Datenschutzerklärung der BKK firmus
für die BKK firmus ePA-App

Allgemeine Datenschutzinformationen

Diese Datenschutzerklärung informiert insbesondere darüber, wer für die jeweiligen Verarbeitungsschritte verantwortlich ist, welche Daten zu welchen Zwecken und auf welcher Rechtsgrundlage verarbeitet werden, wer Daten erhält, wie lange Daten gespeichert werden und welche Rechte betroffene Personen haben.

1. Vorbemerkung, Anwendungsbereich und allgemeine Informationen

1.1 Anwendungsbereich

Die BKK firmus ePA-App ist die ePA-App der BKK firmus. Sie ermöglicht den Zugriff auf Ihre elektronische Patientenakte und soweit freigeschaltet, auf weitere digitale Gesundheitsdienste. Dazu können insbesondere die Anwendung E-Rezept, der TI-Messenger, das Organspende-Register und das Nationale Gesundheitsportal gehören.

Die elektronische Patientenakte ist eine versichertengeführte elektronische Akte. Ihre Nutzung ist freiwillig. Seit dem 15. Januar 2025 stellt die Krankenkasse Versicherten grundsätzlich eine ePA bereit, wenn diese nach vorheriger Information nicht widersprochen haben. Die Nutzung einzelner Zusatzfunktionen kann weitere freiwillige Entscheidungen oder Einwilligungen erfordern.

1.2 Sprachregelung

Aus Gründen der besseren Lesbarkeit wird auf eine geschlechtsspezifische Differenzierung verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1.3 Endgeräte und Betriebssysteme

Diese Datenschutzerklärung gilt für die mobile ePA-App (iOS und Android) sowie für die Desktop-Anwendung für Windows, macOS und Linux. Soweit nachfolgend nicht ausdrücklich zwischen den Betriebssystemen oder Anwendungsvarianten unterschieden wird, umfasst der Begriff „ePA-App“ alle genannten Varianten.

1.4 Bereitstellung von Daten

Die Bereitstellung der für die Registrierung, Identifizierung, Authentisierung und die jeweilige Funktion erforderlichen Daten ist Voraussetzung für den Zugriff auf die betreffenden Funktionen und Inhalte der ePA-App. Ohne diese Daten ist eine Nutzung nicht oder nur eingeschränkt möglich. Freiwillige Zusatzfunktionen können deaktiviert werden, ohne dass hierdurch der gesetzliche Versicherungsschutz beeinträchtigt wird.

1.5 Informationen nach § 343 Abs. 1a SGB V

Diese Datenschutzerklärung informiert insbesondere über die Verarbeitung personenbezogener Daten nach Art. 12 bis 14 Datenschutzgrundverordnung (DSGVO). Ergänzende Informationen zu Funktionsweise, Nutzen, Risiken, Zugriffsmöglichkeiten, Widerspruchsrechten und Steuerungs-möglichkeiten der elektronischen Patientenakte finden Sie in unserem Informationsmaterial nach § 343 Abs. 1a SGB V.

1.6 Datenschutzgrundsätze, Sozialgeheimnis und Informationssicherheit

Wir sind zur Wahrung des Sozialgeheimnisses (§ 35 SGB I) verpflichtet. Die Verarbeitung von Sozialdaten erfolgt nach den Vorgaben der DSGVO sowie den einschlägigen Vorschriften des SGB V und des SGB X. Personen mit Zugriff auf personenbezogene Daten sind zur Vertraulichkeit verpflichtet.

Die Sicherheit der Verarbeitung gewährleisten wir durch technische und organisatorische Maßnahmen nach Art. 25 und Art. 32 DSGVO sowie nach den einschlägigen gesetzlichen und technischen Vorgaben. Die elektronische Patientenakte und die eingesetzten Komponenten der Telematikinfrastruktur unterliegen den gesetzlichen Vorgaben des SGB V sowie den Anforderungen der gematik.

2. Verantwortliche

Verantwortlich für die Bereitstellung der ePA, die ePA-App und für die in dieser Datenschutzerklärung beschriebenen Verarbeitungsvorgänge 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

Die ePA-App ermöglicht auch die Nutzung oder den Aufruf weiterer Dienste und Services.
Bitte beachten Sie, dass für einzelne Verarbeitungen oder Verarbeitungsschritte dieser Dienste gegebenenfalls andere Stellen Verantwortliche im datenschutzrechtlichen Sinne sein können. Dies wird in dieser Datenschutzerklärung bei der Beschreibung der betreffenden Funktion beschrieben.

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

4. Kategorien personenbezogener Daten

Abhängig von der genutzten Funktion in der ePA-App verarbeiten wir folgende Kategorien personen-bezogener Daten:

Kategorie	Beispiele
4.1 Nutzungs-, Verbindungs-, Geräte-, und Protokolldaten	IP-Adresse, Gerätekennung, Betriebssystem, Zeitpunkt und Dauer der Anmeldung, App-Version sowie Zugriffs- und Aktivitätenprotokoll
4.2 Identifizierungs- und Authentisierungsdaten	Ausweisdaten oder eGK-Zertifikat, ICCSN (Kartenkennnummer), App-Code, Gerätebindung, Zeitstempel und Schutzklasse
4.3 Identitäts- und Stammdaten	Name, Geburtsname und -datum, Geschlecht, Anschrift, E-Mail-Adresse, Krankenversichertennummer (KVNR), Versichertenstatus
4.4 Versicherungs- und Verwaltungsdaten	Krankenkassenmitgliedschaft, Versicherungsstatus, Beginn und Ende des Versicherungsverhältnisses, eGK-Daten und Identifizierungsstatus
4.5 Allgemeinmedizinische Inhalte	Gesundheitsdaten: Befunde, Diagnosen, Angaben zu Untersuchungen und Behandlungen, Arzt- und Entlassungsbriefe, Labor- und Bilddaten, ggf. genetische Daten in eingestellten Dokumenten sowie sonstige medizinische Dokumente und Informationen.
4.5.1 Daten der elektronischen Medikationsliste (eML)	Angaben zu verordneten und abgegebenen Arzneimitteln, insbesondere Arzneimittel, Wirkstoff, Stärke, Darreichungsform, Verordnungs- und Abgabedaten, Dosierungs- und Anwendungs-hinweise, Angaben zur Substitution und zum Medikationsstatus sowie technische Zuordnungs- und Verknüpfungsdaten.
4.5.2 Daten des elektronischen Medikationsplans (eMP)	Angaben zur aktuellen und geplanten Medikation, insbesondere Arzneimittel, Wirkstoff, Stärke, Darreichungsform, Dosierung, Einnahme, Anwendung, Anwendungsdauer und Medikationsstatus sowie, soweit vorgesehen und vorhanden, Angaben zur Arzneimitteltherapiesicherheit.
4.6 Berechtigungs-, Vertretungs- und Erklärungsdaten	Zugriffsrechte, Vertretungen, Einwilligungen, Zugriffs-beschränkungen, Zustimmungen zu Nutzungsbedingungen, Bestätigungen von Datenschutzhinweisen, Widersprüche, Widerrufe, Freigaben sowie Zeitpunkt, Status und gegebenenfalls Versionsstand der jeweiligen Erklärung
4.7 Kommunikationsdaten	TI-Messenger-Nachrichten, E-Rezept-Mitteilungen, Anhänge, Absender, Empfänger und Kommunikationsmetadaten
4.8 Standort- und Suchdaten	Freiwillig bereitgestellte Standortdaten, Adressen und Suchkriterien für Apotheken- oder (externe) Kartenfunktionen
4.9 Support- und Fehlerdaten	Support-ID/Code, Ticketdaten, Fehlerbeschreibung, Stacktrace, technische Diagnoseinformationen und freiwillig übermittelte Angaben

4.10 Cookies und vergleichbare Technologien	Session-IDs, Authentifizierungsinformationen, Identifikatoren und interne Nutzerkennungen, JWT-Token-Informationen, Single-Sign-On-Informationen, technische Statusinformationen sowie Sprach-einstellungen.
4.11 Bereitstellung Apotheken-Suche/Karten-Dienst	Standortdaten des Endgeräts (soweit freigegeben), IP-Adresse, Datum und Uhrzeit der Nutzung, technische Geräte- und Verbindungsdaten, Suchparameter und Suchergebnisse, Informationen zur Kartendarstellung und Navigation
4.12 Technische Informationen beim Dokumentenscan	Geräteinformationen, Betriebssysteminformationen, App-Versionen, technische Kennungen, Leistungs- und Diagnosedaten, technische Konfigurationsdaten sowie Ereignis- und Fehlerprotokolle im Zusammenhang mit der Nutzung der Dokumentenscan-Funktion.

5. Zwecke und Rechtsgrundlagen im Überblick

Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung und Nutzung der elektronischen Patientenakte erfolgt überwiegend auf Grundlage gesetzlicher Verpflichtungen und gesetzlich zugewiesener Aufgaben der Krankenkasse. Für einzelne freiwillige Funktionen, insbesondere Push-Benachrichtigungen oder Standortfunktionen, erfolgt die Verarbeitung auf Grundlage einer Einwilligung. Die nachfolgende Übersicht umfasst die wesentlichen Verarbeitungsvorgänge sowie die relevanten Rechtsgrundlagen in detaillierter Form.

Verarbeitung	Zweck der Verarbeitung	Daten-kategorien	Rechtsgrund-lage
5.1 (Technische) Bereitstellung der App	Technische Bereitstellung der mobilen und stationären Anwendung, Aufbau und Verwaltung von Verbindungen und Sitzungen, Darstellung der Benutzeroberfläche sowie Gewährleistung der technischen Funktionsfähigkeit	4.1 bis 4.4 sowie ggf. 4.9 bis 4.11	Art. 6 Abs.1 lit. c & e DSGVO i.V.m. mit § 284 Abs.1 Nr. 20 & §§ 336, 341 & 342 SGB V. Funktionen außerhalb der ePA Art.6 Abs.1 lit. a & ggf. b DSGVO
5.2 Bereitstellung und Führung der elektronischen Patientenakte	Einrichtung, Bereitstellung, Führung und Verwaltung der elektronischen Patientenakte einschließlich Speicherung, Anzeige und Abruf von Gesundheitsdaten	4.1 bis 4.6	Art. 6 Abs.1 lit. c & e DSGVO, Art. 9 Abs. 2 lit. h DSGVO i. V. m. §§ 341 bis 355 SGB V, insb. §§ 342 & 344 SGB V
5.3 Registrierung, Identifizierung und GesundheitsID	Identitätsfeststellung, Registrierung, Bereitstellung der GesundheitsID, Authentisierung und Schutz vor unbefugten Zugriffen	4.1 bis 4.4	Art. 6 Abs.1 lit. c & e DSGVO, ggf. Art. 9 Abs.2 lit. h DSGVO i. V. m. § 291 Abs. 8, § 306 ff. SGB V
5.4 Verwaltung und Nachweis von Berechtigungen, Vertretungen und Erklärungen	Vergabe und Verwaltung von Zugriffsrechten und Vertretungen sowie Umsetzung und Nachweis von Einwilligungen, Widerrufen, Widersprüchen und Zugriffsbeschränkungen.	4.1 und 4.6	Art. 6 Abs.1 lit. c & e DSGVO, Art.9 Abs.2 lit. h DSGVO i. V. m. §§ 336 ff. SGB V
5.5 E-Rezept-Funktionen	Abruf, Verwaltung, Einlösung und Anzeige von E-Rezepten einschließlich der	4.1 bis 4.7	Art. 6 Abs. 1lit. c & e DSGVO, Art. 9 Abs. 2

	Kommunikation mit Apotheken		lit. h DSGVO i. V. m. §§ 360 ff. SGB V
5.6 TI-Messenger und Kommunikationsfunktionen	Bereitstellung eines sicheren Nachrichten- und Kommunikationsdienstes, Versand und Empfang von Nachrichten und Anhängen	4.1, 4.2, 4.3, 4.7	Art. 6 Abs.1 lit. c & e DSGVO, Art. 9 Abs. 2 lit. h DSGVO i. V. m. § 341 ff. SGB V
5.7 Push-Benachrichtigungen	Push-Token, Geräte- und App-Informationen, technische Versand-, Zustellungs- und Statusdaten sowie Informationen über das Vorliegen von Ereignissen, Dokumenten, Nachrichten oder sonstigen Vorgängen innerhalb der genutzten ePA-Funktionen.	4.1, ggf. 4.7	Art.6 Abs.1 lit. a DSGVO; ggf. bei Gesundheitsdaten zusätzlich Art.9 Abs. 2 lit. a DSGVO
5.8 Standort- und Suchfunktionen	Bereitstellung von Karten-, Standort- und Suchfunktionen	4.8	Art. 6 Abs. 1 lit. a DSGVO
5.9 Technischer Betrieb und IT-Sicherheit	Sicherstellung der Verfügbarkeit, Integrität und Sicherheit der App sowie Erkennung und Abwehr von Störungen und Missbrauch	4.1, 4.2, ggf. 4.9	Art. 6 Abs.1 lit. c & e DSGVO i. V. m. §§ 341 ff, § 284 Abs 1 Nr. 20 & den einschlägig. Vorschriften der §§ 336 und 341 ff. SGB V
5.10 Support und Fehleranalyse	Bearbeitung von Support-anfragen und Tickets, Fehleranalyse, Störungs-beseitigung und Qualitätssicherung	4.1 und 4.9	Art. 6 Abs. 1 lit. c und e DSGVO
5.11 Forschungs-datenausleitung	Bereitstellung von ePA-Daten zu Forschungszwecken im gesetzlich vorgesehenen Umfang sowie Verwaltung von Widersprüchen	4.5, 4.6 sowie erforderliche Begleit- und Protokolldaten und Pseudonyme	Art. 6 Abs. 1 lit. c sowie Art. 9 Abs. 2 lit. i, j, Art. 89 DSGVO i. V. m. § 363 SGB V, §§ 303c - 303f SGB V und der FDZGesV;
5.12 Weitergabe an externe Angebote und Services	Weiterleitung zu externen Diensten und gegebenenfalls Übermittlung von Authentisierungsinformationen	abhängig vom jeweiligen Angebot	jeweilige spezialgestz. Grundlage, Art. 6 Abs. 1 lit. b oder Art. 6 Abs. 1 lit. a DSGVO; bei Gesundheitsdaten zusätzlich Art. 9 Abs. 2 DSGVO
5.13 Cookies, lokale Speicher und vergleichbare Technologien	Speicherung von Sicherheits- und Anmeldungseinstellungen Bereitstellung notwendiger technischer Funktionen, Speicherung von Nutzer-entscheidungen, Gewährleistung der sicheren Datenübertragung,	4.10 sowie ggf. 4.1	§ 25 Abs. 2 TDDDG Art. 6 Abs. 1 lit. c & e DSGVO

5.14 **Apothekensuche und externer Kartendienst**	Ermittlung von Apotheken in Ihrer Nähe Anzeige und Visualisierung von Suchergebnissen, Bereitstellung einer Karten- und Navigationsfunktion Verbesserung der Nutzbarkeit der Apothekensuche	4.1 und 4.11	Art. 6 Abs. 1 lit. a DSGVO. § 25 TDDDG.
5.15 **Dokumentenscan-Funktion (Google ML Kit)**	Bereitstellung der Dokumenten-scan-Funktion Fehleranalyse und technische Diagnose, Wartung und Weiterentwicklung der eingesetzten Technologie Nachladen und Aktualisieren technischer Modell-komponenten, Erkennung und Verhinderung von Fehl-funktionen und Missbrauch	4.1, 4.9, 4.12	Art. 6 Abs. 1 lit. a DSGVO

6. Registrierung und Anmeldung

6.1 Registrierung, Identifizierung und GesundheitsID

Für die sichere Nutzung der ePA-App müssen Sie sich registrieren, identifizieren und authentisieren. Die Identifizierung erfolgt über die von uns angebotenen Identifizierungsverfahren.

Identifizierungsverfahren	**Anbieter**
eID-Authentifizierung	Authada
ePass / eID / eGK mit PIN	Nect
PostIdent	Deutsche Post

Im Rahmen der Registrierung und Nutzung werden insbesondere die unter den Ziffern 4.1 bis 4.4 genannten Daten verarbeitet. Die Zwecke und Rechtsgrundlagen der Verarbeitung ergeben sich aus Ziffer 5.3. Informationen zu den beteiligten Stellen und Dienstleistern finden Sie unter Ziffer 16, zur Speicherdauer unter Ziffer 17. Soweit externe Identifizierungsanbieter eingesetzt werden, gelten ergänzend deren Datenschutzhinweise.

6.2 Biometrische Entsperrung

Soweit Ihr Endgerät dies unterstützt, können Sie die ePA-App mithilfe einer biometrischen Funktion Ihres Endgeräts entsperren. Die biometrische Prüfung erfolgt durch das Betriebssystem. Wir erhalten grundsätzlich keine biometrischen Merkmale, sondern nur die technische Information, ob die Prüfung erfolgreich war und je nach Anmeldeart welche Technologie zum Einsatz kam. Sie können die biometrische Entsperrung jederzeit über die Einstellungen der App oder Ihres Endgeräts deaktivieren.

7. Elektronische Patientenakte und Vertretung

7.1 Elektronische Patientenakte

Die ePA dient der sicheren Speicherung und Nutzung Ihrer Gesundheitsinformationen für Ihre medizinische Versorgung. Über die ePA-App können Sie Ihre Akte einsehen und verwalten sowie Berechtigungen, Vertretungen, Zugriffsbeschränkungen, Widersprüche und Löschungen und Protokollinformationen steuern oder einsehen. Die betroffenen Datenkategorien sind unter den Ziffern 4.1 bis 4.6 beschrieben. Die Zwecke und Rechtsgrundlagen ergeben sich aus den Ziffern 5.2 und 5.4. Informationen zu Empfängern und beteiligten Stellen finden Sie unter Ziffer 16, zur Speicherdauer unter Ziffer 17.

7.2 Vertretung

Sie können im gesetzlich und technisch vorgesehenen Umfang andere Personen zur Verwaltung Ihrer ePA berechtigen. Der Umfang der Vertretung richtet sich nach den gesetzlichen und technischen Vorgaben. Umfang und Dauer der Vertretung können über die hierfür vorgesehenen Funktionen verwaltet werden. Der Entzug einer Vertretungsberechtigung erfolgt über die hierfür vorgesehene Funktion der ePA-App und ist nicht über die Ombudsstelle möglich. Vertretende Personen können keine weiteren Vertreter bestimmen und bestimmte persönliche Entscheidungen der vertretenen Person, insbesondere den Widerspruch gegen die Bereitstellung der ePA, nicht selbst erklären.
Vertretende Personen greifen mit ihrer eigenen ePA-App und ihrer eigenen digitalen Identität auf die von ihnen vertretene ePA zu. Hierfür werden insbesondere Identitäts-, Versicherungs-Berechtigungs- und Protokolldaten verarbeitet. Zugriffe einer vertretenden Person werden in der ePA protokolliert. Ergänzende Informationen zu den betroffenen Daten finden Sie unter Ziffer 4.6, zu den Zwecken und Rechtsgrundlagen unter Ziffer 5.4.

8. Dokumentenscan

Soweit diese Funktion angeboten wird, können Sie Dokumente mithilfe der Kamera Ihres Endgeräts erfassen und anschließend in Ihre ePA einstellen. Der Zugriff auf die Kamera oder auf lokal gespeicherte Dateien erfolgt nur, wenn Sie die entsprechende Funktion nutzen und die erforderlichen Geräteberechtigungen erteilen.

Im Rahmen der Nutzung können insbesondere Bild- und Dokumenteninhalte einschließlich darin enthaltener Gesundheitsdaten, Dokumentenmetadaten sowie technische Geräte-, Nutzungs-, Diagnose- und Fehlerdaten verarbeitet werden. Die betroffenen Datenkategorien ergeben sich aus den Ziffern 4.1, 4.5, 4.9 und 4.12, die Zwecke und Rechtsgrundlagen aus Ziffer 5, Informationen zu Empfängern aus Ziffer 16.2 sowie zur Speicherdauer aus Ziffer 17.

Die Verarbeitung der durch die Dokumentenscan-Funktion erfassten Dokumente erfolgt grundsätzlich lokal auf Ihrem Endgerät. Die Inhalte der gescannten Dokumente sowie die daraus erzeugten Scan-Ergebnisse werden im Rahmen des Scanvorgangs weder an die Krankenkasse noch an sonstige Dritte übermittelt. Erst wenn Sie sich entscheiden, ein gescanntes Dokument in Ihre ePA einzustellen, erfolgt die weitere Verarbeitung nach den für die ePA geltenden Regelungen.

Zur Bereitstellung der Dokumentenscan-Funktion wird die Technologie „Google ML Kit Document Scanner“ eingesetzt. Sofern Sie die Dokumentenscan-Funktion nutzen, können im Zusammenhang mit der Bereitstellung dieser Technologie durch den Anbieter technische Nutzungs-, Diagnose- und Fehlerdaten verarbeitet werden. Die hiervon betroffenen Datenkategorien ergeben sich aus den Ziffern 4.1, 4.9 und 4.12, die Zwecke der Verarbeitung aus Ziffer 5.15.

Die Inhalte der gescannten Dokumente sowie die daraus erzeugten Scan-Ergebnisse sind hiervon nicht betroffen und werden nach Angaben des Anbieters nicht an dessen Server übermittelt. Weitere Informationen zur Datenverarbeitung im Zusammenhang mit der eingesetzten Technologie finden Sie in den Datenschutzhinweisen, Nutzungsbedingungen und Produktinformationen des Anbieters.

9. Push-Benachrichtigungen

Push-Benachrichtigungen informieren Sie über Statusänderungen, neue Hinweise oder Ereignisse im Zusammenhang mit den von Ihnen genutzten Funktionen. Die Push-Funktion ist standardmäßig deaktiviert und wird nur verwendet, wenn Sie diese freiwillig aktivieren. Push-Benachrichtigungen werden so gestaltet, dass die eingesetzten Plattform-Dienstanbieter grundsätzlich keine medizinischen Dokumente, Inhalte von Nachrichten oder sonstige Gesundheitsdaten im Klartext erhalten. Die Benachrichtigungen enthalten regelmäßig lediglich allgemeine Status- oder Funktionshinweise und keine medizinischen Inhalte. Gleichwohl kann nicht ausgeschlossen werden, dass die Benachrichtigung im Einzelfall Rückschlüsse auf einen medizinisch relevanten Sachverhalt zulässt.

Für die Zustellung werden insbesondere Push-Token, Geräte- und App-Informationen sowie technische Versand- und Statusdaten verarbeitet. Die betroffenen Datenkategorien ergeben sich aus den Ziffern 4.1 und gegebenenfalls 4.7, die Rechtsgrundlagen aus Ziffer 5.7. Informationen zur Speicherdauer finden Sie unter Ziffer 17.10.

Bei Nutzung der mobilen App können Push-Benachrichtigungen abhängig vom verwendeten Betriebssystem über den Apple Push Notification Service (iOS) oder Firebase Cloud Messaging (Android) bereitgestellt werden. Soweit diese Dienste eingesetzt werden, kann eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums nicht ausgeschlossen werden. Informationen zu den Empfängern und den Garantien für Drittlandübermittlungen finden Sie unter Ziffer 16.2.

10. E-Rezept

Über die E-Rezept-Funktion können Sie elektronische Verordnungen abrufen, anzeigen, verwalten und zur Einlösung an eine Apotheke übermitteln. Je nach Funktionsumfang können außerdem Mitteilungen an Apotheken sowie eine Apothekensuche und Kartenansicht angeboten werden.

Im Zusammenhang mit der E-Rezept-Funktion werden insbesondere Identitäts- und Authentisierungsdaten, Verordnungs- und Dispensierdaten, Kommunikationsdaten sowie technische Verbindungs- und Protokolldaten verarbeitet. Die betroffenen Datenkategorien ergeben sich aus den Ziffern 4.1 bis 4.7, die Zwecke und Rechtsgrundlagen aus Ziffer 5.5.

Wir sind für die durch uns veranlasste Bereitstellung und Einbindung der E-Rezept-Funktion in die ePA-App verantwortlich. Für die Verarbeitung im zentralen E-Rezept-Fachdienst sowie durch ausstellende Leistungserbringer und Apotheken gelten die jeweils gesetzlich zugewiesenen Verantwortlichkeiten. Die beteiligten Stellen und Empfänger sind unter Ziffer 16 beschrieben. Informationen zur Löschung der E-Rezept-Daten und zur Abgrenzung von der elektronischen Medikationsliste finden Sie unter Ziffer 17.3.

11. Apothekensuche und Kartenfunktion (Geolokalisierung via Google Maps)

Zur Suche nach Apotheken in Ihrer Nähe kann die App, sofern Sie dies in den Einstellungen Ihres Endgeräts freigeben, Standortdaten Ihres Geräts verwenden. Die Standortdaten werden genutzt, um über die hierfür vorgesehenen Verzeichnisdienste passende Apotheken zu ermitteln und die Suchergebnisse anzuzeigen.

Die eigentliche Apothekensuche erfolgt über die hierfür vorgesehenen Verzeichnisdienste der Telematikinfrastruktur. Im Rahmen dieses Suchvorgangs werden die für die Suche erforderlichen Standortinformationen verarbeitet, um Apotheken in Ihrer Nähe zu ermitteln.

Zusätzlich wird in der App eine Kartenansicht des externen Anbieters Google bereitgestellt. Sofern Sie die Kartenfunktion nutzen, erfolgt die Darstellung der Suchergebnisse über Dienste von Google Maps. Die Kartenansicht wird erst geladen, nachdem Sie der Nutzung ausdrücklich zugestimmt haben. Die Einwilligung umfasst die hierfür erforderliche Übermittlung von Geräte-, Verbindungs-, Such- und gegebenenfalls Standortdaten an Google. Die Freigabe Ihres Standorts erfolgt über die Einstellungen Ihres Endgeräts. Die Nutzung der Standortfunktion und der Kartenansicht ist freiwillig. Sie können die Standortfreigabe jederzeit über die Einstellungen Ihres Endgeräts erteilen, einschränken oder widerrufen.

Bei Nutzung der Kartenansicht werden personenbezogene Daten an die Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland, übermittelt. Es kann nicht ausgeschlossen werden, dass die Daten dabei auch durch die Google LLC, 1600 Amphitheatre Parkway, Mountain View, California 94043, USA, oder weitere Unternehmen der Google-Unternehmensgruppe bzw. von Google eingesetzte Dienstleister verarbeitet werden. Eine Verarbeitung kann dabei auch in Drittstaaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums, insbesondere in den USA, stattfinden.

Die Google LLC ist nach dem EU-U.S. Data Privacy Framework zertifiziert. Datenübermittlungen in die USA können daher auf den entsprechenden Angemessenheitsbeschluss der Europäischen Kommission gestützt werden. Ergänzend können die Standardvertragsklauseln der Europäischen Kommission Anwendung finden. Weitere Informationen finden Sie in den Datenschutzhinweisen von Google.

12. Nutzung und Übermittlung der ePA-Daten für Forschungszwecke

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

12.1 Zweck und Voraussetzungen der Übermittlung

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

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

12.2 Kategorien der übermittelten Daten

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

12.3 Pseudonymisierung der beteiligten Stellen

Vor der Übermittlung für Forschungszwecke werden die vorgesehenen Daten nach den gesetzlichen Vorgaben pseudonymisiert und verschlüsselt. Unmittelbar identifizierende Angaben werden dabei entfernt oder durch Pseudonyme ersetzt. Die pseudonymisierten und verschlüsselten Daten werden zusammen mit einer technischen Zuordnungsnummer (Arbeitsnummer) an das Forschungsdatenzentrum Gesundheit beim Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) übermittelt. Diese Nummer dient ausschließlich dazu, die auf getrennten Wegen übermittelten Informationen technisch zusammenzuführen. Das zugehörige Lieferpseudonym und die Arbeitsnummer werden getrennt davon an die Vertrauensstelle beim Robert Koch-Institut (RKI) übermittelt.

Die Vertrauensstelle erhält keine Medikationsdaten. Sie wandelt das Lieferpseudonym in ein über mehrere Datenübermittlungen hinweg gleichbleibendes (periodenübergreifendes) Pseudonym um und übermittelt dieses zusammen mit der Arbeitsnummer an das Forschungsdatenzentrum. So können Daten aus verschiedenen Übermittlungen derselben versicherten Person technisch miteinander verknüpft werden, ohne dass Name, Krankenversichertennummer oder andere unmittelbar identifizierende Angaben an das Forschungsdatenzentrum übermittelt werden. Die Vertrauensstelle arbeitet unabhängig und organisatorisch getrennt vom Forschungsdatenzentrum.

12.4 Verwendung der Daten durch das Forschungsdatenzentrum

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

12.5 Dokumentation, Widerspruch und Löschung

Die Übermittlung Ihrer Daten wird in den hierfür vorgesehenen Funktionen der ePA dokumentiert. Dort können Sie insbesondere Informationen über von Ihnen erklärte Widersprüche sowie dokumentierte Datenübermittlungen einsehen.

Sie können der Übermittlung Ihrer Daten jederzeit über die ePA-App oder gegenüber der Ombudsstelle Ihrer Krankenkasse widersprechen. Sie können entweder der Übermittlung insgesamt (Gesamtwiderspruch) oder der Bereitstellung Ihrer Daten für einen oder mehrere der in § 303e Abs. 2 SGB V genannten Zwecke (Teilwiderspruch) widersprechen. Die konkreten Forschungszwecke werden gesetzlich festgelegt.

Ein Widerspruch gegen die Bereitstellung einer ePA nach § 344 Abs. 3 SGB V gilt nach den gesetzlichen Vorgaben ebenfalls als Widerspruch gegen die Übermittlung von ePA-Daten an das Forschungsdatenzentrum.

Bei einem Gesamtwiderspruch werden für die Zukunft keine weiteren ePA-Daten mehr an das Forschungsdatenzentrum (FDZ) übermittelt. Bei einem Teilwiderspruch berücksichtigt das FDZ diesen bei der künftigen Bereitstellung Ihrer Daten für die jeweils widersprochenen gesetzlich vorgesehenen Zwecke.

Bitte beachten Sie, dass einzelne Dokumentations-, Anzeige-, Widerspruchs- und Löschfunktionen aufgrund gesetzlicher, regulatorischer oder technischer Weiterentwicklungen schrittweise bereitgestellt und weiterentwickelt werden. Der Umfang der jeweils verfügbaren Funktionen kann daher vorübergehend von der gesetzlich vorgesehenen Ausgestaltung abweichen. Ihre gesetzlichen Rechte bleiben hiervon unberührt.

Bei einem Widerspruch werden die bereits an das FDZ übermittelten Daten dort grundsätzlich gemäß § 363 Abs. 6 SGB V gelöscht. Eine Ausnahme gilt für Daten, die vor Eingang des Widerspruchs bereits für ein konkretes Forschungsvorhaben verwendet wurden.

Diese Daten dürfen für das betreffende Forschungsvorhaben weiterhin verarbeitet werden. Sie werden nicht mehr für neue Forschungsvorhaben bereitgestellt und nach Abschluss der Bereitstellung für das betreffende Forschungsvorhaben aus der sicheren Forschungsumgebung gelöscht.

Für diese Daten sind das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO sowie das Widerspruchsrecht nach Art. 21 DSGVO gemäß § 363 Abs. 6 Satz 4 SGB V insoweit ausgeschlossen. Weitere Hinweise zu Ihren Datenschutzrechten und den hierfür geltenden gesetzlichen Einschränkungen finden Sie unter Ziffer 19.

13. TI-Messenger

Der TI-Messenger ermöglicht die sichere Kommunikation mit teilnehmenden Leistungserbringern und Einrichtungen.

Verarbeitet werden insbesondere Identitäts- und Authentisierungsdaten, technische Adressierungs-daten, Geräte- und Nutzungsdaten, Kommunikationsmetadaten sowie verschlüsselte Nachrichten und Anhänge.

Nachrichten und Anhänge werden entsprechend den Sicherheitsvorgaben des TI-Messengers verschlüsselt übertragen. Die eingesetzte TIM-Lösung sieht eine Ende-zu-Ende-Verschlüsselung vor, so dass die Kommunikationsinhalte grundsätzlich nur von den an der Kommunikation beteiligten Personen eingesehen werden kann. Technische Dienstleister erhalten grundsätzlich keinen Zugriff auf die Inhalte. Zugriffe auf Mikrofon, Kamera, Dateien oder weitere Gerätefunktionen erfolgen nur, wenn Sie die jeweilige Funktion nutzen und die erforderliche Geräteberechtigung erteilen. Für Push-Benachrichtigungen gelten ergänzend die Informationen unter Ziffer 9. Informationen zu den beteiligten Stellen finden Sie unter Ziffer 16, zur Speicherdauer von Nachrichten und Kommunikationsmetadaten unter Ziffer 17.7.

14. Support und Fehlerbrichte

Wenn Sie den Support, einen Chat, einen Rückrufservice oder ein Ticketsystem nutzen, verarbeiten wir die für die Bearbeitung erforderlichen Kontakt-, Verifikations-, Ticket-, Kommunikations- und gegebenenfalls technischen Diagnosedaten.

Wenn Sie einen Fehlerbericht übermitteln, werden insbesondere Geräte- und Betriebssystem-informationen, App-Version, Fehlerzeitpunkt, Verbindungsstatus, Support-ID, technische Kennungen, Stacktraces und Diagnosedaten verarbeitet. Die betroffenen Datenkategorien ergeben sich auch aus den Ziffern 4.1 und 4.9, die Zwecke und Rechtsgrundlagen aus Ziffer 5.10. Informationen zu den eingesetzten Supportdienstleistern finden Sie unter Ziffer 16, zur Speicherdauer unter Ziffer 17.9.

15. Cookies

Im Rahmen der Registrierung, Anmeldung und Nutzung der GesundheitsID beziehungsweise des Identitätsmanagements (bitIAM) werden technisch erforderliche Cookies und vergleichbare Technologien eingesetzt. Diese dienen insbesondere der Sitzungsverwaltung, der Authentifizierung, der Aufrechterhaltung einer sicheren Anmeldung, der Bereitstellung von Single-Sign-On-Funktionen, der Wiederaufnahme unterbrochener Anmelde- und Authentifizierungsvorgänge sowie der Speicherung technischer Statusinformationen und nutzerspezifischer Einstellungen (z. B. Spracheinstellungen). Ohne diese Technologien können die Funktionen der Registrierung, Identifizierung, Authentifizierung und sicheren Nutzung der ePA-App nicht bereitgestellt werden. Die Speicherung von Informationen auf Ihrem Endgerät sowie der Zugriff auf diese Informationen erfolgen gemäß § 25 Abs. 2 Nr. 2 TDDDG, da die eingesetzten Cookies und vergleichbaren Technologien für die Bereitstellung der ausdrücklich gewünschten Funktionen technisch erforderlich sind.

Die betroffenen Datenkategorien ergeben sich insbesondere aus Ziffer 4.10 sowie gegebenenfalls aus den Ziffern 4.1 und 4.2. Die Zwecke und Rechtsgrundlagen der Verarbeitung ergeben sich aus Ziffer 5.13.

Die in den Cookies enthaltenen Informationen werden ausschließlich zur Durchführung der Anmeldung, Authentifizierung, Sitzungsverwaltung und Bereitstellung der jeweiligen Funktion verarbeitet. Eine Übermittlung an Dritte sowie eine Übermittlung in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erfolgt nicht.

Die eingesetzten Cookies werden grundsätzlich mit Beendigung der Sitzung, bzw. nach einem Logout gelöscht, sofern der Logout über den Browser stattgefunden hat oder nach Ablauf ihrer technischen Gültigkeitsdauer.

16. Empfänger, Dienstleister und Verantwortlichkeiten

Welche personenbezogenen Daten an welche Empfänger übermittelt werden, hängt von den jeweils genutzten Funktionen der ePA-App, den von Ihnen erteilten Berechtigungen, Vertretungen und Einwilligungen sowie den gesetzlichen Vorgaben des Fünften Buches Sozialgesetzbuch (SGB V) ab. Nicht jeder Empfänger erhält sämtliche in dieser Datenschutzerklärung genannten Datenkategorien.

16.1 Empfänger und Empfängerkategorien

Personenbezogene Daten werden nur weitergegeben oder zugänglich gemacht, soweit dies für die jeweils genutzte Funktion erforderlich ist, eine entsprechende Berechtigung besteht oder eine gesetzliche Befugnis oder Verpflichtung dies vorsieht.
Zu den Empfängern können insbesondere gehören:

- Anbieter und Betreiber der ePA-App, des ePA-Aktensystems und weiterer technischer Dienste einschließlich genehmigter Unterauftragnehmer,
- gesetzlich zugriffsberechtigte Leistungserbringer und Einrichtungen, insbesondere Arzt- und Zahnarztpraxen, Krankenhäuser, Apotheken und Pflegeeinrichtungen,
- zugelassene Dienste- und Komponentenanbieter der Telematikinfrastruktur, insbesondere für GesundheitsID, E-Rezept, TI-Messenger und Verzeichnisdienste,
- eingesetzte Identitäts- und Authentifizierungsdienstleister für Registrierungs-, Identifizierungs- und Authentifizierungsverfahren (z. B. Anbieter von eID-, ePass- oder PostIdent-Verfahren),
- von Ihnen berechtigte Vertreterinnen und Vertreter sowie die Ombudsstelle Ihrer Krankenkasse,
- Anbieter freiwillig genutzter externer Dienste, insbesondere Karten-, Navigations-, Push- und App-Store-Dienste,
- die Vertrauensstelle und das Forschungsdatenzentrum Gesundheit im Rahmen der gesetzlichen Forschungsdatenausleitung sowie
- zuständige Aufsichts-, Prüf-, Ermittlungs- und sonstige öffentliche Stellen, soweit eine gesetzliche Befugnis oder Verpflichtung besteht.
- IT-Dienstleister

Je nach Empfänger und genutzter Funktion können insbesondere Identitäts- und Stammdaten, Versicherungsdaten, Identifizierungs- und Authentisierungsdaten, Nutzungs- und Protokolldaten, Berechtigungs- und Vertretungsdaten, Kommunikationsdaten sowie Inhalts- und Gesundheitsdaten einschließlich Medikations-, Verordnungs- und Abgabedaten betroffen sein.

Empfänger, die eigene gesetzliche Aufgaben erfüllen oder personenbezogene Daten für eigene Zwecke verarbeiten, handeln insoweit in eigener datenschutzrechtlicher Verantwortung. Hierzu können insbesondere Leistungserbringer, Apotheken, Behörden, Registerstellen sowie Anbieter externer Dienste gehören. Leistungserbringer erhalten nur Zugriff auf die Daten, die sie aufgrund gesetzlicher Regelungen oder der von Ihnen vorgenommenen Berechtigungen verarbeiten dürfen.

Technische Dienstleister können personenbezogene Daten als Auftragsverarbeiter in unserem Auftrag und nach unseren dokumentierten Weisungen verarbeiten. Sie erhalten personenbezogene Daten nur, soweit dies für die Entwicklung, Weiterentwicklung, Bereitstellung, den Betrieb, die Wartung, die Sicherheit oder den Support der ePA-App erforderlich ist. Sie werden sorgfältig ausgewählt, vertraglich verpflichtet und regelmäßig überprüft.

Soweit für die Registrierung, Identifizierung oder Authentifizierung externe Identitäts- und Authentifizierungsdienstleister eingesetzt werden, verarbeiten diese die hierfür erforderlichen Daten grundsätzlich in eigener Verantwortung oder im gesetzlich vorgesehenen Rollenmodell. Art und Umfang der Verarbeitung sowie die jeweils geltenden Speicher- und Löschfristen richten sich nach dem eingesetzten Verfahren und dem jeweiligen Anbieter.

Externe Karten- und Suchdienste erhalten die für die jeweilige Funktion erforderlichen Geräte-,Verbindungs-, Standort- und Suchdaten (siehe Ziffer 11.) und verarbeiten diese grundsätzlich in eigener datenschutzrechtlicher Verantwortung.

Im Rahmen der Forschungsdatenausleitung (siehe Ziffer 12) werden nur die gesetzlich und technisch vorgesehenen personenbezogenen Daten an das Forschungsdatenzentrum Gesundheit übermittelt. Die Übermittlung personenbezogener Daten erfolgt stets nach dem Grundsatz der Erforderlichkeit und nur insoweit, als dies für die jeweilige Funktion, den jeweiligen Verarbeitungszweck oder zur Erfüllung gesetzlicher Verpflichtungen notwendig ist.

16.2 Verarbeitung in der EU und Drittlandübermittlungen

Die Kernverarbeitung der ePA und der Sozialdaten erfolgt grundsätzlich in Deutschland beziehungsweise innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, soweit im jeweiligen Abschnitt nichts anderes angegeben ist.

Bei freiwillig aktivierten Push-, Karten-, Store- oder Betriebssystemdiensten kann eine Verarbeitung durch Anbieter mit Sitz oder Infrastruktur außerhalb der EU beziehungsweise des EWR nicht ausgeschlossen werden. In diesen Fällen informieren wir funktionsbezogen über Empfänger, Datenkategorien, Rechtsgrundlage und die eingesetzten Garantien nach Art. 44 ff. DSGVO. Bitte beachten Sie auch die Datenschutzhinweise der Datenempfänger.

16.3 Datenweitergabe an Dritte durch Aufruf und ggf. Nutzung externer Seiten

16.3.1 Download der ePA-App

Die ePA-App kann je nach angebotener Variante über den Apple App Store, den Google Play Store, den Microsoft Store oder über unsere Website https://www.bkk-firmus.de/beratung-und-service/elektronische-patientenakte/elektronische-patientenakte heruntergeladen werden. Beim Aufruf des Stores und beim Download verarbeitet der jeweilige Store-Anbieter insbesondere Konto-, Geräte-, Verbindungs-, Nutzungs- und Downloaddaten in eigener Verantwortung. Es gelten die Datenschutzhinweise des jeweiligen Store-Anbieters. Erfolgt der Download über unsere Website oder ein von uns bereitgestelltes Downloadportal, werden die für die Bereitstellung und technische Absicherung des Downloads erforderlichen Daten verarbeitet, insbesondere Protokoll- und Verbindungsdaten wie die IP-Adresse sowie Angaben zum verwendeten Browser und Betriebs-system.

16.3.2 Organspende-Register

Über die ePA-App können Sie zum Organspende-Register wechseln. Für die Anmeldung am Organspende-Register wird Ihre GesundheitsID verwendet. Dabei werden die zur eindeutigen Identifizierung und Authentifizierung erforderlichen Identitäts- und Authentifizierungsdaten sowie technisch erforderliche Verbindungsdaten an das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) als Betreiber des Organspende-Registers übermittelt. Eine Übermittlung von Inhalten Ihrer elektronischen Patientenakte an das Organspende-Register erfolgt hierdurch nicht. Nach der Übergabe erfolgt die weitere Datenverarbeitung im Verantwortungsbereich des BfArM. Es gelten die Datenschutzhinweise des Organspende-Registers.

16.3.3 Nationales Gesundheitsportal

Die ePA-App kann einen Verweis auf das Nationale Gesundheitsportal „gesund.bund.de“ bereitstellen. Mit Aufruf des Portals verlassen Sie die ePA-App und wechseln zu einem externen Angebot des Bundesministeriums für Gesundheit (BMG). Für die Verarbeitung personenbezogener Daten auf dem Nationalen Gesundheitsportal ist allein das BMG verantwortlich. Es gelten die dort bereitgestellten Datenschutzhinweise. Die Krankenkasse erhält grundsätzlich keine Informationen darüber, welche Inhalte Sie auf dem Nationalen Gesundheitsportal aufrufen oder nutzen. Eine Übermittlung von Daten aus Ihrer elektronischen Patientenakte an das Nationale Gesundheitsportal erfolgt durch den bloßen Aufruf des Portals nicht.

16.3.4 Weitere externe Links

Bei Links zu weiteren externen Angeboten wird vor dem Wechsel darauf hingewiesen, dass Sie den Verantwortungsbereich der ePA-App verlassen. Für die Verarbeitung Ihrer Daten auf dem externen Angebot ist die jeweilige externe Stelle verantwortlich. Es gelten die dort bereitgestellten Datenschutzhinweise.

16.3.5 Google Maps

Sofern Sie die Kartenfunktion nutzen, erfolgt die Darstellung der Karteninhalte über Google Maps. In diesem Zusammenhang können insbesondere Geräte-, Verbindungs-, Such- und gegebenenfalls Standortdaten verarbeitet werden. Verantwortlicher Anbieter des Dienstes ist die Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland. Es kann jedoch nicht ausgeschlossen werden, dass Daten im Rahmen der Leistungserbringung auch durch die Google LLC, USA, oder weitere Unternehmen der Google-Unternehmensgruppe verarbeitet werden.

Eine Verarbeitung personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums kann nicht ausgeschlossen werden. Soweit personenbezogene Daten in die USA oder andere Drittländer übermittelt werden, erfolgt die Übermittlung nach Maßgabe der jeweils anwendbaren datenschutzrechtlichen Vorgaben. Weitere Informationen hierzu finden Sie in den Datenschutzhinweisen von Google.

16.3.6 Grenzüberschreitende Gesundheitsdienste

Grenzüberschreitende Gesundheitsdienste werden derzeit schrittweise eingeführt. Die Bereitstellung erfolgt im Einklang mit den jeweils geltenden europäischen und nationalen Rechtsvorgaben für den grenzüberschreitenden Austausch elektronischer Gesundheitsdaten, insbesondere im Rahmen des Europäischen Gesundheitsdatenraums (European Health Data Space – EHDS).

Sobald eine entsprechende Funktion über die ePA-App angeboten wird, können Sie bestimmte Gesundheitsdaten freiwillig für eine konkrete Behandlung in einem anderen Mitgliedstaat der Europäischen Union bereitstellen. Vor der erstmaligen Nutzung werden Sie über die beteiligten Stellen, die verarbeiteten Daten, die Empfänger und die maßgeblichen Rechtsgrundlagen informiert. Die Verarbeitung erfolgt nur, wenn Sie die Funktion nutzen und die hierfür erforderliche Einwilligung erteilen.

17. Speicherdauer und Löschung

Wir speichern personenbezogene Daten nur so lange, wie dies für den jeweiligen Verarbeitungszweck erforderlich ist oder eine gesetzliche Aufbewahrungspflicht beziehungsweise ein anderer Rechtsgrund für die weitere Speicherung besteht. Anschließend werden die Daten gelöscht. Ist eine sofortige Löschung rechtlich oder technisch vorübergehend nicht möglich, wird die Verarbeitung entsprechend eingeschränkt. Für einzelne Daten gelten insbesondere folgende Regelungen:

17.1 Inhalte der ePA

Sie können die in Ihrer ePA gespeicherten Inhalte jederzeit teilweise oder vollständig löschen. Widersprechen Sie der weiteren Bereitstellung Ihrer ePA, wird die ePA nach Maßgabe des § 344 Abs. 3 SGB V gelöscht. Die gelöschten Daten können nicht wiederhergestellt werden.

17.2 Todesfall

Erlangt die Krankenkasse Kenntnis vom Tod einer versicherten Person, wird die ePA gemäß § 344 Abs. 6 SGB V grundsätzlich nach zwölf Monaten gelöscht. Dies gilt nicht, wenn entgegenstehende berechtigte Interessen Dritter geltend gemacht und nachgewiesen werden.

17.3 E-Rezept-Daten

Verordnungsdaten und Dispensierinformationen im E-Rezept-Fachdienst werden gemäß § 360 Abs. 11 SGB V mit Ablauf von 100 Tagen nach der Abgabe des verordneten Arzneimittels gelöscht. Daten, die in die elektronische Medikationsliste Ihrer ePA übernommen wurden, sind hiervon nicht erfasst. Für sie gelten die Löschmöglichkeiten der ePA. Bestimmte Rechnungsdaten können mit Ihrer Einwilligung gemäß § 360 Abs. 13 SGB V für höchstens zehn Jahre gespeichert werden.

17.4 Zugriffs-, Aktivitäts-, Betriebs- und Sicherheitsprotokolle

Zugriffs- und Aktivitätenprotokolle werden so lange gespeichert, wie dies zur Datenschutzkontrolle, zur Sicherstellung des technischen Betriebs, zur Fehlerbehebung oder zur Erkennung und Untersuchung von Sicherheitsvorfällen erforderlich ist. Die konkrete Speicherdauer richtet sich nach dem Schutzbedarf der betroffenen Systeme, den erforderlichen Prüf- und Reaktionszeiträumen sowie der Dauer offener Sicherheits-, Beschwerde- oder Prüfverfahren. Nach Wegfall des jeweiligen Zwecks werden die Daten gelöscht.

17.5 GesundheitsID und Benutzerkonto

Die für die GesundheitsID und das Benutzerkonto erforderlichen Daten werden gespeichert, solange die GesundheitsID beziehungsweise das Benutzerkonto bestehen.

Die Löschung oder Deaktivierung der GesundheitsID beziehungsweise des Benutzerkontos kann entweder auf Veranlassung der versicherten Person oder der Krankenkasse erfolgen, insbesondere im Zusammenhang mit nicht erfolgreich abgeschlossenen Registrierungs-, Gerätebindungs- oder Identifizierungsverfahren oder nach Maßgabe der Prozesse der Krankenkasse.

Nach Löschung bzw. Deaktivierung der GesundheitsID beziehungsweise des Benutzerkontos werden die Daten gelöscht, sobald sie nicht mehr zur Dokumentation der Identifizierung und Beendigung, zur Missbrauchsabwehr, zur Bearbeitung offener Sicherheits-, Support- oder Beschwerdevorgänge, zur Erfüllung gesetzlicher Nachweis- oder Aufbewahrungspflichten oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind.

Die Deinstallation der App führt nicht automatisch zur Löschung der GesundheitsID, des Benutzerkontos oder der elektronischen Patientenakte (ePA).

17.6 Berechtigungen und Erklärungen

Berechtigungen, Vertretungen, Einwilligungen, Widersprüche und Widerrufe werden für die Dauer ihrer Wirksamkeit gespeichert. Die erforderlichen Nachweisdaten werden anschließend so lange aufbewahrt, wie dies zur Erfüllung rechtlicher Rechenschafts- und Nachweispflichten, zur Bearbeitung möglicher Beanstandungen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Danach werden die Daten gelöscht.

17.7 Kommunikationsdaten

TI-Messenger-Nachrichten, Anhänge und Kommunikationsmetadaten werden nur solange gespeichert, wie dies für ihre Übermittlung, Zustellung, Anzeige, Synchronisierung und Verwaltung erforderlich ist. Löschfunktionen stehen im Rahmen der jeweiligen Anwendung zur Verfügung. Die konkrete Speicherdauer richtet sich insbesondere danach, ob die Nachricht zugestellt oder abgerufen wurde, weiterhin im Benutzerkonto angezeigt oder zwischen Endgeräten synchronisiert werden soll oder für einen offenen Support-, Beschwerde- oder Sicherheitsvorgang benötigt wird. Nach Wegfall des Speicherzwecks werden die Daten gelöscht. Der TI-Messenger dient der kurzfristigen Kommunikation und nicht der dauerhaften Archivierung medizinischer Behandlungsunterlagen.

Sofern Inhalte aus dem TI-Messenger zur Bearbeitung eines Anliegens in andere Systeme der Krankenkasse übernommen, dokumentiert oder archiviert werden, gelten für diese Verarbeitungen je nach Sacherhalt die gesetzlichen Aufbewahrungs- und Löschfristen. Die Löschung einer Nachricht im TI-Messenger führt in diesem Fall nicht automatisch zur Löschung der in anderen Systemen gespeicherten Dokumentation.

17.8 Standort-, Such- und Kartendaten

Standortdaten, Adressen und Suchparameter werden in den von uns betriebenen Systemen grundsätzlich nur für die Durchführung des jeweiligen Such-, Karten- oder Navigationsvorgangs verarbeitet und anschließend gelöscht, soweit sie nicht aufgrund einer ausdrücklichen Nutzerentscheidung gespeichert werden. Hiervon zu unterscheiden ist eine etwaige Verarbeitung durch den eingebundenen Kartendienstanbieter, z.B. Google. Für die dort erfolgende Verarbeitung gelten die Datenschutzbestimmungen und Löschregelungen des jeweiligen Anbieters.

17.9 Support- und Fehlerdaten

Supportanfragen, Ticketdaten, Fehlerberichte und technische Diagnoseinformationen werden bis zum Abschluss der Bearbeitung gespeichert. Eine weitere Speicherung erfolgt nur, soweit die Daten noch zur Dokumentation der Bearbeitung, zur Behebung wiederkehrender Fehler, zur Untersuchung eines Sicherheitsvorfalls, zur Erfüllung von Nachweispflichten oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind. Danach werden die Daten gelöscht.

17.10 Push-Benachrichtigungen und technische Kennungen

Wenn Sie die von Ihrer Krankenkasse bereitgestellte Funktion für Push-Benachrichtigungen nutzen, werden die für die Zustellung der Push-Benachrichtigungen erforderlichen Gerätekennungen und Push-Token gespeichert, solange Push-Benachrichtigungen für das betreffende Gerät aktiviert sind.

Wird die Push-Funktion deaktiviert oder ein Push-Token technisch ungültig, werden die zugehörigen Gerätekennungen und Push-Token gelöscht. Sitzungskennungen werden mit Beendigung der jeweiligen Sitzung gelöscht. Anmelde- und Sicherheitstoken werden bis zu ihrem technischen Ablauf, ihrer Ersetzung oder ihrem Widerruf gespeichert. Versand-, Zustellungs- und Fehlerprotokolle zu Push-Benachrichtigungen werden nur so lange gespeichert, wie dies für die Zustellung, Fehleranalyse, Missbrauchsabwehr, die Sicherstellung des technischen Betriebs oder die Bearbeitung konkreter Sicherheits- oder Supportvorgänge erforderlich ist. Nach Wegfall des jeweiligen Zwecks werden die Daten gelöscht.

Soweit für die Zustellung von Push-Benachrichtigungen externe Push-Dienste, insbesondere der Apple Push Notification Service (APNs) oder Firebase Cloud Messaging (FCM), eingesetzt werden, erfolgt die dortige Verarbeitung nach den Datenschutzbestimmungen und Speicherregelungen des jeweiligen Anbieters.

17.11 Krankenkassen- oder Anbieterwechsel

Ein Krankenkassenwechsel führt nicht automatisch zur Löschung Ihrer ePA. Das Aktenkonto wird einschließlich der gespeicherten Inhalte und Einstellungen an den künftig zuständigen ePA-Anbieter verschlüsselt übertragen. Hierzu gehören grundsätzlich auch Berechtigungen, Vertretungen sowie im Aktenkonto gespeicherte Widersprüche und Einschränkungen. Das hierfür erstellte verschlüsselte Exportpaket wird nur vorübergehend für den Aktenumzug gespeichert und anschließend gelöscht. Nach erfolgreichem Abschluss des Umzugs wird das bisherige Aktenkonto bei der bisherigen Krankenkasse gelöscht.

17.12 Dokumentenscan und technische Diagnosedaten

Soweit technische Nutzungs-, Diagnose- oder Fehlerdaten durch den Anbieter der eingesetzten Dokumentenscan-Technologie verarbeitet werden, richten sich Speicherdauer und Löschung dieser Daten nach dessen Datenschutzhinweisen. Weitere Informationen finden Sie in den Datenschutzhinweisen und Nutzungsbedingungen von Google.

18. Automatisierte Entscheidungen

Wir setzen im Rahmen der hier beschriebenen ePA-App grundsätzlich keine ausschließlich automatisierten Entscheidungen einschließlich Profiling ein, die Ihnen gegenüber rechtlicher Wirkung entfalten oder Sie in ähnlicher Weise erheblich beeinträchtigen.

19. Ihre Datenschutzrechte und besonderen Steuerungsmöglichkeiten in der ePA

19.1 Betroffenenrechte nach der DSGVO

Sie haben nach Maßgabe der jeweiligen gesetzlichen Voraussetzungen die nachfolgend beschriebenen Rechte. Der Umfang dieser Rechte kann jedoch insbesondere durch die DSGVO, das Sozialdatenschutzrecht des SGB X und besondere Regelungen des SGB V eingeschränkt sein. Eine besondere Einschränkung gilt nach § 363 Abs. 6 SGB V für Daten, die vor einem Widerspruch bereits für ein konkretes Forschungsvorhaben verwendet wurden. Daneben stehen Ihnen die besonderen Widerspruchs-, Beschränkungs- und Löschmöglichkeiten für die ePA nach dem SGB V zu.

19.1.1 Recht auf Auskunft nach Art. 15 DSGVO

Sie können Auskunft darüber verlangen, ob und welche personenbezogenen Daten wir im Zusammenhang mit der Bereitstellung und Nutzung Ihrer ePA-App verarbeiten. Soweit die gesetzlichen Voraussetzungen erfüllt sind, können Sie außerdem eine Kopie dieser Daten erhalten. In Ihrer ePA gespeicherte Inhalte und Protokolldaten können Sie zusätzlich über die dafür vorgesehenen Funktionen der ePA-App einsehen. Einschränkungen des Auskunftsrechts können sich insbesondere aus § 83 SGB X ergeben.

19.1.2 Recht auf Berichtigung nach Art. 16 DSGVO

Sie können die Berichtigung unrichtiger personenbezogener Daten und, unter Berücksichtigung des jeweiligen Verarbeitungszwecks, die Vervollständigung unvollständiger Daten verlangen. Betrifft Ihr Anliegen medizinische Inhalte, die von einer Arztpraxis, Apotheke, einem Krankenhaus oder einer anderen Stelle erstellt oder in Ihre ePA eingestellt wurden, kann für die fachliche Prüfung und Berichtigung die jeweilige Stelle zuständig sein. In diesem Fall informieren wir Sie über die zuständige Stelle beziehungsweise unterstützen Sie bei deren Ermittlung.

19.1.3 Recht auf Löschung nach Art. 17 DSGVO

Sie können die Löschung Ihrer personenbezogenen Daten verlangen, wenn die gesetzlichen Voraussetzungen erfüllt sind. Das Recht auf Löschung besteht insbesondere nicht, soweit die weitere Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Ergänzende Regelungen für Sozialdaten enthält § 84 SGB X.

Unabhängig vom Recht auf Löschung nach Art. 17 DSGVO können Sie über die hierfür vorgesehenen Funktionen der ePA-App gespeicherte Inhalte, Dokumente, Daten, Berechtigungen, Protokoll-einträge, Vertretungen und sonstige von Ihnen verwaltete Einstellungen im gesetzlich und technisch vorgesehenen Umfang selbst löschen oder entfernen. Darüber hinaus können Sie die vollständige Löschung Ihrer ePA veranlassen. Widersprechen Sie der weiteren Bereitstellung Ihrer ePA, wird diese gemäß § 344 Abs. 3 SGB V unverzüglich und vollständig gelöscht.

19.1.4 Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO

Sie können unter den gesetzlichen Voraussetzungen verlangen, dass Ihre personenbezogenen Daten nur noch eingeschränkt verarbeitet werden, beispielsweise während der Richtigkeit der Daten oder die Rechtmäßigkeit ihrer Verarbeitung geprüft wird. Ergänzende Regelungen für Sozialdaten enthält § 84 SGB X. Hiervon zu unterscheiden sind Ihre besonderen Möglichkeiten nach dem SGB V, den Zugriff einzelner Leistungserbringer oder Einrichtungen auf bestimmte Inhalte oder auf Ihre gesamte ePA zu beschränken.

19.1.5 Recht auf Datenübertragbarkeit nach Art. 20 DSGVO

Sie können personenbezogene Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format erhalten oder deren unmittelbare Übermittlung an einen anderen Verantwortlichen verlangen, soweit dies technisch möglich ist. Das Recht besteht nur, wenn die Verarbeitung automatisiert erfolgt und auf Ihrer Einwilligung oder einem Vertrag beruht. Für Verarbeitungen, die wir aufgrund gesetzlicher Verpflichtungen oder zur Wahrnehmung gesetzlich übertragener Aufgaben im Zusammenhang mit der ePA durchführen, besteht dieses Recht grundsätzlich nicht. Die gesetzlich vorgesehene Übertragung und Weiterführung Ihrer ePA bei einem Krankenkassen- oder Anbieterwechsel bleibt hiervon unberührt.

19.1.6 Recht auf Widerspruch nach Art. 21 DSGVO

Soweit wir Ihre personenbezogenen Daten auf Grundlage von Art. 6 Abs. 1 lit. e oder f DSGVO verarbeiten, können Sie aus Gründen, die sich aus Ihrer besonderen Situation ergeben, Widerspruch gegen die Verarbeitung einlegen. Das Widerspruchsrecht kann nach § 84 Abs. 5 SGB X eingeschränkt sein, wenn ein zwingendes öffentliches Interesse an der Verarbeitung überwiegt oder eine Rechtsvorschrift zur Verarbeitung der Sozialdaten verpflichtet. Die Widerspruchsmöglichkeiten nach den §§ 342 ff. und § 363 SGB V bestehen unabhängig vom Widerspruchsrecht nach Art. 21 DSGVO und richten sich nach den jeweiligen spezialgesetzlichen Voraussetzungen.

19.1.7 Recht auf Widerruf einer Einwilligung nach Art. 7 Abs. 3 DSGVO

Soweit eine Verarbeitung in der ePA-App auf Ihrer Einwilligung beruht, können Sie diese jederzeit mit Wirkung für die Zukunft widerrufen. Der Widerruf einer Einwilligung ist von den besonderen Widerspruchsmöglichkeiten nach dem SGB V zu unterscheiden. Der Widerruf betrifft ausschließlich die Verarbeitung, die auf der jeweiligen Einwilligung beruht. Dies kann beispielsweise bestimmte freiwillige Standort-, Benachrichtigungs- oder Zusatzfunktionen betreffen. Die Rechtmäßigkeit der Verarbeitung, die bis zum Widerruf auf Grundlage Ihrer Einwilligung erfolgt ist, bleibt unberührt. Ein Widerspruch oder Widerruf kann zur Folge haben, dass die auf der jeweiligen Verarbeitung beruhenden Funktionen oder Dienste künftig nicht oder nur noch eingeschränkt genutzt werden können.

19.1.8 Rechte bei automatisierten Entscheidungen nach Art. 22 DSGVO

Sie haben unter den gesetzlichen Voraussetzungen das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die Ihnen gegenüber rechtlicher Wirkung entfaltet oder Sie in ähnlicher Weise erheblich beeinträchtigt. Im Zusammenhang mit der Bereitstellung und Nutzung der ePA-App treffen wir keine solchen ausschließlich automatisierten Entscheidungen, soweit in dieser Datenschutzerklärung nicht ausdrücklich etwas anderes angegeben ist.

19.2 Besondere Steuerungsmöglichkeiten für Ihre ePA

Neben den Rechten nach der DSGVO stehen Ihnen verschiedene gesetzliche Steuerungs- und Widerspruchsmöglichkeiten nach den §§ 342 ff. SGB V zur Verfügung. Hierzu gehören insbesondere:

- der Widerspruch gegen die Einrichtung einer ePA,
- der Widerspruch gegen die weitere Bereitstellung einer bereits angelegten ePA,
- der Widerspruch gegen die Übermittlung und Speicherung bestimmter Daten in der ePA,
- die Beschränkung von Zugriffsrechten (Dokumente, Datensätze oder Datenbereiche),
- der Ausschluss einzelner Leistungserbringer oder Einrichtungen vom Zugriff auf Ihre ePA,
- die Löschung von Inhalten der ePA,
- der Widerspruch gegen einzelne Anwendungsfälle der ePA,
- der vollständige oder auf einzelne gesetzlich vorgesehene Zwecke beschränkte Widerspruch gegen die Übermittlung von ePA-Daten an das Forschungsdatenzentrum.

Diese besonderen Steuerungsmöglichkeiten beruhen auf den Vorschriften des SGB V. Sie sind weder mit dem Widerruf einer Einwilligung nach Art. 7 Abs. 3 DSGVO noch mit dem Widerspruchsrecht nach Art. 21 DSGVO gleichzusetzen. Die Ausübung eines Widerspruchs wirkt sich grundsätzlich nur auf die davon erfasste Funktion oder Datenverarbeitung aus.

19.3 Gesetzliche Einschränkungen Ihrer Rechte

Einzelne Betroffenenrechte nach der DSGVO können gesetzlich eingeschränkt oder ausgeschlossen sein. Dies gilt insbesondere für Daten, die vor einem Widerspruch gegen die Übermittlung von ePA-Daten an das Forschungsdatenzentrum bereits für ein konkretes Forschungsvorhaben verwendet wurden. Diese Daten dürfen für das betreffende Forschungsvorhaben weiterverarbeitet werden. Insoweit sind gemäß § 363 Abs. 6 SGB V das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO und das Widerspruchsrecht nach Art. 21 DSGVO ausgeschlossen.

19.4 Ausübung Ihrer Rechte und Steuerungsmöglichkeiten

Ihre Betroffenenrechte nach der DSGVO und den Widerruf einer Einwilligung können Sie gegenüber der für den jeweiligen Verarbeitungsvorgang Verantwortlichen geltend machen. Die besonderen Widerspruchs-, Beschränkungs- und Löschmöglichkeiten nach dem SGB V können Sie abhängig von der jeweiligen Funktion insbesondere über die dafür vorgesehene Funktion in der ePA-App, gegenüber Ihrer Krankenkasse oder gegenüber der Ombudsstelle Ihrer Krankenkasse ausüben. Bitte wenden Sie sich hierzu an:

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

Soweit eine andere Stelle für den betreffenden Verarbeitungsvorgang verantwortlich ist, informieren wir Sie über die zuständige Stelle beziehungsweise unterstützen Sie bei deren Ermittlung.

19.5 Beschwerderecht nach Art. 77 DSGVO

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten im Zusammenhang mit der ePA-App gegen datenschutzrechtliche Vorschriften verstößt, können Sie sich an die für Ihre Krankenkasse zuständige Datenschutzaufsichtsbehörde wenden. Das Beschwerderecht besteht unbeschadet anderer verwaltungsrechtlicher oder gerichtlicher Rechtsbehelfe.

Für die Krankenkasse ist zuständig:
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

19.6 Zuständige Rechtsaufsicht

Die Rechtsaufsicht überwacht die Krankenkasse in Bezug auf die Einhaltung ihrer gesetzlichen Aufgaben und Pflichten nach dem Sozialrecht. An sie können Sie sich wenden, wenn Sie Fragen oder Beschwerden zur Wahrnehmung dieser Aufgaben haben.

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

20. Stand und Aktualisierung dieser Datenschutzerklärung

Wir aktualisieren diese Datenschutzerklärung, wenn sich rechtliche Vorgaben, technische Funktionen, Empfänger, Rollen, Speicherfristen oder Sicherheitsmaßnahmen wesentlich ändern. Die jeweils aktuelle Fassung ist unter https://www.bkk-firmus.de/beratung-und-service/elektronische-patientenakte/epa-dokumente-zum-download verfügbar.

Stand: 30.10.2026