Datenschutzerklärung KVN.akut App

Letzte Aktualisierung: 29.06.2026

Die Verarbeitung personenbezogener Daten, beispielsweise des Namens, der Anschrift, E-Mail-Adresse oder Telefonnummer einer betroffenen Person, erfolgt stets im Einklang mit der Datenschutz-Grundverordnung ("DSGVO") und in Übereinstimmung mit den für die Kassenärztliche Vereinigung Niedersachsen – KVN, Körperschaft des öffentlichen Rechts geltenden landesspezifischen Datenschutzbestimmungen. Mittels dieser Datenschutzerklärung möchten wir die Öffentlichkeit über Art, Umfang und Zweck der von uns erhobenen, genutzten und verarbeiteten personenbezogenen Daten informieren. Ferner werden betroffene Personen mittels dieser Datenschutzerklärung über die ihnen zustehenden Rechte aufgeklärt.

Die Kassenärztliche Vereinigung Niedersachsen – KVN, Körperschaft des öffentlichen Rechts hat als für die Verarbeitung Verantwortliche zahlreiche technische und organisatorische Maßnahmen umgesetzt, um einen möglichst lückenlosen Schutz der über diese App verarbeiteten personenbezogenen Daten sicherzustellen. Dennoch können Internetbasierte Datenübertragungen grundsätzlich Sicherheitslücken aufweisen, sodass ein absoluter Schutz nicht gewährleistet werden kann.

---

1. Begriffsbestimmungen

Die Datenschutzerklärung der KVN – Kassenärztliche Vereinigung Niedersachen beruht auf den Begrifflichkeiten, die durch den Europäischen Verordnungsgeber beim Erlass der DSGVO verwendet wurden.

2. Name und Anschrift des Verantwortlichen

Verantwortlicher im Sinne der DSGVO, sonstiger in den Mitgliedstaaten der Europäischen Union geltenden Datenschutzgesetze und anderer Bestimmungen mit datenschutzrechtlichem Charakter ist die:

Kassenärztliche Vereinigung Niedersachsen
Berliner Allee 22
30175 Hannover
Deutschland
+49 511 3804800
Website: https://www.kvn.de

Ansprechpartner für Datenschutz
Bei Fragen zur Verarbeitung Ihrer personenbezogenen Daten, sowie zu Ihren Rechten rund um den Datenschutz, wenden Sie sich bitte an:

datenschutzbeauftragter@kvn.de

Diese Datenschutzerklärung der Kassenärztlichen Vereinigung Niedersachsen – KVN, Körperschaft des öffentlichen Rechts („wir“, „uns“ oder „unser“) beschreibt, wie und warum wir auf Ihre personenbezogenen Daten zugreifen, diese erfassen, speichern, verwenden und/oder weitergeben („verarbeiten“) können, wenn Sie unsere mobile Anwendung (KVN.akut App) herunterladen und nutzen.

Haben Sie Fragen oder Bedenken? Wenn Sie diese Datenschutzerklärung lesen, können Sie Ihre Datenschutzrechte und -optionen besser verstehen. Wir sind dafür verantwortlich, Entscheidungen darüber zu treffen, wie Ihre personenbezogenen Daten verarbeitet werden. Wenn Sie mit unseren Richtlinien und Praktiken nicht einverstanden sind, nutzen Sie unsere Dienste bitte nicht. Wenn Sie noch Fragen oder Bedenken haben, wenden Sie sich bitte an datenschutzbeauftragter@kvn.de

2. Geltungsbereich
Diese Datenschutzerklärung gilt für unsere telemedizinische Kommunikationsplattform KVN.akut App (nachfolgend „App"), die als Web-Applikation, mobile App für iOS (Apple) und Android (Google) bereitgestellt wird.
Die App dient der Erbringung telemedizinischer Leistungen im Rahmen des ärztlichen Bereitschaftsdienstes, der über die bundeseinheitliche Rufnummer 116117 erreichbar ist.
Der Geltungsbereich ist Deutschland.
- Die strukturierte medizinische Ersteinschätzung (SmED) von gesundheitlichen Anliegen
- Die Durchführung von Videosprechstunden durch Telemediziner:innen
- Die Festlegung und Auslösung weiterer Versorgungsmaßnahmen, sofern keine fallabschließende telemedizinische Versorgung möglich ist
- Das Bereitstellen und Ausstellen von eRezepten, elektronischen Arbeitsunfähigkeitsbescheinigungen (eAU) und anderen ärztlichen Dokumenten

3. Was sind personenbezogene Daten?
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO). Dazu gehören beispielsweise:

- Name, Adresse, Telefonnummer, E-Mail-Adresse
- Geburtsdatum, Geschlecht
- IP-Adresse, Geräte-ID

- Gesundheitsdaten (z. B. Angaben zu Beschwerden, Diagnosen, Behandlungsverläufe) – diese gehören zu den besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) und unterliegen einem besonders hohen Schutzniveau.
- Krankenversicherungsdaten (Versichertennummer, Krankenkasse, Versichertenstatus)
- Nicht personenbezogen sind Daten, die keinen Rückschluss auf eine bestimmte Person erlauben, z. B. vollständig anonymisierte statistische Auswertungen oder aggregierte Nutzungszahlen.

4. Installation unserer App

Unsere App steht zum Download in den offiziellen App-Stores von Google und Apple bereit: im **Google Play Store** und im **Apple App Store**. Für die Installation der App ist ein Nutzerkonto bei Google bzw. Apple notwendig sowie die Installation der jeweiligen Store-App.

a) App-Installation über den Google Play Store

Bei einem digitalen Endgerät (Smartphone, Tablet o.ä.) mit dem Betriebssystem Android (Hersteller z.B. Samsung, Motorola, LG) nutzen Sie den Dienst **Google Play** der Google Ireland Limited („Google“), Gordon House, Barrow Street, Dublin 4, Irland.

Datenverarbeitung durch Google:
Google erhebt und verarbeitet im Rahmen des App-Downloads und der Nutzung der Store-Software verschiedene Daten, darunter:

- Geräteinformationen und -kennungen
- Netzwerkverbindungen und -zugriffe
- Standortdaten (je nach Berechtigung)
- Nutzungsdaten zur Lizenzprüfung und App-Installation
- Bluetooth-Verbindungen (sofern verwendet)

Google kann diese Daten auch an Server außerhalb der EU, insbesondere in die USA, übertragen. Für Übermittlungen in die USA ist ein angemessenes Datenschutzniveau aufgrund der Zertifizierung des Anbieters unter dem Angemessenheitsbeschluss der Europäischen Kommission (EU-U.S. Data Privacy Framework) gewährleistet.

Weitere Informationen zur Datenverarbeitung durch Google und den Schutz Ihrer Daten finden Sie in den aktuellen Datenschutzrichtlinien von Google:
https://policies.google.com/privacy

Wichtig: Die verantwortliche Stelle für die Datenverarbeitung bei der Nutzung des Google Play Store und der Installation der KVN akut.App ist ausschließlich Google als Betreiber des Google Play Stores, nicht die KVN.

b) App-Installation über den Apple App Store

Bei einem digitalen Endgerät (iPhone, iPad o.ä.) mit dem Betriebssystem iOS nutzen Sie den Dienst **Apple App Store** der Apple Distribution International Ltd., Hollyhill Industrial Estate, Hollyhill Ln, Knocknaheeney, Cork, Irland.

Datenverarbeitung durch Apple:
Apple erhebt und verarbeitet im Zusammenhang mit Ihrer Registrierung und dem Download verschiedene personenbezogene Daten, beispielsweise:

- Name, Adresse, Telefonnummer, E-Mail-Adresse
- Gerätekennungen und IP-Adressen
- Standortdaten (sofern freigegeben)
- Zahlungsinformationen (z.B. Kreditkartendaten)
- Profilinformationen und Nutzungsdaten

Apple übermittelt personenbezogene Daten gegebenenfalls auch an Server außerhalb der EU, insbesondere in die USA. Für Übermittlungen in die USA ist ein angemessenes Datenschutzniveau aufgrund der Zertifizierung des Anbieters unter dem Angemessenheitsbeschluss der Europäischen Kommission (EU-U.S. Data Privacy Framework) gewährleistet.

Weitere Informationen zur Datenverarbeitung durch Apple finden Sie in den aktuellen Datenschutzbestimmungen von Apple:
https://www.apple.com/legal/privacy/de-ww/

Wichtig: Die verantwortliche Stelle für die Datenverarbeitung bei der Nutzung des Apple App Stores und der Installation der KVN akut.App ist ausschließlich Apple als Betreiber des Apple App Stores, nicht die KVN.

5. Welche Daten erfassen wir?

5.1 Daten bei Registrierung und Nutzung der App

Bei der Registrierung und Nutzung unserer App erheben wir folgende personenbezogene Daten, die Sie aktiv eingeben:

Datenart	Zweck	Rechtsgrundlage

Name (Vor- und Nachname)	Identifikation, Behandlung, Abrechnung	Art. 6 Abs. 1 lit. b, c DSGVO; Art. 9 Abs. 2 lit. h DSGVO
Adresse	Identifikation, Abrechnung, ggf. Hausbesuch	Art. 6 Abs. 1 lit. b, c DSGVO
Telefonnummer	Kommunikation (SMS, Anrufe), Verifizierung	Art. 6 Abs. 1 lit. b DSGVO
Geschlecht	Medizinische Ersteinschätzung (SmED)	Art. 9 Abs. 2 lit. a, h DSGVO
Ungefähres Alter	Medizinische Ersteinschätzung (SmED)	Art. 9 Abs. 2 lit. a, h DSGVO
Geburtsdatum	Dient der Identifikation und genaue Altersprüfung der/des Patient:in, falls z.B. ein Krankentransport notwendig ist	Art. 6 Abs. 1 lit. c DSGVO Art. 9 Abs. 2 lit. h DSGVO
Gesundheitszustand (Beschwerden, Symptome)	SmED-Ersteinschätzung, telemedizinische Behandlung	Art. 9 Abs. 2 lit. a, h DSGVO
Krankenversicherungsdaten (Versichertennummer, Krankenkasse, Versichertenstatus)	Identifikation, Abrechnung gegenüber Kostenträgern (z.B. Krankenkasse)	Art. 6 Abs. 1 lit. b, c DSGVO; Art. 9 Abs. 2 lit. h DSGVO

Zwecke der Datenverarbeitung und Rechtsgrundlagen nach DSGVO, SGB V, BMV-Ä, HGB und AO

Die nachfolgende Übersicht zeigt die übergeordneten Verarbeitungszwecke und die jeweils einschlägigen Rechtsgrundlagen. Sie bezieht sich auf die in der vorhergehenden Tabelle genannten Datenarten.

Zweck	**Rechtsgrundlage**
Erbringung telemedizinischer Leistungen (Videosprechstunde)	Art. 9 Abs. 2 lit. h DSGVO; § 365 SGB V i.V.m. Anlage 31b BMV-Ä; Art. 6 Abs. 1 lit. e DSGVO (Sicherstellungsauftrag § 75 SGB V)
Strukturierte Ersteinschätzung (SmED)	Art. 9 Abs. 2 lit. a DSGVO; § 9 Anlage 31c BMV-Ä
Authentifizierung und Identifikation der Patient:innen	Art. 6 Abs. 1 lit. b DSGVO
Abrechnung gegenüber Kostenträgern (z.B. Krankenkasse)	Art. 6 Abs. 1 lit. c DSGVO; Art. 9 Abs. 2 lit. h DSGVO; §§ 295, 301 SGB V

Kommunikation mit Patient:innen (Push, SMS, Telefonie)	Art. 6 Abs. 1 lit. a, b DSGVO
Kommunikation mit Apotheken (z.B. Übermittlung von eRezepten)	Art. 9 Abs. 2 lit. h DSGVO; § 360 SGB V
Ausstellung von eRezepten und eArbeitsunfähigkeitsbescheinigungen (eAU)	Art. 6 Abs. 1 lit. c DSGVO; Art. 9 Abs. 2 lit. h DSGVO; §§ 360, 365 SGB V
Gesetzliche Aufbewahrungspflichten	Art. 6 Abs. 1 lit. c DSGVO; § 630f BGB; §§ 147, 257 HGB/AO

Rechtsgrundlagen der Datenverarbeitung

Die Verarbeitung Ihrer personenbezogenen Daten in der KVN.akut App erfolgt – je nach Verarbeitungsvorgang – auf unterschiedlichen Rechtsgrundlagen der DSGVO. Soweit die Verarbeitung zur Erfüllung des Behandlungsvertrages beziehungsweise zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, stützen wir sie auf Art. 6 Abs. 1 lit. B DSGVO. Soweit gesetzliche Pflichten erfüllt werden müssen, etwa Dokumentations- oder Abrechnungspflichten nach dem SGB V, dem BGB oder steuer- und handelsrechtlichen Vorschriften, erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. E DSGVO in Verbindung mit den jeweils einschlägigen Spezialgesetzen.

Darüber hinaus verarbeitet die Kassenärztliche Vereinigung Niedersachsen personenbezogene Daten in Wahrnehmung ihres gesetzlichen Sicherstellungsauftrags nach § 75 SGB V. In diesen Fällen erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. E DSGVO (Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt) in Verbindung mit § 75 SGB V sowie den weiteren spezialgesetzlichen Regelungen zur vertragsärztlichen Versorgung.
Soweit besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, verarbeitet werden, erfolgt dies zusätzlich auf Grundlage von Art. 9 Abs. 2 lit h DSGVO (Gesundheitsversorgung) und – soweit erforderlich – Art. 9 Abs. 2 lit. a DSGVO (ausdrückliche Einwilligung).

Erklärung der Rechtsgrundlagen:

- Art. 6 Abs. 1 lit. b DSGVO – Vertragserfüllung: Die Datenverarbeitung ist notwendig, um Ihnen die telemedizinische Leistung bereitzustellen.

- Art. 6 Abs. 1 lit. c DSGVO – Gesetzliche Verpflichtung: Die Verarbeitung ist zur Erfüllung gesetzlicher Pflichten erforderlich (z. B. Abrechnungspflichten nach SGB V, ärztliche Dokumentationspflicht nach § 630f BGB).

- Art. 6 Abs. 1 lit. e DSGVO – Öffentliches Interesse: Die Verarbeitung ist zur Wahrnehmung des Sicherstellungsauftrags der KV gemäß § 75 SGB V erforderlich.

- Art. 9 Abs. 2 lit. a DSGVO – Ausdrückliche Einwilligung: Sie haben in die Verarbeitung Ihrer Gesundheitsdaten ausdrücklich eingewilligt.

- Art. 9 Abs. 2 lit. h DSGVO – Gesundheitsversorgung: Die Verarbeitung ist für Zwecke der Gesundheitsversorgung erforderlich und erfolgt durch Fachpersonal, das der ärztlichen Schweigepflicht (§ 203 StGB) unterliegt.

Hinweis: Neben den Rechtsgrundlagen der DSGVO spielen bei unserer App die Vorschriften des SGB V (Sozialgesetzbuch – Gesetzliche Krankenversicherung) eine zentrale Rolle:

- § 75 SGB V – Sicherstellungsauftrag: Die KV ist gesetzlich verpflichtet, die vertragsärztliche Versorgung sicherzustellen – auch durch telemedizinische Angebote.

- § 365 SGB V – Regelt die technischen Anforderungen an Videosprechstunden in der vertragsärztlichen Versorgung, einschließlich Datenschutz und IT-Sicherheit.

- § 360 SGB V – Regelt die elektronische Verordnung (eRezept) und deren Übermittlung.

- Anlage 31b BMV-Ä – Detaillierte Anforderungen an Videodienstanbieter (Verschlüsselung, Zertifizierung, Datenschutz).

- Anlage 31c BMV-Ä – Anforderungen an die Terminservicestelle und das SmED-Verfahren.

- § 147 HGB – regelt die Aufbewahrungspflichten von Handelsbüchern, Inventaren und Geschäftsunterlagen für eine Dauer von sechs Jahren.

- § 257 HGB/AO beschreibt die Pflicht zur ordnungsgemäßen Buchführung und die Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen für steuerliche Zwecke. Für Behandlungsberichte und ähnliche medizinische Unterlagen gilt eine Aufbewahrungspflicht von zehn Jahren.

5.2 Automatisch erfasste Daten

Bei der Nutzung der App werden folgende technische Daten automatisch erfasst:
Auf beiden Betriebssystemen (iOS und Android):

Datenart	Zweck	Rechtsgrundlage
Gerätetyp	Technische Bereitstellung und Optimierung der App	Art. 6 Abs. 1 lit. f DSGVO
Betriebssystem	Technische Bereitstellung und Optimierung der App	Art. 6 Abs. 1 lit. f DSGVO
IP-Adresse (verkürzt)	IT-Sicherheit, Missbrauchsprävention	Art. 6 Abs. 1 lit. f DSGVO
Server-Logfiles	IT-Sicherheit, Fehleranalyse	Art. 6 Abs. 1 lit. f DSGVO
Standortdaten	Vermittlung an regionale Versorgungsstrukturen	Art. 6 Abs. 1 lit. a DSGVO; § 25 Abs. 1 TDDDG
Mikrofon	Durchführung der Videosprechstunde (Audio)	Art. 6 Abs. 1 lit. b DSGVO; § 25 Abs. 2 Nr. 2 TDDDG
Kamera	Durchführung der Videosprechstunde (Video), Fotografie der Versichertenkarte	Art. 6 Abs. 1 lit. b DSGVO; § 25 Abs. 2 Nr. 2 TDDDG
Fotos/Medien/Dateien	Upload medizinischer Dokumente (z. B. Befunde, eGK-Scan)	Art. 6 Abs. 1 lit. a DSGVO; § 25 Abs. 1 TDDDG
Internet-/Netzwerkverbindung	Sicherstellung der Verbindungsqualität für Videosprechstunde und deren Durchführung	Art. 6 Abs. 1 lit. f DSGVO
Push-Token (Push-Nachrichten)	Zustellung von Terminbenachrichtigungen und Versorgungshinweisen	Art. 6 Abs. 1 lit. a DSGVO; § 25 Abs. 1 TDDDG

Zusätzlich nur Geräten mit Betriebssystem Android (z.B. Samsung, LG, Sony, Google, OnePlus):

Datenart	Zweck	Rechtsgrundlage
Deaktivierung der Displaysperre	Aufrechterhaltung der Videosprechstunde ohne Unterbrechung	Art. 6 Abs. 1 lit. b DSGVO; § 25 Abs. 2 Nr. 2 TDDDG

Wichtige Hinweise:

Die Berechtigungen für Standort, Mikrofon, Kamera, Fotos/Medien und Displaysperre werden erst abgefragt und genutzt, wenn Sie die jeweilige Funktion tatsächlich verwenden (sogenannte Runtime Permissions). Dies entspricht dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO).

Die IP-Adresse wird nur in verkürzter (anonymisierter) Form gespeichert, sodass kein vollständiger Personenbezug hergestellt werden kann.

5.3 Kommunikation: Push-Nachrichten und SMS

Wir nutzen Push-Nachrichten und SMS, um Sie über relevante Informationen im Zusammenhang mit Ihrer telemedizinischen Versorgung zu informieren (z. B. Terminbestätigungen, Versorgungshinweise, Statusmeldungen).

- SMS werden über die Dienstleister Vonage B.V. versendet. Hierfür wird Ihre Telefonnummer an den jeweiligen Dienstleister übermittelt.

5.4 Rechtsgrundlagen für Push-Nachrichten und SMS

Die Rechtsgrundlage für den Versand der Push-Benachrichtigungen ist Art. 6 Abs. 1 lit. a DSGVO. Sie können den Empfang der Benachrichtigungen jederzeit an- bzw. ausschalten, indem Sie die Funktion in den Einstellungen der App oder in den Einstellungen Ihres Endgeräts ändern.
Die Rechtsgrundlage dafür ist Art. 6 Abs. 1 lit. b DSGVO für dienstbezogene SMS im Rahmen der telemedizinischen Versorgung.

5.5 Datenschutz bei Push-Nachrichten

Unsere App nutzt für den Versand von Push-Nachrichten den Apple Push Notification Service (APNS) auf iOS-Geräten bzw. Firebase Cloud Messaging (FCM) auf Android-Geräten. Dabei werden bestimmte technische Daten an Apple bzw. Google übermittelt, um die Zustellung der Nachrichten zu ermöglichen (siehe 7.5). Die Aktivierung von Push-Nachrichten erfordert Ihre Einwilligung auf Betriebssystem-Ebene (iOS/Android-Berechtigungen). Sie können Push-Nachrichten jederzeit in den Einstellungen Ihres Gerätes deaktivieren.

5.6 Empfänger und Drittlandtransfer

Empfänger der Daten ist Apple bzw. Google. Eine Übermittlung von Daten in die USA kann nicht ausgeschlossen werden. Für Übermittlungen in die USA ist ein angemessenes Datenschutzniveau aufgrund der Zertifizierung des Anbieters unter dem Angemessenheitsbeschluss der Europäischen Kommission (EU-U.S. Data Privacy Framework) gewährleistet. Weitere Informationen finden Sie in der Datenschutzerklärungen

- Apple: https://www.apple.com/de/legal/privacy/
- Google: https://policies.google.com/privacy

Folgende Daten werden dabei übermittelt:

- **Geräte-Token:** Ein eindeutiger Identifikationscode, der das jeweilige Gerät für die Zustellung von Push-Nachrichten identifiziert.
- **Inhalte der Push-Nachricht:** Die eigentlichen Nachrichteninhalte, wie Text, Symbole oder Töne, die an das Gerät gesendet werden.
- **IP-Adresse:** Die IP-Adresse des Geräts, die während der Zustellung der Nachricht übertragen wird.
- **Metadaten zur Zustellung:** z.B. Betriebssystem, Versionsnummer der App, Informationen über den Status der Zustellung, z.B. ob die Nachricht erfolgreich zugestellt wurde.

Sowohl Apple als auch Google verwenden diese Daten ausschließlich zur Übermittlung der Push-Nachrichten, haben keinen Zugriff auf den Inhalt der Nachrichten und speichern die Inhalte der Nachrichten nicht dauerhaft.

5.7 Hinweis zu § 25 TDDDG – Schutz der Privatsphäre bei Endeinrichtungen

Gemäß § 25 Abs. 1 TDDDG ist die Speicherung von Informationen in Ihrer Endeinrichtung (Smartphone) oder der Zugriff auf bereits gespeicherte Informationen nur zulässig, wenn Sie auf Grundlage klarer und umfassender Informationen eingewilligt haben.
Ausnahme (§ 25 Abs. 2 Nr. 2 TDDDG): Eine Einwilligung ist nicht erforderlich, wenn der Zugriff unbedingt erforderlich ist, um Ihnen den ausdrücklich gewünschten Dienst zur Verfügung zu stellen. Dies betrifft insbesondere:

- Den Kamera- und Mikrofonzugriff für die Durchführung der Videosprechstunde
- Die Internetverbindungsprüfung zur Sicherstellung der Verbindungsqualität
- Die Deaktivierung der Displaysperre (Android) zur unterbrechungsfreien Videosprechstunde
- Technisch notwendige Session-Informationen

Für alle darüber hinaus gehenden Zugriffe (z. B. Standortdaten, Fotos/Medien, Push-Token, Analysedienste) holen wir Ihre Einwilligung gemäß § 25 Abs. 1 TDDDG ein.

6. Einwilligung – Wie und wann holen wir Ihre Zustimmung ein?

Für bestimmte Datenverarbeitungen benötigen wir Ihre ausdrückliche Einwilligung (Art. 6 Abs. 1 lit. a DSGVO, bei Gesundheitsdaten Art. 9 Abs. 2 lit. a DSGVO). Diese kann auf verschiedene Weisen eingeholt werden:

6.1 Einwilligung bei Registrierung

Wenn Sie ein Nutzerkonto in der App anlegen, werden Sie über die Datenverarbeitung informiert und um Ihre Einwilligung gebeten. Dies erfolgt über eine Checkbox, die Sie aktiv setzen müssen, bevor Sie den Registrierungsprozess abschließen können. Die Datenschutzerklärung wird Ihnen dabei zum Lesen bereitgestellt. Das Anlegen eines Kontos ist optional.

Einwilligung per In-App-Dialog
Für bestimmte Funktionen (z. B. Standortzugriff, Push-Nachrichten, Analysedienste) wird Ihre Einwilligung über einen In-App-Dialog (Pop-up) eingeholt, der Sie über den Zweck der Datenverarbeitung informiert und Ihnen die Möglichkeit gibt, zuzustimmen oder abzulehnen.

Betriebssystem-Berechtigungen
Für den Zugriff auf Kamera, Mikrofon, Standort und Fotos/Medien wird die Einwilligung zusätzlich über die Berechtigungsabfragen des Betriebssystems (iOS/Android) eingeholt. Sie können diese Berechtigungen jederzeit in den Geräteeinstellungen widerrufen.

Hinweis: Für die Durchführung einer Videosprechstunde ist die Frage der Kamera und des Mikrofons zwingend notwendig. Die Rechtsgrundlage findet sich unter Ziffer 5.1.

6.2 Consent Management
Die App nutzt ein Consent-Management-System, das Ihnen eine zentrale Übersicht über alle erteilten Einwilligungen bietet und es Ihnen ermöglicht, diese einzeln zu erteilen oder zu widerrufen. Dies ist in den Systemeinstellungen Ihres Endgeräts zugänglich.

6.3 Widerruf der Einwilligung
Sie haben das Recht, Ihre Einwilligung jederzeit und ohne Angabe von Gründen zu widerrufen (Art. 7 Abs. 3 DSGVO). Der Widerruf berührt nicht die Rechtmäßigkeit der Verarbeitung, die auf Grundlage der Einwilligung bis zum Widerruf erfolgt ist. Den Widerruf können Sie wie folgt erklären:

- Über die Einstellungen in der App
- Per E-Mail an datenschutzbeauftragter@kvn.de
- Per Post an die unter Punkt 2 genannte Adresse des Verantwortlichen

7. Weitergabe an Dritte (Auftragsverarbeiter)
Ein Auftragsverarbeiter (nach Art. 28 DSGVO) ist ein externer Dienstleister, der personenbezogene Daten in unserem Auftrag und nach unseren Weisungen verarbeitet. Wir haben mit jedem Auftragsverarbeiter einen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO geschlossen, der die Einhaltung der datenschutzrechtlichen Anforderungen sicherstellt.

Zur Erbringung unserer Dienstleistungen setzen wir folgende Auftragsverarbeiter ein:

Dienstleister	Zweck	Verarbeitete Daten	Standort	Rechtsgrundlage
Amazon Web Services (AWS)	Hosting der Plattform und Unternehmensdaten	Sämtliche in der App verarbeiteten Daten (verschlüsselt gespeichert). Der Anbieter hat keinen Zugriff auf die Daten.	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, 1855 Luxemburg	Art. 6 Abs. 1 lit. f DSGVO
Apple Push Notification Service (APNs)	Zustellung von Push-Nachrichten auf iOS-Geräten	Push-Token, Nachrichteninhalte	Apple Inc.	Art. 6 Abs. 1 lit. a DSGVO
Braze	Erfassung der Nutzung unserer mobilen App, zur Erstellung von Auswertungen, zur bedarfsgerechten Gestaltung (zielgruppengerechter Content, Push-Benachrichtigungen)	E-Mail-Adresse, Geschlecht, Geburtstag, Gerätedaten (Geräte-ID, IP-Adresse), App-Session, Zeitpunkt der Double-Opt-In-Verifizierung, Versicherung (pseudonymisiert), Behandlungsanfrage und -typ (pseudonymisiert)	Braze, Inc., 330 West 34th Street, 18th Floor, New York, NY 10001, USA	Art. 6 Abs. 1 lit. a DSGVO (Einwilligung).
Celonis	Automatisierte Kommunikation mit Patienten und Apotheken, Übermittlung von Abrechnungsinformationen, automatisierter Abgleich von Überweisungen und Rechnungen	Name, Anschrift, Alter, Versichertenstatus, Versichertennummer, Krankenkasse, Diagnosen, Abrechnungsinformationen, E-Mail-Adresse, Mobilnummer	Celonis Deutschland GmbH, Theresienstraße 6, 80333 München, Deutschland	Art. 9 Abs. 2 lit. a und lit. h DSGVO
Firebase Dynamic Links	Bereitstellung optimierter Links zur korrekten Weiterleitung an Webadressen innerhalb der Plattform, unabhängig vom Betriebssystem	Pseudonymisierte Daten zum Gerät des Nutzers	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Art. 6 Abs. 1 lit. a DSGVO

Google Firebase Cloud Messaging (FCM)	Zustellung von Push-Nachrichten auf Android-Geräten	Push-Token, Nachrichteninhalte	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	Art. 6 Abs. 1 lit. a DSGVO
HCQS	Strukturierte Ersteinschätzung von Anliegen vor Vermittlung von Terminanfragen für Videosprechstunde gemäß § 9 Anlage 31c BMV-Ä	Geschlecht, Geburtsdatum, Gesundheitsdaten und Information, ob die Anfrage für Sie selbst oder Ihr Kind erfolgt	Health Care Quality Systems GmbH (SmED), Maschmühlenweg 8–10, D-37073 Göttingen	Art. 9 Abs. 2 lit. a DSGVO; Art. 6 Abs. 1 lit. a DSGVO
Mixpanel	Erfassung des Nutzerverhaltens in unserer App sowie zur Erstellung von Auswertungen und bedarfsgerechten Gestaltung	Daten über das Endgerät (z. B. Browser, Betriebssystem, Spracheinstellungen, IP-Adresse)	Mixpanel, Inc., 405 Howard Street Floor 2, San Francisco, CA 94105, USA	Art. 6 Abs. 1 lit. b DSGVO
Vonage	Bereitstellung der Kommunikation zwischen Ärztin/Arzt und Patient:in per Audiotelefonie und SMS-Versand	SMS-Nachrichten, Telefonnummern von Patienten und Ärzten, Logfiles (IP-Adressen, 2FA-Zeitstempel, technische Daten)	Vonage B.V., Basisweg 10, 1043AP Amsterdam, Niederlande	Art. 9 Abs. 2 lit. h DSGVO
Zendesk	Bearbeitung von Kundenanfragen über ein Ticketsystem	Grund der Anfrage, Anfrage, Name, E-Mail-Adresse	Zendesk Inc., 989 Market Street 300, San Francisco, CA 94102, USA	Art. 6 Abs. 1 lit. b DSGVO

Stripe	Durchführung der Zahlungsabwicklung und Bereitstellung der verfügbaren Zahlungsoptionen	Name des Karteninhabers, E-Mail-Adresse, Anschrift, Zahlungsmethode, Karteninformationen, Ablaufdatum, CVC-Code, Datum, Zeit und Betrag der Transaktion	Stripe Payments Europe Ltd., 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland	Art. 6 Abs. 1 lit. b DSGVO; Art. 9 Abs. 2 lit. h DSGVO
Cloudflare	Analyse des Datenverkehrs und Schutz der Plattform vor Cyber-Angriffen (DDoS-Schutz)	Datenverkehr zwischen App und Server (IP-Adresse, Sicherheitszertifikate, DNS-Login-Daten, Performance-Daten). Eine spezifische Verarbeitung von Gesundheitsdaten erfolgt nicht.	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Art. 6 Abs. 1 lit. f DSGVO

Widerspruchsrecht:
Sie können das Tracking durch Braze und Mixpanel jederzeit deaktivieren:
Aktivieren Sie die entsprechende Funktion im Menüpunkt „Einstellungen" der KVN akut.App.

8. Internationale Datentransfers

Einige unserer Auftragsverarbeiter haben ihren Sitz außerhalb der Europäischen Union / des Europäischen Wirtschaftsraums (EU/EWR) oder können Daten durch Subunternehmer in Drittländern verarbeiten.

8.1 Schutzmechanismen

Wir stellen sicher, dass bei jeder Übermittlung personenbezogener Daten in Drittländer ein angemessenes Datenschutzniveau gewährleistet ist.
Hierfür nutzen wir folgende Mechanismen:

- Angemessenheitsbeschluss gemäß Art. 45 DSGVO: Für Übermittlungen in die USA nutzen wir den EU-US Data Privacy Framework (DPF). Dienstleister, die unter dem DPF zertifiziert sind, bieten ein von der EU-Kommission anerkanntes Datenschutzniveau.

- Standardvertragsklauseln (SCC) gemäß Art. 46 Abs. 2 DSGVO: Zusätzlich oder alternativ schließen wir mit den Dienstleistern die von der EU-Kommission genehmigten Standardvertragsklauseln ab, die vertragliche Garantien für den Schutz Ihrer Daten bieten.

Hinweis: Was sind Standardvertragsklauseln (SCC)? SCC sind von der EU-Kommission genehmigte Vertragsmuster, die Unternehmen außerhalb der EU verpflichten, europäische Datenschutzstandards einzuhalten – auch wenn das lokale Recht ein geringeres Schutzniveau bietet.

8.2 Übersicht Drittlandtransfers

Dienstleister	Sitz	Drittlandtransfer	Schutzmechanismus
AWS	Luxemburg (EU)	Möglich durch Subunternehmer	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Braze	USA	Primär EU; möglich in Drittland	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Cloudflare	USA	Primär EU; möglich in Drittland	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Firebase Dynamic Links	Irland (EU)	Möglich durch Subunternehmer	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Mixpanel	USA	Primär EU; möglich in Drittland	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Stripe	Irland (EU)	Möglich durch Subunternehmer	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO
Zendesk	USA	Möglich durch Subunternehmer	SCC (Art. 46 Abs. 2) / Art. 45 DSGVO

Verarbeitung ausschließlich in EU/EWR:

- Celonis (Deutschland)
- HCQS / SmED (Deutschland)
- Vonage (Niederlande)

9. Speicherdauer & Löschung

Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für den jeweiligen Verarbeitungszweck erforderlich ist oder gesetzliche Aufbewahrungspflichten bestehen (Art. 5 Abs. 1 lit. e DSGVO – Grundsatz der Speicherbegrenzung).

Datentyp	Speicherdauer	Grund

Einwilligungsdaten (vor Registrierung)	Dauer der Zwecknutzung + 3 Jahre	Nachweisbarkeit der Einwilligung (§ 195 BGB – regelmäßige Verjährungsfrist)
Nutzerprofile (mit Behandlungskontext)	10 Jahre nach letzter Behandlung/Nutzung	Ärztliche Dokumentationspflicht (§ 630f Abs. 3 BGB); gesetzliche Aufbewahrungsfristen
Analyse-Daten (Braze, Mixpanel)	Bis zum Widerspruch; bei Account-Löschung auch beim Empfänger gelöscht	Einwilligung (Art. 6 Abs. 1 lit. a DSGVO)
Support – Basisdaten (registrierte Nutzer)	Gemäß Nutzerprofil-Speicherdauer	Vertragserfüllung
Support – Basisdaten (Interessenten)	3 Jahre	Berechtigtes Interesse / Verjährungsfrist
Kommunikations- und Supportdaten	6 Jahre	Handelsrechtliche Aufbewahrungspflicht (§ 257 HGB)
Verifizierungsdaten	Solange Account besteht	Vertragserfüllung / Sicherheit
Gesundheitsdaten (Behandlung)	10 Jahre ab Abschluss der Behandlung	Ärztliche Dokumentationspflicht (§ 630f Abs. 3 BGB)
Terminanfragen (ohne Bestätigung)	Automatische Löschung nach 12 Monaten	Datenminimierung
Terminanfragen (mit bestätigtem Termin)	10 Jahre nach Behandlungsabschluss	Ärztliche Dokumentationspflicht (§ 630f Abs. 3 BGB)
Abrechnungsdaten	10 Jahre	Steuerrechtliche Aufbewahrungspflicht (§§ 147 AO, 257 HGB)
Server-Logfiles	Gemäß technischer Notwendigkeit	IT-Sicherheit

9.1 Löschung bei Kontolöschung

Sollten Sie ein optionales Nutzerkonto in der App angelegt haben und dieses löschen, werden alle nicht mehr aufbewahrungspflichtigen Daten unverzüglich gelöscht. Daten, die gesetzlichen Aufbewahrungspflichten unterliegen (insbesondere Behandlungsdaten und Abrechnungsdaten), werden für die Dauer der jeweiligen Aufbewahrungsfrist gesperrt und anschließend automatisch gelöscht.

Bei Analysediensten (Braze, Mixpanel) werden die mit Ihrem Account verknüpften Daten bei Account-Löschung auch beim jeweiligen Empfänger gelöscht.

10. Ihre Rechte

Als betroffene Person haben Sie nach der DSGVO folgende Rechte:

- Auskunftsrecht (Art. 15 DSGVO)

Sie haben das Recht, eine Bestätigung darüber zu verlangen, ob wir personenbezogene Daten von Ihnen verarbeiten. Ist dies der Fall, haben Sie das Recht auf Auskunft über diese Daten sowie auf weitere Informationen (z. B. Verarbeitungszwecke, Kategorien, Empfänger, Speicherdauer).

- Berichtigungsrecht (Art. 16 DSGVO)

Sie haben das Recht, die unverzügliche Berichtigung unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung haben Sie auch das Recht, die Vervollständigung unvollständiger Daten zu verlangen.

- Löschungsrecht / „Recht auf Vergessenwerden" (Art. 17 DSGVO)

Sie haben das Recht, die unverzügliche Löschung Ihrer personenbezogenen Daten zu verlangen, sofern einer der gesetzlichen Gründe vorliegt (z. B. Daten sind für den Zweck nicht mehr notwendig, Einwilligung wurde widerrufen). Beachten Sie, dass gesetzliche Aufbewahrungspflichten (z. B. § 630f BGB: 10 Jahre für Behandlungsdaten) einer sofortigen Löschung entgegenstehen können.

- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)

Sie haben das Recht, die Einschränkung der Verarbeitung Ihrer Daten zu verlangen, z. B. wenn Sie die Richtigkeit der Daten bestreiten oder die Verarbeitung unrechtmäßig ist, Sie aber keine Löschung wünschen.

- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie haben das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln.

- Widerspruchsrecht (Art. 21 DSGVO)

Sie haben das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung Ihrer Daten Widerspruch einzulegen, wenn die Verarbeitung auf Art. 6 Abs. 1 lit. e oder f DSGVO beruht. Wir verarbeiten die Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe für die Verarbeitung nachweisen.

- Widerrufsrecht (Art. 7 Abs. 3 DSGVO)

Soweit die Verarbeitung auf Ihrer Einwilligung beruht, haben Sie das Recht, die Einwilligung jederzeit zu widerrufen. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt davon unberührt.

Wie können Sie Ihre Rechte ausüben?
Sie können Ihre Rechte auf folgenden Wegen geltend machen:

- **Per E-Mail:** datenschutzbeauftragter@kvn.de
- **Über das Formular auf der Webseite der Kassenärztlichen Vereinigung Niedersachsen** www.kvn.de
- **Per Brief**

Kassenärztliche Vereinigung Niedersachsen
Berliner Allee 22
30175 Hannover
Deutschland

Wir werden Ihre Anfrage unverzüglich, spätestens innerhalb eines Monats nach Eingang bearbeiten (Art. 12 Abs. 3 DSGVO). In komplexen Fällen kann diese Frist um weitere zwei Monate verlängert werden, worüber wir Sie informieren.

11. Automatisierte Einzelentscheidungen (Art. 22 DSGVO)
Im Rahmen der strukturierten medizinischen Ersteinschätzung (SmED) wird auf Basis Ihrer Angaben (Geschlecht, Alter, Gesundheitsbeschwerden) eine automatisierte Empfehlung zur Versorgungsebene ausgesprochen (z. B. Telemedizin, Bereitschaftsdienstpraxis, Notaufnahme, Rettungsdienst).

Hinweis: Was bedeutet das? Art. 22 DSGVO schützt Sie vor Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen und rechtliche oder ähnlich erhebliche Wirkung für Sie entfalten.

Ihre Rechte in diesem Zusammenhang:

- Recht auf menschliche Überprüfung: Sie haben das Recht, eine Überprüfung der automatisierten Einschätzung durch eine natürliche Person (z. B. eine:n Mitarbeiter:in der Terminservicestelle oder eine:n Telemediziner:in) zu verlangen.

- Recht auf Darlegung des eigenen Standpunkts: Sie können Ihren eigenen Standpunkt darlegen und ergänzende Informationen mitteilen, die bei der Ersteinschätzung möglicherweise nicht berücksichtigt wurden.

- Recht auf Anfechtung: Sie können die Entscheidung anfechten.

- Rechtsgrundlage: Art. 22 Abs. 2 lit. c DSGVO (ausdrückliche Einwilligung) in Verbindung mit Art. 9 Abs. 2 lit. a DSGVO. Im Rahmen der telemedizinischen Versorgung erfolgt stets eine ärztliche Überprüfung durch die/den Telemediziner:in, der/die die fallabschließende Versorgung übernimmt oder weitere Versorgungsmaßnahmen festlegt.

12. Sicherheit Ihrer Daten

Wir treffen umfangreiche technische und organisatorische Maßnahmen (TOMs) gemäß Art. 32 DSGVO, um Ihre personenbezogenen Daten vor unbefugtem Zugriff, Verlust, Zerstörung oder Veränderung zu schützen:

12.1 Technische Maßnahmen:

- Ende-zu-Ende-Verschlüsselung der Videosprechstunde gemäß § 365 SGB V i.V.m. Anlage 31b BMV-Ä
- Transportverschlüsselung (TLS/SSL) für alle Datenübertragungen zwischen App und Server
- Verschlüsselte Speicherung personenbezogener Daten auf den Servern (AES-256 oder vergleichbar)
- Verkürzte IP-Adresse zur Minimierung des Personenbezugs
- DDoS-Schutz durch Cloudflare
- Zertifizierter Videodienst gemäß den Anforderungen der Anlage 31b BMV-Ä
- Runtime Permissions – Geräteberechtigungen werden nur bei Bedarf abgefragt

12.2 Organisatorische Maßnahmen:

- Auftragsverarbeitungsverträge (AVV) mit allen externen Dienstleistern gemäß Art. 28 DSGVO
- Ärztliche Schweigepflicht (§ 203 StGB) für alle an der Behandlung beteiligten Telemediziner:innen
- Zugriffskontrollen – Nur berechtigtes Fachpersonal hat Zugriff auf Behandlungsdaten
- Regelmäßige Sicherheitsüberprüfungen und Penetrationstests
- Schulung aller Mitarbeiter:innen in Datenschutz und Informationssicherheit
- Dokumentierte Prozesse für Datenschutzvorfälle (Art. 33, 34 DSGVO)

12.3 Datenschutz-Folgenabschätzung (DSFA)

Hinweis: Was ist eine DSFA? Eine Datenschutz-Folgenabschätzung ist ein strukturierter Prozess, mit dem die Risiken einer Datenverarbeitung systematisch identifiziert, bewertet und durch geeignete Maßnahmen minimiert werden. Sie ist insbesondere bei der Verarbeitung von Gesundheitsdaten in großem Umfang vorgeschrieben.

Aufgrund der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten (Gesundheitsdaten) wurde gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt. Diese analysiert die Risiken der Datenverarbeitung für die Rechte und Freiheiten der betroffenen Personen und definiert Maßnahmen zur Risikominimierung. Aufgrund der durchgeführten DSFA und der implementierten technischen und organisatorischen Maßnahmen (TOM) besteht ein akzeptables Risiko für die Rechte und Freiheiten der betroffenen Personen. Die Verarbeitungstätigkeit kann wie beschrieben fortgeführt werden. Die DSFA wird regelmäßig überprüft und bei Bedarf aktualisiert.

13. Besonderheiten

13.1 Datenfreigabe an Dritte im Rahmen der Versorgung

Im Rahmen Ihrer telemedizinischen Behandlung können Daten an folgende Stellen übermittelt werden, sofern dies für Ihre Versorgung erforderlich ist:

- Weiterbehandelnde Ärzt:innen / Fachärzt:innen – wenn der/die Telemediziner:in weitere Versorgungsmaßnahmen festlegt
- Apotheken – zur Einlösung von eRezepten (über Celonis)
- Krankenkassen / Kostenträger – zur Abrechnung der erbrachten Leistungen
- Bereitschaftsdienstpraxen / Notaufnahmen / Rettungsdienst – bei Weitervermittlung an andere medizinische Fachkräfte

Rechtsgrundlage:

Art. 9 Abs. 2 lit. h DSGVO (Gesundheitsversorgung); Art. 6 Abs. 1 lit. c DSGVO (gesetzliche Pflicht, z. B. Abrechnungspflicht); § 73 Abs. 1b SGB V (Übermittlung im Rahmen vertragsärztlicher Versorgung).

Diese Übermittlungen erfolgen ausschließlich im Rahmen der gesetzlichen Vorgaben und unter Wahrung der ärztlichen Schweigepflicht (§ 203 StGB).

13.2 Video- und Audioübertragung (Videosprechstunde)

Die Videosprechstunde erfolgt als synchrone Echtzeit-Kommunikation zwischen Patient:in und Telemediziner:in.

Dabei gilt:

- Die Übertragung erfolgt Ende-zu-Ende-verschlüsselt gemäß den Anforderungen des § 365 SGB V i.V.m. Anlage 31b BMV-Ä

- Video- und Audiodaten werden grundsätzlich nicht aufgezeichnet, es sei denn, dies ist für die Dokumentation der Behandlung erforderlich und Sie haben hierin ausdrücklich eingewilligt
- Die Teilnahme an der Videosprechstunde ist freiwillig und erfolgt auf Grundlage Ihrer Einwilligung
- Die Verbindungsdaten (Metadaten) werden nach spätestens drei Monaten gelöscht und dürfen nur für die zur Abwicklung der Videosprechstunde notwendigen Abläufe genutzt werden

13.3 Elektronische Rezepte (eRezepte) und elektronische Arbeitsunfähigkeitsbescheinigung (eAU)

Über die App können durch Telemediziner:innen eRezepte und eAU ausgestellt und übermittelt werden.

- eRezepte werden verschlüsselt über die Telematikinfrastruktur (TI) an den zentralen Rezeptdienst übermittelt und können von Ihnen bei einer Apotheke Ihrer Wahl eingelöst werden
- Die eAU wird elektronisch an Ihre Krankenkasse und ggf. an Ihren Arbeitgeber übermittelt
- Die Verarbeitung erfolgt auf Grundlage von Art. 9 Abs. 2 lit. h DSGVO und § 360 SGB V (eRezept) bzw. den einschlägigen Regelungen zur eAU

Hinweis: Was ist die Telematikinfrastruktur (TI)? Die TI ist das geschützte digitale Netzwerk des deutschen Gesundheitswesens, das von der gematik GmbH betrieben wird. Sie ermöglicht den sicheren Austausch von Gesundheitsdaten zwischen Leistungserbringern, Kostenträgern und Versicherten.

13.4 Nutzung durch Minderjährige

Die App kann von Personen ab 16 Jahren eigenständig genutzt werden. Dies entspricht der Altersgrenze gemäß Art. 8 DSGVO i.V.m. § 2 Abs. 1 TDDDG für die eigenständige Einwilligung in die Datenverarbeitung bei digitalen Diensten.
Für Personen unter 16 Jahren ist die Einwilligung durch die/den Erziehungsberechtigte:n erforderlich. Die App kann von Erziehungsberechtigten genutzt werden, um telemedizinische Leistungen für ihre Kinder in Anspruch zu nehmen. Hierzu wird im SmED-Verfahren abgefragt, ob die Anfrage für die eigene Person oder für ein Kind erfolgt. Die Rechtsmäßigkeit der Verarbeitung erfolgt dann durch die Einwilligung des/der Träger:in der elterlichen Verantwortung.

14. Änderungen dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung anzupassen, um sie an geänderte rechtliche Anforderungen oder technische Änderungen anzupassen. Die jeweils aktuelle Version gilt.

Sofern eine wesentliche Änderung (z. B. neue Verarbeitungszwecke, neue Auftragsverarbeiter, Änderung der Rechtsgrundlagen) Ihre Einwilligung erfordert, werden wir diese erneut einholen.

Letzte Aktualisierung: 29.06.2026

15. Kontakt & Beschwerden

Kontakt bei Fragen zum Datenschutz:

Kassenärztliche Vereinigung Niedersachsen

E-Mail: datenschutzbeauftragter@kvn.de

Beschwerde bei der Datenschutzbehörde:

Sie haben das Recht, sich bei der zuständigen Datenschutz-Aufsichtsbehörde zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer Daten gegen die DSGVO verstößt.

Zuständige Aufsichtsbehörde für Niedersachsen:

Die Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5
30159 Hannover

Telefon: +49 (0511) 120 45 00
Telefax: +49 (0511) 120 45 99

E-Mail: poststelle@lfd.niedersachsen.de

Ende der Datenschutzerklärung