Datenschutzerklärung der BKK firmus
für die BKK firmus ePA-App

Allgemeines

1.1 Vorbemerkungen

Die BKK firmus ePA-App ist die App der BKK firmus, mit der Sie auf Ihre elektronische Patientenakte (ePA) sowie weitere Funktionenzugreifen können. Der Versicherte kann 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:

- „Versicherter“
- „Vertreter“

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:

BKK firmus
Gottlieb-Daimler-Straße 11
28237 Bremen
Telefon: +49 (0)421-64343
Telefax: +49 (0)421-6434-451
Webseite: www.bkk-firmus.de
E-Mail: epa@bkk-firmus.de

1.3 Kontaktdaten Datenschutzbeauftragter des Verantwortlichen

BKK firmus
Gottlieb-Daimler-Straße 11
28237 Bremen
Deutschland
Telefon: +49 (0)421-6434-454
E-Mail: datenschutz@bkk-firmus.de
Website: www.bkk-firmus.de

1.4 Zuständige Datenschutzaufsicht

Der/Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Graurheindorferstraße 153
53117 Bonn
Telefon: +49 (0)228 997799-0
E-Mail: poststelle@bfdi.bund.de

1.5 Zuständige Rechtsaufsicht

Bundesamt für Soziale Sicherung
Friedrich-Ebert-Allee 38
53113 Bonn
Telefon: +49 (0)228-619-0Fax:
+49 (0)228 997799-5550
E-Mail: poststelle@bfdi.bund.de

1.6 Allgemeine 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 BKK firmus angeboten. Dabei arbeitet die BKK firmus 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.

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 jeweiligen Krankenkasse 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 Downloaden 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. 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 innerhalb der Europäischen Union

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

1.11 Ihre Rechte als Betroffener

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 Aufent-haltsorts, 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:

https://www.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 BKK firmus wenden.

1.12 Automatisierte Entscheidungsfindung

Wir setzen keine Verarbeitungsvorgänge ein, die auf einer automatisierten Entscheidungsfin-dung einschließlich Profiling nach 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. 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.

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 des Versicherten. Dies ist besonders wichtig bei Anwendungen, die sensible Gesundheitsdaten verarbeiten. Zur sicheren Identifizierung werden von der gematik 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 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 des 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 digitale Identität erhalten, die anschließend für die Authen-tisierung genutzt werden kann.

Konkrete Verfahren für die Anmeldung an der GesundheitsID sind eID, elektronische Gesundheitskarte oder App-Code (bzw. Biometrie).

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

2.3.2 Authentisierung mittels elektronischer Gesundheitskarte

Im Rahmen der kontinuierlichen Weiterentwicklung der Sicherheits- und Nutzungsprozesse für den Zugriff auf die Anwendung der elektronischen Patientenakte (ePA) wird neben der Authentisierung mittels GesundheitsID an der Desktop-ePA-App eine alternative Zugangsoption angeboten: die Authentisierung mittels der elektronischen Gesundheitskarte (eGK) und der dazuge-hörigen 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.

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 des Versicherten
- Titel
- Namenszusatz
- Vorsatzwort (z.Bsp.: „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, u. a. Gerätemodell, Name des Gerätes

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 unbefug-ter Kenntnisnahme nach § 217f Abs. 4b SGB V.

Die Datenverarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit.a sowie Art. 9 Abs. 2 lit. h 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 digitalen Identität erfolgt in folgenden Fällen:

- Löschung durch die versicherte Person: Versicherte haben jederzeit die Möglichkeit, die vollständige Löschung ihres Benutzeraccounts über die ePA-App zu veranlassen.

- Löschung durch die Krankenkasse bzw. Ombudsstelle im Auftrag der versicherten Person: Die Krankenkasse kann auf Grundlage eines nachgewiesenen schriftlichen Auftrags der versicherten Person die Löschung des Benutzeraccounts veranlassen. Auch in diesem Fall erfolgt eine vollständige Datenlöschung.

- Löschung im Falle eines Krankenkassenwechsels: Die Krankenkasse informiert den Nutzer über die bevorstehende Löschung und teilt ihm mit, zu welchem Datum die Löschung seitens der Krankenkasse durch Beauftragung der BITMARCK GmbH vollzogen wird.

- Löschung im Todesfall: Der Tod der versicherten Person führt nicht automatisch zur sofortigen Löschung der gespeicherten personenbezogenen Daten. Diese bleiben für einen Zeitraum gespeichert, sofern keine gesetzliche Verpflichtung oder ein berechtigter Löschantrag durch die Erbengemeinschaft oder Bevollmächtigten vorliegt.

Es erfolgt eine vollständige und unwiderrufliche Löschung sämtlicher personenbezogener Daten, die in diesem Zusammenhang gespeichert sind. Eine Authentisierung mittels digitaler Identität (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) auf den Endgeräten führt nicht automatisch zur Löschung der digitalen Identität. Diese bleibt bestehen, sofern keine gesonderte Löschung beauftragt bzw. selbst durchgeführt wird.

3 Anwendung elektronische Patientenakte (ePA)

3.1 Beschreibung und Umfang der Datenverarbeitung

3.1.1 Verarbeitete personenbezogene Daten

Die elektronische Patientenakte „ePA“ wird als Anwendung innerhalb der ePA-App unseren Versicherten zur Verfügung gestellt. Wir legen eine individuelle und ausschließlich von unserem Versicherten verwendete elektronische Patientenakte (ePA) an, welche unser Versicherter eigenständig souverän und autonom verwalten und verwenden kann. Voraussetzung für die Nutzung der Anwendung ePA ist die vorherige Zustimmung zu den Nutzungsbedingungen. Ein Versicherter kann in seiner ePA eine oder mehrere vertretende Personen hinzufügen, siehe hierzu Kapitel 3.2.

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

- Krankenversichertennummer
- Name, Vorname
- Geburtsdatum des Versicherten
- Beginn und Ende Versicherungsverhältnis
- IdentDataTime (Zeitstempel für die vollzogene Identifizierung des Versicherten)
- 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 Personen-abgleich 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.)

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.

3.1.2 Push-Benachrichtigungen

Die mobile ePA-App bietet die Möglichkeit, Push-Benachrichtigungen an das Endgerät des Ver-sicherten 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. „Neu-es Dokument verfügbar"), die ausschließlich durch die ePA-App und den jeweiligen Fachdienst entschlüsselt werden können – dem Push Provider sind diese Inhalte tech-nisch 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 über-tragen 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.

3.2 Berechtigung vertretender 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 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 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 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 unserem 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 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 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 Information 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: Informationsmaterial zur ePA zur Verfügung.

4 Anwendung E-Rezept

4.1 Beschreibung und Umfang der Datenverarbeitung

Der Versicherte kann 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 kann der Versicherte 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 des Versicherten
- je nach verwendetem Authentisierungsmittel:
  - ein Pseudonym bei Nutzung der Online-Ausweisfunktion. Dabei ruft der verwendete Anbieter erstmalig alle uns zugänglichen Daten des Personalausweises zum Personen-abgleich 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 dispensierten E-Rezepten und E-Verordnungen

4.2 Rechtsgrundlage für die Datenverarbeitung

Rechtsgrundlage für die Nutzung der Anwendung E-Rezept ist die Einwilligung unseres 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 Standort-daten) 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.

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 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). 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 Bestätigungs-hakens 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

5.1.1 Verarbeitete personenbezogene Daten

Der Versicherte kann, 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 den Versicherten zustimmen. Darüber hin-aus können berechtigte Akteure den Versicherten kontaktieren, wenn dieser einer Kommunikation zustimmt.

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 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 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, soll der TI-M-Nutzer selbst bestimmen können, wer ihn in neue Chaträume einladen darf. Dies dient dem Versicherten zur eigenständigen Steuerung seines Chataufkommens.

Art der Daten:

Die BKK firmus erhebt und verarbeitet zur initialen Einrichtung und anschließenden

Verwaltung des TI-Messengers personenbezogene Daten des Versicherten. Diese

Daten sind nach-stehend 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 des Versicherten
    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 des Versicherten kann nur Chatinhalte zwischen Versichertem und Krankenkasse einsehen.
   b. Schutzstatus für geschützte und besonders geschützte Personen werden dabei berücksichtigt und sind nur für berechtigte Mitarbeiter 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:

Für erweiterte Funktionen des TI-Messengers kann der Versicherte freiwillig in den Zugriff auf sein Mikrofon, sein Standort und/oder seine Kamera einwilligen.

5.1.2 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 App-le). 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 De-vice 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.

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 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.

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 den Versicherten besteht zudem die Möglichkeit seine 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.

Der Versicherte ist selbst für die Inhalte verantwortlich, die er mit anderen Teilnehmenden einer Chat-Kommunikation teilt.

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). Wechselt der Versicherte aus der ePA-App in das OGR, werden die Daten zur Gesundheits-ID 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). Für alle Inhalte auf gesund.bund.de ist das BMG verantwortlich.

7 Erfassung der Daten für einen Fehlerreport

Wir benötigten die im Folgenden aufgeführten Informationen, wenn ein Versicherter einen Fehler meldet 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	Nokia
	Model	Nokia 4.2 (QKQ1.191008.001)
	Architecture	arm64-v8a
	Battery Level	100%
	Orientation	Portrait
	Memory	Total: 2.8 GB / Free: 1.4 GB
	Capacity	Total: 20.2 GB / Free: 17.0 GB
	Simulator	False
	Boot Time	2021-08-18T07:29:28.162Z
	Timezone	Europe/Amsterdam
	archs	[arm64-v8a, armeabi-v7a, armeabi]
	battery_temperature	31 C
	brand	Nokia
	charging	True
	connection_type	Wifi
	language	de_DE
	low_memory	False
	manufacturer	HMD Global
	online	True
	screen_density	1.875
	screen_dpi	300
	screen_height_pixels	1370
	screen_resolution	1370x720
	screen_width_pixels	720
APP -bezogene Daten	**Start Time**	**2021-08-18T07:52:25.904Z**
	Bundle ID	**com.rise_world.epa.integration.debug**
	Bundle Name	**ePA**
	Version	**1.2.0**
	Build	**123070**
Betriebssystem	**Name**	**Android**
	Version	**10 (00EEA_2_290)**
	Kernel Version	**4.9.186-perf+**
	Rooted	**No**

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
USERID bezogene Daten	**Die UserId ist eine UUID und wird pro App Session neu generiert.**		
TAGS	ID	66cfbd07-1881-4975-bc2f-41a81f9d0907	
	androidSDK	29	Android SDK Version
	applicationId	com.rise_world.epa.integration.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	epaIntegration	App flavor
	gitHash	bc5853d	Git Hash
	level	error	Loglevel
	os Android	10	Android Version
	os.name	Android	Betriebsystemname
	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
StackTrace	**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 dem Versicherten für die elektronische Kontaktaufnahme mit der BKK firmus genutzt werden können.

8.2 Chatbot

Die Beantwortung von Fragen zur ePA-App kann über einen automatisierten Chatbot erfolgen. Ein Chatbot ist ein digitaler Assistent, mit dem Sie durch Text- oder Spracheingabe kommunizieren können. 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

a. die Beantwortung von Fragen zur ePA-App,
b. den Dialog zur Annahme von Störungen mit Hinweis auf bestehende Störungen und der Möglichkeit, sich zu einer solchen über 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.

8.3 Vorgangsbearbeitungssystem

Alle Anfragen, welche über den Chatbot nicht gelöst werden können, werden zur weiteren Bearbeitung mit Hilfe eines sog. Vorgangsbearbeitungssystems erfasst und dokumentiert. Diese Anfragen werden persönlich von den Supportmitarbeitern bearbeitet. Sollte der Versicherte diesbezüglich einen Rückruf wünschen, muss noch optional eine Telefonnummer angegeben werden.

Gegebenenfalls muss zusätzlich noch eine Vorgangsbearbeitungsnummer auf Nachfrage durch den Versicherten angegeben werden; diese wird durch das Vorgangsbearbeitungssystem automatisch erzeugt und dem Versicherten übergeben.

Sollten die gemeldeten Themen nicht durch diese Variante beantwortet werden können, wird ebenfalls automatisiert ein anlassbezogenes internes Bearbeitungsticket erstellt. Je nach Bedarf wird diese Anfrage an einen verantwortlichen Mitarbeiter weitergeleitet und – insofern diese Option durch den Versicherten gewählt wurde – ein Rückruf initiiert.

Nimmt ein Versicherter die Möglichkeit des Rückrufs wahr, so werden die in der Eingabemaske eingegeben Daten an uns übermittelt und gespeichert.

Die folgenden Daten sind durch den Versicherten einzugeben:

a. Name,
b. Kassenzugehörigkeit,
c. E-Mail-Adresse und
d. Telefonnummer.

8.4 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-App erforderlich sind.

8.5 Zweck der Datenverarbeitung

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

8.6 Dauer der Speicherung

Die Verarbeitung der Daten unserer Versicherten erfolgt grundsätzlich innerhalb der europäischen Union auf deutschen Servern in Rechenzentren in Deutschland. Mögliche Abweichungen hierzu sind in den einzelnen Kapiteln (vgl. Kapitel 3.1, 4.4, 5.1) separat aufgeführt. 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 Krankenkasse entscheidet, dass spätestens drei Jahre nach Schließung des Vorgangstickets diese Daten gelöscht werden sollen.