Datenschutzerklärung

der Kaufmännischen Krankenkasse – KKH für die ePA-App

Inhaltsverzeichnis

A. Allgemeines 3

Vorbemerkung 4

A.1 Verantwortliche Stelle 4

A.2 Zuständige Aufsichtsbehörden 4

A.3 Allgemeines zur Datenverarbeitung 4

A.4 Anbieter der ePA-App 4

A.5 Einbindung von Dritten und Empfänger personenbezogener Daten 5

A.6 Datenerhebung von Informationen beim Download der ePA-App 5

A.7 Datenverarbeitung außerhalb der Europäischen Union 5

A.8 Betroffenenrechte 5

A.9 Löschung von Daten 5

A.10 Automatisierte Entscheidungsfindung 5

A.11 Beschwerderecht bei einer Aufsichtsbehörde 6

A.12 Recht auf Widerruf der Datenschutzerklärung 6

B. Registrierung, Identifizierung und Authentisierung 6

B.1 Registrierung und Identifizierung 6

B.2 Authentisierung (Anmeldung) 6

B.3 Authentisierung mittels GesundheitsID 7

B.4 Authentisierung mittels elektronischer Gesundheitskarte (eGK) 7

C. Bereitstellung der ePA durch die Krankenkasse 8

C.1 Beschreibung und Umfang der Datenverarbeitung 8

C.2 Push-Benachrichtigungen 9

C.3 Berechtigung vertretender Person 10

C.4 Rechtsgrundlage für die Datenverarbeitung 10

C.5 Zweck der Datenverarbeitung 10

C.6 Dauer der Speicherung 10

C.7 Widerspruchsmöglichkeiten für die Nutzung der ePA-App 11

C.8 Absprünge auf das Organspenderegister des Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) und gesund.bund.de 12

D. Nutzung Anwendung E-Rezept 12

D.1 Beschreibung und Umfang der Datenverarbeitung 12

D.2 Rechtsgrundlage für die Datenverarbeitung 12

D.3 Kartenfunktion 12

D.4 Zweck der Datenverarbeitung 13

D.5 Dauer der Speicherung 13

D.6 Widerrufsmöglichkeiten für die Nutzung der Anwendung E-Rezept-Moduls 13

E. Nutzung Anwendung TI-Messenger (TI-M) 13
E.1 Beschreibung und Umfang der Datenverarbeitung 13
E.1.1 Art der Daten 13
E.1.2 Push-Benachrichtigungen 14
E.2 Rechtsgrundlage für die Datenverarbeitung 15
E.3 Zweck der Datenverarbeitung 15
E.4 Dauer der Speicherung 15
E.5 Inhalte der Chat-Kommunikation 15
E.6 Hinweise zu den Rechten als Betroffener 15
E.7 Widerrufsmöglichkeiten für die Nutzung der Anwendung TI-Messenger 16
E.8 Hinweise zum Beschwerderecht 16

F. IAM-Registrierungsprozess für die ePA 16
F.1 Beschreibung und Umfang der Datenverarbeitung 16
F.2 Erfassung der Daten für einen Fehlerreport 16
F.2.1 Automatisiert übermittelte Daten 16
F.2.2 Manuell übermittelte Daten 17
F.3 Rechtsgrundlage für die Datenverarbeitung 17
F.4 Zweck der Datenverarbeitung 17
F.5 Dauer der Speicherung 17
F.6 Widerspruchmöglichkeiten gegen die ePA 17

G. Nutzung der ePA / Datenspeicher über die App 17
G.1 Beschreibung und Umfang der Datenverarbeitung für den Versicherten 17
G.1.1 Start mit Login Maske 17
G.1.2 Nutzung der ePA 18
G.1.3 Nutzung E-Rezept-Modul 18
G.1.4 Nutzung Organspende-Register (OGR) 18
G.1.5 Patientensouveränität in der ePA-App 18
G.2 Nutzung und Übermittlung von ePA-Daten für Forschungszwecke 19
G.2.1 Zweck und Voraussetzungen der Übermittlung 19
G.2.2 Kategorien der übermittelten Daten 19
G.2.3 Pseudonymisierung und beteiligte Stellen 19
G.2.4 Verwendung der Daten durch das Forschungsdatenzentrum 19
G.2.5 Dokumentation, Widerspruch und Löschung 20
G.3 Beschreibung und Umfang der Datenverarbeitung für vertretende Personen 20
G.4 Rechtsgrundlage für die Datenverarbeitung 20
G.4.1 Zweck der Datenverarbeitung 20
G.4.2 Dauer der Speicherung 20

H. Kontaktvarianten 21
H.1 Beschreibung und Umfang der Datenverarbeitung 21
H.2 ePA-Servicehotline 21
H.3 Chatbot 21
H.4 Vorgangsbearbeitungssystem (ITSM) 21
H.5 Rechtsgrundlage für die Datenverarbeitung 22
H.6 Zweck der Datenverarbeitung 22
H.7 Dauer der Speicherung 22
H.8 Speicherorte aller ePA-App-spezifischen Daten 22

A. Allgemeines

Die Informationen des Spitzenverbandes Bund der Krankenkassen zur elektronischen Patientenakte (ePA) nach § 343 Abs. 1a SGB V finden Sie als PDF auf unserer Website.

Die ePA-App ist die App der Kaufmännischen Krankenkasse (KKH). mit der Sie auf Ihre ePA sowie weitere Funktionen zugreifen können. Der Versicherte kann zwischen folgenden Anwendungen bzw. Absprüngen in der ePA-App wählen:

- Anwendung der ePA
- Anwendung Meine KKH (App)
- Anwendung E-Rezept
- Anwendung TI-Messenger (TI-M)
- Absprung zu Organspende-Register (OGR)
- Absprung zu gesund.bund

Mit diesen Funktionen ist die ePA-App ein zentraler Bestandteil der Digitalisierung im Gesundheitswesen und soll die medizinische Versorgung verbessern, indem relevante Gesundheitsdaten sicher und übersichtlich gespeichert und geteilt werden können.

Die ePA-App mit ihren Anwendungen wird all unseren Versicherten zur freiwilligen Nutzung zur Verfügung gestellt. Dieses Dokument enthält wichtige Informationen zur Datenverarbeitung im Rahmen der Nutzung der ePA-App.

Die Vorgaben zur ePA werden durch die Nationale Agentur für Digitale Medizin (gematik GmbH) unter der Rechtsaufsicht des Bundesministeriums für Gesundheit (BMG) sowie im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) erstellt.

Die Umsetzung dieser Vorgaben erfolgt unter strengen Sicherheitsauflagen und sowohl der Entwicklungsprozess selbst, der Programmcode als auch der Betrieb der Lösung werden durch unabhängige, zertifizierte und akkreditierte Stellen im Rahmen einer Zulassung sowie kontinuierlichen Audits geprüft. Für jede Zulassung ist ein Sicherheitsgutachten erforderlich, das sowohl eine technische als auch eine funktionale Eignung prüft.

Vorbemerkung
Im Sinne einer besseren Lesbarkeit und eines vereinfachten Bearbeitungsverfahren wurde die gendergerechte Ansprache durch die einheitliche Verwendung der Formulierungen:

- „Versicherter“
- „Vertreter“
- „Nutzer“

ersetzt. Mit der Benutzung dieser Begriffe sind immer ohne Einschränkung alle Geschlechter gemeint.

Kompatible Endgeräte und Betriebssysteme
Die ePA-App ist für die Nutzung auf mobilen Endgeräten (z. B. Smartphones) sowie auf stationären Endgeräten (z. B. PCs, Laptops) vorgesehen. Im weiteren Verlauf dieses Dokuments wird die Anwendung auf mobilen Endgeräten als mobile ePA-App und auf stationären Endgeräten als Desktop-ePA-App bezeichnet. Sofern der Begriff ePA-App ohne weitere Spezifizierung verwendet wird, bezieht sich dieser auf beide Varianten.
Die mobile ePA-App ist für die Betriebssysteme iOS und Android verfügbar. Die Desktop-ePA-App kann unter den Betriebssystemen Windows, macOS und Linux verwendet werden.

A.1 Verantwortliche Stelle

Die verantwortliche Stelle im Sinne von §§ 341 Abs. 4 Satz 1, 307 Abs. 4 SGB V in Verbindung mit Art. 4 Ziffer 7 der Datenschutz-Grundverordnung ist die:

Kaufmännische Krankenkasse – KKH
Karl-Wiechert-Allee 61
30625 Hannover
Telefon: 0800 5548640554
E-Mail: datenschutzservice@kkh.de

Unsere Datenschutzbeauftragte erreichen Sie unter der o. g. Anschrift oder per E-Mail unter: ***datenschutz@kkh.de***

A.2 Zuständige Aufsichtsbehörden

Die Bundesdatenschutzbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorfer Straße 153, 53117 Bonn
Telefon: +49 (0)228 997799-0
Fax: +49 (0)228 997799-5550
E-Mail: poststelle@bfdi.bund.de

Bundesamt für Soziale Sicherung
Friedrich-Ebert-Allee 38, 53113 Bonn
Telefon: +49 (0)228-619-0
Telefax +49 (0)228619-1870

A.3 Allgemeines zur Datenverarbeitung

Wir verarbeiten personenbezogene Daten unserer Versicherten, soweit dies zur Bereitstellung bzw. Nutzung einer funktionsfähigen ePA erforderlich ist. Sofern kein Widerspruch gegen die ePA für alle vorliegt, erfolgt die Verarbeitung personenbezogener Daten unserer Versicherten auf der Grundlage der dahingehenden gesetzlichen Verpflichtung aus § 344 SGB V. Die ePA wird kraft Gesetzes allen unseren Versicherten zur Verfügung gestellt (vgl. § 342 Abs. 1 SGB V).

Die Nutzung der ePA-App ist für unsere Versicherten freiwillig. Sie werden von uns weder bevorzugt noch benachteiligt, wenn Sie von Ihrem Widerspruchsrecht Gebrauch machen.

A.4 Anbieter der ePA-App

Die ePA-App, sowie alle dazugehörigen Anwendungen (ePA, TI-Messenger, E-Rezept), werden Ihnen von Ihrer KKH angeboten. Dabei arbeitet die Krankenkasse mit Industriepartnern zusammen, die die ePA-App technisch entwickeln und betreiben. Sie müssen grundlegende Vorgaben der gematik GmbH einhalten und ein strenges Zulassungsverfahren durchlaufen. Dies dient der Sicherheit Ihrer Daten.

A.5 Einbindung von Dritten

Für die Bereitstellung und Nutzung der ePA-App arbeitet die KKH mit technischen Dienstleistern zusammen. Hierzu gehören insbesondere Unternehmen der BITMARCK-Unternehmensgruppe sowie gegebenenfalls weitere eingebundene Dienstleister.
Personenbezogene Daten werden nur weitergegeben oder zugänglich gemacht, soweit dies für die jeweilige Funktion erforderlich ist, eine entsprechende Berechtigung vorliegt oder eine gesetzliche Befugnis beziehungsweise Verpflichtung besteht.

Abhängig von der genutzten Funktion können insbesondere folgende Stellen Empfänger personenbezogener Daten sein:

- Technische Dienstleister: Anbieter und Betreiber der ePA-App, des ePA-Aktensystems und weiterer technischer Dienste einschließlich eingesetzter Unterauftragnehmer.
- Leistungserbringende: Beispielsweise Arztpraxen, Krankenhäuser und Apotheken, soweit diese nach den gesetzlichen Vorgaben zum Zugriff berechtigt sind.
- Dienste der Telematikinfrastruktur: Zugelassene Anbieter und Betreiber der GesundheitsID, des E-Rezepts, des TI-Messengers sowie weiterer erforderlicher Dienste.
- Identifizierungsdienstleister: Anbieter der für die Registrierung, Identifizierung und Authentisierung eingesetzten Verfahren.
- Berechtigte Personen und Stellen: Von Versicherten eingerichtete Vertretungen sowie die Ombudsstelle der KKH im Rahmen ihrer jeweiligen Aufgaben.
- Externe Dienste: Beispielsweise Anbieter von Karten- und Suchfunktionen, Push-Benachrichtigungen oder App-Stores, soweit die entsprechenden Funktionen genutzt werden.

Nicht jeder Empfänger erhält Zugriff auf sämtliche personenbezogenen Daten. Art und Umfang der Verarbeitung richten sich nach der jeweiligen Funktion, den gesetzlichen Vorgaben und den erteilten Berechtigungen. Technische Dienstleister, die personenbezogene Daten im Auftrag der KKH verarbeiten, werden entsprechend den datenschutzrechtlichen Anforderungen vertraglich verpflichtet. Soweit Stellen personenbezogene Daten zur Erfüllung eigener gesetzlicher Aufgaben oder in eigener datenschutzrechtlicher Verantwortung verarbeiten, gelten die jeweiligen gesetzlichen Bestimmungen und Datenschutzhinweise dieser Stellen. Weitere Informationen zu den einzelnen Datenverarbeitungen finden Sie in den nachfolgenden Kapiteln dieser Datenschutzerklärung.

A.6 Datenerhebung von Informationen beim Download der ePA-App

Der Download der ePA-App erfolgt je nach Version über die Stores von Apple, Google und Microsoft oder über die Webseite ***epaclient.de***. Beim Herunterladen der App werden notwendige Informationen an den von Ihnen gewählten Store von Apple, Google oder Microsoft übermittelt. Dabei kann es sich um personenbezogene Daten handeln. Die Verantwortung für die Datenverarbeitung liegt ausschließlich bei den jeweiligen Stores von Apple, Google oder Microsoft.

A.7 Datenverarbeitung außerhalb der Europäischen Union

Eine Verarbeitung der Daten unserer Versicherten außerhalb der Europäischen Union findet nicht statt. Alle ePA-bezogenen Datenverarbeitungen finden ausschließlich in Deutschland statt.

A.8 Betroffenenrechte

Unsere Versicherten haben folgende Rechte:

- Das Recht auf Auskunft nach Art. 15 DSGVO über die sie betreffenden personenbezogenen Daten. Diesbezüglich können sich unsere Versicherten jederzeit an uns wenden.
- Das Recht auf Berichtigung unrichtiger Daten nach Art. 16 DSGVO oder auf Löschung nach Art. 17 DSGVO oder auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, soweit ihnen dieses Recht gesetzlich zusteht.
- Ein Widerspruchsrecht gegen die Verarbeitung der personenbezogenen Daten im Rahmen der gesetzlichen Vorgaben.

A.9 Löschung von Daten

Wir löschen die ePA unserer Versicherten grundsätzlich dann, wenn ein Widerspruch gegen die ePA vorliegt. Widersprüche, die die Versicherten über ihre ePA-App abgeben, führen zur sofortigen Löschung der gesamten Akte. Widersprüche gegen die, die bei der Krankenkasse eingereicht werden, können zu einer späteren Löschung der gesamten Akte führen.

Dieser Aufschub bis zur Umsetzung der vollständigen und unwiderruflichen Löschung soll den Versicherten Zeit und die Möglichkeit bieten, um ihre Dokumente herunterzuladen und zu sichern.

A.10 Automatisierte Entscheidungsfindung

Wir setzen keine Verarbeitungsvorgänge ein, die auf einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 DSGVO beruhen.

A.11 Beschwerderecht bei einer Aufsichtsbehörde

Unsere Versicherten haben das Recht, sich über die Verarbeitung personenbezogener Daten bei einer der in Ziffer A.3 genannten Aufsichtsbehörden zu beschweren.

A.12 Recht auf Widerruf der Datenschutzerklärung

Eine datenschutzrechtliche Einwilligungserklärung ist mit der Einführung der ePA 3.0 und abweichend von den vorherigen Versionen obsolet, weil die ePA kraft gesetzlicher Vorgabe grundsätzlich allen Versicherten zur Verfügung gestellt wird. Hierbei ist keine datenschutzrechtliche Einwilligungserklärung der Versicherten mehr erforderlich.

B. Registrierung, Identifizierung und Authentisierung

Für die Nutzung der ePA-App ist in der Regel eine personenbezogene Registrierung, eine sichere Identifizierung sowie eine fortlaufende Authentisierung erforderlich. Diese mehrstufigen Verfahren dienen der eindeutigen Feststellung der Identität der nutzenden Person und der Absicherung des Zugriffs auf sensible Gesundheitsdaten. Die Verarbeitung der dabei erhobenen personenbezogenen Daten erfolgt zur Erfüllung gesetzlicher Vorgaben gemäß Art. 6 Abs. 1 lit. a DSGVO in Verbindung mit den Bestimmungen des Sozialgesetzbuches Fünftes Buch (SGB V), insbesondere den §§ 291a und 336 ff. SGB V, sowie unter Berücksichtigung der Anforderungen an den Schutz besonders schützenswerter Gesundheitsdaten nach Art. 9 DSGVO.

B.1 Registrierung und Identifizierung

Registrierung bezeichnet den ersten Schritt, bei dem Versicherte ihre persönlichen Daten angeben, um ein Benutzerkonto in der Anwendung zu erstellen. Dies umfasst typischerweise Angaben wie Name, Geburtsdatum, Krankenversichertennummer und E-Mail-Adresse. Die Registrierung ermöglicht eine individuelle Zuordnung der App-Nutzung zur jeweiligen Person und legt die Grundlage für alle weiteren Funktionen.

Identifizierung ist der Prozess der eindeutigen Feststellung der Identität des Versicherten.
Dies ist besonders wichtig bei Anwendungen, die sensible Gesundheitsdaten verarbeiten. Zur sicheren Identifizierung werden gesetzlich vorgeschriebene Verfahren verwendet, beispielsweise die Nutzung der elektronischen Gesundheitskarte mit PIN oder die Online-Ausweisfunktion des Personalausweises. Durch die Identifizierung wird sichergestellt, dass nur berechtigte Personen Zugriff auf ihre persönlichen Gesundheitsdaten erhalten.

Über das Profil (Icon Profilbild) kann der Versicherte seine persönlichen Daten zu seinem Benutzerkonto verwalten. Sie müssen bei der erstmaligen Registrierung als versicherte Person folgenden Dokumenten zustimmen:

- Einwilligungserklärung zum IAM (Einwilligung in die Nutzung des IAM)
- Nutzungsbedingungen des IAM

B.2 Authentisierung (Anmeldung)

Authentisierung bezeichnet die Überprüfung der Zugriffsberechtigung des Versicherten beim Anmelden bzw. Login in der Anwendung.

Dabei kommen sichere Verfahren zum Einsatz, wie Passwörter, PINs, biometrische Merkmale (z. B. Fingerabdruck oder Gesichtserkennung) oder Mehr-Faktor-Authentifizierung. Die Authentisierung schützt die Daten vor unbefugtem Zugriff und gewährleistet, dass nur autorisierte Versicherte auf die geschützten Informationen zugreifen können.

B.3 Authentisierung mittels GesundheitsID

Für den Zugriff auf die Anwendungen in der ePA-App (d.h. die Anmeldung) erfolgt die Authentisierung der Versicherten über die sog. GesundheitsID – die digitale Identität im Gesundheitswesen. Dieses Verfahren gewährleistet eine sichere und datenschutzkonforme Authentisierung im Gesundheitswesen.

Voraussetzung für die Nutzung der GesundheitsID ist die vorherige Anlage eines Benutzeraccounts durch die Registrierung und Identifizierung in der ePA-App. Dabei wird sichergestellt, dass nur berechtigte Versicherte eine digitale Identität erhalten, die anschließend für die Authentisierung genutzt werden kann.

Die Verarbeitung personenbezogener Daten im Rahmen der Authentisierung via GesundheitsID dient ausschließlich dem Zweck, die berechtigte Nutzung der digitalen Gesundheitsdienste sicherzustellen. Hierdurch wird gewährleistet, dass nur der rechtmäßige Versicherte Zugriff auf seine Gesundheitsdaten erhält.

Mithilfe der GesundheitsID können Versicherte auf die Anwendungen innerhalb der ePA-App zugreifen. Hierzu gehören:

- Anwendung ePA
- Anwendung E-Rezept
- Anwendung TI-Messenger
- Absprung und Authentisierung am Organspende-Register

B.4 Authentisierung mittels elektronischer Gesundheitskarte (eGK)

Im Rahmen der kontinuierlichen Weiterentwicklung der Sicherheits- und Nutzungsprozesse für den Zugriff auf die Anwendung der ePA wird neben der Authentisierung mittels GesundheitsID an der Desktop-ePA-App eine alternative Zugangsoption angeboten: die Authentisierung **mittels der eGK** und der dazugehörigen **persönlichen Identifikationsnummer (PIN)**.

Diese alternative Authentisierungsmethode erfordert keine vorherige Registrierung oder separate Identifizierung des Versicherten. Es wird kein Benutzeraccount angelegt; es handelt sich somit um einen „Gastzugang “(Anmeldung ohne Benutzeraccount). Die Authentisierung erfolgt direkt über die Daten der elektronischen Gesundheitskarte einschließlich der PIN.

Der Funktionsumfang bei Nutzung der Authentisierung via eGK und PIN ist eingeschränkt und beschränkt sich ausschließlich auf den Zugang zur elektronischen Patientenakte (ePA). Die Nutzung weiterer digitaler Gesundheitsanwendungen ist über diesen Zugangsweg nicht möglich.

Umfang der verarbeiteten Daten
Im Rahmen der Authentisierung mittels eGK und PIN werden folgende personenbezogene Daten verarbeitet:

- Persönliche PIN
- Krankenversichertennummer
- Zugangsnummer

Diese Daten werden während des Authentisierungsprozesses temporär gespeichert und ausschließlich zur Verifikation der Berechtigung zur Nutzung der ePA verwendet.

Die vorstehend genannten Daten werden nur so lange gespeichert, wie dies zur Erfüllung des Zwecks der Authentisierung erforderlich ist. Nach erfolgreicher Verifikation und Wegfall des Zwecks werden die Daten unverzüglich gelöscht.

C. Bereitstellung der ePA durch die Krankenkasse

C.1 Beschreibung und Umfang der Datenverarbeitung

Die ePA wird allen unseren Versicherten zur Verfügung gestellt. Wir legen eine individuelle und ausschließlich von unserem Versicherten verwendete ePA an, welche unser Versicherter eigenständig souverän und autonom verwalten und verwenden kann. Ein Versicherter kann in seiner ePA eine oder mehrere vertretende Personen, hinzufügen; siehe hierzu Kapitel D.2.

Bei der Bereitstellung der ePA werden folgende personenbezogene Daten unseres Versicherten herangezogen:

- Angaben des amtlichen Ausweisdokuments
- Anzahl der aktiven elektronischen Gesundheitskarten (eGK). Die Anzahl der aktiven eGK, die dem identifizierten Versicherten im eGK-System zugeordnet sind. Eine Karte gilt dabei im eGK-System als aktiv, wenn sie weder gesperrt oder logisch gelöscht ist. In der Regel ist immer nur eine eGK aktiv.
- Name, Vorname
- Geburtsdatum des Versicherten
- Geburtsort des Versicherten
- Versichertenart (z. B.: Mitglied, Familienversicherter, Rentner)
- Beginn und Ende des Versicherungsverhältnisses
- IdentDataTime (Zeitstempel für die vollzogene Identifizierung des Versicherten)
- Schutzklasse für die Identifikation (mit oder ohne eGK)
- Identifizierungsverfahren (z. B. in der Filiale oder Postident)
- Meldeadresse: Länderkennzeichen, PLZ, Ort; Straße, Hausnummer
- Ende der Registrierung (Ja oder Nein)
- Zeitpunkt Registrierungsbeginn
- Titel
- Namenszusatz
- Vorsatzwort (z. B.: „von“, „de“, „van“)
- Geschlecht
- je nach verwendetem Authentisierungsmittel:
  - ein Pseudonym bei Nutzung der Online-Ausweisfunktion. Dabei ruft der verwendete Anbieter erstmalig alle uns zugänglichen Daten des Personalausweises zum Personenabgleich ab und erzeugt ein Pseudonym. Jedes weitere Mal erfolgt der Abgleich durch das vom Anbieter erzeugte Pseudonym.
  - das Zertifikat der eGK bei Nutzung der elektronischen Gesundheitskarte
- VIP-Kennzeichen
- ICCSN (Kartenkennnummer auf der Rückseite der eGK)

- istNfcEgk (Dieser Wert gibt an, ob die im Aufruf bezeichnete eGK für „Near Field Communication“ (NFC) ausgerüstet ist.)
- istPinBriefVersandt (Dieser Wert gibt an, ob zu der im Aufruf bezeichneten eGK ein PIN-Brief versandt wurde.)
- pinBriefVersandDatum (Zeitpunkt zu dem der PIN-Brief-Versand dem KAMS (Kartenanwendungsmanagementsystem) gemeldet wurde.)

Hinweis für Android-Geräte: Die ePA-App bietet eine Dokumentenscan-Funktion, mit der physische Dokumente per Gerätekamera erfasst und verarbeitet werden können. Unter Android basiert diese Funktion auf dem Google-Dienst ML Kit. Für die Nutzung ist daher unter Android eine gesonderte Zustimmung zu den ergänzenden Nutzungsbedingungen erforderlich. Die Verarbeitung der gescannten Inhalte erfolgt ausschließlich lokal auf Ihrem Gerät, es werden keine Dokumentinhalte an Google oder Dritte übermittelt. Google kann jedoch technische Nutzungsdaten (z. B. Geräteinformationen, Leistungsdaten) für Stabilität und Fehleranalyse erheben, ohne Bezug zu den gescannten Dokumenten.

C.2 Push-Benachrichtigungen

Die mobile ePA-App bietet die Möglichkeit, Push-Benachrichtigungen an das Endgerät des Versicherten zu übermitteln, um diesen über Ereignisse in seiner elektronischen Patientenakte zu informieren, beispielsweise über neu eingestellte Dokumente. Diese Funktion ist standardmäßig deaktiviert. Die Nutzung setzt voraus, dass der Versicherte Push-Benachrichtigungen sowohl in der ePA-App als auch in den Betriebssystemeinstellungen seines Endgeräts manuell aktiviert. Die Aktivierung erfolgt auf freiwilliger Basis und kann vom Versicherten jederzeit mit Wirkung für die Zukunft über die Einstellungen des Endgeräts widerrufen werden. Rechtsgrundlage für die im Rahmen der Push-Benachrichtigungen erfolgenden Datenverarbeitungen ist die Einwilligung des Versicherten gemäß Art. 6 Abs. 1 lit. a DSGVO.

Technische Datenübermittlung

Für die Übermittlung von Push-Benachrichtigungen werden technische Dienste der jeweiligen Betriebssystemhersteller (Push Provider) eingesetzt. Bei der erstmaligen Aktivierung der Funktion wird durch den Push Provider ein gerätespezifischer Identifikator (Push-Token) erzeugt und in der Folge an den ePA-Aktensystemdienst übermittelt. Auf der Grundlage dieses Push-Tokens erfolgt die Zustellung von Benachrichtigungen an das Endgerät des Versicherten.

Verarbeitete Daten

Im Rahmen der Zustellung von Push-Benachrichtigungen werden die nachfolgend aufgeführten Daten verarbeitet:

- Push-Token des Endgeräts (gerätespezifischer Identifikator)
- Technische Geräteinformationen (insbesondere Gerätetyp und App-Identifier)
- Zeitpunkt der Erstellung der Push-Benachrichtigung
- Anzahl der ungelesenen Push-Benachrichtigungen
- Kennung des Kostenträgers des Versicherten (Weitergabe ausschließlich an den App-Anbieter; eine Übermittlung an den Push Provider oder den Aktensystemdienst erfolgt nicht)
- Verschlüsselte Benachrichtigungsinhalte (Nachricht, Empfänger, Ereignisart, z.B. „Neues Dokument verfügbar“), die ausschließlich durch die ePA-App und den jeweiligen Fachdienst entschlüsselt werden können – dem Push Provider sind diese Inhalte technisch nicht zugänglich

Eingesetzte Push Provider

In Abhängigkeit vom verwendeten Betriebssystem werden folgende plattformspezifische Push Provider eingesetzt:

- **Apple iOS:** Apple Push Notification Service (APNs), Apple Inc., USA
- **Android:** Firebase Cloud Messaging (FCM), Google LLC, USA

Datenschutzniveau und Drittlandübermittlung
Im Rahmen der Nutzung der eingesetzten Push Provider kann nicht ausgeschlossen werden, dass die Daten in Drittländer außerhalb der Europäischen Union (z.B in die USA), übertragen werden. Für diese Drittländer besteht möglicherweise kein mit der Europäischen Union vergleichbares Datenschutzniveau. Bei den an die Push Provider übermittelten Daten handelt es sich jedoch nicht um Nachrichteninhalte, da diese ausschließlich in verschlüsselter Form übertragen werden und den Push Providern technisch nicht zugänglich sind.

Typische Risiken einer Drittlandübermittlung:
- Mögliche Erschwernis bei der Durchsetzung von Betroffenenrechten, insbesondere hinsichtlich Auskunfts- und Löschungsansprüchen
- Fehlende oder eingeschränkte Möglichkeit zur Kontrolle einer Weiterverarbeitung oder Weiterübermittlung der Daten durch den Push Provider
- Fehlende oder eingeschränkte Datenschutzaufsicht durch unabhängige Behörden
- Möglicher Zugriff staatlicher Stellen auf die beim Push Provider gespeicherten Daten ohne wirksamen Rechtsschutz

Spezifisches Risiko in Bezug auf die übermittelten Daten:
Die im Rahmen der Push-Benachrichtigung an den Push Provider übermittelten Daten enthalten weder Gesundheitsdaten noch Kommunikationsinhalte, da Benachrichtigungsinhalte ausschließlich in verschlüsselter Form übermittelt werden und dem Push Provider technisch nicht zugänglich sind.
Ein Risiko, dass ein Zugriff auf sensible personenbezogene Daten erfolgen kann, ist vor diesem Hintergrund als sehr gering zu bewerten.

Für die Nutzung des Dienstes Firebase Cloud Messaging gelten ergänzend die Datenschutz- und Sicherheitshinweise zu Firebase sowie die allgemeine Google Datenschutzerklärung. Für die Nutzung des Apple Push Notification Service gilt die Apple Datenschutzrichtlinie.

C.3 Berechtigung vertretender Person
Versicherte können für ihre Patientenakte eine oder mehrere vertretende Personen berechtigen.
Die vertretende Person nutzt die eigene ePA-App ihrer Krankenkasse zur Wahrnehmung der Vertretung. Bei der Einrichtung werden der Name, die E-Mail-Adresse und die Versichertennummer (KVNR) angegeben und gespeichert. Wenn die vertretende Person in der Patientenakte als Vertretung handelt, können alle technisch möglichen Aktionen anstelle des Versicherten ausgeführt werden.

Vertretende Personen können keine weiteren vertretenden Personen für die vertretene Patientenakte einrichten und auch nicht die Patientenakte für den Versicherten insgesamt widersprechen. Bei der Vertretung innerhalb der ePA erfolgt eine Datenverarbeitung wie in Kapitel C.1 beschrieben.

C.4 Rechtsgrundlage für die Datenverarbeitung
Rechtsgrundlage für die Anlage der ePA ist § 344 Abs. 1 Satz 1 SGB V.

C.5 Zweck der Datenverarbeitung
Die Verarbeitung personenbezogener Daten im Rahmen der Registrierung, Identifizierung und Authentisierung dient im Gesundheitswesen folgenden Zwecken:
- Rechtssichere Identifikation der versicherten Person zur Erstellung und Nutzung einer digitalen Identität im Sinne der gesetzlichen Vorgaben, insbesondere zur Nutzung der elektronischen Patientenakte (ePA), des E-Rezepts sowie weiterer digitaler Gesundheitsanwendungen.
- Sicherstellung des Zugriffs nur durch berechtigte Personen und Schutz besonders schützenswerter Gesundheitsdaten gemäß Art. 9 DSGVO.
- Verhinderung von Identitäts- und Datenmissbrauch durch den Einsatz starker Authentisierungsverfahren und zertifizierter Identitätsprüfungen.

C.6 Dauer der Speicherung

Die Daten werden gelöscht, sobald sie für die Erreichung des Zwecks ihrer Erhebung nicht mehr erforderlich sind und keine Aufbewahrungspflichten mehr bestehen.

C.7 Widerspruchsmöglichkeiten für die Nutzung der ePA-App

Versicherte haben im Zusammenhang mit der Nutzung der elektronischen Patientenakte (ePA) verschiedene Widerspruchsmöglichkeiten. Diese richten sich nach den Vorgaben des Fünften Sozialgesetzbuches (§§ 344 und 353 SGB V) sowie der Datenschutz-Grundverordnung (DSGVO).

1. **Widerspruch gegen die Nutzung der ePA insgesamt** (§ 342 Abs. 2 Nr. 1 lit. g SGB V)
   Die Nutzung der ePA ist freiwillig. Versicherte können der Einrichtung oder weiteren Nutzung der ePA jederzeit widersprechen. Infolge des Widerspruchs wird die ePA deaktiviert, und alle darin gespeicherten Daten werden gemäß den gesetzlichen Vorgaben gelöscht. Weitere Informationen hierzu finden Sie unter Kapitel 3.5

2. **Widerspruch gegen Zugriffe durch Leistungserbringende** (§ 342 Abs. 2 Nr. 1 lit. h SGB V)
   Versicherte haben jederzeit die Möglichkeit, einzelne Leistungserbringende (z.B. Arztpraxen, Apotheken, Krankenhäuser) den Zugriff auf ihre ePA zu verweigern. Infolgedessen können diese Leistungserbringende nicht (mehr) auf die Akte zugreifen – auch nicht im Rahmen eines Behandlungskontextes.

3. **Widerspruch gegen das Einstellen von Leistungsauskünften durch die Krankenkasse** (§ 342 Abs. 2 Nr. 1 lit. g SGB V)
   Gemäß § 341 SGB V können gesetzliche Krankenkassen Auskünfte zu in Anspruch genommenen Leistungen automatisiert in die ePA übermitteln. Versicherte können dieser Datenübermittlung jederzeit widersprechen. Die Krankenkasse ist in diesem Fall verpflichtet, keine weiteren Leistungsauskünfte in die ePA zu übertragen und zu speichern. Ein bereits erfolgter Datenimport bleibt vom Widerspruch unberührt, kann aber manuell durch die versicherte Person mithilfe der ePA-App gelöscht werden.

4. **Widerspruch gegen die Teilnahme am digital gestützten Medikationsprozess** (§ 342 Abs. 2a Nr. 1 lit. d SGB V)
   Die Teilnahme am digital gestützten Medikationsprozess nach § 360 Abs. 2 SGB V ermöglicht es, die elektronische Medikationsliste, (E-Rezept-Daten, vgl. Punkt 5), den elektronischen Medikationsplan sowie Informationen zur Arzneimitteltherapiesicherheit innerhalb der ePA bereitzustellen und durch berechtigte Leistungserbringende, wie Arztpraxen, zu verwalten.

   Versicherte können dieser Teilnahme jederzeit widersprechen. Die Folge ist, dass im Behandlungsalltag durch Leistungserbringende keine Medikationsdaten aus der ePA verwendet und eingesehen werden können. Zudem werden in der ePA bereits gespeicherte Informationen zum elektronischen Medikationsplan und Informationen zur Arzneimitteltherapiesicherheit gelöscht. Eine erneute Speicherung solcher Informationen in der ePA ist ausgeschlossen, solange der Widerspruch besteht.

5. **Widerspruch gegen das Einstellen von E-Rezept-Daten aus dem E-Rezept-Fachdienst in die ePA** (§ 342 Abs. 2a Nr. 1 lit. d SGB V)
   Versicherte können zudem der automatisierten Übernahme von E-Rezept-Daten aus dem E-Rezept-Fachdienst in die ePA widersprechen.

   Ein solcher Widerspruch hat zur Folge, dass keine Verordnungs- und Dispensierdaten aus E-Rezepten mehr in der ePA gespeichert werden. Sofern entsprechende Daten bereits in der ePA vorhanden sind, werden diese gelöscht. Ein solcher Widerspruch schließt automatisch die Teilnahme am digital gestützten Medikationsprozess (vgl. Punkt 4) aus.

Versicherte haben verschiedene Möglichkeiten, ihre Widerspruchsrechte im Zusammenhang mit der ePA auszuüben. Die Ausübung dieser Rechte kann entweder eigenständig über die ePA-Anwendung oder mithilfe ihrer Krankenkasse bzw. Ombudsstelle (§§ 342 Abs. 2 Nr. 1 lit. s, t und 342a SGB V) erfolgen

C.8 Absprünge auf das Organspenderegister des Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) und gesund.bund.de

Für alle Inhalte im Organspenderegister ist die Bundeszentrale für gesundheitliche Aufklärung verantwortlich. Für alle Inhalte auf ***gesund.bund.de*** ist das Bundesministerium für Gesundheit verantwortlich

D. Nutzung Anwendung E-Rezept

D.1 Beschreibung und Umfang der Datenverarbeitung

Der Versicherte kann in der ePA-App über das E-Rezept-Modul alle elektronischen Verordnungen, die von Ärztinnen und Ärzten sowie Zahnärztinnen und Zahnärzten ausgestellt wurden, über den Fachdienst E-Rezept abrufen. Dabei werden die Daten wie in Kapitel B.1 beschrieben verarbeitet sowie Standortdaten und Versichertennummer. Die Anmeldung am Fachdienst E-Rezept erfolgt über einen elektronischen Identitätsnachweis (z. B. elektronische Gesundheitskarte oder 2D-Code) welches Versichertenstammdaten (z. B. Name und Versichertennummer) enthält.

Kommunikation zwischen ePA-App und Apotheken

Rezepte: Apotheken erhalten das Zugriffsrecht für das im Fachdienst E-Rezept gespeicherte E-Rezept. Eine direkte Kommunikation zwischen der ePA-App und der Apotheke erfolgt dabei nicht, da die ePA-App direkt mit dem Kommunikationssystem der Apotheke kommuniziert.
Mitteilungen: Die Kommunikation mit der Apotheke läuft über den Fachdienst E-Rezept, der die Mitteilungen archiviert. Die ePA-App lädt die Mitteilungen vom Fachdienst E-Rezept und speichert sie auf dem Gerät.

D.2 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Nutzung des E-Rezept-Moduls ist die Einwilligung unseres Versicherten gemäß Art. 6 Abs. 1 lit. a DSGVO i. V. m. § 360 Abs. 10 SGB V.

Kommunikation zwischen Apotheken und Versicherten via ePA-App

Es besteht die Möglichkeit Mitteilungen zwischen Apotheke und Versicherten auszutauschen. Die Archivierung der Nachrichten erfolgt über den E-Rezept-Fachdienst. Die ePA-App ruft die Mitteilungen aus dem E-Rezept-Fachdienst ab und speichert sie lokal auf dem Gerät. Der Nachrichtenaustausch erfolgt zweckgebunden in Bezug auf das Einlösen eines E-Rezeptes. E-Rezepte, unabhängig davon, ob sie eingelöst wurden oder nicht, werden spätestens nach 100 Tagen im Fachdienst gelöscht. Damit erfolgt auch eine Löschung des zweckgebundenen Nachrichtenaustausches.

D.3 Kartenfunktion

Bei Verwendung der Apothekensuche werden Ihre Suchkriterien (z.B. Adressen oder Standortdaten) an einen sogenannten FHIR-Verzeichnisdienst übermittelt. Der FHIR-Verzeichnisdienst ist ein technischer Dienst, der auf Basis eines standardisierten Datenformats Informationen zu Leistungserbringern wie z.B. Apotheken bereitstellt. Der FHIR-Verzeichnisdienst stellt der App daraufhin eine Liste mit den zu den Suchkriterien passenden Apotheken bereit.

Hinweis für Android-Geräte: Für die Kartenansicht nutzt die App mit Ihrer Zustimmung den Kartendienst Google Maps. Die App übergibt dann Ihren Standort (sofern Sie diesen freigegeben haben) und die Standorte der gefundenen Apotheken an eine Schnittstelle Ihres Betriebssystems (Google Maps- Schnittstelle). Diese Schnittstelle ist Bestandteil der Google Play Services, die auf Ihrem Gerät bereits installiert sind. Für die Nutzung von Google Maps gelten die Nutzungsbedingungen für Google Maps/Google Earth und die Google Datenschutzerklärung.

D.4 Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die Nutzung der Anwendung E-Rezept durch den Versicherten zum Abruf und zur Einlösung von ausgestellten Rezepten.

D.5 Dauer der Speicherung

Für den Versicherten besteht die Möglichkeit Rezepte selbst zu löschen, ansonsten werden die Rezepte nach 100 Tagen durch den Fachdienst E-Rezept gelöscht (§ 360 Abs. 11 SGB V). Zugriffsprotokolle im Fachdienst E-Rezept werden nicht auf dem Gerät gespeichert und können nicht gelöscht werden (automatische Löschung nach drei Jahren (§ 309 SGB V).

D.6 Widerrufsmöglichkeiten für die Nutzung der Anwendung E-Rezept-Moduls

Die unter diesem Abschnitt beschriebenen Datenverarbeitungen sind zur Nutzung des E-Rezept-Moduls durch den Versicherten zwingend erforderlich. Der Versicherte kann seine Einwilligung zur Nutzung des E-Rezept-Moduls jederzeit widerrufen, durch Entfernen des gesetzten Bestätigungshakens in der ePA-App.

E. Nutzung Anwendung TI-Messenger (TI-M)

E.1 Beschreibung und Umfang der Datenverarbeitung

Der Versicherte kann in der ePA-App über den TI-M mit berechtigten Akteuren (Leistungserbringer, Leistungserbringerinstitutionen, Kostenträger) kommunizieren, sofern diese einer Gesprächseinladung durch den Versicherten zustimmen. Darüber hinaus können berechtigte Akteure den Versicherten kontaktieren, wenn dieser einer Kommunikation zustimmt.

Kommunikation zwischen dem TI-M in der ePA-App und anderen TI-M-Teilnehmern

Die Kommunikation findet über den TI-M in der ePA-App des Versicherten statt und befähigt diesen mit anderen von der gematik zugelassenen TI-M-Diensten zu kommunizieren.
Die Kommunikation zwischen den TI-M-Diensten erfolgt end-to-end-verschlüsselt.
Die Adressierung der Akteure innerhalb von TI-M erfolgt über die TI-M-Adresse. Zusätzlich zu den technischen systemseitigen Prüfungen, die im Hintergrund stattfinden, soll der TI-M-Nutzer selbst bestimmen können, wer ihn in neue Chaträume einladen darf. Dies dient dem Nutzer zur eigenständigen Steuerung seines Chataufkommens.

E.1.1 Art der Daten

Die Krankenkasse erhebt und verarbeitet zur initialen Einrichtung und anschließenden Verwaltung des TI-M personenbezogene Daten des Nutzers. Diese Daten sind nachstehend aufgeführt:

1. In Kapitel B.1 aufgeführten Daten
2. Zusätzlich Daten, die bei jeder Nutzung von TI-M verarbeitet werden müssen:
   a. E-Mail-Adresse des Nutzers
   b. Zusatz: Meldeadresse
   c. TI-M-Adresse
   d. interne Geräte-ID
   e. Version des Betriebssystems

f. Zeitpunkt des Zugriffs
g. IP-Adresse
h. Krankenversicherungsnummer

3. Inhalte der Chatkommunikation
4. Freiwillige Einwilligung zur Datenverarbeitung:
   a. Für erweiterte Funktionen des TI-Messengers kann der Nutzer der App freiwillig in den Zugriff auf sein Mikrofon, seinen Standort und/oder seine Kamera einwilligen.
   a. Push-Benachrichtigung: Die Aktivierung dieser Funktion erfolgt freiwillig durch die Zustimmung des Nutzers und kann jederzeit in den Einstellungen des Geräts vom Nutzer deaktiviert werden.

E.1.2 Push-Benachrichtigungen

Versicherte können in ihrem TI-M-Profil festlegen, ob sie Push-Benachrichtigungen zu neuen Nachrichten erhalten möchten. Die Einstellung ist im Standard ausgeschaltet und muss sowohl im TI-Messenger in der ePA-App als auch im Betriebssystem des Smartphones aktiviert werden. Die Aktivierung dieser Funktion erfolgt freiwillig durch die Zustimmung des Versicherten und kann jederzeit in den Einstellungen des Geräts vom Versicherten deaktiviert werden. Durch die Zustimmung erlaubt der Versicherte die Verarbeitung von Daten durch die Anbieter des Betriebssystems seines Endgeräts (Google über den Dienst Firebase Cloud Messaging oder Apple). Der Zweck der Datenverarbeitung ist die Zustellung der Push-Notifikationen.

Zur Bereitstellung der Notifikationen werden Push-Tokens und technische Metadaten verwendet. Push Tokens sind Gerätezusatzidentifikatoren (Google/Firebase Registration ID; Apple Device Token) in Form von pseudonymisierte Gerätekennungen, die ausschließlich zur Zuordnung der Push-Services dienen. Weiterhin werden für die Push-Notifikation die Application ID (ID der TI-M-Anwendung), Event ID (identifiziert das Matrix Event), Room ID (ID des Chatraums) und Anzahl der ungelesenen Nachrichten des Users verarbeitet. Ein Rückschluss auf die Person oder in der ePA-App gespeicherte personenbezogene Daten ist dabei nicht möglich. Im Rahmen der Zustellung von Push-Benachrichtigungen werden die nachfolgend aufgeführten Daten verarbeitet:

- Push-Token des Endgeräts (gerätespezifischer Identifikator)
- Technische Geräteinformationen (insbesondere Gerätetyp und App-Identifier)
- Zeitpunkt der Erstellung der Push-Benachrichtigung
- Anzahl der ungelesenen Push-Benachrichtigungen
- Kennung des Kostenträgers des Versicherten (Weitergabe ausschließlich an den App-Anbieter; eine Übermittlung an den Push Provider oder den Aktensystemdienst erfolgt nicht)
- Verschlüsselte Benachrichtigungsinhalte (Nachricht, Empfänger, Ereignisart, z.B. „Neue Nachricht“), die ausschließlich durch den TI-Messenger in der ePA-App und den jeweiligen Fachdienst entschlüsselt werden können – dem Push Provider sind diese Inhalte technisch nicht zugänglich

Datenschutzniveau und Drittlandübermittlung

Im Rahmen der Nutzung der eingesetzten Push Provider kann nicht ausgeschlossen werden, dass die Daten in Drittländer außerhalb der Europäischen Union (z.B in die USA), übertragen werden. Für diese Drittländer besteht möglicherweise kein mit der Europäischen Union vergleichbares Datenschutzniveau. Bei den an die Push Provider übermittelten Daten handelt es sich jedoch nicht um Nachrichteninhalte, da diese ausschließlich in verschlüsselter Form übertragen werden und den Push Providern technisch nicht zugänglich sind.

Typische Risiken einer Drittlandübermittlung

- Mögliche Erschwernis bei der Durchsetzung von Betroffenenrechten, insbesondere hinsichtlich Auskunfts- und Löschungsansprüchen
- Fehlende oder eingeschränkte Möglichkeit zur Kontrolle einer Weiterverarbeitung oder Weiterübermittlung der Daten durch den Push Provider
- Fehlende oder eingeschränkte Datenschutzaufsicht durch unabhängige BehördenMöglicher Zugriff staatlicher Stellen auf die beim Push Provider gespeicherten Daten ohne wirksamen Rechtsschutz

Spezifisches Risiko in Bezug auf die übermittelten Daten
Die im Rahmen der Push-Benachrichtigung an den Push Provider übermittelten Daten enthalten weder Gesundheitsdaten noch Kommunikationsinhalte, da Benachrichtigungsinhalte ausschließlich in verschlüsselter Form übermittelt werden und dem Push Provider technisch nicht zugänglich sind. Ein Risiko, dass ein Zugriff auf sensible personenbezogene Daten erfolgen kann, ist vor diesem Hintergrund als sehr gering zu bewerten. Für die Nutzung des Google Dienstes gelten die Informationen zu Datenschutz und Sicherheit in Firebase für das Firebase Cloud Messaging sowie die allgemeine Google Datenschutzerklärung. Für die Nutzung der Apple Push Notification Services gilt die Apple Datenschutzrichtline.

E.2 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlagen für die Zurverfügungstellung des TI-M sind §§ 342 Abs. 1 Satz 2, Abs. 2 Nr. 2.

E.3 Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die Bereitstellung und die freiwillige Nutzung der Anwendung TI-M durch den Versicherten zur Teilnahme an einem sicheren, interoperablen elektronischen Sofortnachrichtendienst. Es ist wichtig zu verstehen, dass jedwede Chat-Kommunikation mit anderen TI-M-Teilnehmern eine automatische Datenverarbeitung nach sich zieht, um die Funktionsfähigkeit des Dienstes zu gewährleisten.

E.4 Dauer der Speicherung

Die Daten werden gelöscht, sobald sie für die Erreichung des Zweckes ihrer Erhebung nicht mehr erforderlich sind und keine Aufbewahrungspflichten mehr bestehen. Für den Nutzer besteht zudem die Möglichkeit seine Daten im TI-Messenger selbst zu verwalten und löschen.

- Der Nutzer kann Daten selbst löschen
- Daten, die durch die Nutzung entstehen (umfasst Chatkommunikationen, technische/betriebliche Daten)
- Die Krankenkasse kann eine automatische Löschfrist festlegen

Die genauen Verfahrensweisen zum Thema Löschen können unter Punkt 11 „Löschen in TI-M“ in den Nutzungsbedingungen nachgelesen werden.

E.5 Inhalte der Chat-Kommunikation

Alle Inhalte, die Sie über die Chat-Kommunikation des TI-M austauschen - seien es Texte, Bilder, Dokumente oder Sprachnachrichten - sind durch eine Ende-zu-Ende-Verschlüsselung davor geschützt, dass Dritte, die nicht Teilnehmende des Chats sind, diese Inhalte sehen können. Dazu gehören insbesondere auch die verantwortliche Krankenkasse und der IT-Dienstleister.
Der Nutzer ist selbst für die Inhalte verantwortlich, die er mit anderen Teilnehmenden einer Chat-Kommunikation teilt.

E.6 Hinweise zu den Rechten als Betroffener

Weiterführende Informationen gemäß Artikel 13 DSGVO finden Sie unter Punkt A.10 dieser Datenschutzerklärung. Bei Fragen zur Verarbeitung Ihrer Daten und zur Ausübung Ihrer Rechte gemäß der DSGVO wenden Sie sich bitte direkt an die unter A.1 genannte verantwortliche Krankenkasse, die Ihnen die Nutzung der ePA-App ermöglicht hat. Diese ist der datenschutzrechtlich Verantwortliche und somit für die Bearbeitung Ihrer Anliegen zuständig.

E.7 Widerrufsmöglichkeiten für die Nutzung der Anwendung TI-Messenger

Die unter diesem Abschnitt beschriebenen Datenverarbeitungen sind zum Zwecke der Anmeldung und Nutzung des TI-Messengers durch den Versicherten zwingend erforderlich. Die Verarbeitung personenbezogener Daten im Rahmen des TI-Messengers erfolgt auf Grundlage einer ausdrücklichen Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

Die Erteilung der Einwilligung ist freiwillig und kann jederzeit mit Wirkung für die Zukunft durch Entfernen des gesetzten Bestätigungshakens in der ePA-App widerrufen werden, ohne dass daraus Nachteile entstehen. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt unberührt. Im Falle eines Widerrufs ist die Nutzung des TI-Messengers jedoch nicht mehr möglich.

E.8 Hinweise zum Beschwerderecht

Weiterführende Informationen zu Ihrem Recht auf Beschwerde bei einer Aufsichtsbehörde können in Kapitel A.11 nachgelesen werden.

F. IAM-Registrierungsprozess für die ePA

Die in den nachfolgenden Abschnitten beschriebenen Datenverarbeitungsprozesse sind für die Nutzung der ePA-App zwingend erforderlich.

F.1 Beschreibung und Umfang der Datenverarbeitung

Für die Nutzung der ePA-App und den damit verbundenen Zugriff auf das ePA-Aktensystem des Versicherten müssen Verifikationsverfahren durchgeführt werden, um zu überprüfen, ob die Person, welche die Nutzung der App möchte, auch tatsächlich unser Versicherter ist.

Diese Prozessabläufe sind nachfolgend beschrieben: Im Rahmen des Verifikationsverfahrens werden folgende Daten verarbeitet:

- E-Mail-Adresse
- Krankenversichertennummer
- Postleitzahl
- individuelles Passwort
- Die letzten sechs Stellen der Kennnummer der eGK (ICCSN)

Beim Registrierungsverfahren werden vorstehende Daten temporär gespeichert.Nach Verifikation der eingegebenen Daten durch die KKH wird der Versicherte als Nutzer der ePA angelegt und zur Nutzung freigeschaltet. Der Versicherte erhält hierzu eine Bestätigung der KKH.

F.2 Erfassung der Daten für einen Fehlerreport

Wir benötigen die im Folgenden aufgeführten Informationen, wenn ein Versicherter einen Fehler meldet und die Ursache analysiert werden muss.

F.2.1 Automatisiert übermittelte Daten

Für die ePA-Apps für iOS und Android sowie die Desktop-App wird im Fehlerfall ein Report erstellt und dieser wird automatisch an das Business Service Management (BSM) versendet. Dieser enthält Informationen über das verwendete Gerät, app-spezifische Daten wie z. B. die App-Version und Informationen über das Betriebssystem des Gerätes. Diese übermittelten Daten werden ausschließlich zur Fehlerbehebung analysiert.

F.2.2 Manuell übermittelte Daten

Für die ePA-Apps für iOS und Android sowie die Desktop App wird im Fehlerfall einen Report erstellt. Zusätzlich zu dem automatisiert übermittelten Report können Nutzer Daten manuell an das Business Service Management (BSM) versenden, wie z. B. UserID, Android SDK-Version, Gerätebezeichnung, Umgebung oder Support-Code.

F.3 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für den IAM-Registrierungsprozess der ePA und die hierbei verarbeiteten Daten ist gegeben durch Art. 6 Abs. 1 lit. c DSGVO i.V.m. §§ 342 Abs. 1, 344 Abs. 1 Satz 1 SGB V.

F.4 Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die rechtssichere Identifikation des Versicherten sowie die Verhinderung von Daten- und Identitätsmissbrauch.

F.5 Dauer der Speicherung

Die Daten werden gelöscht, sobald sie für die Erreichung des Zweckes ihrer Erhebung nicht mehr erforderlich sind und keine Aufbewahrungspflichten mehr bestehen. Dies ist der Fall, wenn die ePA gekündigt und final gelöscht wurde.

F.6 Widerspruchmöglichkeiten gegen die ePA

Für eine bestehende ePA kann der Widerspruch bei der Krankenkasse nach § 344 Abs. 3 SGB V oder in der App nach § 342 Abs. 2g SGB V, § 344 Abs. 3 SGB V geltend gemacht werden.

Ein Widerspruch bei der Krankenkasse führt zu einer zu einer Löschung nach einem Zeitraum von 90 Tagen.

Ein Widerspruch in der App kann vom Versicherten eigenständig angestoßen werden und nach Bestätigung zur Löschung wird unverzüglich die ePA des Versicherten gelöscht.

Ein Widerspruch gegen die initiale Anlage der ePA ist gegenüber der Krankenkasse nach § 342 Abs. 1 Satz 2 SGB V, § 344 Abs. 1 SGB V möglich. Der Widerspruch zu initialer Anlage der ePA hat zu Folge, dass für den Versicherten keine ePA angelegt wird.

Des Weiteren kann der Versicherte einen Widerspruch gegen das Einspielen der Abrechnungsdaten nach § 305 Abs. 1 Satz 3 SGB V bei der Krankenklasse einreichen oder nach § 342 Abs. 2 SGB V in der App vornehmen.

G. Nutzung der ePA/Datenspeicher über die App

G.1 Beschreibung und Umfang der Datenverarbeitung für den Versicherten

G.1.1 Start mit Login-Maske

Der Versicherte startet die App, nach erfolgter Registrierung und Identifizierung. Zuerst erscheint die Login Maske, in die der Versicherte seine Zugangsdaten (Versichertennummer und Passwort sowie zur Auswahl App-Code, Gesundheitskarte oder Personalausweis) eingibt. Alternativ können, unter bestimmten Voraussetzungen, auch biometrische Verfahren (z. B. Fingerabdruck oder Gesichtserkennung) für die Anmeldung in der ePA-App genutzt werden

G.1.2 Nutzung der ePA

Beim ersten Start der Anwendung erhält der Versicherte einen ersten Überblick über die Nutzungsmöglichkeiten seiner ePA-App. Beim regulären Start kann der Versicherte zwischen den folgenden Anwendungen wählen:

- Anwendung der elektronischen Patientenakte
- Anwendung E-Rezept-Modul
- Anwendung Organspende-Register (OGR)

Diese Anwendungen können unabhängig voneinander genutzt werden. Die Anmeldeinformationen werden dabei in die jeweilige Anwendung übernommen.

Über das Profilbild kann der Nutzende seine Patientenakte aufrufen und seine persönlichen Daten verwalten.

Folgende Bereiche werden angezeigt:

1. Praxen und Einrichtungen
2. Sie vertretende Personen
3. DiGAS – Gesundheitsapps
4. Ihre Krankenkasse
5. Über die Patientenakte
6. Geräte verwalten
7. E-Mail-Adresse für Benachrichtigungen verwalten
8. Benachrichtigungen & Hinweise
9. Einwilligungen & Widersprüche
10. Aktivitätenprotokoll

Es werden die Daten gespeichert, die der Versicherte in seine digitale Patientenakte einstellt, bzw. die von Dritten dorthin hochgeladen werden. Hierbei kann es sich auch um Gesundheitsdaten nach Artikel 9 der DSGVO handeln.

G.1.3 Nutzung E-Rezept-Modul

Der Versicherte kann in der ePA-App über das E-Rezept-Modul alle elektronischen Verordnungen, die von Ärztinnen und Ärzten sowie Zahnärztinnen und Zahnärzten ausgestellt wurden, über den Fachdienst E-Rezept abrufen. Zusätzlich kann der Versicherte weitere Inhalte wie z. B. Medikamentendaten und Einnahmehinweise einsehen sowie mit der Apotheke kommunizieren.

G.1.4 Nutzung Organspende-Register (OGR)

Die ePA-App enthält einen Absprung zur Website des OGR. Wechselt der Nutzer aus der ePA-App in das OGR, wird die Gesundheits-ID zur Authentisierung an das Webportal weitergleitet, um die Anmeldung zu vereinfachen. Die BZgA ist für alle Inhalte verantwortlich. Die KKH haftet nicht für die Inhalte dieser Webseite.

G.1.5 Patientensouveränität in der ePA-App

Versicherte haben das Recht,

- zu wissen, welche Daten von ihnen gespeichert werden,
- dass ihre Daten geändert werden, wenn sie falsch sind,
- dass ihre Daten gelöscht werden, wenn sie nicht mehr gebraucht werden,
- dass nur so viele Daten gesammelt werden, wie nötig sind, und
- sich ihre Daten als Datei zuschicken zu lassen.

Diese Rechte sind in der Datenschutz-Grundverordnung (DSGVO), Artikel 13 bis 21, geregelt. Die Preisgabe persönlicher Informationen wird folglich durch die Versicherten selbst kontrolliert und gesteuert.

Zusätzlich steht die Information zur aktuell genutzten App-Version bereit.

G.2 Nutzung und Übermittlung von ePA-Daten für Forschungszwecke

Die in diesem Abschnitt beschriebene Übermittlung von ePA-Daten an das Forschungsdatenzentrum beginnt erst zu dem gesetzlich und technisch vorgesehenen Zeitpunkt. Vor Beginn der erstmaligen Übermittlung wird die Möglichkeit bereitgestellt, der Forschungsdatennutzung zu widersprechen.

G.2.1 Zweck und Voraussetzungen der Übermittlung

Bestimmte Daten aus Ihrer elektronischen Patientenakte werden für gesetzlich festgelegte Zwecke, insbesondere für Forschung und die Verbesserung der Gesundheitsversorgung, an das Forschungsdatenzentrum Gesundheit (FDZ) übermittelt. Rechtsgrundlagen für die Verarbeitung sind Art. 6 Abs. 1 lit. c sowie Art. 9 Abs. 2 lit. i und j DSGVO in Verbindung mit § 363 SGB V und der Forschungsdatenzentrum-Gesundheit-Verordnung (FDZGesV). Die Verarbeitung erfolgt unter Beachtung der Schutzvorgaben des Art. 89 Abs. 1 DSGVO.

Eine Übermittlung erfolgt nur, wenn

- Sie der bereitgestellten ePA nicht nach § 344 Abs. 3 SGB V widersprochen haben
- Sie den Zugriff auf die betreffenden Daten nicht beschränkt haben,
- Sie der Übermittlung an das FDZ nicht widersprochen haben und
- die Daten zuverlässig automatisiert pseudonymisiert werden können.

G.2.2 Kategorien der übermittelten Daten

Nach dem derzeit umgesetzten technischen Stand werden ausgewählte strukturierte Daten aus dem E-Rezept-Verfahren übermittelt, die Bestandteil der in Ziffer 4.5.1 beschriebenen elektronischen Medikationsliste (eML) sind. Hierzu gehören insbesondere Angaben zu Arzneimittelverordnungen, Arzneimittelabgaben sowie den jeweils zugehörigen Arzneimitteln. Das Verfahren erfasst nach dem derzeitigen technischen Stand ausschließlich die hierfür vorgesehenen strukturierten Daten aus dem E-Rezept-Verfahren.

G.2.3 Pseudonymisierung und beteiligte Stellen

Vor der Übermittlung für Forschungszwecke werden die vorgesehenen Daten nach den gesetzlichen Vorgaben pseudonymisiert und verschlüsselt. Unmittelbar identifizierende Angaben werden dabei entfernt oder durch Pseudonyme ersetzt. Die pseudonymisierten und verschlüsselten Daten werden zusammen mit einer technischen Zuordnungsnummer (Arbeitsnummer) an das Forschungsdatenzentrum Gesundheit beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) übermittelt. Diese Nummer dient ausschließlich dazu, die auf getrennten Wegen übermittelten Informationen technisch zusammenzuführen. Das zugehörige Lieferpseudonym und die Arbeits-nummer werden getrennt davon an die Vertrauensstelle beim Robert Koch-Institut (RKI) übermittelt. Die Vertrauensstelle erhält keine Medikationsdaten. Sie wandelt das Lieferpseudonym in ein über mehrere Datenübermittlungen hinweg gleichbleibendes (periodenübergreifendes) Pseudonym um und übermittelt dieses zusammen mit der Arbeitsnummer an das Forschungsdatenzentrum. So können Daten aus verschiedenen Übermittlungen derselben versicherten Person technisch miteinander verknüpft werden, ohne dass Name, Krankenversichertennummer oder andere unmittelbar identifizierende Angaben an das Forschungsdatenzentrum übermittelt werden. Die Vertrauensstelle arbeitet unabhängig und organisatorisch getrennt vom Forschungsdatenzentrum.

G.2.4 Verwendung der Daten durch das Forschungsdatenzentrum

Das FDZ gibt die Daten nicht automatisch unmittelbar an Forschende weiter. Interessierte Stellen müssen einen Antrag stellen und darlegen, für welchen gesetzlich zulässigen Zweck sie die Daten benötigen. Nach Prüfung des Antrags kann das FDZ anonymisierte Datensätze für genehmigte Forschungsprojekte bereitstellen oder pseudonymisierte Daten in einer besonders geschützten digitalen Umgebung zugänglich machen. Die pseudonymisierten Daten dürfen diese sichere Verarbeitungsumgebung nicht verlassen. Ergebnisse werden außerhalb dieser Umgebung grundsätzlich nur in anonymisierter Form bereitgestellt.

G.2.5 Dokumentation, Widerspruch und Löschung

Die Übermittlung Ihrer Daten wird in den hierfür vorgesehenen Funktionen der ePA dokumentiert. Dort können Sie insbesondere Informationen über von Ihnen erklärte Widersprüche sowie dokumentierte Datenübermittlungen einsehen. Sie können der Übermittlung Ihrer Daten jederzeit über die ePA-App oder gegenüber der Ombudsstelle Ihrer Krankenkasse widersprechen.

Sie können entweder der Übermittlung insgesamt (Gesamtwiderspruch) oder der Bereitstellung Ihrer Daten für einen oder mehrere der in § 303e Abs. 2 SGB V genannten Zwecke (Teilwiderspruch) widersprechen. Die konkreten Forschungszwecke werden gesetzlich festgelegt.

Ein Widerspruch gegen die Bereitstellung einer ePA nach § 344 Abs. 3 SGB V gilt nach den gesetzlichen Vorgaben ebenfalls als Widerspruch gegen die Übermittlung von ePA-Daten an das Forschungsdatenzentrum. Bei einem Gesamtwiderspruch werden für die Zukunft keine weiteren ePA-Daten mehr an das Forschungsdatenzentrum (FDZ) übermittelt. Bei einem Teilwiderspruch berücksichtigt das FDZ diesen bei der künftigen Bereitstellung Ihrer Daten für die jeweils widersprochenen gesetzlich vorgesehenen Zwecke.
Bitte beachten Sie, dass einzelne Dokumentations-, Anzeige-, Widerspruchs- und Löschfunktionen aufgrund gesetzlicher, regulatorischer oder technischer Weiterentwicklungen schrittweise bereitgestellt und weiterentwickelt werden. Der Umfang der jeweils verfügbaren Funktionen kann daher vorübergehend von der gesetzlich vorgesehenen Ausgestaltung abweichen. Ihre gesetzlichen Rechte bleiben hiervon unberührt. Bei einem Widerspruch werden die bereits an das FDZ übermittelten Daten dort grundsätzlich gemäß § 363 Abs. 6 SGB V gelöscht. Eine Ausnahme gilt für Daten, die vor Eingang des Widerspruchs bereits für ein konkretes Forschungsvorhaben verwendet wurden. Diese Daten dürfen für das betreffende Forschungsvorhaben weiterhin verarbeitet werden. Sie werden nicht mehr für neue Forschungsvorhaben bereitgestellt und nach Abschluss der Bereitstellung für das betreffende Forschungsvorhaben aus der sicheren Forschungsumgebung gelöscht. Für diese Daten sind das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Widerspruchsrecht nach Art. 21 DSGVO gemäß § 363 Abs. 6 Satz 4 SGB V insoweit ausgeschlossen. Weitere Hinweise zu Ihren Datenschutzrechten und den hierfür geltenden gesetzlichen Einschränkungen finden Sie unter Kapitel A.

G.3 Beschreibung und Umfang der Datenverarbeitung für vertretende Personen

Versicherte können für ihre Patientenakte einen oder mehrere vertretende Personen berechtigen. Die vertretende Person nutzt die eigene ePA-App ihrer Krankenkasse zur Wahrnehmung der Vertretung. Bei der Einrichtung werden Name, E-Mail-Adresse und Versichertennummer (KVNR) angegeben und gespeichert. Wenn die vertretende Person in der Patientenakte als Vertretung handelt, können alle technisch möglichen Aktionen anstelle des Versicherten ausgeführt werden.

Vertretende Personen können keine weiteren vertretenden Personen für die vertretene Patientenakte einrichten und auch nicht die Patientenakte für den Versicherten insgesamt löschen. Bei der Vertretung innerhalb der ePA erfolgt eine Datenverarbeitung wie in Kapitel D1 beschrieben.

G.4 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Speicherung personenbezogener Daten in der ePA ist §§ 342 Abs. 1 SGB V, 344 Abs. 1 Satz 1 SGB V.

G.4.1 Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die Nutzung der ePA durch den Versicherten zur Archivierung und Verwendung seiner individuellen Gesundheitsinformationen.

G.4.2 Dauer der Speicherung

Die Daten werden durch den Versicherten gelöscht, wenn er entscheidet, dass die in der ePA gespeicherten Daten nicht mehr benötigt werden. Zudem werden sämtliche Inhaltsdaten gelöscht, wenn der Versicherte seiner ePA insgesamt widerspricht.

H. Nutzung und Übermittlung von ePA-Daten für Forschungszwecke

H.1 Zweck und Voraussetzungen der Übermittlung

Bestimmte Daten aus Ihrer elektronischen Patientenakte werden für gesetzlich festgelegte Zwecke, insbesondere für Forschung und die Verbesserung der Gesundheitsversorgung, an das Forschungsdatenzentrum Gesundheit (FDZ) übermittelt. Rechtsgrundlagen für die Verarbeitung sind Art. 6 Abs. 1 lit. c sowie Art. 9 Abs. 2 lit. i und j DSGVO in Verbindung mit § 363 SGB V und der Forschungsdatenzentrum-Gesundheit-Verordnung (FDZGesV). Die Verarbeitung erfolgt unter Beachtung der Schutzvorgaben des Art. 89 Abs. 1 DSGVO.

Eine Übermittlung erfolgt nur, wenn
- Sie der bereitgestellten ePA nicht nach § 344 Abs. 3 SGB V widersprochen haben
- Sie den Zugriff auf die betreffenden Daten nicht beschränkt haben,
- Sie der Übermittlung an das FDZ nicht widersprochen haben und
- die Daten zuverlässig automatisiert pseudonymisiert werden können.

H.2 Kategorien der übermittelten Daten

Nach dem derzeit umgesetzten technischen Stand werden ausgewählte strukturierte Daten aus dem E-Rezept-Verfahren übermittelt, die Bestandteil der in Ziffer 4.5.1 beschriebenen elektronischen Medikationsliste (eML) sind. Hierzu gehören insbesondere Angaben zu Arzneimittelverordnungen, Arzneimittelabgaben sowie den jeweils zugehörigen Arzneimitteln. Das Verfahren erfasst nach dem derzeitigen technischen Stand ausschließlich die hierfür vorgesehenen strukturierten Daten aus dem E-Rezept-Verfahren.

H.3 Chatbot

Die Beantwortung von Fragen zur ePA kann über einen automatisierten Chatbot erfolgen. Ein Chatbot ist ein digitaler Assistent, mit dem durch Text- oder Spracheingabe kommuniziert werden kann. Über den Chatbot erhalten die Versicherten Zugang zu standardisierten Supportprozessen und Leistungsinhalten des Versichertenhelpdesks (VHD) im Rahmen der ePA. Die grundsätzliche Funktionalität umfasst dabei:

a. die Beantwortung von Fragen zur ePA-App,
b. den Dialog zur Annahme von Störungen mit Hinweis auf bestehende Störungen und der Möglichkeit, sich durch die Erstellung eines Tickets zu registrieren,
c. die Möglichkeit zum Übergang in einen Live-Chat-Dialog,
d. die Möglichkeit zur Platzierung eines Rückrufwunsches, und
e. die Hinweisfunktion, dass hier keine Beratung zum Versicherungsverhältnis stattfindet.

Verarbeitete Daten sind hierbei die bereits vom Versicherten hinterlegten Verifikationsdaten, sowie die von ihm freiwillig, im Chatbot eingegebenen Daten. Anfragen werden im Chatbot geloggt. Eine Erfassung von Kontaktdaten sowie eine Dokumentation als Ticket erfolgt nicht.

Kann eine Frage zur ePA-App nicht im Chat mit dem Chatbot beantwortet werden oder benötigt der Versicherte anderweitige direkte Unterstützung – beispielsweise bei der Meldung einer Störung – besteht die Möglichkeit, diese ad hoc über einen Live-Chat anzufordern oder einen Rückrufwunsch anzugeben.

H.4 Vorgangsbearbeitungssystem (ITSM)

Alle Anfragen, die über den Chatbot nicht gelöst werden können, werden zur weiteren Bearbeitung mit Hilfe eines sogenannten Vorgangsbearbeitungssystems erfasst und dokumentiert. Diese Anfragen werden persönlich von unseren Supportmitarbeitern bearbeitet. Sollte der Versicherte diesbezüglich einen

H.5 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Verarbeitung der Daten ist Art. 6 Abs. 1 lit. b DSGVO, da die im Rahmen der Kontaktaufnahme durchgeführten Datenverarbeitungsvorgänge für die ordnungsgemäße Abwicklung des Nutzungsvertrags mit dem Versicherten über die ePA erforderlich sind.

H.6 Zweck der Datenverarbeitung

Die in diesem Abschnitt beschriebene Verarbeitung personenbezogener Daten wird durchgeführt, um Kontaktaufnahmen unserer Versicherten bearbeiten zu können und infolgedessen den Nutzungsvertrag über die ePA-App mit dem Versicherten durchführen zu können.

H.7 Dauer der Speicherung

Die Daten werden gelöscht, sobald sie für die Erreichung des Zwecks ihrer Erhebung nicht mehr erforderlich sind und keine Aufbewahrungspflichten mehr bestehen. Dies ist der Fall, wenn die Krankenkasse entscheidet, dass spätestens drei Jahre nach Schließung des Vorgangstickets diese Daten gelöscht werden sollen.

H.8 Speicherorte aller ePA-App-spezifischen Daten

Alle ePA-App-spezifischen Daten werden in Deutschland aufbewahrt.