

**Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung - (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477), § 314 Informationspflichten der Gesellschaft für Telematik**

Die Gesellschaft für Telematik ist verpflichtet, auf ihrer Internetseite und in analogem Format Informationen für die Versicherten in präziser, transparenter, verständlicher, leicht zugänglicher und barrierefreier Form zur Verfügung zu stellen über

- 1. Die Struktur und die Funktionsweise der Telematikinfrastruktur..... 2
- 2. Die grundlegenden Anwendungsfälle und Funktionalitäten der elektronischen Patientenakte..... 2
- 3. Die Rechte der Versicherten im Umgang mit Daten in der elektronischen Patientenakte ..... 5
- 4. Den besonderen Schutz von Gesundheitsdaten nach der Verordnung (EU) 2016/679 11
- 5. Art und Umfang der Zugriffsrechte zugriffsberechtigter Personen nach dem Vierten Abschnitt sowie die Zwecke der Verarbeitung von Daten in der elektronischen Patientenakte durch diese zugriffsberechtigten Personen .....11
- 6. Die Datenverarbeitungsvorgänge bei der Übermittlung von Daten in die elektronische Patientenakte und bei der Erhebung und Verarbeitung von Daten aus der elektronischen Patientenakte durch zugriffsberechtigte Personen .....12
- 7. Die Benennung der Verantwortlichen für die Daten im Hinblick auf die verschiedenen Datenverarbeitungsvorgänge .....13
- 8. Die Pflichten der datenschutzrechtlich Verantwortlichen und die Rechte des Versicherten gegenüber den datenschutzrechtlich Verantwortlichen nach der Verordnung (EU) 2016/679 .....13
- 9. Die Maßnahmen zur Datensicherheit .....17
- 10. Die Aufgaben der koordinierenden Stelle gemäß § 307 Absatz 5 Satz 2 und 3 .....17

## 1. Die Struktur und die Funktionsweise der Telematikinfrastuktur

Der Begriff "Telematik" ist eine Kombination der Wörter "Telekommunikation" und "Informatik". Als Telematik wird die Vernetzung verschiedener IT-Systeme und die Möglichkeit bezeichnet, Informationen aus unterschiedlichen Quellen miteinander zu verknüpfen.

Die Telematikinfrastuktur (TI) vernetzt alle Akteure des Gesundheitswesens im Bereich der Gesetzlichen Krankenversicherung und gewährleistet den sektoren- und systemübergreifenden sowie sicheren Austausch von Informationen. Sie ist ein geschlossenes Netz, zu dem nur registrierte Nutzer (Personen oder Institutionen) mit einem elektronischen Heilberufs- und Praxisausweis Zugang erhalten.

Um allen Datenschutzerfordernungen gerecht zu werden und insbesondere die medizinischen Daten von Patienten zu schützen, wird in der Telematikinfrastuktur auf starke Informationssicherheitsmechanismen gesetzt. Die sichere, verschlüsselte Kommunikation zwischen bekannten Kommunikationspartnern sowie der Schutz vor dem Zugriff auf sensible Informationen sind daher das Fundament der Telematikinfrastuktur.

Damit die sichere Kommunikation und der Schutz von sensiblen Informationen in der Telematikinfrastuktur langfristig gewährleistet sind, werden die verwendeten kryptographischen Verfahren durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelmäßig überprüft und an die neuesten Entwicklungen angepasst.

Die Telematikinfrastuktur bietet Versicherten und Leistungserbringern verschiedene Anwendungen. Diese lassen sich in Pflichtanwendungen und freiwillige Anwendungen unterscheiden. Zuletzt hat der Gesetzgeber die Vorgaben im E-Health-Gesetz, das Ende 2015 in Kraft getreten ist, aktualisiert.

Die Pflichtanwendungen sind für alle Mitglieder der gesetzlichen Krankenkassen verbindlich. Dazu zählen der Online-Abgleich der Versichertenstammdaten auf der elektronischen Gesundheitskarte, das elektronische Empfangen und Einlösen einer Verordnung (eVerordnung) mit der Karte sowie die Verwendung der Europäischen Krankenversicherungskarte (EHIC) auf der Rückseite.

Ob Versicherte das Angebot der freiwilligen Anwendungen nutzen wollen, entscheiden sie ganz allein. Nur mit ihrer Zustimmung können beispielsweise Notfalldaten auf der elektronischen Gesundheitskarte hinterlegt oder eine versichertenbezogene Arzneimitteldokumentation angelegt werden. Die Hoheit über seine Daten liegt allein beim Patienten. Weitere Informationen unter <https://www.gematik.de/telematikinfrastuktur/>

## 2. Die grundlegenden Anwendungsfälle und Funktionalitäten der elektronischen Patientenakte

siehe Informationen zur elektronischen Patientenakte nach § 343 SGB V durch den Spitzenverband Bund der Krankenkassen im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Was ist die elektronische Patientenakte?

Mit einer elektronischen Patientenakte (ePA) können Sie als Patientin bzw. Patient und die an Ihrer Behandlung beteiligten Leistungserbringer persönliche Gesundheits- und Krankheitsdaten sicher digital hochladen, speichern und verarbeiten, lesen und teilen und selbstverständlich auch löschen. Leistungserbringer werden im deutschen Gesundheitswesen alle Personengruppen und Einrichtungen genannt, die im Rahmen der gesetzlichen Krankenversicherung (GKV) Leistungen erbringen. Hierzu zählen zum Beispiel Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Krankenhäuser und Apotheken.

Wenn Sie die von Ihrer Krankenkasse zur Verfügung gestellte App nutzen, haben Sie jederzeit die Möglichkeit, Ihre Gesundheitsdaten einzusehen. Möglich wird das durch die Einbindung in ein hochsicheres Netzwerk, die sogenannte Telematikinfrastruktur. An dieses Netzwerk sind bzw. werden Ärztinnen und Ärzte, Krankenhäuser, Apotheken, Krankenkassen und andere Akteurinnen und Akteure im deutschen Gesundheitswesen angeschlossen.

Für die selbstständige Nutzung der ePA stellt Ihnen Ihre Krankenkasse eine sicherheitsgeprüfte und von der Gesellschaft für Telematik (gematik) zugelassene App für Ihr mobiles Endgerät zur Verfügung. Sie können die App für Android- oder iOS-Betriebssysteme auf Ihrem Smartphone oder Ihrem Tablet installieren. Falls Sie kein mobiles Endgerät besitzen oder aber die App Ihrer Krankenkasse aus anderen Gründen nicht verwenden wollen, können Sie dennoch die ePA nutzen. Allerdings stehen Ihnen in diesem Fall einige Funktionen nur eingeschränkt oder gar nicht zur Verfügung. Beispielsweise können Sie ohne App persönlich keine Dokumente in die ePA einstellen.

In Ihre ePA können Sie selbst Dokumente hochladen, oder Sie bitten z. B. Ihre behandelnden Ärztinnen und Ärzte in der Praxis oder im Krankenhaus, Kopien der relevanten Unterlagen in Ihre Akte zu übertragen. Die Originaldokumentation Ihrer Behandlung verbleibt aus rechtlichen Gründen stets bei dem Sie behandelnden Leistungserbringer. Nur Sie bestimmen, wer Zugriff auf Ihre Akte erhält. Krankenkassen haben keinen Zugriff auf die Akteninhalte.

Die ePA enthält in der ersten Stufe zwei Speicherbereiche: Ein Bereich ist den Versichertendokumenten vorbehalten. Hier können Sie Ihre relevanten Dokumente über die App eigenständig hochladen. Auf diesen Bereich haben nur Sie Zugriff sowie von Ihnen berechnete Leistungserbringer. Ein zweiter Bereich steht für sogenannte Arztdokumente zur Verfügung. Das sind Dokumente, welche Leistungserbringer wie Ärztinnen und Ärzte oder Krankenhäuser auf Ihren ausdrücklichen Wunsch hin in Ihre ePA hochladen. Diesen Bereich können nur Sie und die zugriffsberechtigten Leistungserbringer einsehen. Wichtig: In der ersten Stufe im Jahr 2021 kann jeder zugriffsberechtigte Leistungserbringer jedes Dokument einsehen und herunterladen, das in dem von Ihnen zum Zugriff freigegebenen Speicherbereich liegt. Eine verfeinerte Berechtigungssteuerung wird mit Stufe 2 ab 2022 möglich sein.

Die Dokumente in Ihrer Akte sind stets verschlüsselt abgelegt und können nur auf den Endgeräten der von Ihnen Berechtigten entschlüsselt werden. Der Aktenbetreiber hat also keine Möglichkeit, Ihre hochsensiblen Gesundheitsdaten einzusehen. Der Schlüssel ist sicher hinterlegt. Er besteht aus zwei Teilen, die an getrennten Orten aufbewahrt werden, zum einen von Ihrem ePA-Anbieter, zum anderen von einem zentralen, von der gematik bestimmten Schlüsseldienstbetreiber. Für den Zugriff auf die ePA werden beide Schlüsselteile benötigt. Nur Sie und die von Ihnen Berechtigten verfügen über den kompletten Schlüssel - weder der ePA-Anbieter noch der Schlüsseldienstbetreiber, die jeweils nur einen Teil des Schlüssels aufbewahren, können also auf die ePA zugreifen. Der Schlüssel befindet sich bewusst nicht auf Ihrer elektronischen Gesundheitskarte (eGK), damit Sie auch bei einem (geplanten oder ungeplanten) Austausch der eGK weiterhin Zugriff auf Ihre Akte haben.

Damit Sie und die von Ihnen Berechtigten gezielt nach Dokumenten in Ihrer Akte suchen können, werden zusätzliche Informationen über Merkmale Ihrer Dokumente gespeichert, die sogenannten Metadaten. Diese Daten verarbeitet das Aktensystem in einer auf höchstem Niveau sicherheitsgeprüften und vertrauenswürdigen technischen Umgebung, auf die weder der Aktenbetreiber noch die Krankenkasse Zugriff hat.

Was muss ich grundsätzlich zur elektronischen Patientenakte wissen?

Mit Beginn des Jahres 2021 bieten die Krankenkassen ihren Versicherten elektronische Patientenakten (ePA) an. Welche grundsätzlichen Rechte und Möglichkeiten gehen damit für Sie einher?

Ist die ePA verpflichtend?

Das Nutzen der ePA ist für Sie freiwillig. Entscheiden Sie sich dafür, bedarf es Ihrer Einwilligung in die Datenverarbeitung gegenüber der Krankenkasse. Ihre Einwilligung wird im Rahmen des Antrags zur Einrichtung Ihrer ePA abgefragt – noch bevor die Akte technisch eingerichtet und eröffnet wird.

Wer bietet die ePA an und betreibt sie?

Die ePA wird von den Krankenkassen zur Verfügung gestellt und Ihnen als Versicherten angeboten. Dabei arbeiten die Krankenkassen mit Industriepartnern zusammen, die die entsprechenden Akten nach der Spezifikation, also den technischen und nicht-technischen Anforderungen, der Gesellschaft für Telematik (gematik GmbH) entwickeln und betreiben. Alle ePA-Anbieter müssen mit ihrem Aktensystem und den dazugehörigen Versicherten-Apps ein Zulassungsverfahren gegenüber der gematik durchlaufen, bei dem die Einhaltung aller Anforderungen an Funktionalität, Betrieb, Sicherheit und Datenschutz nachgewiesen werden muss.

Ihre Krankenkasse arbeitet mit einer Firma zusammen, um Ihnen die ePA bereitzustellen.

Ein Zugriff der Krankenkasse auf die in Ihrer Akte gespeicherten Daten ist in Stufe 1 der ePA nicht möglich. Bestimmte technische Maßnahmen verhindern dies. Gleiches gilt auch für den Zugriff des Betreibers. Auch er kann aufgrund technischer Maßnahmen nicht auf Ihre Akte zugreifen. Die Einhaltung dieser Maßnahmen wird von der gematik bei der Zulassung und in regelmäßigen Überprüfungen überwacht.

Was kann ich in meiner elektronischen Patientenakte speichern?

In der ersten Ausbaustufe der elektronischen Patientenakte (ePA), die ab dem 1. Januar 2021 zur Verfügung steht, können Sie unter Verwendung der von der Krankenkasse bereitgestellten App eigene Gesundheitsdaten speichern. Dies können beispielsweise eigenständig geführte Diabetes-Tagebücher sein oder digitalisierte Befunde aus früheren Behandlungen, die Ihnen Ihre Ärztinnen und Ärzte auf Papier bereitgestellt haben, oder aber weitere eigene Aufzeichnungen zu Ihrem Gesundheitszustand.

An Ihrer Behandlung beteiligte Ärztinnen und Ärzte können, sofern Sie eine entsprechende Berechtigung erteilen, die folgenden Daten in der ePA ablegen:

- medizinische Daten Ihrer Behandlung, z. B. Befunde, Diagnosen und Therapiemaßnahmen
- Arztbriefe, die im Zuge einer (zahn-)ärztlichen Behandlung erstellt wurden
- elektronischer Medikationsplan oder Notfalldatensatz, falls Sie diese bereits auf Ihrer elektronischen Gesundheitskarte (eGK) nutzen

Gesetzliche Vertreterinnen und Vertreter können auf die Akte der zu vertretenden Person zugreifen. So können Eltern beispielsweise eine ePA ihres mitversicherten Kindes führen. Weitere Möglichkeiten der Vertretung wird es in den kommenden Stufen der ePA geben.

Wie melde ich mich bei der ePA an?

Zur Anmeldung bei der ePA nutzen Sie die von Ihrer Krankenkasse bereitgestellte App und entweder die eGK mit PIN oder aber wahlweise und auf Ihren Wunsch ein kassenspezifisches, den Vorgaben der gematik entsprechendes alternatives Zugangsverfahren, das ohne den Einsatz der eGK auskommt. Die Anmeldung mit eGK und die Anmeldung ausschließlich per Smartphone haben ein unterschiedliches Sicherheitsniveau, aber das alternative Verfahren wird für einen Übergangszeitraum vom Bundesamt für Sicherheit in der Informationstechnik (BSI) akzeptiert. Dabei ist das bei der Anmeldung mit der eGK erreichbare Sicherheitsniveau höher, da hierbei ein vom BSI zertifizierter Sicherheitsstandard erreicht wird. Eine entsprechende Zertifizierung gibt es bei der Authentifizierung ohne eGK, ausschließlich mithilfe Ihres mobilen Endgeräts nicht. Ihre Kasse informiert Sie umfassend über die zur Verfügung stehenden Möglichkeiten sowie über potenzielle Risiken und darüber, wie Sie diese vermeiden können. Wichtig dabei ist, dass Sie sich für die Nutzung dieser alternativen Zugangsmöglichkeit explizit gegenüber Ihrer Krankenkasse entscheiden müssen.

Was benötige ich zum Zugriff auf meine Daten?

Unabhängig davon, wie Sie sich bei der ePA authentifizieren, nutzen Sie eine von Ihrer Krankenkasse bereitgestellte App auf Ihrem Smartphone oder einem anderen geeigneten Endgerät, um auf die ePA zuzugreifen. Diese App ist nach den Vorgaben des BSI und der Gesellschaft für Telematik (gematik) erstellt und sicherheitsgeprüft. Mit ihr können Sie sämtliche Funktionen der ePA selbstständig nutzen, u. a.:

- Dokumente einstellen, einsehen, herunterladen und löschen
- Berechtigungen erteilen und entziehen
- Zugriffe auf die ePA anhand der Protokolldaten kontrollieren
- ePA vollständig schließen

Versicherte ohne geeignete Endgeräte können eine ePA bei Ihrer Krankenkasse beantragen und anlegen lassen. In diesem Fall erfolgt die Berechtigungsvergabe für den Zugriff direkt beim Besuch in der Arztpraxis, im Krankenhaus oder bei einem anderen Leistungserbringer. Auch wenn Sie grundsätzlich mittels App auf die ePA zugreifen, können Sie natürlich diese Art der Berechtigungsvergabe vor Ort ebenfalls nutzen, etwa um einen Leistungserbringer zu berechtigen, bei dem Sie gerade sind.

### **3. Die Rechte der Versicherten im Umgang mit Daten in der elektronischen Patientenakte**

siehe Informationen zur elektronischen Patientenakte nach § 343 SGB V durch den Spitzenverband Bund der Krankenkassen im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Wer hat wie Zugriff auf die elektronische Patientenakte?

In der elektronischen Patientenakte (ePA) können medizinische Daten von Leistungserbringern, z. B. von Ihrer Hausärztin bzw. Ihrem Hausarzt, gespeichert werden, aber auch Gesundheitsdaten, die Sie selbst einstellen. Damit Leistungserbringer auf Daten in Ihrer ePA zugreifen oder Daten hinzufügen können, müssen Sie ihnen zuvor eine Berechtigung erteilen. Ebenso müssen Sie gegenüber den zugreifenden Leistungserbringern in die Datenverarbeitung einwilligen.

Die Einwilligung gegenüber den Leistungserbringern erteilen Sie, indem Sie ihnen Zugriff auf die ePA gewähren. Dazu nutzen Sie die von Ihrer Krankenkasse bereitgestellte App. Sie können den Zugriff aber auch direkt vor Ort, in der Praxis oder im Krankenhaus, mithilfe

Ihrer elektronischen Gesundheitskarte (eGK) und den dort verfügbaren Geräten gewähren. Solche Geräte wie z. B. das Kartenterminal sind von der Gesellschaft für Telematik (gematik) geprüft und zugelassen.

Wie berechtige ich einen an meiner Behandlung beteiligten Leistungserbringer?

Ein Leistungserbringer kann auf die Daten, die in Ihrer persönlichen ePA gespeichert sind, erst dann zugreifen, wenn Sie ihm hierzu eine Berechtigung erteilt haben. Das Erteilen der Berechtigung mit den technischen Mitteln der Telematikinfrastruktur (TI) – App oder Kartenterminal in der Arztpraxis oder im Krankenhaus – entspricht der Einwilligung in die Datenverarbeitung. Sämtliche Berechtigungen, die Sie erteilen, werden in Ihrer ePA gespeichert. Mithilfe der von der Krankenkasse bereitgestellten App können Sie diese jederzeit einsehen und bei Bedarf anpassen.

Wen Sie berechtigen dürfen, regelt der Gesetzgeber in § 352 SGB V. Dort werden folgende Einrichtungen und Personengruppen genannt. Die zuerst folgenden Personengruppen sind bereits an die TI angeschlossen:

- Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Psychotherapeutinnen und -therapeuten sowie Angestellte dieser Berufsgruppen
- Personen, die in einem Krankenhaus oder einer Rehaklinik beschäftigt sind
- Apothekerinnen und Apotheker sowie Personen, die bei diesen beschäftigt sind
- Krankenhäuser

Die nachfolgenden Gruppen werden Schritt für Schritt an die TI angeschlossen, sodass Sie ihnen dann auch eine Zugriffsberechtigung erteilen können:

- Gesundheits- und Krankenpflegerinnen und -pfleger, Gesundheits- und Kinderkrankenpflegerinnen und -pfleger, Altenpflegerinnen und -pfleger, Pflegefachfrauen und Pflegefachmänner sowie deren Helferinnen und Helfer, die in die medizinische oder pflegerische Versorgung der Versicherten eingebunden sind
- Hebammen, Entbindungspfleger und Physiotherapeutinnen und -therapeuten sowie deren angestellte Helferinnen und Helfer sowie Auszubildende
- Ärztinnen und Ärzte sowie andere Personen, die bei einer für den Öffentlichen Gesundheitsdienst zuständigen Behörde tätig sind, soweit dies zur Erfüllung ihrer Aufgaben nach dem Infektionsschutzgesetz erforderlich ist
- Fachärztinnen und -ärzte für Arbeitsmedizin sowie Betriebsärztinnen und -ärzte

Welche rechtlichen Vorgaben für Leistungserbringer gibt es?

Auch wenn Sie eine Berechtigung erteilt haben, darf ein Leistungserbringer nur auf Daten in Ihrer persönlichen ePA zugreifen, wenn dieser Leistungserbringer in Ihre Behandlung eingebunden ist und wenn die Daten aus Ihrer ePA für Ihre Versorgung erforderlich sind. Dies ist darin begründet, dass rechtlich zwischen der technischen Erteilung einer Zugriffsberechtigung und der „Erlaubnis“ in die Datenverarbeitung, der sogenannten Einwilligung, zu unterscheiden ist. Selbst wenn Sie eine technische Berechtigung für einen Leistungserbringer erteilt haben, der nicht in Ihre Behandlung eingebunden ist, darf dieser nicht auf Ihre ePA-Daten zugreifen. Denn der Zugriff setzt eine rechtsgültige Einwilligung voraus. Diese muss freiwillig, für einen konkreten Fall, nach ausreichender Information des Betroffenen und unmissverständlich abgegeben werden.

Sie können einem Leistungserbringer die Einwilligung in die Verarbeitung Ihrer in der ePA gespeicherten Daten auch wieder entziehen, indem Sie an diesen Leistungserbringer beispielsweise eine E-Mail senden und die Einwilligung widerrufen. Natürlich ist es empfehlenswert, dies nach Möglichkeit auch dadurch zu bekräftigen, dass Sie die Zugriffsrechte entziehen. Dies können Sie in der von Ihrer Krankenkasse zur Verfügung

gestellten App durchführen. Falls Sie die App nicht nutzen, können Sie dem betroffenen Leistungserbringer diese Rechte beispielsweise bei Ihrem nächsten Besuch in der Praxis entziehen, indem Sie eine neue Berechtigung mit einer Dauer von einem Tag erteilen. Mit Ablauf des eingestellten Tages kann der Leistungserbringer nicht länger auf die ePA zugreifen.

Für einige Leistungserbringer hat der Gesetzgeber festgelegt, dass diese grundsätzlich nur bestimmte Informationen in Ihrer ePA einsehen dürfen. Über diese gesetzlich festgelegten Zugriffsrechte hinaus können Sie keine Berechtigung zum Zugriff erteilen. Zum Beispiel darf eine Apothekerin bzw. ein Apotheker keine Daten aus Ihrem elektronischen Zahn-Bonusheft einsehen. Sie können der Apothekerin bzw. dem Apotheker deshalb auch keinen Zugriff auf Ihr elektronisches Zahn-Bonusheft erlauben.

Zum Start der ePA am 1. Januar 2021 sind die Möglichkeiten bei den Zugriffsberechtigungen noch eingeschränkt. Die ePA bietet Ihnen dann nur zwei Bereiche, in die Dokumente eingestellt werden können. Dies sind die Bereiche „Dokumente von Leistungserbringern“ und „Dokumente von Versicherten“. Die Bereiche können in der App Ihrer Krankenkasse etwas anders heißen. Bei Fragen hilft Ihnen Ihre Krankenkasse gerne weiter.

Im Bereich „Dokumente von Leistungserbringern“ finden Sie alle Dokumente, die Leistungserbringer in Ihre ePA eingestellt haben. Dokumente, die Sie selbst in Ihre ePA geladen haben, finden Sie im Bereich „Dokumente von Versicherten“. Sie können für jeden dieser Bereiche entscheiden, ob Sie einem Leistungserbringer Zugriff auf den Bereich erlauben wollen oder nicht. Dabei erlauben Sie immer den Zugriff auf den kompletten Bereich. Das bedeutet, dass alle Dokumente in diesem Bereich vom Leistungserbringern gelesen werden können - es sei denn, Sie löschen diese.

Befindet sich zum Beispiel im Bereich „Dokumente von Versicherten“ ein Krankenhaus-Entlassbrief und Sie wollen nicht, dass Ihre Zahnärztin bzw. Ihr Zahnarzt oder die Betriebsärztin bzw. der Betriebsarzt darauf zugreift, sollten Sie ihr bzw. ihm keinen Zugriff auf den Bereich „Dokumente von Versicherten“ gewähren. Das bedeutet aber, dass Ihre Zahnärztin bzw. Ihr Zahnarzt auch alle anderen Dokumente in diesem Bereich nicht sehen kann. Alternativ könnten Sie den Krankenhaus-Entlassbrief aus Ihrer ePA löschen. Dann können aber auch alle anderen Leistungserbringer diesen Krankenhaus-Entlassbrief nicht mehr lesen.

Bitte achten Sie anfangs – bis zum 1. Januar 2022 - darauf, Dokumente, die ein anderer Leistungserbringer nicht lesen soll, vorab zu entfernen oder diesem keinen Zugriff auf den entsprechenden Bereich zu erlauben. Bitte beachten Sie, dass gelöschte Dokumente nur durch Sie selbst oder eine Ärztin bzw. einen Arzt, der bzw. dem Sie das Dokument zur Verfügung gestellt haben, erneut in die ePA eingestellt werden können, um wieder verfügbar zu sein. Es empfiehlt sich daher, Dokumente vor dem Löschen aus der ePA an einem privaten, sicheren Ort zu speichern.

Wie funktioniert die Erteilung von Berechtigungen konkret?

Alle Krankenkassen bieten ihren Versicherten eine ePA-App an. Mit dieser App können Sie Ihre ePA bequem verwalten. Dort stellen Sie ein, wer welche Daten in Ihrer ePA einsehen kann. Sie bestimmen auch, wie lange Sie den Zugriff erlauben wollen. Voreingestellt sind sieben Tage. Sie können diesen Zeitraum aber auch verkürzen (Mindestdauer ein Tag) oder auf bis zu 540 Tage verlängern. Nach Ablauf der von Ihnen gewählten Zeit endet die Berechtigung für den jeweiligen Leistungserbringer automatisch. Er kann die Dokumente dann nicht mehr in der ePA einsehen. Für die Praxisdokumentation lokal heruntergeladene Kopien sind allerdings für den Leistungserbringer weiterhin verfügbar. Grundsätzlich können Sie einmal erteilte Berechtigungen jederzeit wieder entziehen. Wenn Sie Hilfe bei der Bedienung der App brauchen, hilft Ihnen Ihre Krankenkasse gerne weiter.

Wenn Sie keine App nutzen oder wenn Sie Ihr Smartphone z. B. beim Arztbesuch einmal nicht zur Hand haben, können Sie trotzdem Zugriffe auf Ihre ePA erlauben. Dazu benötigen Sie Ihre eGK und die dazugehörige PIN (persönliche Identifikationsnummer). Der Vorgang funktioniert ähnlich wie das Bezahlen mit Bankkarte und PIN im Supermarkt. Die eGK wird in einem Lesegerät beim Leistungserbringer eingelesen. Anschließend geben Sie Ihre PIN ein und bestätigen so, welche Daten der Leistungserbringer einsehen darf. Sollten Sie die PIN nutzen wollen, aber noch keine erhalten haben, wenden Sie sich bitte an Ihre Krankenkasse.

Wer muss Daten in meine elektronische Patientenakte einstellen, wenn ich es wünsche?

Die elektronische Patientenakte (ePA) lebt davon, dass in ihr möglichst viele Ihrer Gesundheitsdaten abgelegt sind – erst dann entfaltet sie für Sie und Ihre behandelnden Ärztinnen und Ärzte den vollen Mehrwert. Neben den Daten, die Sie selbst einspeisen, kommt es dabei natürlich auch ganz entscheidend auf die Daten an, die im Rahmen Ihrer Behandlungen bei Ärztinnen bzw. Ärzten und im Krankenhaus erhoben werden. Welche Ansprüche haben Sie aber, dass diese Behandlungsdaten in Ihre ePA aufgenommen werden?

Sie haben gegenüber Ihren behandelnden Ärztinnen und Ärzten sowie anderen Leistungserbringern einen Anspruch auf die Übermittlung und Speicherung der im Rahmen der Behandlung anfallenden Daten in Ihrer ePA. Voraussetzung ist natürlich, dass Sie vorher eine Berechtigung zum Zugriff auf Ihre ePA erteilt haben

Zudem haben Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte sowie Psychotherapeutinnen und -therapeuten, die an Ihrer Behandlung beteiligt sind, Sie bei der Erstbefüllung der ePA zu unterstützen. Die Unterstützungsleistung umfasst die Übermittlung medizinischer Daten an die ePA und ist auf medizinische Daten aus der konkreten aktuellen Behandlung beschränkt.

Darüber hinaus haben Sie das Recht, die Speicherung der Daten aus dem Notfalldatensatz und die Daten des elektronischen Medikationsplans von Ärztinnen und Ärzten, Zahnärztinnen und –ärzten oder Apothekerinnen und Apothekern zu verlangen. Ändert sich etwas in Ihrem Medikationsplan oder in Ihrem Notfalldatensatz, haben Sie das Recht, dass Ihre Ärztin bzw. Ihr Arzt diese Daten sowohl in der ePA als auch auf der eGK aktualisiert. Sprechen Sie Ihre Ärztin bzw. Ihren Arzt darauf an, wenn Sie hierzu Fragen haben.

Anspruch haben Sie auch darauf, von Ärztinnen und Ärzten sowie anderen Leistungserbringern die Löschung von Dokumenten und Daten zu verlangen, die diese in Ihre ePA hochgeladen haben.

Kann ich Dokumente in der ePA oder die ganze Akte löschen?

Das Prinzip der Freiwilligkeit bedeutet natürlich auch, dass Sie jederzeit das Recht haben, in die Akte eingestellte Dokumente zu löschen oder von einem berechtigten Leistungserbringer löschen zu lassen. Einen Löschvorgang könnte auf Ihren ausdrücklichen Wunsch hin z. B. eine Ärztin oder ein Arzt vornehmen, die oder der Sie behandelt).

Wie behalte ich den Überblick darüber, wer etwas an meiner Akte geändert hat?

Die ePA zeichnet Vorgänge, die von Ihnen berechnigte Institutionen durchführen, in einem Protokoll auf. Dabei unterscheidet die ePA die Protokollierung von Verwaltungsvorgängen, das sogenannte Verwaltungsprotokoll, und Vorgängen, die unmittelbar im Zusammenhang mit Ihren medizinischen Daten stehen, das sogenannte Aktenprotokoll.

Wenn Sie die App Ihrer Krankenkasse nutzen, stellt Ihnen diese die Inhalte beider Protokolle komfortabel und einheitlich dar, sodass Sie grundsätzlich nicht zwischen beiden Protokollen unterscheiden müssen.

### Das Verwaltungsprotokoll

Im Verwaltungsprotokoll speichert die ePA alle Vorgänge, die nicht direkt ein Dokument oder dessen Metadaten betreffen und administrativen Charakter haben. Dies sind beispielsweise die An- oder Abmeldung berechtigter Benutzerinnen und Benutzer, die Erteilung oder der Entzug von Berechtigungen. Ebenso umfasst das Verwaltungsprotokoll den technischen Zeitpunkt der Einrichtung der ePA sowie Einträge bei Schließung der ePA. Die Protokolleinträge des Verwaltungsprotokolls werden am Ende des dritten auf ihre Generierung folgenden Jahres automatisch durch das Aktensystem gelöscht. Diese Löschfrist gilt auch, wenn Sie die Akte schließen. Folglich liegen diese Protokolleinträge auch dann noch bis zu drei Jahre vor, wenn Sie die ePA geschlossen haben.

Einträge im Verwaltungsprotokoll speichert die ePA - anders als die restlichen in ihr abgelegten Daten - in einer Form, in welcher der Anbieter auf diese Daten zugreifen kann. Der Zugriff durch den Anbieter ist jedoch nur mit Ihrer Einwilligung zulässig, beispielsweise um Sie bei technischen Problemen unterstützen zu können.

### Das Aktenprotokoll

Im Aktenprotokoll speichert Ihre ePA alle Zugriffe, die in direktem Zusammenhang mit ihren Dokumenten stehen. Diese sind beispielsweise der Abruf, das Einstellen oder das Löschen eines Dokuments. Einträge im Aktenprotokoll sind dabei auf die gleiche Weise geschützt wie die Metadaten zu Ihren Dokumenten. Die Daten werden ein Jahr nach Erstellung des Protokolleintrags beim nächsten Zugriff auf die ePA gelöscht. Stets bleiben jedoch die letzten 50 Einträge, unabhängig von der Jahresfrist, bestehen.

Was muss ich tun, wenn ich die ePA nicht mehr will?

Sie haben grundsätzlich und jederzeit die Möglichkeit, Ihre ePA komplett zu schließen, also löschen zu lassen. Dazu müssen Sie die erteilte Einwilligung zur Nutzung der ePA gegenüber Ihrer Krankenkasse widerrufen. Diese Kündigung der ePA bzw. der Widerruf zur Nutzung muss gegenüber Ihrer Krankenkasse in einer geeigneten Form ausgesprochen werden. Dies kann beispielsweise über die von Ihrer Krankenkasse bereitgestellte App geschehen. Zum genauen Vorgehen wenden Sie sich an Ihre Krankenkasse.

Von der Löschung betroffen sind alle Inhalte Ihrer Akte - sämtliche Dokumente, erteilte Berechtigungen und Protokolleinträge - mit Ausnahme der Einträge des Verwaltungsprotokolls. Die Verantwortung zur Sicherung der in Ihrer Akte gespeicherten Dokumente obliegt in diesem Fall Ihnen als ePA-Nutzerin bzw. ePA-Nutzer. Wenn Sie bestimmte Dokumente auch nach Schließung Ihrer ePA behalten wollen, müssen Sie diese anderweitig speichern.

Nutzen Sie die von Ihrer Krankenkasse bereitgestellte App zum Zugriff auf die ePA, haben Sie die Möglichkeit, die Protokolldaten ebenfalls auf Ihrem eigenen Endgerät zu sichern. Die App bietet Ihnen dazu eine entsprechende Funktion an. Neben der Sicherung der Dokumente ist auch die Sicherung der Protokolldaten aus Sicht des Datenschutzes sinnvoll, damit Sie später nachvollziehen können, wer Zugriff auf Ihre Akte hatte.

Habe ich Nachteile bei meiner Gesundheitsversorgung, wenn ich die ePA nicht nutze?

Sollten Sie sich dazu entscheiden, die ePA nicht nutzen zu wollen, entstehen Ihnen hieraus keine Nachteile für Ihre Gesundheitsversorgung. Diese wird auch zukünftig durch die etablierten Verfahren gewährleistet bleiben.

Als Zusatzangebot sorgt die ePA in Zukunft aber für eine gesteigerte Transparenz Ihrer medizinischen Daten. So besitzen Sie im Rahmen einer ePA-Nutzung den Vorteil, die Dokumente, Befunde oder Informationen Ihrer Behandlung digital einsehen und an ausgewählte Leistungserbringer wie Ärztinnen und Ärzte oder Krankenhäuser weitergeben zu können bzw. diesen den Zugriff auf Ihre Daten zu erlauben. Dieser digitale, durch Sie initiierte und gesteuerte Datenaustausch kann dabei helfen, Ihre medizinische Versorgung

zu verbessern. Durch den Zugriff auf relevante Gesundheitsdaten in Ihrer ePA unterstützen Sie die behandelnden Ärztinnen und Ärzte und andere Leistungserbringer dabei, die bestmögliche therapeutische Entscheidung treffen zu können, unerwünschte Wirkungen abzuwenden sowie unnötige Doppeluntersuchungen und eventuelle Überbehandlungen zu vermeiden.

Was muss ich bei Nutzung der App beachten?

Die ePA-Apps, die Ihnen den selbstständigen Zugriff auf Ihre Gesundheitsdaten über Ihre eigenen Endgeräte wie Smartphones oder Tablets ermöglichen, haben die Krankenkassen nach den Vorgaben der gematik und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erstellt. Zusätzlich durchlaufen die Apps eine Sicherheitsprüfung. Diese kann nur von Prüfstellen durchgeführt werden, die bei der gematik und dem BSI akkreditiert sind. Um die Sicherheit Ihrer ePA-Daten zu gewährleisten, ist es unabdingbar, dass Sie ausschließlich von der gematik zugelassene Apps nutzen, die Sie aus einer vertrauenswürdigen Quelle heruntergeladen haben. Vertrauenswürdige Quellen sind für das iOS-Betriebssystem der App Store von Apple sowie Google Play für Android.

Nach der Installation muss die entsprechende App im Rahmen der ersten Nutzung freigeschaltet werden. Hierfür sind grundsätzlich zwei Wege vorgesehen: Der sicherste Weg ist die Freischaltung via eGK mit NFC-Übertragungsstandard, also mit einer kontaktlosen Schnittstelle, wie sie heute bereits auf vielen EC- und Kreditkarten zu finden ist, und der dazugehörigen PIN, die Sie von Ihrer Krankenkasse erhalten. Alternativ können Sie die ePA mittels eines von Ihrer Krankenkasse zur Verfügung gestellten Aktivierungscode freischalten. Diese Aktivierung bleibt auch bei einem Wechsel des Endgeräts gültig, also auch dann, wenn Sie Ihre ePA mal über Ihr Smartphone, mal übers Tablet nutzen wollen. Die Übermittlung des Aktivierungscode ist kassenspezifisch. Bei Fragen dazu wenden Sie sich bitte an Ihre Krankenkasse.

Dem Schutz dieser Zugangsmittel kommt besonders hohe Bedeutung zu. Bei Verlust oder Verdacht auf Missbrauch müssen sie umgehend bei der Krankenkasse gesperrt werden, um die Sicherheit der ePA zu gewährleisten. Die Krankenkassen bieten hierfür verschiedene Sperrmöglichkeiten an (z. B. telefonisch oder online). Um die ePA sicher vom eigenen Smartphone oder Tablet aus zu nutzen, müssen Sie zudem für den Schutz Ihrer jeweiligen Endgeräte Sorge tragen. Entsprechende Anweisungen, die Sie hierfür ausführen müssen, finden sich in der Dokumentation der App. Ebenso sollten Sie die Empfehlungen des BSI zur Endgerätesicherheit befolgen. Das BSI stellt hierfür ein Informationsangebot im Internet bereit: <https://www.bsi-fuer-buerger.de>.

Ich will meine Krankenkasse wechseln. Kann ich meine in der ePA gespeicherten Daten einfach mitnehmen?

Die ePA wird Ihnen von Ihrer Krankenkasse angeboten. Sollten Sie die Krankenkasse wechseln und eine ePA auch bei Ihrer neuen Krankenkasse nutzen wollen, so müssen Sie dies gegenüber der neuen Krankenkasse erklären. In der ersten Stufe der ePA, im Zeitraum vom 1. Januar 2021 bis zum 1. Januar 2022, ist noch keine automatische Übernahme der ePA-Daten beim Wechsel von einer Krankenkasse zu einer anderen möglich. Sie können die Datenübertragung aber auf folgendem Wege selbst vornehmen: Laden Sie die Daten über die von Ihrer Krankenkasse zur Verfügung gestellte App auf Ihr Endgerät herunter. Von hier aus können Sie Ihre Daten anschließend in Ihre neue ePA einspielen. Sollten dabei Dokumente von Leistungserbringern übertragen werden, können Sie einen Leistungserbringer im Rahmen Ihrer Behandlung, dem Sie Zugriff auf die Akte gewähren, bitten, diese in der neuen Akte als leistungserbringerrelevant zu kennzeichnen. Ihre Krankenkasse berät Sie gerne zum Verfahren der Datenübernahme.

Ab 1. Januar 2022 besteht die Möglichkeit der automatischen Datenübernahme, sodass der Export über die App nicht erforderlich ist.

#### 4. Den besonderen Schutz von Gesundheitsdaten nach der Verordnung (EU) 2016/679

Gesundheitsdaten bedürfen eines besonderen Schutzes. Die Versicherten haben das Recht, selbst zu bestimmen, welche personenbezogenen Daten sie von sich preisgeben möchten und wer sie verwenden darf. Dieses Recht auf informationelle Selbstbestimmung hat auch der Gesetzgeber im Blick. Daher stehen der Datenschutz und die Informationssicherheit beim Aufbau eines digitalen Gesundheitsnetzes in Deutschland im Mittelpunkt. Mehr zur Datensicherheit im [Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur](#)

#### 5. Art und Umfang der Zugriffsrechte zugriffsberechtigter Personen nach dem Vierten Abschnitt sowie die Zwecke der Verarbeitung von Daten in der elektronischen Patientenakte durch diese zugriffsberechtigten Personen

siehe Informationen zur elektronischen Patientenakte nach § 343 SGB V durch den Spitzenverband Bund der Krankenkassen im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Welcher Leistungserbringer darf auf welche Daten in der ePA zugreifen?

Welcher Leistungserbringer auf welche Daten zugreifen darf, haben wir für Sie in der folgenden Tabelle zusammengefasst. Natürlich ist der Zugriff auf die Daten in Ihrer ePA immer nur unter der Voraussetzung möglich, dass Sie den jeweiligen Leistungserbringer dazu berechtigt haben und dieser an die TI angeschlossen ist.

Berufsgruppe	Mögliche Verwendung medizinischer Informationen über Versicherte	Mögliche Verwendung der von Versicherten zur Verfügung gestellten Gesundheitsinformationen
Ärztinnen/Ärzte, Zahnärztinnen/Zahnärzte, Psychotherapeutinnen und therapeuten, Krankenhäuser, Rehakliniken	- Verarbeitung	Verarbeitung
Apothekerinnen/Apotheker	Auslesen, Speicherung und Verwendung sowie Verarbeitung des elektronischen Medikationsplans	Auslesen, Speicherung und Verwendung
Gesundheits- und Krankenpflegerinnen und -pfleger,	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung

Gesundheits- und Kinderkrankenpflegerinnen und -pfleger, Altenpflegerinnen und -pfleger, Pflegefachfrauen und Pflegefachmänner sowie deren Helferinnen und Helfer		
Hebammen/Entbindungspfleger	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung
Physiotherapeutinnen/Physiotherapeuten	Auslesen, Speicherung und Verwendung sowie Verarbeitung von Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen oder Früherkennungsuntersuchungen, von Behandlungsberichten und sonstigen untersuchungs- und behandlungsbezogenen medizinischen Informationen, die sich aus der physiotherapeutischen Behandlung ergeben	Auslesen, Speicherung und Verwendung
Arbeitsmedizinerinnen/Arbeitsmediziner, Betriebsärztinnen/Betriebsärzte	Auslesen, Speicherung und Verwendung	Auslesen, Speicherung und Verwendung
Öffentlicher Gesundheitsdienst	Verarbeitung, soweit für Aufgabenerfüllung erforderlich	Verarbeitung, soweit für Aufgabenerfüllung erforderlich

## 6. Die Datenverarbeitungsvorgänge bei der Übermittlung von Daten in die elektronische Patientenakte und bei der Erhebung und Verarbeitung von Daten aus der elektronischen Patientenakte durch zugriffsberechtigte Personen

siehe Informationen zur elektronischen Patientenakte nach § 343 SGB V durch den Spitzenverband Bund der Krankenkassen im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Welche Rechte habe ich gegenüber meiner Krankenkasse hinsichtlich der Datenverarbeitungsvorgänge der ePA?

Ihre Rechte gegenüber der Krankenkasse ergeben sich aus den gesetzlichen Bestimmungen der Datenschutz-Grundverordnung (DS-GVO). Im Sinne dieser Verordnung ist die Krankenkasse „Verantwortlicher“, da dies durch den Gesetzgeber bestimmt wurde. Sie als Versicherte bzw. Versicherter können gegenüber Ihrer Krankenkassen die „Rechte der betroffenen Person“ nach der DS-GVO geltend machen. Hierzu zählt insbesondere, dass die Krankenkassen verpflichtet sind, die Versicherten über die Erhebung von personenbezogenen Daten zu informieren (Art. 13, Art. 14 DS-GVO). Ferner haben die Versicherten das Recht auf Auskunft, ob und ggf. zu welchem Zweck bestimmte

personenbezogene Daten von der Krankenkasse bzw. ihren Auftragnehmern verarbeitet werden (Art. 15 DS-GVO), das Recht auf Berichtigung unrichtiger personenbezogener Daten (Art. 16 DS-GVO), das Recht auf Löschung personenbezogener Daten (Art. 17 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO), das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO) und das Widerspruchsrecht (Art. 21 DS-GVO).

Dabei ist zu beachten, dass der Gesetzgeber diese Rechte ausgeschlossen hat, wenn die Wahrnehmung der Rechte von der Krankenkasse als datenschutzrechtlich verantwortlicher Stelle nicht oder nur unter Umgehung von Schutzmechanismen wie insbesondere der Verschlüsselung oder der Anonymisierung gewährleistet werden kann. Diese Einschränkung besteht, weil die Krankenkasse als verantwortliche Stelle aufgrund der bestehenden Verschlüsselungsmechanismen technisch keinen Zugriff auf die in der ePA gespeicherten Daten hat. Dementsprechend kann sie beispielsweise Auskunfts- oder Korrekturbitten Ihrerseits zu in der ePA gespeicherten Daten (z. B. zu Ihren Arztbriefen) nicht nachkommen. Aus diesem Grund stellt Ihnen die Krankenkasse eine App zur selbstständigen Wahrnehmung Ihrer Rechte im Sinne der DS-GVO zur Verfügung. Allerdings können Sie mithilfe der App keine von Ihrem Leistungserbringer zur Verfügung gestellten Daten korrigieren. Sollten also Korrekturen dieser Daten erforderlich sein, wenden Sie sich bitte an den Sie behandelnden Leistungserbringer.

Welche Daten tauscht die Krankenkasse mit dem Betreiber der ePA aus?

Um Ihre ePA einzurichten, tauschen die Krankenkasse und der jeweilige Industriepartner administrative personenbezogene Informationen aus. Zudem prüft Ihre Krankenkasse bzw. der Anbieter der ePA anhand Ihrer Krankenversicherungsnummer, ob bereits eine Patientenakte für Sie existiert. Ein Austausch von personenbezogenen Gesundheitsdaten findet an dieser Stelle nicht statt.

## **7. Die Benennung der Verantwortlichen für die Daten im Hinblick auf die verschiedenen Datenverarbeitungsvorgänge**

In der Telematikinfrastruktur findet die Datenverarbeitung zum großen Teil in verschiedenen arbeitsteiligen Prozessen statt. Es gibt daher im Rahmen der Verarbeitung von personenbezogenen Daten des Versicherten in der Telematikinfrastruktur häufig nicht nur eine Person oder Stelle, die die Daten des Versicherten verarbeitet und hierfür datenschutzrechtlich verantwortlich ist.

Der Gesetzgeber hat im Rahmen des Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur, kurz: Patientendaten-Schutz-Gesetz oder PDSG, die datenschutzrechtliche Verantwortlichkeit gesetzlich bestimmt.

Im Folgenden werden die Akteure aufgeführt, die hiernach für die Verarbeitung der unterschiedlichen personenbezogenen Daten des Versicherten in der Telematikinfrastruktur datenschutzrechtlich verantwortlich sind. Von der Darstellung ausgenommen sind die jeweiligen Verantwortlichkeiten für Datenverarbeitungsprozesse, die außerhalb der Telematikinfrastruktur stattfinden, wie zum Beispiel die Verarbeitung von Daten des Versicherten in einer Arztpraxis für die keine Komponenten oder Dienste der Telematikinfrastruktur genutzt werden.

### **Versichertenstammdaten**

Die elektronische Gesundheitskarte enthält verpflichtend für alle Versicherten die Verwaltungsdaten der Versicherten (Versichertenstammdaten). Hiervon umfasst sind unter anderem der Name des Versicherten, sein Geburtsdatum, seine Anschrift und sein Geschlecht, die Bezeichnung der ausstellenden Krankenkasse, die Krankenversicherungsnummer, der Tag des Beginns des Versicherungsschutzes sowie der Versichertenstatus (siehe auch § 291a Abs. 2 SGB V).

Die Versichertenstammdaten auf der elektronischen Gesundheitskarte werden beim Arztbesuch einmal im Quartal mit den bei der Krankenkasse vorliegenden Daten abgeglichen und, falls notwendig, aktualisiert (§ 291b Abs. 2 SGB V).

**Verantwortlicher Akteur**

Krankenkassen	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Versichertenstammdaten auf der elektronischen Gesundheitskarte</li> <li>▪ Versichertenstammdatenabgleich</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Versichertenstammdaten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastuktur</li> </ul>
Anbieter des zentralen Netzes	<ul style="list-style-type: none"> <li>▪ Übermittlung der Versichertenstammdaten</li> </ul>

**Daten der elektronischen Patientenakte**

Entscheidet sich der Versicherte eine elektronische Patientenakte zu nutzen, werden im Rahmen der Anlage der Patientenakte zunächst administrative Daten über den Versicherten gespeichert.

Weiterhin kann der Versicherte entscheiden, welche Gesundheitsdaten über ihn in der elektronischen Patientenakte gespeichert werden und wer berechtigt sein soll, diese Daten zu verarbeiten. Die Speicherung von Daten kann durch den Versicherten entweder selbst über sein Versichertenfrontend (Benutzeroberfläche, die den Versicherten für den Zugang und die Verwaltung ihrer elektronischen Patientenakte zur Verfügung zu stellen ist / ePA-App) oder durch eine Person oder Stelle, der der Versicherte ein entsprechendes Zugriffsrecht erteilt hat, vorgenommen werden.

**Verantwortlicher Akteur**

Krankenkasse	<ul style="list-style-type: none"> <li>▪ Verarbeitung von administrativen Daten im Aktensystem</li> <li>▪ Verarbeitung von Gesundheitsdaten im Aktensystem</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastuktur</li> </ul>
Anbieter des zentralen Netzes	<ul style="list-style-type: none"> <li>▪ Übermittlung der Daten der elektronischen Patientenakte</li> </ul>

**Elektronische Notfalldaten**

Der Versicherte kann sich entscheiden medizinische Daten, die für seine Notfallversorgung erforderlich sein können, auf seiner elektronischen Gesundheitskarte zu speichern.

**Verantwortlicher Akteur**

Krankenkasse	<ul style="list-style-type: none"> <li>▪ Verarbeitung der elektronischen Notfalldaten auf der elektronischen Gesundheitskarte</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastuktur</li> </ul>

**Hinweise auf das Vorhandensein und den Aufbewahrungsort von Vorsorgevollmachten oder Patientenverfügungen**

Der Versicherte kann sich entscheiden, auf seiner elektronischen Gesundheitskarte persönliche Erklärungen zu speichern, die Hinweise zum Ablageort und damit zugleich zum Vorhandensein von Patientenverfügungen und Vorsorgevollmachten enthalten.

**Verantwortlicher Akteur**

Krankenkasse	<ul style="list-style-type: none"> <li>▪ Verarbeitung der persönlichen Erklärungen auf der elektronischen Gesundheitskarte</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastuktur</li> </ul>

**Daten des elektronischen Medikationsplans**

Der Versicherte kann sich entscheiden, einen elektronischen Medikationsplan zur Prüfung der Arzneimitteltherapiesicherheit anzulegen. Derzeit werden diese Daten auf der elektronischen Gesundheitskarte des Versicherten gespeichert.

**Verantwortlicher Akteur**

Krankenkasse	<ul style="list-style-type: none"> <li>▪ Verarbeitung des elektronischen Medikationsplans auf der elektronischen Gesundheitskarte</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastuktur</li> </ul>

Daten des Versicherten, die über das sichere Übermittlungsverfahren „Kommunikation im Medizinwesen“ (kurz: KIM) übertragen werden

KIM ermöglicht den Leistungserbringern untereinander eine sichere digitale Kommunikation.

**Verantwortlicher Akteur**

Anbieter des KIM-Dienstes	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den Dienst</li> </ul>
Leistungserbringer	<ul style="list-style-type: none"> <li>▪ Verarbeitung der Daten durch den jeweiligen Leistungserbringer unter Verwendung der dezentralen Komponenten der Telematikinfrastruktur</li> </ul>
Anbieter des zentralen Netzes	<ul style="list-style-type: none"> <li>▪ Übermittlung der Daten</li> </ul>

**8. Die Pflichten der datenschutzrechtlich Verantwortlichen und die Rechte des Versicherten gegenüber den datenschutzrechtlich Verantwortlichen nach der Verordnung (EU) 2016/679**

Ein datenschutzrechtlich Verantwortlicher muss die nach der DSGVO **bestehenden datenschutzrechtlichen Pflichten** erfüllen. Zu diesen Pflichten zählen u.a.:

- die Einhaltung der Grundsätze der Datenverarbeitung nach der DSGVO und die Erbringung des Nachweises der Einhaltung (*Art. 5 Abs. 1 und 2 DSGVO*);
- die Umsetzung technischer und organisatorischer Maßnahmen zur Sicherstellung und des Nachweises der Einhaltung der DSGVO (*Art. 24, 25 und 32 DSGVO*);
- das Führen eines Verzeichnisses von Verarbeitungstätigkeiten (*Art. 30 DSGVO*);
- die Meldung von Datenschutzverletzungen ab deren Kenntnisnahme nach Möglichkeit binnen 72 Stunden bzw. die unverzügliche Benachrichtigung betroffener Personen (*Art. 33 und 34 DSGVO*);
- ggf. die Durchführung einer Datenschutz-Folgenabschätzung (*Art. 35 und 36 DSGVO*); und
- ggf. die Benennung eines Datenschutzbeauftragten (*Art. 37 DSGVO; vgl. auch § 38 BDSG*).

Zudem muss der Verantwortliche den **Rechten der betroffenen Person** nachkommen. Konkret haben die Versicherten als betroffene Personen nach der DSGVO die folgenden Rechte gegenüber Verantwortlichen:

- Recht auf **Information** (*Art. 12-14 DSGVO*): Recht, vom Verantwortlichen bestimmte Angaben (z.B. die Zwecke und Rechtsgrundlage der Verarbeitung sowie ggf. Dauer der Speicherung) mitgeteilt zu bekommen (grundsätzlich im Zeitpunkt der Erhebung der personenbezogenen Daten);
- Recht auf **Auskunft** (*Art. 15 DSGVO*): Recht, vom Verantwortlichen jederzeit Auskunft über bestimmte Informationen und eine Kopie der Daten zu verlangen;

- Recht auf **Berichtigung** (Art. 16 DSGVO): Recht, die Berichtigung unrichtiger Daten und ggf. Vervollständigung der Daten zu verlangen;
- Recht auf **Löschung** und „**Vergessenwerden**“ (Art. 17 DSGVO): Recht, vom Verantwortlichen in bestimmten Fällen (v.a. im Falle des Zweckfortfalls) die unverzügliche Löschung der Daten zu verlangen;
- Recht auf **Einschränkung der Verarbeitung** (Art. 18 DSGVO): Recht, in bestimmten Fällen die Einschränkung der Datenverarbeitung zu verlangen;
- Recht auf **Datenübertragbarkeit** (Datenportabilität) (Art. 20 DSGVO): Recht, Daten in einem strukturierten, gängigen und maschinenlesbaren Format vom Verantwortlichen zu erhalten oder an einen anderen Verantwortlichen zu übermitteln; und
- **Widerspruchsrecht** (Art. 21 DSGVO): Recht, der Datenverarbeitung in bestimmten Fällen zu widersprechen (z.B. bei Datenverarbeitung aufgrund eines berechtigten Interesses nach Art. 6 Abs. 1 S. 1 f) DSGVO).

## 9. Die Maßnahmen zur Datensicherheit

Alle Informationen zu den Maßnahmen zur Datensicherheit finden Sie ebenfalls im [Whitepaper Datenschutz und Informationssicherheit in der Telematikinfrastruktur](#).

## 10. Die Aufgaben der koordinierenden Stelle gemäß § 307 Absatz 5 Satz 2 und 3

Die Gesellschaft für Telematik richtet den Nutzern der Telematikinfrastruktur eine koordinierende Stelle ein. Die koordinierende Stelle stellt den Nutzern allgemeine Informationen zur Telematikinfrastruktur zur Verfügung und erteilt den Nutzern Auskünfte über Zuständigkeiten innerhalb der Telematikinfrastruktur. Hierzu gehören insbesondere die datenschutzrechtlich Verantwortlichen in der Telematikinfrastruktur, an die sich Betroffene bei datenschutzrechtlichen Anliegen wenden können. Sofern möglich, vermittelt die koordinierende Stelle Anfragen, die nicht unmittelbar von der koordinierenden Stelle selbst beantwortet werden können, an die zuständigen Stellen. Die koordinierende Stelle erreichen Sie über: [datenschutzlotse@gematik.de](mailto:datenschutzlotse@gematik.de)