

# DATENSCHUTZERKLÄRUNG

## Datenschutzerklärung der IKK classic für die IKK classic ePA-App

Version 4, Stand 11.12.2025

### Inhalt

1.	Allgemeines .....	3
1.1	Vorbemerkungen .....	3
1.2	Name und Anschrift des Verantwortlichen.....	4
1.3	Kontaktdaten Datenschutzbeauftragter des Verantwortlichen .....	4
1.4	Zuständig für die Datenschutzaufsicht.....	4
1.5	Zuständig für die Rechtsaufsicht .....	4
1.6	Allgemeines zur Datenverarbeitung.....	4
1.7	Anbieter der ePA-App .....	5
1.8	Einbindung von Dritten.....	5
1.9	Datenerhebung von Informationen beim Download der ePA-App .....	5
1.10	Datenverarbeitung außerhalb der Europäischen Union .....	5
1.11	Ihre Rechte als betroffene Person .....	5
1.12	Automatisierte Entscheidungsfindung .....	6
2.	Registrierung, Identifizierung und Authentisierung .....	6
2.1	Überblick .....	6
2.2	Registrierung und Identifizierung .....	6
2.3	Authentisierung (Anmeldung) .....	6
2.3.1	Authentisierung mittels GesundheitsID .....	7
2.3.2	Authentisierung mittels elektronischer Gesundheitskarte.....	7
2.4	Umfang der Datenverarbeitung .....	8
2.5	Rechtsgrundlage der Datenverarbeitung .....	8
2.6	Zweck der Datenverarbeitung.....	9
2.7	Dauer der Speicherung und Löschung der Daten .....	9
3	Anwendung elektronische Patientenakte (ePA) .....	9
3.1	Beschreibung und Umfang der Datenverarbeitung .....	9
3.2	Berechtigung vertretender Person.....	10
3.3	Rechtsgrundlage für die Datenverarbeitung .....	10
3.4	Zweck der Datenverarbeitung.....	10
3.5	Dauer der Speicherung und Löschung von Daten .....	11
3.6	Widerspruchsrechte im Zusammenhang mit der elektronischen Patientenakte .....	11
3.7	Informationen zur elektronischen Patientenakte (ePA) nach § 343 Abs. 1a SGB V .....	12
4	Anwendung E-Rezept.....	12
4.1	Beschreibung und Umfang der Datenverarbeitung .....	12
4.2	Rechtsgrundlage für die Datenverarbeitung .....	13
4.3	Kommunikation zwischen Apotheken und Versicherten via ePA-App .....	13
4.4	Kartenfunktionen .....	13
4.5	Zweck der Datenverarbeitung.....	13
4.6	Dauer der Speicherung.....	13
4.7	Widerrufsmöglichkeiten für die Nutzung der Anwendung E-Rezept .....	13
5	Anwendung TI-Messenger (TI-M).....	13
5.1	Beschreibung und Umfang der Datenverarbeitung .....	13
5.2	Rechtsgrundlage für die Datenverarbeitung .....	15
5.3	Zweck der Datenverarbeitung.....	15
5.4	Dauer der Speicherung.....	15
5.5	Inhalte der Chat-Kommunikation .....	15
6	Absprünge zum Organspende-Register und zum Nationalen Gesundheitsportal.....	15
7	Erfassung der Daten für einen Fehlerreport .....	16
7.1	Automatisiert übermittelte Daten .....	16
7.2	Manuell übermittelte Daten .....	17

7.3	Rechtsgrundlage für die Datenverarbeitung .....	17
7.4	Zweck der Datenverarbeitung.....	17
7.5	Dauer der Speicherung.....	18
8	Support bei Fragen zur ePA-App.....	18
8.1	Beschreibung und Umfang der Datenverarbeitung .....	18
8.2	Chatbot .....	18
8.3	Service-Hotline.....	18
8.4	Vorgangsbearbeitungssystem (ITSM) .....	18
8.5	Rechtsgrundlage für die Datenverarbeitung .....	18
8.6	Zweck der Datenverarbeitung.....	19
8.7	Dauer der Speicherung.....	19

## Vorwort

Die IKK classic nimmt den Schutz Ihrer personenbezogenen Daten sehr ernst. Als Körperschaft des öffentlichen Rechts unterliegen wir den datenschutzrechtlichen Bestimmungen insbesondere nach der Europäischen Datenschutz-Grundverordnung (DSGVO), dem Sozialgesetzbuch (SGB) und des Bundesdatenschutzgesetzes (BDSG). Wir stellen durch technische und organisatorische Maßnahmen sicher, dass die Vorschriften über den Datenschutz sowohl von uns als auch von unseren externen Dienstleistern jederzeit und in vollem Umfang beachtet werden. Unsere Mitarbeiterinnen und Mitarbeiter sind auf die Einhaltung des Sozial- und Datengeheimnisses ausnahmslos schriftlich verpflichtet worden und werden laufend weitergebildet.

Diese Datenschutzerklärung klärt die Nutzenden über die Art, den Umfang und die Zwecke der Datenverarbeitung für die ePA-App auf.

### 1. Allgemeines

#### 1.1 Vorbemerkungen

Die IKK classic ePA-App ist die App der IKK classic, mit der Sie auf Ihre elektronische Patientenakte (ePA) sowie weitere Funktionen zugreifen können. Die Versicherten können zwischen folgenden Anwendungen bzw. Absprüngen in der ePA-App wählen:

- Anwendung der elektronischen Patientenakte (ePA)
- 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 zu den Funktionen der ePA-App 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.

#### Hinweise zur Sprachregelung

Im Sinne einer besseren Lesbarkeit und einem vereinfachtem Bearbeitungsverfahren wurde die gendergerechte Ansprache durch die einheitliche Verwendung der Formulierungen:

- „Versicherten“

- „Nutzenden“
- „Vertretenden“

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.

### **1.2 Name und Anschrift des Verantwortlichen**

Der Verantwortliche 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:

IKK classic (Körperschaft des öffentlichen Rechts)

Tannenstraße 4 b

01099 Dresden

E-Mail: [info@ikk-classic.de](mailto:info@ikk-classic.de)

### **1.3 Kontaktdaten Datenschutzbeauftragter des Verantwortlichen**

Unseren Datenschutzbeauftragten erreichen Sie per Mail unter: [datenschutz@ikk-classic.de](mailto:datenschutz@ikk-classic.de)

### **1.4 Zuständig für die Datenschutzaufsicht**

Der/Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Graurheindorferstraße 153

53117 Bonn

Telefon: +49 (0)228 997799-0

Fax: +49 (0)228 997799-5550

E-Mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

### **1.5 Zuständig für die Rechtsaufsicht**

Bundesamt für Soziale Sicherung

Friedrich-Ebert-Allee 38

53113 Bonn

Telefon: +49 (0)228-619-0

Telefax +49 (0)228619-1870

### **1.6 Allgemeines zur Datenverarbeitung**

Wir verarbeiten personenbezogene Daten unserer Versicherten, soweit dies zur Bereitstellung bzw. Nutzung einer funktionsfähigen ePA-App mitsamt ihren verschiedenen Anwendungen erforderlich ist. Die

Nutzung der ePA-App und ihrer Anwendungen ist für unsere Versicherten freiwillig. Ihnen entsteht kein Nachteil, sofern sie sich gegen die Nutzung der ePA-App entscheiden.

### **1.7 Anbieter der ePA-App**

Die ePA-App, sowie alle dazugehörigen Anwendungen (ePA, TI-Messenger, E-Rezept), wird Ihnen von der IKK classic angeboten. Dabei arbeitet die IKK classic mit der BITMARCK GmbH, Krupp-Straße 64, 45145 Essen, zusammen, die die ePA-App technisch entwickelt und betreibt. Die BITMARCK GmbH muss grundlegende Vorgaben der gematik GmbH (im Folgenden: gematik) einhalten und ein strenges Zulassungsverfahren durchlaufen. Dies dient der Sicherheit Ihrer Daten.

### **1.8 Einbindung von Dritten**

Im Rahmen der Leistungserbringung kann es erforderlich sein, dass externe Auftragnehmer sowie deren Subauftragnehmer Zugriff auf personenbezogene Daten erhalten. Diese werden unter Berücksichtigung datenschutzrechtlicher Anforderungen sorgfältig ausgewählt und sind verpflichtet, sämtliche einschlägigen gesetzlichen Vorgaben – insbesondere gemäß der Datenschutz-Grundverordnung (DSGVO) – sowie die produktspezifischen Anforderungen der IKK classic zu erfüllen. Zur Sicherstellung einer datenschutzkonformen Verarbeitung wird mit sämtlichen Dienstleistern eine Vereinbarung zur Auftragsverarbeitung (AVV) gemäß Art. 28 DSGVO geschlossen. Die Verarbeitung der Daten wird im Folgenden erläutert.

### **1.9 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 Website [epaclient.de](http://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.

### **1.10 Datenverarbeitung außerhalb der Europäischen Union**

Die Verarbeitung der Daten unserer Versicherten erfolgt grundsätzlich innerhalb der europäischen Union auf deutschen Servern in Rechenzentren in Deutschland. Mögliche Abweichungen bei der Verarbeitung personenbezogener Daten ohne Versichertenbezug sind in den einzelnen Kapiteln (vgl. Kapitel 3.1, 4.4, 5.1) separat aufgeführt.

### **1.11 Ihre Rechte als betroffene Person**

Sie haben das Recht auf:

- Auskunft zu den über Sie verarbeiteten Daten,
- Widerruf von Einwilligungserklärungen

und unter bestimmten rechtlichen Voraussetzungen auf

- Berichtigung unrichtiger Daten,
- Löschung von Daten,
- Einschränkung der Verarbeitung der Daten,
- Datenübertragbarkeit,
- Widerspruch gegen die Verarbeitung.

Unsere Versicherten haben zudem das Recht, sich über die Verarbeitung personenbezogener Daten bei der Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Eine Liste mit den Kontaktdaten aller Datenschutzbeauftragten in Deutschland steht Ihnen unter folgendem Link zur Verfügung: [bfdi.bund.de/DE/Infothek/Anschriften\\_Links/anschriften\\_links-node.html](http://bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html)

Zur Ausübung Ihrer Rechte können Sie sich entweder schriftlich oder per E-Mail an die IKK classic wenden.

## 1.12 Automatisierte Entscheidungsfindung

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

## 2. Registrierung, Identifizierung und Authentisierung

### 2.1 Überblick

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.

### 2.2 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 der 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) können Versicherte ihre persönlichen Daten zu ihrem Benutzeraccount 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

### 2.3 Authentisierung (Anmeldung)

**Authentisierung** bezeichnet die Überprüfung der Zugriffsberechtigung der Versicherten beim Anmelden bzw. Login an 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.

### **2.3.1 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 GesundheitsID 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 befugte Versicherte Zugriff auf ihre Gesundheitsdaten erhalten.

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

- Anwendung elektronische Patientenakte (ePA)
- Anwendung E-Rezept
- Anwendung TI-Messenger
- Absprung und Authentisierung am Organspende-Register

### **2.3.2 Authentisierung mittels elektronischer Gesundheitskarte**

Für den Zugriff auf die Anwendung der elektronischen Patientenakte (ePA) an der Desktop-ePA-App wird eine Zugangsoption angeboten: die Authentisierung mittels der elektronischen Gesundheitskarte (eGK) und der dazugehörigen persönlichen Identifikationsnummer (PIN).

Diese Authentisierungsmethode erfordert keine vorherige Registrierung oder separate Identifizierung der Versicherten in der Desktop-ePA-App. 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. Damit die PIN zur eGK zugestellt werden kann, ist vorher eine anderweitige Identifizierung (beispielsweise über die IKK classic ePA-App oder IKK classic App oder ohne Nutzung einer App in einem Servicecenter der IKK classic) erforderlich.

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.

## 2.4 Umfang der Datenverarbeitung

Für die Nutzung der ePA-App ist die Durchführung eines standardisierten Verfahrens zur Registrierung, Identifizierung und Authentisierung erforderlich. Ziel dieser Prozesse ist die rechtssichere Feststellung der Identität der versicherten Person sowie die Einrichtung und Verwaltung einer digitalen Identität. Nur so kann sichergestellt werden, dass ausschließlich berechtigte Personen Zugriff auf die elektronische Patientenakte und damit auf besonders schützenswerte Gesundheitsdaten erhalten.

Folgende Daten werden verarbeitet:

- Krankenversichertennummer
- Anzahl der aktiven elektronischen Gesundheitskarten (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.)
- Versichertenart (z. B.: Mitglied, Familienversicherter, Rentner)
- Beginn und Ende Versicherungsverhältnis
- E-Mail-Adresse
- Name, Vorname
- Geburtsdatum der versicherten Person
- Titel
- Namenszusatz
- Vorsatzwort (z. B.: „von“, „de“, „van“)
- Geschlecht
- VIP-Kennzeichen
- IdentDataTime: (Zeitstempel für die vollzogene Identifizierung des Versicherten)
- Schutzklasse für die Identifikation (mit oder ohne eGK)
- Identifizierungsverfahren (z. B. in der Filiale oder Postident)
- ICSSN
- ggf. die Ausweisnummer des Personalausweises, des Aufenthaltstitels, der eID-Karte oder des Reisepasses,
- 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
- ist NfcEgk (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.)
- Daten zu den verwendeten Geräten, unter anderem Gerätmodell, Name des Gerätes

Bei der Identifizierungsart „Postident“ verarbeitet die Deutsche Post temporär die verwendete E-Mail-Adresse.

## 2.5 Rechtsgrundlage der Datenverarbeitung

Rechtsgrundlagen für die Registrierung, Identifizierung und Authentisierung (Anmeldung) sind § 306 Abs. 2 Nr. 2 lit. a SGB V, § 291 Abs. 8 SGB V, in Verbindung mit der Richtlinie des GKV-Spitzenverbandes zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Abs. 4b SGB V.

Die Datenverarbeitung für die GesundheitsID erfolgt auf Grundlage von Art. 6 Abs. 1 lit. a sowie Art. 9 Abs. 2 lit. a DSGVO in Verbindung mit den einschlägigen Regelungen des SGB V, insbesondere §§ 291a und 336 ff. SGB V.

## 2.6 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.

## 2.7 Dauer der Speicherung und Löschung der Daten

Die im Rahmen der Registrierung, Identifizierung und Authentisierung verarbeiteten personenbezogenen Daten werden ausschließlich für die Zwecke erhoben und gespeichert, für die sie erforderlich sind. Die Löschung der Daten erfolgt gemäß den geltenden datenschutzrechtlichen Vorgaben, insbesondere nach Maßgabe von Art. 5 Abs. 1 lit. e DSGVO sowie den spezialgesetzlichen Regelungen des Sozialgesetzbuches Fünftes Buch (SGB V), sobald der jeweilige Verarbeitungszweck entfällt und keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

**Die Löschung der GesundheitsID erfolgt in folgenden Fällen:**

- Löschung durch die versicherte Person: Versicherte haben jederzeit die Möglichkeit, die vollständige Löschung ihres Benutzeraccounts über die ePA-App oder IKK classic App zu veranlassen.
- Löschung durch die IKK classic im Auftrag der versicherten Person: Die IKK classic kann auf Grundlage eines nachgewiesenen schriftlichen Auftrags der versicherten Person die Löschung des Benutzeraccounts veranlassen. Auch in diesem Fall erfolgt eine vollständige Datenlöschung.

Es erfolgt eine vollständige und unwiderrufliche Löschung sämtlicher personenbezogener Daten, die in diesem Zusammenhang gespeichert sind. Eine Authentisierung mittels GesundheitsID an der ePA-App und ihren Anwendungen ist anschließend nicht mehr möglich.

Die Deinstallation oder Löschung einzelner digitaler Anwendungen (z. B. der ePA-App) führt nicht automatisch zur Löschung der GesundheitsID. Diese bleibt bestehen, sofern keine gesonderte Löschung beauftragt wird.

## 3 Anwendung elektronische Patientenakte (ePA)

### 3.1 Beschreibung und Umfang der Datenverarbeitung

Die elektronische Patientenakte „ePA“ wird als Anwendung innerhalb der ePA-App unseren Versicherten zur Verfügung gestellt. Wir legen eine individuelle und ausschließlich von unseren Versicherten verwendete ePA an, welche unsere Versicherte eigenständig, souverän und autonom verwalten und verwenden können. Voraussetzung für die Nutzung der Anwendung ePA ist die vorherige Zustimmung zu den Nutzungsbedingungen. In der ePA-App können eine oder mehrere vertretende Personen hinzugefügt werden, siehe hierzu Kapitel 3.2. Bei der Bereitstellung der ePA werden folgende personenbezogene Daten unserer Versicherten herangezogen:

- Krankenversichertennummer
- Name, Vorname
- Geburtsdatum der versicherten Person
- Beginn und Ende Versicherungsverhältnis
- IdentDateTime (Zeitstempel für die vollzogene Identifizierung der versicherten Person)
- Schutzklasse für die Identifikation (mit oder ohne eGK)

- Identifizierungsverfahren (z. B. in der Filiale oder Postident)
- 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
- 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.)

Bei der Identifizierungsart „Postident“ verarbeitet die Deutsche Post temporär die verwendete E-Mail-Adresse.

#### **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.

### **3.2 Berechtigung vertretender Person**

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 wird 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 in der ePA-App anstelle des Versicherten ausgeführt werden.

Vertretende Personen können keine weiteren vertretenden Personen für die vertretene Patientenakte einrichten und auch nicht gegen die Patientenakte für den Versicherten insgesamt widersprechen.

Bei der Vertretung innerhalb der ePA erfolgt eine Datenverarbeitung wie in Kapitel 3.1 beschrieben.

### **3.3 Rechtsgrundlage für die Datenverarbeitung**

Sofern kein Widerspruch gegen die ePA vorliegt, erfolgt die Verarbeitung personenbezogener Daten unserer Versicherten auf der Grundlage der dahingehenden gesetzlichen Verpflichtung aus dem §§ 342 Abs. 1, 344 Abs. 1 Satz 1 SGB V. Die ePA wird kraft Gesetzes allen Versicherten, die nicht widersprochen haben, zur Verfügung gestellt (vgl. § 342 Abs. 1 Satz 2 SGB V).

### **3.4 Zweck der Datenverarbeitung**

Zweck der Datenverarbeitung ist die Bereitstellung der ePA nach den gesetzlichen Vorgaben des SGB V. In diesem Zusammenhang bedarf es der Zuordnung einer konkreten ePA zu unseren Versicherten.

### 3.5 Dauer der Speicherung und Löschung von Daten

Die in der elektronischen Patientenakte (ePA) gespeicherten Gesundheitsdaten werden grundsätzlich lebenslang gespeichert, sofern keine gesetzlich vorgeschriebene oder vertraglich vereinbarte Löschfrist entgegensteht (§ 342 Abs. 1 Satz 2 SGB V). Dies dient der kontinuierlichen medizinischen Versorgung und der Nachvollziehbarkeit medizinischer Behandlungen.

Verwaltungsdaten, die im Zusammenhang mit der Führung der ePA stehen (z. B. Zugriffsrechte, Versicherteninformationen, Logdaten), werden ebenfalls lebenslang gespeichert, soweit dies zur Erfüllung der gesetzlichen Zwecke erforderlich ist. Die Speicherung erfolgt mindestens bis:

- zum Tod der versicherten Person (§ 344 Abs. 6 SGB V),
- dem Widerspruch zur Nutzung der ePA (§ 342 Abs. 2 Nr. 1 lit. g SGB V),
- oder einem Wechsel der Krankenkasse, sofern keine gesetzliche Verpflichtung zur weiteren Aufbewahrung besteht (§ 284 Abs. 3 SGB V).

Bestimmte Daten unterliegen gesetzlichen Aufbewahrungsfristen, insbesondere gemäß § 309 Abs. 3 SGB V (z. B. Aktivitätenprotokolle der ePA). Nach Ablauf dieser Fristen erfolgt eine zweckgebundene Löschung der betreffenden Daten.

### 3.6 Widerspruchsrechte im Zusammenhang mit der elektronischen Patientenakte

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 ihre 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 von dem 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 Behandlungsaltag 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 elektronischen Patientenakte (ePA) auszuüben. Die Ausübung dieser Rechte kann entweder eigenständig über die Anwendung ePA oder mithilfe ihrer Krankenkasse bzw. Ombudsstelle (§§ 342 Abs. 2 Nr. 1 lit. s, t und 342a SGB V) erfolgen.

### **3.7 Informationen zur elektronischen Patientenakte (ePA) nach § 343 Abs. 1a SGB V**

Der Spitzenverband Bund der Krankenkassen erfüllt die gesetzliche Vorgabe nach § 343 Abs. 3 SGB V zur Bereitstellung von Informationen rund um die elektronische Patientenakte (ePA) und stellt hierzu entsprechendes Informationsmaterial nach § 343 Abs. 1a SGB V unter [ikk-classic.de/ePA](http://ikk-classic.de/ePA) unter „Wo finde ich weitere Informationen rund um die ePA?“ zur Verfügung.

## **4 Anwendung E-Rezept**

### **4.1 Beschreibung und Umfang der Datenverarbeitung**

Die Versicherten können in der ePA-App über die Anwendung E-Rezept alle elektronischen Verordnungen, die von Ärztinnen und Ärzten sowie Zahnärztinnen und Zahnärzten ausgestellt wurden, über den Fachdienst E-Rezept abrufen. Der Fachdienst E-Rezept ist ein zentraler Server in der Telematikinfrastruktur der gematik zur Ausführung der Fachanwendung E-Rezept. Zusätzlich können die Versicherten weitere Inhalte wie z. B. Medikament und Einnahmehinweise einsehen sowie mit der Apotheke kommunizieren. Voraussetzung für die Nutzung der Anwendung E-Rezept ist die vorherige Zustimmung zu den Nutzungsbedingungen sowie die Einwilligung zur Datenverarbeitung. Es werden die im Kapitel 2 genannten sowie die folgenden Daten verarbeitet:

- Krankenversichertennummer
- Name, Vorname
- Vorsatzwort (z. B.: „von“, „de“, „van“)
- Titel
- Namenszusatz
- Geburtsdatum der versicherten Person
- 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
  - Standortdaten
- Angaben zu verordneten und dispesierte E-Rezepten und E-Verordnungen.

#### **4.2 Rechtsgrundlage für die Datenverarbeitung**

Rechtsgrundlage für die Nutzung der Anwendung E-Rezept ist die Einwilligung unserer Versicherten nach Art. 6 Abs. 1 lit. a DSGVO i.V.m. §§ 360 Abs. 10, 361 Abs. 2 Nr. 3, 361a Abs. 2 SGB V.

#### **4.3 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.

#### **4.4 Kartenfunktionen**

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.

#### **4.5 Zweck der Datenverarbeitung**

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

#### **4.6 Dauer der Speicherung**

Für Versicherte 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). Ein Aufruf der E-Rezepte über die ePA-App ist danach nicht mehr möglich.

Zugriffe auf E-Rezepte werden gemäß § 309 SGB V für drei Jahre im E-Rezept-Fachdienst protokolliert und anschließend automatisiert gelöscht. Die Protokolldaten dienen ausschließlich der Nachvollziehbarkeit und sind über die Anwendung E-Rezept einsehbar, jedoch nicht exportierbar. Eine lokale Speicherung oder ein Download der Aktivitätenprotokolle ist derzeit nicht möglich.

#### **4.7 Widerrufsmöglichkeiten für die Nutzung der Anwendung E-Rezept**

Die unter dem Abschnitt 4.1 beschriebenen Datenverarbeitungen sind zur Nutzung des E-Rezepts durch den Versicherten zwingend erforderlich. 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 (vgl. Art. 7 Abs. 3 DSGVO). Die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt unberührt. Im Falle eines Widerrufs ist die Nutzung der Anwendung E-Rezept jedoch nicht mehr möglich.

### **5 Anwendung TI-Messenger (TI-M)**

#### **5.1 Beschreibung und Umfang der Datenverarbeitung**

Die Versicherten können, nach Zustimmung zu den Nutzungsbedingungen des TI-Messengers, in der ePA-App über den TI-Messenger mit berechtigten Akteuren (Leistungserbringer, Leistungserbringerinstitutionen, Kostenträger) kommunizieren, sofern diese ebenso einen TI-Messenger-

Dienst nutzen und einer Gesprächseinladung durch die Versicherten zustimmen. Darüber hinaus können berechtigte Akteure die Versicherten kontaktieren, wenn diese einer Kommunikation zustimmen.

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

Die Kommunikation findet über den TI-Messenger in der ePA-App der Versicherten statt und befähigt diesen mit anderen von der gematik zugelassenen TI-M-Diensten zu kommunizieren.

Die Kommunikation zwischen den TI-M-Diensten erfolgt Ende-zu-Ende-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, sollen die TI-M-Nutzenden selbst bestimmen können, wer sie in neue Chaträume einladen darf. Dies dient den Versicherten zur eigenständigen Steuerung des Chataufkommens.

**Art der Daten:**

Die IKK classic erhebt und verarbeitet zur initialen Einrichtung und anschließenden Verwaltung des TI-Messengers personenbezogene Daten der Versicherten. Diese Daten sind nachstehend aufgeführt:

1. in Kapitel 2 sowie 3.1 aufgeführten Daten
2. zusätzlich Daten, die bei jeder Nutzung des TI-Messengers verarbeitet werden müssen
  - a. E-Mail-Adresse der versicherten Person
  - 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

Die Verarbeitung der Inhalte der Chatkommunikation unterscheidet sich je nachdem, welche Akteure am Chat beteiligt waren. Die Krankenkasse als Anbieter des TI-Messengers speichert grundsätzlich alle Inhalte der Chatkommunikation verschlüsselt ab.

- a. Die Krankenkasse der Versicherten kann nur Chatinhalte zwischen Versicherten und Krankenkasse einsehen.
- b. Schutzstatus für geschützte und besonders geschützte Personen werden dabei berücksichtigt und sind nur für berechtigte Mitarbeitende der Krankenkasse einsehbar.
- c. Die Krankenkasse hat keine Möglichkeit, Chatinhalte von Konversationen einzusehen, an denen sie nicht beteiligt ist/war, z. B. Kommunikation zwischen Versicherten und Leistungserbringer ohne Beteiligung der Krankenkasse.

4. Freiwillige Einwilligung zur Datenverarbeitung:

- a. Für erweiterte Funktionen des TI-Messengers können die Versicherten freiwillig in den Zugriff auf ihr Mikrofon, ihren Standort und/oder ihre Kamera einwilligen.
- b. Push-Benachrichtigung:

Versicherte können in ihrem TI-M-Profil festlegen, ob sie Push-Benachrichtigungen erhalten möchten. Die Einstellung ist im Standard ausgeschaltet und muss sowohl in der TI-Messenger-Anwendung als auch im Betriebssystem des Smartphones aktiviert werden. Die Aktivierung dieser Funktion erfolgt freiwillig durch die Zustimmung der Versicherten und kann jederzeit in den Einstellungen des Geräts vom Versicherten deaktiviert werden. Durch die Zustimmung

erlauben die Versicherten 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. 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](#).

## **5.2 Rechtsgrundlage für die Datenverarbeitung**

Rechtsgrundlagen für die Zurverfügungstellung des TI-Messengers (= Sofortnachrichtendienst) sind § 342 Abs. 1 Satz 2, Abs. 2 Nr. 2 in Verbindung mit § 284 Abs. 1 Nr. 20, Abs. 3 SGB V.

## **5.3 Zweck der Datenverarbeitung**

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

## **5.4 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 die Versicherten besteht zudem die Möglichkeit ihre Daten im TI-Messenger selbst zu verwalten und löschen. Außerdem kann die Krankenkasse eine automatische Löschfrist für inaktive Chats festlegen.

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

## **5.5 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.

Die Versicherten sind selbst für die Inhalte verantwortlich, die sie mit anderen Teilnehmenden einer Chat-Kommunikation teilen.

## **6 Absprünge zum Organspende-Register und zum Nationalen Gesundheitsportal**

Die ePA-App enthält nach § 342 Abs. 2 Nr. 3 SGB V i.V.m. § 291 Abs. 8 SGB V einen Absprung zur Website des Organspende-Registers (OGR). Wechseln die Versicherten aus der ePA-App in das OGR, werden die Daten zur GesundheitsID für die Authentisierung an das Webportal weitergeleitet, um die

Anmeldung zu vereinfachen. Für alle Inhalte im Organspenderegister ist die Bundeszentrale für gesundheitliche Aufklärung verantwortlich.

Weiterhin enthält die ePA-App nach § 342 Abs. 2 Nr. 1 lit. r SGB V einen Absprung zum Nationalen Gesundheitsportal ([gesund.bund.de](http://gesund.bund.de)). Für alle Inhalte auf gesund.bund.de ist das BMG verantwortlich.

## 7 Erfassung der Daten für einen Fehlerreport

Wir benötigen die im Folgenden aufgeführten Informationen, wenn Versicherte einen Fehler melden und die Ursache analysiert werden muss.

### 7.1 Automatisiert übermittelte Daten

Für die ePA-App wird im Fehlerfall ein Report erstellt und dieser wird automatisch an den zuständigen Dienstleister versendet.

Diese übermittelten Daten werden ausschließlich zur Fehlerbehebung analysiert.

Daten	Wert	Beispiel
DEVICE- bezogene Daten	Family Model Architecture Battery Level Orientation Memory Capacity Simulator Boot Time Timezone archs battery_temperature brand charging connection_type language low_memory manufacturer online screen_density screen_dpi screen_height_pixels screen_resolution screen_width_pixels	Nokia Nokia 4.2 (QKQ1.191008.001) arm64-v8a 100% Portrait Total: 2.8 GB / Free: 1.4 GB Total: 20.2 GB / Free: 17.0 GB False 2021-08-18T07:29:28.162Z Europe/Amsterdam [arm64-v8a, armeabi-v7a, armeabi] 31 C Nokia True Wifi de_DE False HMD Global True 1.875 300 1370 1370x720 720
APP -bezogene Daten	Start Time Bundle ID Bundle Name Version Build	2021-08-18T07:52:25.904Z <a href="com.rise_world.epa.integration.debug">com.rise_world.epa.integration.debug</a> ePA 1.2.0 123070
Betriebssystem	Name Version	Android 10 (00EEA_2_290)

	<b>Kernel Version</b>	<b>4.9.186-perf+</b>
	<b>Rooted</b>	<b>No</b>

## 7.2 Manuell übermittelte Daten

Für die ePA-App wird im Fehlerfall ein Report erstellt. Zusätzlich zu dem automatisiert übermittelten Report können Versicherte die folgenden Daten manuell an den zuständigen Dienstleister versenden.

Die folgenden Informationen können zusätzlich im Fehlerfall an den zuständigen Dienstleister übermittelt werden. Diese übermittelten Daten werden ausschließlich zur Fehlerbehebung analysiert.

Daten	Wert	Beispiel	Erläuterung
<b>USERID bezogene Daten</b>	<b>Die UserId ist eine UUID und wird pro App Session neu generiert.</b>		
<b>TAGS</b>	ID	66cfbd07-1881-4975-bc2f-41a81f9d0907	
	androidSDK	29	Android SDK Version
	applicationId	com.rise_world.epa.integratio n.debug	App bundle name
	buildJob	epa-android/develop	Gitlab build job
	device	Nokia 4.2	Gerätebezeichnung
	device.family	Nokia	Produktgruppe
	dist	123070	Gitlab-Pipeline-ID
	environment	debug	Umgebung
	fdvSdk	1.2.0	Android SDK
	fdvSdkModule	1.2.2	C++ SDK
	flavor	epalIntegration	App flavor
	gitHash	bc5853d	Git Hash
	level	error	Loglevel
	os Android	10	Android Version
<b>StackTrace</b>	os.name	Android	Betriebssystemname
	os.rooted	no	Gerootetes Gerät
	release	1.2.0	App Release Version
	supportId	B88G-KDVD-YNEK	Support-Code
	user	id:66cfbd07-1881-4975-bc2f-41a81f9d0907	UserId
<b>StackTrace</b> Umfasst die technische Beschreibung des aufgetretenen Fehlers.			

## 7.3 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Datenübermittlung im Fehlerfall ist §§ 342 Abs. 1 Satz 2, 344 Abs. 1 Satz 1, 2 SGB V in Verbindung mit den in diesem Dokument genannten Rechtsgrundlagen der Datenverarbeitungen der einzelnen ePA-App-Anwendungen.

## 7.4 Zweck der Datenverarbeitung

Zweck der Datenverarbeitung ist die Wiederherstellung der Funktionsfähigkeit der ePA-App und ihrer Anwendungen im Fehlerfall.

## **7.5 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 der Fehler identifiziert und behoben ist.

## **8 Support bei Fragen zur ePA-App**

### **8.1 Beschreibung und Umfang der Datenverarbeitung**

In der ePA-App sind diverse Kontaktkanäle enthalten, die von Versicherten für die elektronische Kontaktaufnahme mit der IKK classic genutzt werden können.

#### **8.2 Chatbot**

Die Beantwortung von Fragen zur ePA-App kann über einen automatisierten Chatbot erfolgen. Über den Chatbot erhalten die Versicherten Zugang zu standardisierten Supportprozessen und Leistungsinhalten des Versichertenhelpdesks (VHD) im Rahmen der ePA-App. Die grundsätzliche Funktionalität umfasst dabei

- die Beantwortung von bereits definierten Fragen zur ePA-App, die die Versicherten auswählen können (keine Freitexteingabe), sowie
- die Möglichkeit zur telefonischen Kontaktaufnahme mit dem VHD der IKK classic rund um die Uhr.

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 benötigen die Nutzenden anderweitige direkte Unterstützung – beispielsweise bei der Meldung einer Störung – besteht die Möglichkeit, diese über die direkte telefonische Kontaktaufnahme beim VHD der IKK classic anzufordern.

#### **8.3 Service-Hotline**

Die Beantwortung von Fragen zur ePA-App und Hilfe bei technischen Problemen bietet der VHD der IKK classic den Nutzenden über die kostenlose Servicehotline. Der VHD löst und beantwortet allgemeine Fragen rund um die ePA sowie Anfragen zum Handling der Benutzeroberfläche der ePA-App. Es werden Serviceeinschränkungen der an der ePA beteiligten Systeme inkl. des Signaturzertifikats sowie des App-Frontends qualifiziert und der VHD bezieht ggf. den Support des IT-Dienstleisters zur weiteren Bearbeitung ein.

#### **8.4 Vorgangsbearbeitungssystem (ITSM)**

Alle Anfragen, welche der VHD nicht selbständig lösen kann, werden zur weiteren Bearbeitung in einem Ticketbearbeitungssystem erfasst und dokumentiert. Hier werden keine personenbezogenen Daten erfasst oder übermittelt.

#### **8.5 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 den Nutzenden über die ePA-App erforderlich sind.

## **8.6 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 den Nutzenden durchführen zu können.

## **8.7 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 Kasse entscheidet, dass spätestens drei Jahre nach Schließung des Vorgangstickets diese Daten gelöscht werden sollen.