Jahres viel zu tun – externe Kunden haben Vorrang). Hierzu sind individuelle, turnusmäßige Löschzeiten festgelegt, siehe 7. Interne Vorgaben.

## 4.Durchführung der Löschung

Daten werden, je nach Datenträger gem. DIN 66399 folgendermaßen gelöscht bzw. vernichtet:

- Papier: z.B. vorzugsweise über die Entsorgungstonne des Dienstleisters Sicherheitsstufe 5 respektive nach gesetzlichen Anforderungen gemäß der Abschnitte 12 bis 14,oder
- digitale Datenträger (z.B. Festplatte, USB-Stick): ausschließlich über die Sicherheitsstufe 5, siehe Abschnitt 13.

## 5. Prozessuales Vorgehen zur Umsetzung der Löschung

a. Erfassen der personenbezogenen Daten

Für jede Abteilung werden die personenbezogenen Daten erfasst, die dort verarbeitet werden, notiert wird dabei:

- Art der Daten
- Die durchschnittliche Verweildauer in Bearbeitung
- Ob und wie lange die Daten aufbewahrungspflichtig sind
- Ob es sich um besondere personenbezogene Daten handelt
- Auf welchem Datenträger diese gespeichert werden.

Diese Informationen werden im Verzeichnis von Verarbeitungstätigkeiten hinterlegt, siehe Anhang DaMS.

b. Gruppieren der Datenarten

Die Daten, die dem gleichen Zweck dienen, werden zusammengefasst, wenn sie die gleiche Aufbewahrungsdauer aufweisen und / oder ob es sich um besondere personenbezogene Daten handelt. Zusätzlich werden Gruppen für Daten gebildet, die mittels Auftragsdatenverarbeitung verarbeitet werden.

c. Löschklassen bilden

Aus einem noch abstrakten Startdatum und der Bearbeitungszeit plus Aufbewahrungsfrist werden Löschklassen gebildet; es wird dabei versucht, die Anzahl der Löschklassen möglichst gering zu halten.

d. Löschregeln bilden

Mit der Einordnung der Datensätze in die Löschklassen ergibt sich jeweils ein konkretes Startdatum und auch damit ein konkretes Datum, ab wann der Datensatz zu löschen ist. Das ist die auf den Datensatz anwendbare Löschregel.

e. Überführung von Daten in die Archivierung

Es wird idealerweise bereits zu diesem Zeitpunkt festgelegt, wann und wie lange die Daten archiviert werden und wann diese entsprechend auch aus dem Archiv zu löschen sind.

f. Sonderfälle vorsehen

Wenn ein Betroffener es wünscht, oder sich herausstellt, dass ein Datensatz nicht gesetzeskonform erhoben wurde, kann es sein, dass außerhalb der Regel ein Datensatz gelöscht werden muss.

Zur Vorgehensweise: Es wird ein Datenschutzteam einberufen, bestehend aus verantwortlichem Bereich sowie Datenschutzbeauftragter. Dieses Team stellt fest, an welchen Stellen personenbezogene Daten gespeichert sind, und bearbeitet den Vorgang innerhalb von 4 Wochen. Die ggf. anstehende Löschung wird entweder systemisch oder organisatorisch nach dem 4-Augen-Prinzip protokolliert.

g. Löschprozesse einrichten

Es werden regelmäßige „Löschläufe“ vorgesehen, die automatisch gestartet werden, die Löschvorgänge mitprotokollieren und wenn Fehler auftreten, eine entsprechende Meldung an einen Mitarbeiter weitergeben.

Im Falle von Fehlern wird der tangierte Bereich/Abteilung benachrichtigt. Die Löschprotokolle sind von den jeweiligen Bereichen/Abteilungen sicher aufzubewahren. Ein Löschvorgang im Sonderfall wird nach 5. f. protokolliert, so dass dem Betroffenen oder der Aufsichtsbehörde beleget werden kann, dass die Daten gelöscht wurden.

h. Auftragsdatenverarbeitung prüfen

Wenn Daten zur Auftragsverarbeitung herausgeben werden, sind die Verträge hinsichtlich des Aspektes, ob dort schon Klauseln zur Löschung enthalten sind, zu prüfen. Gegebenenfalls müssen die Verträge angepasst werden.

Um dem Auftragnehmer eine angemessene Frist setzen zu können, ist zu überprüfen, wie lange im Betrieb gebraucht wird, empfangene Daten zu prüfen. Vom Auftragnehmer wird ein Beleg über die Löschung (Löschprotokoll) verlangt.

## 6. Protokollierung

Jede ordnungsgemäße Vernichtung wird dokumentiert. Daraus muss hervorgehen, wer was wann gelöscht/vernichtet hat. Diese Protokolle werden für 3 Jahre, ggf. für unterschiedliche Datenarten unterschiedliche Zeitpunkte bestimmen aufbewahrt.

## 7. Interne Vorgaben

Folgende internen Vorschriften sind für den gesamten Geltungsbereich verbindlich:

I. Es wird folgendes Löschintervall festgelegt: **März eines jeden Jahres/Jahresende.**
II. Falls keine Aufbewahrungsfristen für Dokument- oder Datenarten festgelegt werden können, weil bspw. keiner gesetzlichen oder anderweitigen Regelung oder Vorgabe Dritter zuordenbar, so wird nach interner Richtlinie gemäß gelistetem Anhang vorgegangen.

## 8. Verantwortlichkeit

Die Geschäftsführung und die Organisationseinheit Operations – Team Compliance ist dafür verantwortlich, dass jegliche Dokumente gemäß den nachstehend genannten Vorgaben gelöscht (d.h. für die Definition der Löschfristen, deren Einhaltung und tatsächlicher Durchführung), verwahrt und verwaltet werden.

Dateieigentümer ist der Leiter derjenigen Abteilung, welche hauptverantwortlich ist für die Speicherung und Verarbeitung der jeweiligen personenbezogenen Daten.

## 9.Gesetzliche Aufbewahrungsfristen

Das Team Compliance in der Organisationseinheit Operations sind über die in ihrem Bereich einschlägigen gesetzlichen Aufbewahrungsfristen entsprechend der §§ 257 HGB und 147 AO informiert. Sie definieren auf Basis dieser Informationen angemessene Löschfristen für die von Qurasoft durchgeführten Verarbeitungstätigkeiten und dokumentieren sie in der Übersicht der Verarbeitungstätigkeiten, sofern aufgrund der Komplexität eine andere Darstellung wie bspw. einen Matrizen-Übersicht nicht sinnvoller erscheint. Als Hilfestellung dient eine im Anhang befindliche Übersicht über wichtige gesetzliche Aufbewahrungsfristen.

Für weitere Informationen zu diesen Fristen, ist das Team Compliance zu kontaktieren

### 9.1 Beginn der Aufbewahrungsfrist

Der Beginn der Aufbewahrungsfrist richtet sich nach den Vorgaben der nationalen Gesetzgebung.

Alle Dokumente die weniger als ein Jahr aufzubewahren sind, beginnt die Aufbewahrungsfrist mit Abschluss der Geschäftsvorfalls.

Soweit für einzelne Vorgänge Kompetenzen, Kontrollen, Unterschriften etc. und deren Dokumentation verlangt werden, ist immer eine bildliche Archivierung vorzunehmen, soweit durch die inhaltliche Aufbewahrungsform nicht die geforderte Dokumentation sicherzustellen ist.

Die Aufbewahrungsfrist für Verträge oder vertragsähnliche Dokumente hat mit Beendigung des Vertrages bzw. Vorgangs zu beginnen.

Sind die oben festgelegten Mindestaufbewahrungsfristen sowie die sich anschließende Löschung bzw. Sperrung der Dokumente derzeit aus technischen Gründen nicht einzuhalten, sind die Mindestaufbewahrungsfristen sowie die Löschung bzw. Sperrung bei einem Systemwechsel zwingend zu berücksichtigen.

Sollte der für die Dokumente verantwortliche Bereich trotz eines Systemwechsel davon abweichen, ist vorab die Genehmigung der Geschäftsführung einzuholen.

### 9.2 Nach Ablauf der Aufbewahrungsfristen

Dokumente, welche einer Aufbewahrungspflicht unterliegen und die Mindestaufbewahrungsfrist bzw. Aufbewahrungsfrist erreicht ist, sind zu löschen.

Anstelle der Löschung tritt die Sperrung des Zugriffs auf die einzelnen Dokumente, wenn der Aufwand der Löschung unverhältnismäßig hoch ist.

Vor Einsatz der Sperre anstelle der Löschung, ist der Datenschutzbeauftragte des Unternehmens zu kontaktieren.

## 10.Aufbewahrungsformen

### 10.1. Aufbewahrungsform „inhaltlich“

Die Aufbewahrungsform „inhaltlich (1)“ bedeutet, dass nicht zwingend das Dokument aufbewahrt werden muss, sondern es ausreichend ist, den Inhalt eines einmal erstellten Dokuments bis zum Ende der Aufbewahrungsfrist jederzeit wiederherstellen zu können.

### 10.2. Aufbewahrungsform „bildlich“

Die Aufbewahrungsform „bildlich (2)“ bedeutet, dass ein einmal erstelltes Dokument digital - mittels digitaler Erfassung (scannen) oder per direkter Übertragung in die digitale Ablage - aufzubewahren ist. Die Aufbewahrungsform „inhaltlich“ ist dabei ausgeschlossen.

#### 10.2.1. Anmerkung(en)

Sollte es kostengünstiger sein, Dokumente, welche grundsätzlich einer niedrigeren Aufbewahrungsform unterliegen (inhaltlich -> bildlich -> Original), in einer höheren Form aufzubewahren, kann dies jederzeit vorgenommen werden.

Ausnahmen hiervon stellen beispielsweise die Vorgaben der Grundsätze der Prüfbarkeit digitaler Unterlagen dar.

Bei Dokumenten mit steuerlich relevantem Inhalt, soweit diese originär digital sind, sind auch die Inhalts- und Formatierungsdaten auf einem maschinell auswertbaren Datenträger aufzubewahren.

Diese Regelung gilt für alle Geschäftspartner, welche der Buchführungs- und Aufzeichnungspflicht unterliegen (GoB).

### 10.3. Aufbewahrungsform „Original“

Die Aufbewahrungsform „Original (3)“ bedeutet, dass einmal erstellte Dokumente in Papierform aufzubewahren sind.

Eine parallele Sicherung des Dokuments kann digital, unter Berücksichtigung des Schutzbedarfes, erfolgen.

### 10.4. Generelle Aufbewahrungsform

Generell ist die digitale Form als Aufbewahrungsform anzuwenden. Siehe hierzu Punkt 10.2. Aufbewahrungsform „bildlich“.

#### 10.4.1. Speicherung von analogen Dokumenten mittels scannen

Analoge Dokumente sind im Anschluss an den Scanvorgang auf digitalen Datenträgern zu archivieren.

### 10.4.2. Speicherung von originären digitalen Dokumenten

Originär digitale Dokumente müssen, soweit eine inhaltliche Speicherung zulässig ist, durch Übertragung der Inhalts- und Formatierungsdaten auf einen digitalen Datenträger archiviert werden.

Bei originär digitalen Dokumenten muss technisch sichergestellt sein, dass während des Übertragungsvorgangs auf das Speichermedium eine Bearbeitung nicht möglich ist. Die Indexierung hat wie bei gescannten Dokumenten zu erfolgen.

Das so archivierte digitale Dokument darf nur unter dem zugeteilten Index bearbeitbar und verwaltbar sein.

Die Bearbeitungsvorgänge sind zu protokollieren und mit dem Dokument zu speichern. Das bearbeitete Dokument ist als “Kopie” zu kennzeichnen. Die gespeicherten Dokumente müssen während der gesamten Aufbewahrungsfrist jederzeit reproduzierbar sein.

### 10.5. Bildliche Wiedergabe

Bei der Speicherung auf Datenträgern ist bei bestimmten Unterlagen sicherzustellen, dass die Wiedergabe mit der Originalunterlage bildlich übereinstimmt.

Der Verzicht auf einen herkömmlichen Beleg darf die Möglichkeit der Prüfung des betreffenden Buchungsvorgangs in formeller und sachlicher Hinsicht nicht beeinträchtigen.

Der Erhalt der Verknüpfung zwischen Index, digitalem Dokument und Datenträger muss während der gesamten Aufbewahrungsfrist gewährleistet sein.

Die Originalunterlagen dürfen darüber hinaus nur vernichtet werden, soweit sie nicht nach anderen Rechtsvorschriften im Original aufbewahrt werden müssen.

Im Allgemeinen sind beleghafte Dokumente in geeigneter Form aufzubewahren. Insbesondere sind die Vorschriften zum Brandschutz zu beachten.

## 11. Recht auf Löschung durch Betroffenen

Personen, deren Daten von uns gespeichert werden, haben unter Umständen ein Recht auf Löschung nach Art. 17 DSGVO. Insbesondere gilt:

- Verantwortung: Verantwortlich für die Beantwortung des Löschungsbegehrens und dessen Durchführung ist der jeweilige Dateneigentümer (s.o.).

- Frist: Sollten Behandler*innen ihren Benutzeraccount widerrufen, wird das Benutzerkonto sowie die Daten unverzüglich nach Eingang des Widerrufs innerhalb von 10 Werktagen gelöscht, sofern dem keine rechtliche Verpflichtungen gegenüberstehen. Das Ergebnis der Löschung muss dem Antragsteller zudem spätestens innerhalb eines Monats mitgeteilt werden. (Ausnahmen von dieser Vorgehensweise sollten mit unserem Datenschutzbeauftragten abgestimmt werden).

- Löschung: Wenn der Betroffene die Löschung seiner Daten wünscht, muss dem nachgekommen werden, wenn einer dieser Fälle vorliegt:

    - seine Daten sind mittlerweile nicht mehr notwendig (weil die Zwecke entfallen sind und auch keine gesetzlichen Aufbewahrungsfristen bestehen)

    - seine Daten wurden unrechtmäßig verarbeitet

o der Betroffene hat seine Einwilligung widerrufen (sofern seine Einwilligung die Rechtsgrundlage für die Verarbeitung war)

o der Betroffene hat Widerspruch eingelegt (sofern sich unsere Datenverarbeitung auf die Rechtsgrundlage der „berechtigten Interessen“ stützt und der Fall durch den Datenschutz-beauftragten geprüft wurde)

o der Betroffene hat Widerspruch gegen Direktwerbungeingelegt

▪ Keine Löschung: Eine Löschung ist ausnahmsweise nicht erforderlich, wenn die Daten nicht in der IT gespeichert sind (z.B. Papierakten, Mikrofiche und die Löschung nur mit unverhältnismäßig hohem Aufwand möglich wäre und das Löschungsinteresse als gering anzusehen ist. Anstelle einer Löschung müssen die Daten dann als „eingeschränkt für die Verarbeitung“ markiert werden, (§ 35 BDSG n.F.).

▪ Wenn Daten zuvor veröffentlicht, wurden: In diesem Fall müssen darüber hinaus angemessene Maßnahmen getroffen werden, um andere Datenverarbeiter über die Löschung zu informieren (Art. 17 Abs. 2DSGVO).

## 12. Aufbau eines datenschutzkonformen Löschkonzepts

Die Erfassung der personenbezogenen Daten samt Löschfristen erfolgt gemäß Abschnitt 9. Die Daten werden automatisiert gelöscht, sofern dies systemisch möglich ist. Andernfalls erfolgt die Löschung manuell gemäß Abschnitt 7.

## 13. Ermittlung des Schutzbedarfs und Zuordnung der Schutzklasse

Um bei der Datenträgervernichtung dem Wirtschaftlichkeits- bzw. Angemessenheitsprinzip Rechnung zu tragen, ist es notwendig, die Daten in Schutzklassen einzuteilen. Dabei ist der Grad der Schutzbedürftigkeit ausschlaggebend für die zu treffende Wahl der Sicherheitsstufe in Bezug auf die Vernichtung der Datenträger.

Schutzklasse 1

Normaler Schutzbedarf für interne Daten:

▪ Gebräuchlichste Einstufung von Informationen und für größere Gruppen bestimmt.

▪ Unberechtigte Offenlegung oder Weitergabe hätte begrenzte negative Auswirkungen auf das Unternehmen.

▪ Der Schutz von personenbezogenen Daten muss gewährleistet sein. Andernfalls besteht die Gefahr, dass der Betroffene in seiner Stellung und in seinen wirtschaftlichen Verhältnissen beeinträchtigt wird.

Schutzklasse 2

Hoher Schutzbedarf für vertrauliche Daten:

▪ Beschränkung der Informationen auf kleinen Personenkreis erforderlich.

▪ Eine unberechtigte Weitergabe hätte erhebliche Auswirkungen auf das Unternehmen und könnte gegen vertragliche Verpflichtungen oder Gesetze verstoßen.

▪ Der Schutz personenbezogener Daten muss hohen Anforderungen genügen. Andernfalls besteht die Gefahr, dass der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt wird.

Schutzklasse 3

Sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten:

▪ Beschränkung der Informationen auf sehr kleinen, namentlich bekannten Kreis von Zugriffsberechtigten erforderlich.

▪ Eine unberechtigte Weitergabe hätte ernsthafte (existenzbedrohende) Auswirkungen auf das Unternehmen und/oder würde gegen Berufsgeheimnisse, Verträge und Gesetze verstoßen. DOC-PRIVACY-8 Version 1 11 Stand: 01.10.2023

▪ Der Schutz personenbezogener Daten muss unbedingt gewährleistet sein. Andernfalls kann es zu einer Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen kommen.

## 14. Sicherheitsstufen für Datenträger

Tabelle 1 stellt die verschiedenen Sicherheitsstufen für Datenträger dar.

| Sicherheitsstufe | Erläuterung |
|---|---|
| 1 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten ohne besondere Hilfsmittel und Fachkenntnisse, jedoch nicht ohne besonderen Zeitaufwand möglich ist<br><br>*Empfohlen z. B. für Datenträger mit allgemeinen Daten, die unlesbar gemacht werden sollen.* |
| 2 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nur mit Hilfsmitteln und besonderem Aufwand möglich ist<br><br>*Empfohlen z. B. für Datenträger mit internen Daten, die unlesbar gemacht werden sollen.* |
| 3 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter erheblichem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist<br><br>*Empfohlen z. B. für Datenträger mit sensiblen und vertraulichen Daten.* |
| 4 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter außergewöhnlich hohem Aufwand (Personen, Hilfsmittel, Zeit) möglich ist<br><br>*Empfohlen z. B. für Datenträger mit besonders sensiblen und vertraulichen Daten.* |
| 5 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nur unter Verwendung gewerbeunüblicher Einrichtungen bzw. Sonderkonstruktionen, sowie forensische Methoden, möglich ist<br><br>*Empfohlen z. B. für Datenträger mit geheim zu haltenden Daten* |
| 6 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nach dem Stand der Technik unmöglich ist<br><br>*Empfohlen z. B. für Datenträger mit geheim zu haltenden Daten, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind.* |
| 7 | **Datenträgervernichtung** derart, dass die Reproduktion der auf ihnen wiedergegebenen Daten nach dem Stand von Wissenschaft und Technik unmöglich ist<br><br>*Empfohlen für Datenträger mit streng geheim zu haltenden Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind.* |

### 14.1 Auswahl der Sicherheitsstufe

Fallen Datenträger unterschiedlicher Sicherheitsstufen an der Anfallstelle an, so ist aus ökologischen und ökonomischen Gründen die Trennung in die verschiedenen Sicherheitsstufen an der Anfallstelle empfohlen. Ist dies nicht möglich, so muss eine Vernichtung grundsätzlich und einheitlich gemäß der höheren Sicherheitsstufe erfolgen, um das Risiko einer unzureichenden Vernichtung von Datenträgern mit sensiblen Daten durch eine fehlerhafte Zuordnung zu minimieren.

Bei der Wahl der geeigneten Sicherheitsstufe ist die Speicherdichte und/oder die Größe der Informationsdarstellung auf dem Datenträger zu berücksichtigen. Wenn Farbe oder andere Eigenschaften des Datenträgers eine Rekonstruktion erleichtern, sollte gegebenenfalls eine höhere Sicherheitsstufe gewählt werden.

### 14.2 Beeinflussung der Sicherheitsstufe

Vermischen und Verpressen der vernichteten Datenträger erschwert die Reproduktion. Eine Beeinflussung des möglichen Informationsgehaltes einzelner Materialteilchen erfolgt hierdurch nicht.

Für Datenträger mit Informationsdarstellung in Originalgröße oder Informationsdarstellung verkleinert, die in der Sicherheitsstufe eins, zwei oder drei vernichtet wurden, kann durch Vermischen und Verpressen, einmal die nächsthöhere, jedoch maximal die Sicherheitsstufe vier, Anwendung finden.

Die Erhöhung der Sicherheitsstufe muss durch die Verantwortliche Stelle bestimmt werden, sofern das Schutzniveau und die geltenden Vorschriften es zulassen.

Hierzu ist eine Mindestmenge von 100 kg an Datenträgern erforderlich, die in einem Durchgang ununterbrochen in der Maschine oder Einrichtung vernichtet werden muss.

Die Sicherheitsstufe der Maschine und wie diese gewährleistet wird, ist dabei offen und deutlich anzuzeigen.

Ist die Möglichkeit gegeben, die Datenträger jederzeit direkt vor Ort durch den jeweils Verantwortlichen der Daten zu vernichten, so erhöht dies die Sicherheit und ist anderen Verfahren vorzuziehen, sofern die ausgewählte Sicherheitsstufe verwendet wird.

## 15. Zuordnung von Schutzklassen und Sicherheitsstufen

Die Zuordnung der drei Schutzklassen zu den Sicherheitsstufen kann mit Tabelle 2 vorgenommen werden, sollte aber je Einzelfall in einer Risikoanalyse ermittelt werden.

| Schutzklasse | Sicherheitsstufe n | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | x[a] | x[a] | x | | | | |
| 2 | | | x | x | x | | |
| 3 | | | | x | x | x | x |

[a] für personenbezogene Daten ist diese Kombination nicht anwendbar.

Tabelle 2 – Zuordnung Sicherheitsstufen und Schutzklassen

## 16. Wann müssen Daten vernichtet werden?

| | |
|---|---|
| Datenträger und Papierunterlagen, die personenbezogene Daten enthalten, müssen vernichtet werden, wenn sie nicht mehr für den ursprünglichen Zweck verwendet werden. Eine längere Aufbewahrung darf nur erfolgen, wenn Gesetze oder Rechtsvorschriften dies fordern. | |
| 1. | **Ist der Zweck der Daten entfallen?**<br>Es kommt maßgeblich auf den ursprünglichen Zweck an: Ist er entfallen? Beispiel: Kundendaten sind nicht mehr erforderlich, weil der Vertrag gekündigt wurde.<br>Hinweis: Eine Vorratshaltung für andere denkbare Zwecke ist nicht zulässig. |
| | Nein:<br>Die Daten sind im eigenen Interesse länger aufzubewahren<br><br>Ja:<br>Prüfen Sie weiter<br>⬇ |
| 2. | **Liegt eine gesetzliche Aufbewahrungspflicht vor?**<br>Prüfen Sie, ob in einem Gesetz oder einer Rechtsvorschrift eine Mindestaufbewahrungsdauer vorgeschrieben ist. Die Anlage enthält einige typische Fristen. |
| | Nein:<br>Die Daten müssen kurzfristig vernichtet werden.<br><br>Ja:<br>Prüfen Sie weiter<br>⬇ |
| 3. | **Wann läuft die Aufbewahrungspflicht aus?**<br>Die Aufbewahrungsfrist ist in der Regel in Jahren angegeben.<br>- Start der Frist: mit der Beendigung des Vertrags/Vorgangs<br>- Ende der Frist: Im Jahr des Ablaufs der Frist, und zwar generell am 31.12. |
| | Frist ist abgelaufen<br>Die Daten müssen kurzfristig vernichtet werden.<br><br>Frist ist nicht abgelaufen<br>Die Daten müssen bis zum Ende der Frist weiter aufbewahrt werden. |

## 17. Geltungsbereich

Der Geltungsbereich dieser Richtlinie erstreckt sich vollumfänglich und verpflichtend auf die Organisation der Qurasoft GmbH und damit auch auf alle Mitarbeiter und Mitarbeiterinnen und der mit ihr verbundenen Bereiche und Standorte.

Sie gilt ohne zeitliche und örtliche Einschränkungen. Dritte sind in den jeweils relevanten Punkten zu verpflichten.

# Anlage 1

| Bezeichnung (alphabetisch sortiert) | (gesetzl.) Aufbewahrungs-frist (in Jahren) |
|---|---|
| Abmahnungen von Arbeitnehmern | nicht festgelegt; spätestens beim Ausscheiden |
| Abtretungsunterlagen (Zessionen) | 6 |
| An-, Ab- und Ummeldungen der AOK und Ersatzkassen | 6 |
| Anträge auf Arbeitnehmersparzulage | 6 |
| Anwesenheitsliste (z.B. Stempelkarten), soweit für Lohnbuchhaltung erforderlich | 10 |
| Arbeitsunfähigkeitsbescheinigungen (bei Auswirkung auf Lohn) | 10 |
| Arbeitsunfähigkeitsbescheinigungen (ohne Auswirkung auf Lohn) | 1 - 3 |
| Bankauszüge, Bankbelege | 10 |
| Beitragsabrechnungen zur Sozialversicherung | 10 |
| Belege, Sammelbelege, Beleglisten soweit Buchungsunterlagen | 10 |
| Bewerbungen | 6 Monate nach Ablehnung |
| Bewirtungsunterlagen | 10 |
| Bürgschaftsinformationen (nach Vertragsende) | 6 |
| Darlehensunterlagen | 10 |
| Dauerauftragsunterlagen | 6 |
| Debitorenbuchhaltung | 10 |
| E-Mail mit steuerrelevantem Inhalt | 10 |
| Essenmarkenabrechnungen | 10 |
| Fahrtkostenerstattungsunterlagen | 10 |
| Gehaltslisten | 10 |
| Geschäftsbriefe | 6 |
| Geschenknachweise | 10 |
| Inkassobücher, -karteien, -quittungen | 10 |
| Jahreslohnnachweise für Berufsgenossenschaften | 10 |
| Kontoauszüge | 10 |
| Kreditorenbuchhaltung | 10 |
| Lastschriftanzeigen | 10 |
| Lohnkontenarten | 10 |
| Lohnlisten | 10 |
| Lohnsteuer-Jahresausgleichsunterlagen | 10 |
| Mahnvorgänge | 6 |
| Mietverträge (nach Vertragsende) | 6 |
| Offenbarungseidanträge | 6 |
| Pachtverträge (nach Vertragsende) | 6 |
| Patientenakten (Krankengeschichte), ambulant und stationär | 10 - 30 |
| Pensionskassenunterlagen | 10 |
| Personalunterlagen | 6 |
| Pfändungsunterlagen | 10 |
| Prämienunterlagen (z.B. Versicherung), soweit Buchungsunterlagen | 10 |
| Provisionsabrechnungen mit Unterlagen | 10 |
| Quittungen, wenn Buchungsunterlagen | 10 |
| Rechnungen und -unterlagen | 10 |
| Rechtsstreitfälle mit allen Unterlagen, Klageakten (nach Verfahrensabschluss) | 6 |

| Bezeichnung (alphabetisch sortiert) | gesetzl. Aufbewahrungs-frist (in Jahren) |
|---|---|
| Reisekostenabrechnungen | 10 |
| Schriftwechsel (auch innerbetrieblich) | 6 |
| Sozialversicherungsunterlagen | 6 |
| Spendenbescheinigungen | 10 |
| Strahlenschutz-Anwendungen (Aufzeichnungen) | 30 |
| Strahlenschutz-Anwendungen (Röntgenbilder) | 10 |
| Strahlenschutz-Belehrungen (RÖV) | 30 |
| Strahlenschutz-Gesundheitsakte (RÖV) | 30 |
| Strahlenschutz-Messergebnisse (RÖV) | 30 |
| Telefonkostennachweise | 10 |
| Überstundenlisten (nicht buchhaltungsrelevant) | 2 |
| Überstundenlisten (buchhaltungsrelevant) | 10 |
| Urlaubsanträge | 0 (Vernichtung nach Abschluss des |
| Urlaubsgenehmigung (soweit buchungsrelevant z.B. wg. | Vorgangs 10 |
| Urlaubsgeld) Verträge | 6 nach Vertragsende |

# Anlage 2

## Gesetzliche Aufbewahrungsfristen

Die Tabelle enthält einen Überblick über einige der wichtigsten gesetzlichen Aufbewahrungsfristen in Deutschland. Jahresfristen enden immer zum Ende des letzten Kalenderjahres.

| Art der Unterlagen | Aufbewahrungsdauer | Rechtsgrundlage |
|---|---|---|
| **Arbeitnehmerüberlassung – Geschäftsunterlagen des Verleihers** | 3 Jahre | § 7 Abs. 2 AÜG |
| **Arbeitsmittelprüfung – Aufzeichnungen über Prüfungsergebnisse** | angemessene Zeit (mindestens bis zur nächsten Prüfung) | § 11 BetrSichV |
| **Arbeitszeitnachweise (allgemein)** | 2 Jahre | § 16 Abs. 2 ArbZG |
| **Bewerbungsunterlagen** | eine gesetzliche Frist existiert nicht; Empfehlung: 6-9 Monate, bis zum Ablauf der variablen Klagefristen | § 15 Abs. 4 AGG, § 61 Abs. 1 ArbGG |
| **DEÜV-Bescheinigung über Datenübermittlungen** | bis zum Ablauf des auf die letzte Prüfung folgenden Kalenderjahres | § 25 DEÜV |
| **Doppelbesteuerungsbescheinigung** | 6 Jahre | § 39b Abs. 6 i.V.m. § 41 Abs. 1 EStG |
| **Fahrtenschreiber-Schaublätter** | 1 Jahr | § 57a Abs. 2 StvZO |
| **Fahrtkostenerstattung** | 6 Jahre | § 41 Abs. 1 EStG i.V.m. R 38 der Lohnsteuerrichtlinien |
| **Heimarbeit-Entgeltbelege** | 3 Jahre | § 13 HAGDV 1 |
| **Heimarbeit-Personenlisten** | bis zum Ablauf des Kalender- jahres, das auf das Jahr der Anlegung folgt | § 9 Abs. 3 HAGDV 1 |

| | | |
|---|---|---|
| **Infektionsschutzgesetz – Gesundheitszeugnis und letzte Dokumentation der Belehrung** | bis zum Ausscheiden des Arbeitnehmers | § 43 Abs. 5 IfSG |
| **Jugendarbeitsschutz-Unterlagen** | 2 Jahre | § 50 Abs. 2 JArbSchG |
| **Ladenschlussgesetz-Verzeichnisse und Unterlagen** | 1 Jahr | § 22 Abs. 3 Nr. 2 LadSchlG |