Datenschutzerklärung für TK-Safe und die elektronische Patientenakte

Seit dem 1. Januar 2021 bietet die Techniker Krankenkasse (TK) ihren Versicherten die "elektronische Patientenakte" - kurz: ePA - an. Gesetzlich Versicherte (im Folgenden: Versicherte) haben die Möglichkeit, ihre gesundheitsbezogenen Dokumente mit der ePA lebenslang sicher zu verwalten. Die Nutzung der ePA ist freiwillig und kann jederzeit beendet und wieder aufgenommen werden. Seit dem 15.01.2025 verfügt jeder Versicherte, der nicht widersprochen hat, über eine ePA („ePA für alle“, § 342 fünftes Buch Sozialgesetzbuch, im Folgenden SGB V). Auch mit der ePA für alle bleibt die Nutzung freiwillig.

Stand: 15.01.2025

Diese Datenschutzerklärung informiert Sie in Ihrer Funktion als Nutzer bzw. ePA-Akteninhaber selbst oder als sogenannte ePA-Vertretung für einen Versicherten (gemäß Ziffer 2.6) über die Erhebung, Verarbeitung und Nutzung Ihrer personenbezogenen Daten.
Gemäß § 341 Abs. 4 Satz 1 SGB V ist die Techniker Krankenkasse, Bramfelder Straße 140, 22305 Hamburg für die Verarbeitung der Daten im Rahmen der ePA verantwortlich.

Das Angebot der ePA wird durch die von der TK beauftragte Firma IBM Deutschland GmbH nach den Vorgaben der TK erbracht. IBM unterliegt den datenschutzrechtlichen Anforderungen und der datenschutzrechtlichen Kontrolle der TK.

Inhalt - Übersicht:

1. Allgemeine Informationen zur ePA

1.1 Definition ePA

Die ePA bietet Versicherten die Möglichkeit der selbstbestimmten elektronischen Speicherung, Übermittlung und Verwaltung Ihrer personenbezogenen Gesundheitsdaten. Mit der ePA können gesundheitsbezogene Daten zwischen Versicherten und denjenigen, die an der medizinischen Behandlung beteiligt sind, ausgetauscht werden. Die Vorgaben für die ePA werden von der gematik GmbH (Nationale Agentur für Digitale Medizin) erstellt. Damit ist sichergestellt, dass Sie über die ePA unabhängig vom Anbieter ein Leben lang einen sicheren Datenspeicher zur Verfügung haben. Die Hoheit über die ePA liegt bei Ihnen als versicherte Person. Sie entscheiden, welcher Dritte auf die ePA und die darin enthaltenen Dokumente zugreifen darf. Die Berechtigungen können je Praxis oder Institution mit zeitlicher Einschränkung vergeben und jederzeit wieder entzogen werden.

Eine ePA wird jedem Versicherten unabhängig von der jeweiligen Krankenkasse der versicherten Person zur Verfügung gestellt. Bei einem Wechsel der Krankenkasse wird Ihre ePA mit den bestehenden Inhalten und Einstellungen bei der anderen Krankenkasse weitergeführt.

1.2 Rechtsgrundlagen

Rechtsgrundlagen für die Verarbeitung Ihrer personenbezogenen Daten in der ePA sind:

Ihre Einwilligung nach Artikel 6 Abs. 1 Satz 1 Buchstabe a in Verbindung mit Artikel 9 Abs. 2 Buchstabe a Datenschutzgrundverordnung (DSGVO),

Ihre Einwilligung nach § 344 Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung, die gesetzliche Verpflichtung der TK zur Verfügungstellung der ePA nach Artikel 6 Abs. 1 Satz 1 Buchstabe c DSGVO in Verbindung mit § 341 Abs. 1 SGB V.

1.3 Kenntnisnahme der Datenschutzerklärung und Zustimmung in die Datenverarbeitung

Um die ePA zu nutzen, ist es erforderlich, dass Sie die Datenschutzerklärung zur Kenntnis nehmen und in die Datenverarbeitung gem. § 344 SGB V einwilligen.

Die Kenntnisnahme der Datenschutzerklärung wird von der TK gespeichert. Bei einem Widerspruch gegen die Datenschutzerklärung wird der Zugang zur ePA bis zur erneuten Einwilligung in diese Datenschutzerklärung gesperrt. Bei Beendigung der ePA wird diese Information nach Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht.

1.4 Datenspeicherung, Datenverwaltung und Schutz Ihrer Daten

Ihre Daten werden ausschließlich innerhalb der Europäischen Union bei der IBM Deutschland GmbH (nachfolgend IBM genannt) - gespeichert und verarbeitet. Ihre Daten werden hierbei stets verschlüsselt gespeichert.

Zum Schutz Ihrer Daten wurden technische und organisatorische Sicherheitsmaßnahmen implementiert, um Ihre Daten vor unbefugtem Zugriff und sonstigem Missbrauch zu schützen.

(a) Verschlüsselung der Daten

Die Dokumente der ePA werden verschlüsselt im Aktensystem abgelegt. Weder die IBM als Betreiber noch die TK als Anbieter der Akte haben Zugriff auf die Klartext-Daten der Dokumente. Nur Sie oder durch Sie Berechtigte können auf diese zugreifen. Zur Sicherung Ihrer Daten sind mehrere digitale Schlüssel erforderlich. Diese bezeichnen wir nachfolgend als Schlüsselmaterial.

Die eingesetzten Verschlüsselungsmechanismen orientieren sich an aktuellen und zukünftigen Verfahren und Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

(b) Löschfristen

Für die Verarbeitung und Löschung der von Ihnen in der ePA gespeicherten Stammdaten (Titel, Vorname, Nachname, Versichertennummer) und Gesundheitsdaten sind Sie grundsätzlich selbst verantwortlich. IBM kann diese Daten nicht einsehen und bietet Ihnen allein die technischen Funktionalitäten zur Speicherung, Aufbewahrung und Löschung Ihrer Daten. Die von Ihnen in der ePA gespeicherten Daten werden so lange aufbewahrt, wie ein gültiger Nutzungsvertrag mit Ihnen besteht. Die Daten werden spätestens innerhalb von 14 Tagen nach Beendigung des Nutzungsvertrages vollständig und unwiderruflich im Rahmen der allgemeinen Löschungsroutinen gelöscht.

Die Speicherdauer Ihrer personenbezogenen Daten, die nicht originärer Inhalt der ePA sind, richtet sich nach dem jeweiligen Zweck der Datenverarbeitung. Sofern der Zweck der Datenverarbeitung entfällt, erfolgt die Löschung der Daten.

Wenn in dieser Datenschutzerklärung nicht anders geregelt, werden Ihre Daten daher für die folgende Dauer gespeichert:

Ihre Zuordnungs- und Referenznummern (technische Referenznummer, ePA-Kundennummer) sowie Ihre Krankenkassenzugehörigkeit werden nach Beendigung der ePA nach Ziffer 1.5 - zusammen mit Angaben zur Art der Kündigung bzw. der sonstigen Vertragsbeendigung, Datum und Uhrzeit der Kündigung sowie Zeitpunkt des Vertragsendes (Datum, ggf. Uhrzeit) für einen Zeitraum von drei Jahren gespeichert.

Die für Abrechnungszwecke gespeicherten Daten über Ihre Nutzung der ePA werden nicht länger als 15 Monate gespeichert. Die Rechtsgrundlage dazu stellt § 284 Abs. 1 Nr. 20 SGB V dar.

Die zu Nachweiszwecken erfassten Protokolldaten (wie etwa zur Protokollierung des Akzeptierens dieser Datenschutzerklärung oder der Nutzungsbedingungen von TK-Safe oder des erfolgreichen Imports von Daten) werden - zusammen mit Ihrer ePA-Kundennummer und Ihrer technischen Referenznummer nach Beendigung des Nutzungsvertrages noch für einen Zeitraum von drei Jahren aufbewahrt.

Sämtliche vorstehend aufgeführten Daten werden nach Ablauf der genannten Zeiträume, wie von der gematik in den Vorgaben zur Telematik spezifiziert, vollständig gelöscht, es sei denn, dass einer Löschung gesetzliche Aufbewahrungspflichten entgegenstehen oder eine längere Speicherung im konkreten Fall zur Erfüllung rechtlicher Verpflichtungen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Die zur Fehleranalyse, Gewährleistung der Systemsicherheit sowie Verhinderung von Missbrauch und Aufdeckung und Verfolgung von Straftaten oder Verstößen gegen die Nutzungsbedingungen gespeicherten Log-Daten (einschließlich Ihrer ePA-Kundennummer) und die IP-Adresse Ihres Endgeräts, mit dem Sie die ePA nutzen, werden jeweils sieben Tage nach der entsprechenden Protokollierung gelöscht, es sei denn, dass innerhalb dieses Zeitraums ein Vorfall festgestellt wurde, der eine weitere Aufklärung, Untersuchung und/oder Verfolgung erfordert.

(c) Erfassung von Nutzungsdaten zu Abrechnungszwecken

Das Angebot der ePA ist für Sie kostenfrei. Die Kosten für Ihre Nutzung der ePA trägt die TK.

Um die Abrechnung der Nutzung der ePA seitens IBM mit der TK zu ermöglichen, werden folgende Informationen über die Nutzung der ePA erhoben, gespeichert und verarbeitet:

Datum und Uhrzeit des letzten Zugriffs auf die ePA pro Quartal (es werden stets nur die Informationen über einen Zeitraum der jeweils fünf letzten Quartale erfasst und gespeichert)

- technische Referenznummer
- Krankenversicherungsnummer
- Krankenkassenzugehörigkeit

Art, Datum und Uhrzeit des Widerspruchs (soweit anwendbar) bzw. Art, Datum und Uhrzeit einer sonstigen Vertragsbeendigung (soweit anwendbar) Rechtsgrundlage der Datenverarbeitung ist §284 Abs. 1 Nr. 20 SGB V. Diese für Abrechnungszwecke gespeicherten Daten liegen im Regelfall ausschließlich in aggregierter und anonymisierter Form zu Zwecken der Rechnungsstellung seitens der IBM vor. Allein bei Widersprüchen im Hinblick auf den Umfang Ihrer tatsächlichen Nutzung der ePA kann es im Rahmen der Rechnungsprüfung erforderlich sein, dass gegenüber der TK der Zeitpunkt des letzten Zugriffs auf die ePA pro Quartal (über einen Zeitraum der letzten fünf Quartale) sowie Ihre technische Referenznummer offengelegt wird, sodass ein Abgleich der Rechnungsdaten mit den von der TK zur Nutzung der ePA erfassten Daten möglich ist. Weitere Daten erhält die TK nicht.

Auch IBM selbst erhält im Rahmen dieses Abgleichs keinerlei Informationen, welche eine Identifizierung der einzelnen Nutzer der ePA ermöglichen würde.

Die Verarbeitung der Daten zu Abrechnungszwecken ist Voraussetzung der Erfüllung des Vertrages mit Ihnen über die Nutzung der ePA. Ihre Daten werden für keine anderen Zwecke verwendet oder sonst an Dritte weitergegeben.

1.5 Beendigung der ePA

(a) Kontoschließung der ePA

Sie haben folgende Möglichkeiten Ihre ePA zu schließen:

Widerspruch gegen die Nutzung der ePA über TK-Safe, https://tk.de oder über einen Antrag bei der TK in Textform.

Beachten Sie, dass Sie in Ihrer Funktion als ePA-Vertretung gemäß Ziffer 2.6 generell nicht dazu berechtigt sind, einen Widerspruch gegen die ePA auszusprechen.

(b) Datenlöschung der ePA

Eine Löschung sämtlicher ePA-Daten wird durch folgende Anwendungsfälle ausgelöst:

Widerspruch gegen die ePA
Die Löschung der Daten Ihrer ePA erfolgt in diesem Fall sechs Wochen nach Ihrem Widerspruch. Bis zu diesem Zeitpunkt können Sie den Widerspruch noch zurücknehmen.

Sämtliche gespeicherten Daten werden nach Beendigung der ePA vollständig gelöscht, es sei denn, dass einer Löschung gesetzliche Aufbewahrungspflichten entgegenstehen oder eine längere Speicherung im konkreten Fall zur Erfüllung rechtlicher Verpflichtungen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

1.6 Datenweitergabe an sonstige Dritte

Ihre Daten werden streng vertraulich behandelt.

Soweit dies nicht in dieser Datenschutzerklärung ausdrücklich vorgesehen ist, gibt die TK Ihre Daten nicht an sonstige Dritte weiter, es sei denn, Sie haben in die Weitergabe ausdrücklich eingewilligt. Zudem besteht die Möglichkeit, dass die TK zur Weitergabe Ihrer Daten gesetzlich verpflichtet ist.

Des weiteren werden technische Dienstleister genutzt, die dabei unterstützen, die ePA bereitzustellen. Hierbei handelt es sich um folgende Unternehmen mit Sitz in der Europäischen Union:

Unternehmen, die der IBM-Gruppe nachgeordnet sind
a. IBM Deutschland Customer Support Services GmbH, Sitz in Deutschland
b. IBM Client Innovation Center Germany, Sitz in Deutschland
c. IBM iX Berlin GmbH, Sitz in Deutschland
d. IBM Client Innovation Austria GmbH, Sitz in Österreich
e. IBM Česká republika, spol. s r.o., Sitz in Tschechien
f. IBM Polska sp. z o.o, Sitz in Polen
g. IBM Romania S.R.L., Sitz in Rumänien

Weitere eigenständige Unterauftragnehmer der IBM Deutschland GmbH:

a. achelos GmbH, Sitz in Deutschland
b. arvato systems GmbH, Sitz in Deutschland

c. Equinix (Germany) GmbH, Sitz in Deutschland
d. levigo systems gmbh, Sitz in Deutschland
e. modzero GmbH, Sitz in Deutschland
f. retarus GmbH, Sitz in Deutschland
g. SThree GmbH, Sitz in Deutschland

Diese Unternehmen helfen dabei die ePA technisch zu betreiben und die Ihnen angebotenen Funktionalitäten und Dienste bereitzustellen sowie technischen Support zu leisten. Unter keinen Umständen werden Ihre personenbezogenen Daten in ein Drittland außerhalb des Europäischen Wirtschaftsraums übermittelt. Die Dienstleister werden ausschließlich im Auftrag und gemäß den Weisungen der TK an IBM tätig und sind verpflichtet, sämtliche notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um Ihre Daten gemäß den datenschutzrechtlichen Erfordernissen zu schützen. Eine Weitergabe an Dritte oder Verwendung für andere Zwecke ist ihnen nicht gestattet.

1.7 Support

Als Anbieter der ePA steht Ihnen die TK für alle diesbezüglichen Fragen zur Verfügung.

2. Allgemeine Funktionen der ePA

Die ePA ermöglicht es Ihnen, Ihre Daten zu speichern, zu verwalten oder mit an der medizinischen Behandlung beteiligten Leistungserbringern oder Institutionen (z. B. Ärzte oder Krankenhäuser) auszutauschen und zu teilen.

2.1 Austausch von Dokumenten

Sie als versicherte Person und an der medizinischen Behandlung beteiligte Leistungserbringer können Dokumente einsehen und einstellen. Das Format und Merkmale des Dokuments sind seitens der gematik vorgegebenen. Treffen Sie die Entscheidung, dass ein Dokument nicht mehr relevant ist oder nicht mehr für andere zur Verfügung stehen soll, können Sie es löschen. Beachten Sie, dass von Ihnen berechtigte Praxen und Institutionen während der Dauer der

vergebenen Berechtigung, die in Ihrer ePA enthaltenen Dokumente herunterladen können.

Folgende Informationen können Sie und an der medizinischen Behandlung beteiligte Leistungserbringer in der ePA speichern.

Beispielsweise:

- Arztbriefe und Krankenhausentlassungsberichte
- Befunde (u.a. Allergologie- und Laborbefunde)
- Diagnosen
- Fotodokumentationen
- Patienteninformationen
- Pflegedokumentationen
- Schwangerschafts- und Geburtsdokumentationen
- Therapiedokumentationen
- Medizinische Pässe, wie z. B. das Zahnbonusheft oder der Impfpass
- Abrechnungsdaten der Krankenkassen
- Dokumente aus Digitalen Gesundheitsanwendungen

2.2 Austausch weiterer Informationen

Neben der Speicherung von Dokumenten ist auch das Speichern von Datensätzen in der ePA möglich, die sich aus der medizinischen Behandlung ergeben.

2.2.1 Der digital gestützte Medikationsprozess

Der digital gestützte Medikationsprozess besteht aus der elektronischen Medikationsliste und dem elektronischen Medikationsplan. Die elektronische Medikationsliste wird mit eRezept-Daten befüllt und enthält somit Informationen zur Verordnung eines Medikaments durch einen Arzt sowie zur Ausgabe eines Medikaments in der Apotheke. Der elektronische Medikationsplan ist eine digitale Version des Bundeseinheitlichen Medikationsplans.

2.3 Zugriffsrechte von berechtigten Leistungserbringern auf Dokumente

Sie entscheiden, wer Zugriff auf Dokumente in Ihrer ePA erhalten soll, indem Sie Leistungserbringerinstitutionen für ihre ePA berechtigen. Welche Dokumente einzelne Leistungserbringerinstitutionen (z. B. Arztpraxen) einsehen können ist gesetzlich für die Berufsgruppen und Dokumentenkategorien festgelegt.

Sie haben die Möglichkeit einzelne Dokumente oder ganze Dokumentenkategorien vor allen Leistungserbringerinstitutionen (z. B. Arztpraxen) zu verbergen.

2.3.1 Verbergen von einzelnen Dokumenten

Sie können entscheiden, ob ein Dokument für alle ihre berechtigten Leistungserbringerinstitutionen (z.B. Arztpraxen) oder nur für Sie selbst und ihre Vertretung einsehbar sein soll. Sie können jederzeit einzelne Dokumente verbergen oder wieder sichtbar machen.

2.3.2 Verbergen von Dokumentenkategorien

Jedes Dokument in Ihrer ePA ist einer Dokumentenkategorie zugeordnet. Sie können entscheiden, ob eine Dokumentenkategorie für alle ihre berechtigten Leistungserbringerinstitutionen (z.B. Arztpraxen) oder nur für Sie selbst und ihre Vertretung einsehbar sein soll. Auch Dokumentenkategorien können Sie jederzeit verbergen oder wieder sichtbar machen.

Es gibt die nachfolgend aufgeführten Dokumentenkategorien:

- Eigene Dokumente
- Befunde
- Pflegedokumente
- eArztbriefe
- Arbeitsunfähigkeitsbescheinigungen
- Notfalldaten
- Zahnbonusheft
- Kinderuntersuchungsheft und Kinderuntersuchungsheft (vor 2025)
- Mutterpass
- Impfpass

- Abrechnungsdaten
- Dokumente aus Digitalen Gesundheitsanwendungen
- Rehabilitationsdokumente
- Elektronische Abschriften der Patientenakte
- Sonstige Dokumente (z. B. Dokumente aus Disease-Management-Programmen)

2.3.3 Erteilung von Berechtigungen

Die Leistungserbringerinstitutionen (z. B. Ihre Arztpraxis) können auf Daten, die in Ihrer ePA gespeichert sind, erst dann zugreifen, wenn Sie dafür eine Berechtigung erteilt haben. Sämtliche Berechtigungen, werden in Ihrer ePA gespeichert.

Die Erteilung der Berechtigung erfolgt über folgende Wege:

- Automatisiert über das Einlesen Ihrer elektronischen Gesundheitskarte bspw. beim Arztbesuch (es sei denn Sie haben zuvor widersprochen)
- Manuell über ein mobiles Endgerät (über TK-Safe in der TK-App)
- Manuell über die stationäre Desktop-Anwendung "TK-Safe"

Über jede dieser Möglichkeiten können Sie einstellen, wer Daten in Ihrer ePA einsehen kann. Berechtigungen können jederzeit wieder entzogen werden. Unabhängig davon legen Sie einen Zeitraum für die Dauer der Zugriffsmöglichkeit fest. Sie können dabei zwischen einem Tag bis zu "unbegrenzt" wählen oder der Zeitraum wird automatisch durch einen Behandlungskontext (siehe Abschnitt Behandlungskontext) vorgegeben. Nach Ablauf des Zeitraums endet die Berechtigung für die jeweilige Leistungserbringerinstitution automatisch. Diese kann danach nicht mehr auf die Daten in Ihrer ePA zugreifen. Daten, die vom Leistungserbringer bereits heruntergeladen wurden, sind jedoch hiervon nicht betroffen. Für diese gelten gesonderte datenschutz- und berufsrechtliche Bestimmungen.

Behandlungskontext

Ein begrenzter Berechtigungszeitraum beginnt automatischen mit den Einlesen Ihrer elektronischen Gesundheitskarte beispielsweise bei einem Arztbesuch. Der Behandlungskontext besteht für Arztpraxen, Krankenhäuser, Rehabilitationseinrichtungen, Zahnarztpraxen, Psychotherapeutische Praxen,

Pflegeeinrichtungen, Geburtshilfe, Psychotherapeutische Praxen für 90 Tage. Für öffentliche Gesundheitseinrichtungen, Apotheken und Arbeitsmedizin für 3 Tage.

2.3.4 Widerspruch gegen eine Leistungserbringerinstitution erteilen

Sie haben die Möglichkeit einen Widerspruch gegen Leistungserbringerinstitutionen zu erteilen. Nach Erteilung eines Widerspruchs kann diese weder auf die Daten Ihrer ePA zugreifen noch wird sie beim Einlesen Ihrer elektronischen Gesundheitskarte berechtigt (Behandlungskontext).

Einen Widerspruch können Sie entweder über ein mobiles Endgerät (über TK-Safe in der TK-App). über die stationäre Desktop-Anwendung "TK-Safe" oder über die Ombudsstelle TK erteilen.

Über die gleichen Möglichkeiten können Sie ihren Widerspruch jederzeit zurücknehmen.

2.3.5 Digitale Gesundheitsanwendungen (DiGA) berechtigen

Sie können auch Digitalen Gesundheitsanwendungen den Zugriff auf die ePA gewähren.

Anders als die Zugriffsmöglichkeit von Leistungserbringern können Digitale Gesundheitsanwendungen keine Dokumente in Ihrer ePA lesen oder löschen, sondern lediglich Dokumente einstellen. Sie vergeben die Berechtigung an eine Digitale Gesundheitsanwendung immer unbefristet. Ein Löschen der DiGA-Berechtigung ist jederzeit möglich.

2.3.6 Initiale Berechtigungen

Ihre Krankenkasse, der E-Rezept Fachdienst (Rezeptdienst) und die Ombudsstelle TK erhalten automatisch eine Berechtigung bei Aktivierung Ihres Aktenkontos. Diese können keine Dokumente lesen oder löschen. Die initialen Berechtigungen sind dauerhaft gültig und können nicht gelöscht werden.

2.4 Zugriffsrechte von berechtigten Leistungserbringern auf weitere Informationen

2.4.1 Zugriff auf Daten aus dem digital gestützten Medikationsprozess

Leistungserbringende, die Sie für den Zugriff Ihrer ePA berechtigt haben, haben zunächst auch Zugriffsrechte auf die Daten aus dem digitalgestütztem Medikationsprozess. Sie haben die Möglichkeit, dieses Zugriffsrecht allen Leistungserbringenden zu entziehen. Es besteht keine Möglichkeit, das Zugriffsrecht einzelnen Leistungserbringenden zu entziehen, die Zugriff auf Ihre ePA haben.

Außerdem haben Sie die Möglichkeit, dem digital gestütztem Medikationsprozess zu widersprechen. Dann werden die erhobenen Daten gelöscht und es können keine weiteren Daten über den digital gestützten Medikationsprozess eingestellt werden.

2.5 Protokolle und Aktivitäten in der ePA

(a) Zugriffe und Veränderungen in der ePA

Die im Rahmen des Dokumentenmanagements der ePA anfallenden Aktivitäten werden im Nutzungsverlauf protokolliert, sodass Sie alle Zugriffe und vorgenommenen Veränderungen von Berechtigten nachvollziehen können. Zu diesen Aktivitäten gehören insbesondere:

- Einstellen, Verändern und Löschen von Dokumenten und Rezeptdaten
- Vergabe, Verändern und Löschen von Zugriffsberechtigungen und Widerspruchsentscheidungen
- Abrufen von Daten (z. B. von Dokumenten)

Die Daten der Protokollierung umfassen insbesondere:

- Nutzername des Zugreifenden
- Art des Zugriffs (ausgeführte Aktivität)
- Zeitpunkt des Zugriffs

Diese Protokolldaten werden zur Vertragserfüllung sowie zur Wahrung der berechtigten Interessen (Nachweiszwecke) gespeichert und verarbeitet, soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist. Die Protokolldaten werden entsprechend § 309 Abs. 1 SGB V für drei Jahre gespeichert und nach Ablauf dieser Frist gelöscht.

Sie haben jederzeit die Möglichkeit, insbesondere bei der Kündigung Ihrer ePA, Ihre Protokolldaten im signierten pdf-Format zu speichern. Der signierte Export stellt sicher, dass die Daten aus Ihrer ePA stammen und nicht verändert wurden. Zudem steht Ihnen ein nicht-signierter Export der Protokolldaten im JSON-Format zur Verfügung, der es Ihnen ermöglicht, die Daten zu einem späteren Zeitpunkt in TK-Safe einzulesen und in gewohnter Form anzuzeigen.

Nach der Beendigung Ihrer ePA werden die Protokolldaten nur noch eingeschränkt gespeichert. Sie werden nach drei Jahren gelöscht und stehen ausschließlich für durch Sie angeforderte Auskünfte oder aufsichtsrechtliche Kontrollen zur Verfügung.

(b) Log-Daten und IP-Adressen

Es werden systemseitig Log-Daten der Zugriffe auf die Systemumgebung und Applikationen der ePA auf den Servern von IBM protokolliert (Datum, Zeitpunkt, Anforderung/Vorgang, Fehlermeldung), um potenzielle Störungen der ePA zu analysieren und mögliche Fehlerursachen zu identifizieren und zu beheben. Zu diesen Zwecken kann in den Log-Daten auch Ihre ePA-Kundennummer gespeichert werden. Es ist IBM grundsätzlich nicht möglich, von Ihrer ePA-Kundennummer Rückschlüsse auf Ihre Person zu ziehen.

Daneben protokolliert IBM die IP-Adressen der Endgeräte, mit denen Sie die ePA nutzen, sowie den dazugehörigen Vorgang (Anforderung/Vorgang, Datum, Uhrzeit), um potenzielle Angriffe von außen gegen die Systemumgebung der ePA nachvollziehen und abwehren zu können.

2.6 Zugriff auf die ePA durch ePA-Vertretungen

Bei ePA-Vertretungen handelt es sich z. B. Freunde, Bekannte oder Familienmitglieder, die Ihnen oder denen Sie aktiv Zugriff auf die eigene ePA einrichten können.

Die Besonderheiten der ePA-Vertretung werden im Folgenden erläutert.

(a) Zulassung einer ePA-Vertretung auf die ePA

Sie können bis zu fünf Personen als ePA-Vertretung einrichten. Dies ist ausschließlich über die Nutzung von TK-Safe in der TK-App oder in der Desktop-Anwendung möglich.

Mit der Anlage einer ePA-Vertretung erteilen Sie der Vertretung Zugriff auf Ihre ePA. Die ePA-Vertretung erhält damit Zugang auf die dort gespeicherten Daten und das Recht als Vertretung für Sie zu handeln (Ziffer 2.6 (b)).

Bei Anlage einer ePA-Vertretung, wird diese per E-Mail darüber informiert, dass im Rahmen der Vertretungsberechtigung im ePA-Aktensystem folgende Daten der ePA-Vertretung verarbeitet, werden:

- Vor- und Nachname
- Versichertennummer
- E-Mail-Adresse
- Technische Referenznummern

Wenn eine ePA-Vertretung die Vertretungsberechtigung beenden möchte oder das Einverständnis zur Verarbeitung seiner Daten widerruft, kann die Vertretung dies Ihnen gegenüber erklären. In diesen Fällen sind Sie dazu verpflichtet, die entsprechende ePA-Vertretung umgehend in Ihrer ePA zu beenden. Die ePA-Vertretung selbst hat auch die Möglichkeit seine Vertretungs-Rechte über die Verwaltung seiner Vertretung in Ihrer ePA zu löschen. Über die Möglichkeiten der Beendigung der Vertretungs-Rechte wird Ihre Vertretung in der oben benannten E-Mail in Kenntnis gesetzt.

Rechtsgrundlage der Datenverarbeitung ist die Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO. Die Vertretung hat jederzeit mit Wirkung für die Zukunft das Recht seine Einwilligung zu widerrufen. Dies kann in TK-Safe oder postalisch erfolgen.

(b) Rechte der ePA-Vertretung

Sobald Sie eine ePA-Vertretung erfolgreich angelegt und über die TK-Ident-App bestätigt haben, hat die ePA-Vertretung Zugriff auf Ihre ePA und erhält folgende Rechte:

- sich in Ihre ePA anmelden und abmelden
- Berechtigungen für Leistungserbringerinstitutionen (z. B. Arztpraxen) vergeben
- Vergebene Berechtigungen anzeigen
- Berechtigung für Leistungserbringerinstitutionen (z. B. Arztpraxen) ändern
- Berechtigung für Leistungserbringerinstitutionen (z. B. Arztpraxen) löschen
- seine eigene Berechtigung löschen
- Dokumente einstellen
- Dokumente suchen
- Dokumente löschen
- Dokumente herunterladen
- Protokolldaten einsehen
- PIN der eGK ändern
- PIN der eGK mit PUK entsperren
- Benachrichtigungsadresse für Geräteautorisierung aktualisieren

Wenn Sie eine ePA-Vertretung löschen, kann sich die ePA-Vertretung nicht mehr in Ihrer ePA anmelden und alle hier aufgeführten Rechte nicht mehr wahrnehmen.

(c) Einschränkungen der Rechte einer ePA-Vertretung

Eine ePA-Vertretung kann

- keine weitere Vertretung für Ihre ePA einrichten
- keine weiteren bestehenden Vertretungen für Ihre ePA löschen
- keinen Widerspruch gegen das Einstellen von Abrechnungsdaten der Krankenkasse einlegen
- keinen Widerspruch gegen die Nutzung der ePA aussprechen

(d) Anmeldung als ePA-Vertretung

In der Funktion als ePA-Vertretung kann sich diese - sofern diese TK-versichert ist - über TK-Safe in der TK-App oder der Desktop-Anwendung als ePA-Vertretung anmelden.

Um sich als ePA-Vertretung anzumelden, braucht diese die entsprechenden Rechte gemäß Ziffer 2.6 (a) und die Anmeldedaten der Person, die vertreten werden darf.

Bei der Anmeldung als ePA-Vertretung werden die folgenden Daten verarbeitet:

- Vor- und Nachname
- Versichertennummer
- E-Mail-Adresse
- Technische Referenznummern

Nutzt die ePA-Vertretung TK-Safe über die TK-App auf einem mobilen Endgerät, wird das von Ihnen ausgewählte Profilbild (nur für Sie sichtbar, freiwilliger Service) verarbeitet.

Wenn eine ePA-Vertretung in der ePA einer zu vertretenden Person Aktivitäten durchführt (z. B. das Hochladen eines Dokumentes), werden Informationen zu dieser Person (Autor / Ersteller) gespeichert und die Aktionen im Protokoll der ePA dokumentiert. Die zu vertretende Person sowie, falls vorhanden, andere berechtigte ePA-Vertretungen, die auf die ePA zugreifen können, können diese Informationen einsehen.

(e) Besonderheiten bei krankenkassenübergreifenden ePA-Vertretungen

Für den Akteninhaber:
Die Einrichtung einer ePA-Vertretung ist unabhängig von der Krankenkasse. Eine ePA-Vertretung kann also auch eine Person vertreten, die bei einer anderen Krankenkasse versichert ist. Deshalb ist es möglich, dass sich Ihre ePA-Vertretung über eine App oder die Desktop-Anwendung einer anderen Krankenkasse in Ihre ePA anmeldet. Ihre ePA wird damit durch das Frontend einer anderen Krankenkasse dargestellt.

Für die ePA-Vertretung:
Für die Funktion der ePA-Vertretung kann daher nicht nur die Datenschutzerklärung der eigenen Krankenkasse wichtig sein, sondern auch die Datenschutzerklärung der Krankenkasse, bei der die zu vertretende Person versichert ist.

3. Ergänzende Informationen zur Nutzung der ePA über mobile Endgeräte

Zusätzlich zu den unter Ziffern 1 und 2 beschriebenen Möglichkeiten der allgemeinen Informationen und der Nutzung der ePA gelten die nachfolgenden ergänzenden Bestimmungen hinsichtlich der Nutzung der ePA über mobile Endgeräte - hier über die TK-App.

3.1 Datenverarbeitung bei der Anlage und Aktivierung eines ePA-Kontos

Neben den nach 1.4 erfassten Daten, werden darüber hinaus bei der Nutzung der ePA über ein mobiles Endgerät folgende personenbezogene Daten verarbeitet:

Bei der Registrierung des Smartphones für die ePA ist eine E-Mail-Adresse erforderlich, an die ein Freischaltcode geschickt wird. Mit der verifizierten E-Mail-Adresse des Versichertenbereiches *Meine-TK* wird sichergestellt, dass eine der TK bekannte E-Mail-Adresse des Nutzers verwendet wird. Ist bereits eine Benachrichtigungsadresse für die elektronische Patientenakte vorhanden, wird diese E-Mail-Adresse bevorzugt. Sollte die Benachrichtigungsadresse über die mobile App TK-Safe durch den Nutzer geändert werden, wird der Änderungsprozess für die *Meine-TK* E-Mail-Adresse verwendet. Anschließend wird diese Adresse automatisch an IBM übermittelt und als neue Benachrichtigungsadresse für die ePA hinterlegt.

Über den TK-Kundenservice kann die individuelle Benachrichtigungsadresse ausschließlich für die Patientenakte geändert werden. Dabei wird eine neue E-Mail-Adresse durch den Kundenservice erfasst und nach anschließender Verifizierung von der TK in die elektronische Patientenakte des Users übertragen. Die Meine-TK E-Mail-Adresse bleibt dann unverändert.

Zur Personalisierung und individuellen Ansprache werden der Vor- und Nachname des Nutzers übertragen.
Diese Daten werden - mit Ausnahme der E-Mail-Adresse - ausschließlich verschlüsselt übermittelt. IBM kann auf diese verschlüsselten Daten nicht zugreifen.

Die Rechtsgrundlage ist hinsichtlich der Datenerhebung § 67a SGB X i.V.m. § 341 SGB V, hinsichtlich der Übermittlung der Daten § 69 SGB X i.V.m. § 341 SGB V und im Übrigen § 67b SGB X i.V.m. § 341 SGB V.

Neben den oben genannten Daten werden weitere Daten lokal auf dem Gerät des Nutzers gespeichert. Dazu gehören in der App getroffene Auswahlen und Einwilligungen, insbesondere:

- erteilte Einwilligungen für die kassenindividuellen Zusatzleistungen nach Ziffer 3.3
- das von Ihnen ausgewählte Profilbild (freiwilliger Service)

Zusätzlich ist zur Verschlüsselung der Daten die Erzeugung eines ausschließlich Ihnen bekannten Sicherheitsschlüssels notwendig. Die Erstellung des persönlichen Sicherheitsschlüssels ist für die Nutzung der kassenindividuellen Zusatzleistungen nach Ziffer 3.3 innerhalb Ihrer ePA notwendig. Sie müssen diesen Schlüssel speichern, um die Registrierung fortzusetzen.

3.2 Login

Für die Anmeldung in die ePA ist es notwendig, dass Sie eine digitale Gesundheits-ID haben. Die Erstellung dieser Gesundheits-ID und zukünftige Anmeldungen erfolgen in TK-Ident.

Login mit dem Identity Provider (TK-Ident)

Es ist notwendig, dass Sie dazu die gleichnamige App herunterladen und sich dort registrieren. Im Anschluss kann die von Ihnen hinterlegte digitale Identität dazu genutzt werden, um den TK-Safe Login und andere Vorgänge (z.B. Einrichtungen von ePA-Vertretungen) in der ePA freizugeben. Der sichere, verschlüsselte Zugriff erfolgt über einen Authorisierungsserver und ist ausschließlich für den Akteninhaber und von dem Akteninhaber berechtigte ePA-Vertretungen möglich.

Die für die Nutzung des Identity Providers geltenden Datenschutzbestimmungen entnehmen Sie bitte der App "TK-Ident".

Der Login kann nur auf einem von Ihnen freigegebenen Gerät durchgeführt werden. Dafür werden während des Logins von TK-Safe die Geräte-ID sowie der Gerätename Ihres Endgerätes an das Aktensystem übermittelt.

Zum zusätzlichen Schutz vor einem Zugriff von Unbefugten auf Ihre ePA in TK-Safe wird empfohlen auf Ihrem Endgerät den Geräteschutz (Passwort, Mustersperre, o.ä.) zu aktivieren. Dabei sind triviale Kennwort-, Passwort- und Entsperrmuster (1234, 1111, etc.) sowie der Download von Inhalten und Applikationen aus nicht vertrauenswürdigen Quellen auf dem Endgerät zu vermeiden.

Ein sicheres Passwort enthält Groß- und Kleinbuchstaben sowie Ziffern und mindestens 1 Sonderzeichen. Es sollte zudem keinen Bezug zu Ihrer Person haben, wie z. B. Ihr Name, Ihre Anschrift oder Ihr Geburtsdatum.

Achten Sie bei der Erstellung einer PIN darauf, dass Sie verschiedene, nicht aufeinander folgende Ziffern wählen und es sich um Ziffern handelt, die nicht leicht erraten werden können, wie z. B. Ihr Geburtsdatum.

3.3 Kassenindividuelle Zusatzfunktionen für TK-Versicherte in TK-Safe

Neben dem durch die gematik standardisierten Bereich der ePA bietet die TK ihren Versicherten individuelle Zusatzfunktionen in TK-Safe an. Diese weiteren kassenindividuellen Zusatzleistungen stehen ausschließlich Versicherten der TK und ausschließlich über die Nutzung von TK-Safe in der TK-App zur Verfügung. Alle oben genannten an der medizinischen Behandlung Beteiligten sowie ePA-Vertreter haben keinen Zugriff auf diese Zusatzleistungen. Bei diesen nicht-standardisierten Services, die auf unterschiedlichsten sozialrechtlichen Grundlagen beruhen, handelt es sich z. B. um Hinweise oder Empfehlungen zu den Themen Vorsorge oder Impfungen. Die Funktionalitäten bzw. Leistungsbereiche dieser Angebote können durch die TK jederzeit verändert, erweitert, eingeschränkt, ganz oder teilweise eingestellt werden. Weitere Informationen dazu erhalten Sie im Folgenden:

3.3.1 Datenspeicherung, Datenverwaltung und Schutz Ihrer Daten

Zusätzlich zu den unter 1.4 beschriebenen Hinweisen ist bei der Speicherung, Verwaltung und dem Schutz Ihrer Daten bei Kassenindividuellen Zusatzfunktionen folgendes zu beachten:

Für die kassenindividuellen Services sind zusätzlich Daten erforderlich. Hierüber erhalten Sie vor der Datenübertragung eine entsprechende Information. Sie müssen der Übertragung Ihrer Daten separat zugestimmt haben. Ihre Gesundheitsdaten werden nur auf Grundlage Ihrer Einwilligung erhoben, gespeichert und verarbeitet, Rechtsgrundlage ist insoweit Art. 6 Abs. 1 lit. a i.V.m. Art. 9 DSGVO. Dies dient dem Zweck, um Ihnen im Rahmen der Durchführung des Nutzungsvertrages die Funktionalitäten bereitstellen zu können (d.h. um Ihnen die Speicherung und Verwaltung Ihrer Gesundheitsdaten und Nutzung der diesbezüglichen Services zu ermöglichen).

Ihre Gesundheitsdaten werden für keine anderen Zwecke verarbeitet und ohne Ihre Zustimmung nicht an Dritte weitergegeben.

Grundsätzlich sind Ihre personenbezogenen Daten verschlüsselt. Eine Ausnahme besteht dann, wenn Sie die kassenindividuellen Zusatzservices (Impfservice, Zahnservice, Vorsorgeservice, Empfehlungsservice) nutzen, bei denen technisch bedingt bestimmte notwendige Daten (Diagnosen, Geschlecht, Geburtsdatum, Wohnort, Impfungen bzw. Vorsorgeuntersuchungen, Informationen zu Heil- und Kostenplänen und optionale Angaben zu chronischen Krankheiten und Tätigkeiten) für IBM kurzfristig einsehbar sind, um Ihnen den jeweiligen Dienst zur Verfügung zu stellen. Anschließend werden die Daten seitens IBM stets sofort gelöscht.

Ziffer 3.3.2 beschreibt genauer, welche Daten in welchen Funktionen verarbeitet werden.

3.3.2 Verarbeitung von Gesundheitsdaten im kassenindividuellen Zusatzbereich

(a) Manuelle Eingabe, Speicherung und Verwaltung von Gesundheitsdaten

Im Rahmen Ihrer Nutzung können Sie etwa in den folgenden Leistungsbereichen Gesundheitsdaten manuell eingeben, speichern und verwalten:

Impfungen: Angaben zu Ihren Impfungen, wie etwa Bezeichnung der Impfung (z. B. Influenza, Varizellen), Tag der Impfung, Art der Impfung (etwa Immunisierung,

Auffrischung), Impfstoff, Chargennummer, Name des durchführenden Arztes, durchlebte impfrelevante Krankheiten, chronische Krankheiten, Tätigkeiten.

Vorsorge: Angaben zu Ihren Vorsorgeuntersuchungen, wie etwa Art der Vorsorgeuntersuchung (z. B. Hautkrebsscreening, Darmkrebsfrüherkennung), Tag der Vorsorgeuntersuchung, Name des durchführenden Arztes.

Medikamente: Angaben zu Ihren Medikamenten, wie etwa Pharmazentralnummer (PZN), Name des Medikaments, Wirkstoff, rezeptpflichtig, rezeptfrei, ggf. Medikationsplan sowie Bestätigungen der Medikamenteneinnahmen.

Arztbesuch: Angaben zu Ihren Arztbesuchen, wie etwa Name des Arztes, Fachrichtung, Art des Besuches, Grund der Behandlung, Datum, Uhrzeit, Notiz (Freitextfeld).
Darüber hinaus können Ihnen künftig weitere Leistungsbereiche bereitgestellt oder bestehende Leistungsbereiche angepasst werden. Sie können die aktuellen Leistungsbereiche und Funktionalitäten jederzeit in TK-Safe einsehen.

Die von Ihnen gespeicherten Daten werden ausschließlich auf Grundlage der von Ihnen erteilten Einwilligung verarbeitet. Sie sind weder gesetzlich noch vertraglich verpflichtet, etwaige Daten anzugeben, und können in sämtlichen Leistungsbereichen stets frei entscheiden, ob und welche Daten Sie eingeben möchten. Sie können Ihre manuell eingegebenen Daten jederzeit individuell bearbeiten und/oder löschen. Zudem können Sie Ihre Daten jederzeit - im Rahmen des Datenexports sämtlicher im individuellen Zusatzbereich gespeicherter Daten - über die TK-Safe-Funktionalität des "Datenexports" in Ihrem Nutzerprofil exportieren.

(b) Automatische Übertragung und Aktualisierung von Gesundheitsdaten der TK

Im Rahmen der Anwendung können Sie neben der manuellen Eingabe von Daten ferner einen Service nutzen, um Daten direkt von der TK anzufordern und automatisch aktualisieren zu lassen. Die Aktualisierung Ihrer Daten erfolgt immer dann, wenn Sie TK-Safe öffnen. Sie können bei der Aktivierung dieses Services entscheiden, ob Sie die Daten zu sämtlichen Ihnen angezeigten Leistungsbereichen automatisch importieren wollen, oder ob Sie eine Auswahl der Leistungsbereiche treffen möchten, für die Sie die Daten von Ihrer Krankenkasse automatisch anfordern wollen. Der Service kann jederzeit aktiviert oder deaktiviert werden.

Für TK-Versicherte können Daten für die folgenden Leistungsbereiche über eine automatische Aktualisierung angefordert werden:

Abrechnungsdaten: Diagnosen nach ICD-10 Kodierung

Medikamente: Angaben zu Ihren Medikamenten, wie etwa ausgebende Apotheke (Name, Adresse), Abgabedatum, Pharmazentralnummer (PZN), Name des Medikaments, Darreichungsform (z. B. Trockensaft), Menge, Wirkstoffbezeichnung, verordnender Arzt (Name, Adresse, Fachgruppe - soweit bekannt), Verordnungsdatum und Anzahl, Preis, Zuzahlung und zusätzliche Kosten.

Arzt & Impfung: Abrechnungsrelevante Angaben über Ihre Behandlungen, wie etwa Abrechnungszeitraum, Abrechnende Praxis (Bezeichnung und Adresse - soweit bekannt), Sachkosten und Honorarkosten, Diagnose, Tag der Behandlung, Gebührenposition, behandelnder Arzt (Name, Adresse, Fachgruppe - soweit bekannt), ggf. Angaben zu durchgeführten Impfungen an dem Termin (Bezeichnung der Impfung).

Zahngesundheit: Abrechnungsrelevante Angaben über Ihre Behandlungen, wie etwa Abrechnungsart, Abrechnungszeitraum, Zahnarzt (Name, Adresse - soweit bekannt), Laborkosten, Kundenanteil, Zuschuss, Honorarkosten und sonstige Kosten, ggf. Kostenplandatum und Zeitraum, Behandlungsdatum, Gebührenpositionen.

Krankenhaus: Abrechnungsrelevante Angaben über Ihre Behandlungen, wie etwa Abrechnungszeitraum, Abrechnendes Krankenhaus (Bezeichnung und Adresse - soweit bekannt), Sachkosten und Honorarkosten, Diagnose, Tag der Behandlung, Gebührenposition, behandelnder Arzt (Name, Adresse, Fachgruppe - soweit bekannt).

Arbeitsunfähigkeit (AU): Abrechnungsrelevante Angaben über Ihre Behandlungen, wie etwa Abrechnungszeitraum, Abrechnende Praxis (Bezeichnung und Adresse - soweit bekannt), Sachkosten und Honorarkosten, Diagnose, Tag der Behandlung, Gebührenposition, behandelnder Arzt (Name, Adresse, Fachgruppe - soweit bekannt), Dauer der Krankschreibung.
Sie können die Ihnen aktuell zur Auswahl stehenden Leistungsbereiche und Funktionalitäten jederzeit im Nutzerprofil einsehen.

Im Rahmen eines Datenimports können immer nur die bei der TK für den jeweiligen Leistungsbereich vorhandenen Gesundheitsdaten übertragen werden. Sie werden mit Ausnahme des Medikamenten-Bereichs für alle Leistungsbereiche rückwirkend für die letzten vier Jahre übertragen, für den Medikamente-Bereich sechs Jahre.

Sie können die von der TK importierten Daten jederzeit für einen oder sämtliche Leistungsbereiche löschen. Eine solche Löschung ist jedoch immer nur insgesamt für sämtliche der in den einzelnen Leistungsbereichen importierten Daten möglich.

Der automatische Import und die Aktualisierung Ihrer Daten erfolgt auf Grundlage Ihrer Einwilligung. Ihnen steht es frei, die Importfunktion zu nutzen und Ihre Einwilligung in die automatische Übertragung und Aktualisierung Ihrer Daten zu erteilen oder Ihre Daten manuell einzugeben. Ohne Erteilung Ihrer Einwilligung können Sie den Service nicht nutzen. Sie können den Service jederzeit aktivieren oder deaktivieren.

3.3.3 Weitere Services

Ihnen stehen spezifische weitere Services zur Verfügung. Sie können jederzeit selbst entscheiden, welche dieser Services Sie nutzen und aktivieren möchten und welche Daten Sie bereitstellen wollen. Nachfolgend beschreiben wir Ihnen, wie Ihre Daten verarbeitet werden, wenn Sie die einzelnen Services aktivieren und nutzen:

Impf- und Vorsorgehinweise, Daten zur Zahngesundheit, sowie individuelle Empfehlungen: In den Leistungsbereichen "Impfungen" und "Vorsorge" können Sie Informationen zu Ihren Impfungen bzw. Ihrer Vorsorge hinterlegen und verwalten. Zudem können Sie sich Ihre persönlichen Hinweise zu Impfungen bzw. Vorsorgeuntersuchungen erstellen lassen sowie individuelle Empfehlungen einsehen.

Zur Nutzung dieser Services werden die folgenden Daten verarbeitet: Ihre hinterlegten bisherigen Impfungen und Vorsorgeuntersuchungen (ggf. manuell eingetragen oder von der TK übertragen), Diagnosedaten sowie Ihr Geschlecht, Ihren Wohnort (Auf Basis des Wohnortes können Endemiegebiete ermittelt und entsprechende Empfehlungen ausgespielt werden) und Ihr Geburtsdatum (wenn noch nicht in der ePA hinterlegt, werden beide Daten automatisch bei Aktivierung des Services von der TK an IBM übertragen). Für die Erstellung der Impfhinweise werden die von Ihnen gespeicherten Daten mit den Empfehlungen der Ständigen Impfkommission (STIKO) abgeglichen und daraus Impfhinweise für Sie generiert. Zusätzlich zu den oben genannten Informationen können Sie optionale Angaben zu chronischen Krankheiten und Tätigkeiten vornehmen, um auf Ihre Lebenssituation angepasste Empfehlungen angezeigt zu bekommen. Für die Erstellung der Vorsorgehinweise werden die von Ihnen gespeicherten Daten mit den Ihnen gesetzlich zustehenden Vorsorgeuntersuchungen auf Grundlage der

Empfehlungen des Gemeinsamen Bundesauschusses abgeglichen und daraus Vorsorgehinweise für Sie generiert. Die Richtigkeit der Impf- bzw. Vorsorgehinweise hängt von der Vollständigkeit und Qualität der in TK-Safe hinterlegten Daten ab.

Daten zur Zahngesundheit werden mit Ihrer Zustimmung im Zahnservice angezeigt. Seit dem 1. Januar 2023 wird der Heil- und Kostenplan den Patienten nicht mehr auf Papier ausgestellt, sondern direkt digital an die Krankenkasse übermittelt. Diese an die TK übermittelten Daten des jeweiligen Heil- und Kostenplans (HKP) stellen wir für Sie im Zahnservice dar.

Die TK kann die Richtigkeit und Vollständigkeit, der von Ihnen eingegebenen oder importierten Daten nicht überprüfen. Besprechen Sie die Ihnen angezeigten Impf- und Vorsorgehinweise mit Ihrem Arzt, um mit ihm zu entscheiden, welche Impfungen bzw. welche Vorsorgeuntersuchungen für Sie sinnvoll sind. Zur Erstellung der Impf- und Vorsorgehinweise werden die gespeicherten Daten (Geschlecht, Geburtsdatum, Wohnort sowie die Informationen über Ihre Impfungen bzw. Vorsorgeuntersuchungen) und optional angegebene Informationen zu chronischen Krankheiten und Tätigkeiten) auf Ihrem Endgerät mit Ihrem privaten Schlüssel entschlüsselt und über eine Transportverschlüsselung an den Server von IBM gesendet, auf dem TK-Safe betrieben wird. Dort sind Ihre Daten technisch bedingt für IBM kurzfristig einsehbar, um Ihre persönlichen Impf- bzw. Vorsorgehinweise zu erstellen. Anschließend werden die Hinweise über eine Transportverschlüsselung an Ihr Endgerät gesendet und die zur Erstellung der Hinweise auf dem Server von IBM verarbeiteten Daten umgehend wieder gelöscht. Die von Ihnen in TK-Safe eingegebenen Daten (Geschlecht, Geburtsdatum, Wohnort, Impfungen bzw. Vorsorgeuntersuchungen) und optional angegebene Informationen zu chronischen Krankheiten und Tätigkeiten) bleiben jedoch in TK-Safe in den jeweiligen Leistungsbereichen in für die TK und IBM nicht einsehbarer Form verschlüsselt gespeichert. Für den Heil- und Kostenplans (HKP) werden folgende Daten der jeweiligen HKPs bei der IBM gespeichert: Datum, Praxis, Zahnschema, Therapieschritt, Interimsversorgung, Immeddiatversorgung, Festzuschusstabelle, bewilligte Festzuschuss Summe, Behandlungskosten Insgesamt, Eigenanteil, zahnärztliches Honorar Bema, zahnärztliches Honorar Goz, Material und Laborkosten, Antragsnummer, Bewilligungsstatus, Beendigungsdatum.
Die von Ihnen generierten Impf- und Vorsorgehinweise werden nur für die Dauer Ihrer jeweiligen Nutzung vorgehalten. Bei einer späteren erneuten Anmeldung müssen Sie die Impf- bzw. Vorsorgehinweise also neu generieren. Dies ist

notwendig, damit die Ihnen angezeigten Hinweise immer Ihre jeweils aktuell hinterlegten Daten berücksichtigen.

Arztverzeichnis: Im Rahmen der Nutzung von TK-Safe können Sie sich ein Arztverzeichnis anlegen. Sie können sich die Ärzte, die aus den bereits von Ihnen eingewilligten übertragenden Abrechnungsdaten ermittelt wurden, zusammengefasst in einem Arztverzeichnis anzeigen lassen. Die jeweiligen Ärzte erhalten hierüber keine Information.
Zu jedem Arzt sind Kontaktdaten und, wenn vorhanden, weitere Informationen wie z. B. Öffnungszeiten ersichtlich. Diese weiteren Informationen fragt die TK je Abruf bei der Stiftung Gesundheit an. Es werden zu keinem Zeitpunkt Informationen über Sie oder Ihre Abrechnungsdaten an die Stiftung Gesundheit übermittelt. Die Stiftung Gesundheit dient hier ausschließlich als Informationsgeber.

Übertragung des Entlassbriefs von Ihrem teilnehmenden Krankenhaus: Im Rahmen Ihrer Nutzung von TK-Safe können Sie zudem Ihren Entlassbrief (als PDF-Dokument) von dem Sie behandelnden Krankenhaus importieren, sofern dieses an TK-Safe angebunden ist. Für diesen Zweck werden Sie im Rahmen der Aktivierung dieses Services um Ihre Einwilligung gebeten, dass Ihre Versichertennummer an Ihr Krankenhaus zur Anforderung des Entlassbriefs übermittelt wird. Der Entlassbrief wird verschlüsselt übertragen und Ihnen in TK-Safe angezeigt. Sie können den gespeicherten Entlassbrief jederzeit wieder löschen. Sollten die Informationen in dem Entlassbrief unrichtig oder unvollständig sein, wenden Sie sich bitte an Ihr Krankenhaus, um die Daten berichtigen oder vervollständigen zu lassen. Sie müssen dann den Entlassbrief löschen und einen neuen Import des berichtigten oder vervollständigten Entlassbriefs von Ihrem Krankenhaus anfordern.
Die Datenverarbeitung im Rahmen der vorstehenden Services erfolgt ausschließlich auf Grundlage Ihrer Einwilligung, die Sie im Rahmen der Aktivierung des jeweiligen Services erteilen. Die Rechtsgrundlage der jeweiligen Datenverarbeitung ist somit Art. 6 Abs. 1 S. 1 lit. a i.V.m. Art. 9 DSGVO.

Eine entsprechende Widerrufsmöglichkeit Ihrer Einwilligung steht Ihnen in Ihrem Nutzerprofil zur Verfügung.

3.4 Erfassung und Analyse von aggregierten Nutzungsdaten

Es werden ferner anonymisierte Informationen über Art und Umfang der Nutzung der ePA erfasst und analysiert (z. B. wann und in welchen Leistungsbereichen Datenobjekte gespeichert, bearbeitet oder gelöscht werden, wie lange und zu welchen Zeiten die ePA genutzt wird, welche Leistungsbereiche häufiger oder weniger häufig genutzt werden).

Die Informationen über das Nutzungsverhalten werden stets nur in anonymisierter und aggregierter Form verarbeitet, ohne dass ein Rückschluss auf Ihre Person oder die Person anderer Nutzer möglich wäre.

Die hiermit verbundene Verarbeitung erfolgt, um das allgemeine Nutzungsverhalten der Nutzer der ePA besser zu verstehen sowie die ePA und ihre einzelnen Funktionalitäten zu verbessern. Die Rechtsgrundlage ist in diesem Fall die Einwilligung nach Art. 6 Abs 1 lit. a) DSGVO.

4. Ergänzende Informationen zur Nutzung der ePA über die Desktop-Anwendung von TK-Safe (Die Desktop-Anwendung steht voraussichtlich ab März 2025 zur Verfügung)

Zusätzlich zu den unter Ziffer 2 beschriebenen Möglichkeiten der Nutzung der ePA gelten die nachfolgenden ergänzenden Bestimmungen hinsichtlich der Nutzung der ePA über die stationäre Desktop-Anwendung TK-Safe.

4.1 Anmeldung in einem ePA-Konto über die Desktop-Anwendung

Um sich über die Desktop-Anwendung TK-Safe anzumelden, müssen Sie sich über die jeweiligen Stores Ihres Betriebssystems die aktuelle Version der Desktop-Anwendung lokal herunterladen.

Für die Anmeldung gibt es zwei Optionen:

Kartenlesegerät
Kartenlesegerät, das den aktuellen Sicherheitsstandards entspricht, Ihre elektronische Gesundheitskarte sowie die dazugehörige PIN, die Sie über https://tk.de anfordern können.

Anmeldung mit Identity Provider
Alternativ ist eine Anmeldung mit dem Identity Provider TK-Ident möglich. Das Login-Verfahren ist in 3.2 beschrieben.

(a) Anlegen eines Nutzerkontos und Kenntnisnahme der Datenschutzerklärung sowie der Nutzungsbedingungen von TK-Safe

Um die Desktop-Anwendung zu nutzen, müssen Sie nach Installation der Desktop-Anwendung einen lokalen Benutzer anlegen. Sie generieren einen Sicherheitsschlüssel gemäß der Vorgabe in der Desktop-Anwendung, um Ihre Daten sicher zu verschlüsseln. Jedes Gerät, über das Sie auf die Desktop-Anwendung zugreifen, hat seinen eigenen Sicherheitsschlüssel zur Ver- und Entschlüsselung Ihrer ePA.

Sie werden anschließend gebeten einen Benutzernamen sowie ein Kennwort festzulegen. Es handelt sich dabei um die Zugangsdaten Ihres Nutzerkontos. Bei Verlust dieser Zugangsdaten ist eine Wiederherstellung nicht möglich. Um erneut über die Desktop-Anwendung Zugriff auf die Daten der ePA zu erhalten, müssen Sie einen neuen lokalen Benutzer anlegen.

Bei erstmaliger Anmeldung mit Ihrem zuvor angelegten Nutzerkonto ist es zur Verwendung der Desktop-Anwendung erforderlich, dass Sie uns bestätigen, dass Sie die Datenschutzerklärung und die Nutzungsbedingungen von TK-Safe zur Kenntnis genommen haben. Die Kenntnisnahme wird verschlüsselt lokal auf Ihrem verwendeten Gerät in Ihrem Benutzerprofil gespeichert.

Zum zusätzlichen Schutz vor einem Zugriff von Unbefugten auf Ihre ePA in TK-Safe wird empfohlen auf Ihrem Endgerät den Geräteschutz (Passwort, Mustersperre, o.ä.) zu aktivieren. Dabei sind triviale Kennwort-, Passwort- und Entsperrmuster (1234, 1111, etc.) sowie der Download von Inhalten und Applikationen aus nicht vertrauenswürdigen Quellen auf dem Endgerät zu vermeiden.

Ein sicheres Passwort enthält Groß- und Kleinbuchstaben sowie Ziffern und mindestens 1 Sonderzeichen. Es sollte zudem keinen Bezug zu Ihrer Person haben, wie z. B. Ihr Name, Ihre Anschrift oder Ihr Geburtsdatum.

Achten Sie bei der Erstellung einer PIN darauf, dass Sie verschiedene, nicht aufeinander folgende Ziffern wählen und es sich um Ziffern handelt, die nicht leicht erraten werden können. Vermeiden Sie daher z.B. Ihr Geburtsdatum.

(b) E-Mail-Verifikation für Nutzer der Desktop-Anwendung

Eine ePA lässt sich über die Desktop-Anwendung nur auf einem freigeschalteten Endgerät öffnen. Um das Endgerät freizuschalten, brauchen Sie eine verifizierte E-Mail-Adresse.

Sofern für Sie in Ihrer ePA noch keine E-Mail-Adresse hinterlegt ist, ist solch eine bei erstmaliger Anmeldung zu hinterlegen und zu verifizieren. Dazu werden Sie auf eine Webseite weitergeleitet, wo Sie Ihre gewünschte - zu verifizierende - E-Mail-Adresse eintragen müssen. An diese erhalten Sie unmittelbar eine E-Mail mit einem Aktivierungscode. Durch den Klick auf diesen Link wird Ihre E-Mail-Adresse verifiziert und gespeichert.

(c) Anmeldeverfahren für ePA-Vertretung

ePA-Vertretungen steht ein separater Anmeldebereich bei der Anmeldung zur Verfügung. So ist sichergestellt, dass die Vertretung auf Ihre ePA zugreifen kann ohne, dass die Vertretung selbst über eine eigene ePA verfügt.

4.2 Eingeschränkte Möglichkeiten in der Anwendung

Sie haben im Rahmen des Zugriffs auf Ihre ePA über die Desktop-Anwendung mit wenigen Ausnahmen die gleichen Möglichkeiten wie über die Nutzung von TK-Safe über die Endgeräte der Leistungserbringer bzw. die TK-App.

Folgende Anwendungsbereiche sind über die Desktop-Anwendung nicht möglich:

- die Registrierung für die ePA
  (Nutzen Sie dafür die TK-App oder das schriftliche Formular.)
- die Nutzung der kassenindividuellen Zusatzleistungen
- den Widerspruch gegen die Nutzung der ePA
  (Nutzen Sie dafür das in 1.5 beschriebene Verfahren)
- Der Widerspruch gegen das Einstellen von Abrechnungsdaten als PDF in die ePA.

5. Datenschutzrechtliche Betroffenenrechte

Gemäß den gesetzlichen Bestimmungen zum Datenschutz haben Sie jederzeit das Recht:

Auskunft über Ihre verarbeiteten Daten sowie eine Kopie dieser Daten zu verlangen (Recht auf Auskunft - Art. 15 DSGVO);

die Berichtigung unrichtiger Daten und, unter Berücksichtigung der Zwecke der Verarbeitung, die Vervollständigung unvollständiger Daten zu verlangen (Recht auf Berichtigung - Art. 16 DSGVO);

bei Vorliegen berechtigter Gründe die Löschung Ihrer Daten zu verlangen (Recht auf Löschung - Art. 17 DSGVO);

die Einschränkung der Verarbeitung Ihrer Daten zu verlangen, sofern die gesetzlichen Voraussetzungen gegeben sind) (Recht auf Einschränkung der Verarbeitung - Art. 18 DSGVO);

bei Vorliegen der gesetzlichen Voraussetzungen die von Ihnen bereitgestellten Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten an einen anderen Verantwortlichen, zum Beispiel bei einem Anbieterwechsel, zu übermitteln oder, soweit dies technisch machbar ist, durch IBM übermitteln zu lassen (Recht auf Datenübertragbarkeit - Art. 20 DSGVO)

nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu sein, sofern die gesetzlichen Voraussetzungen hierfür nicht vorliegen; eine automatisierte Entscheidungsfindung wird von der TK gegenwärtig nicht durchgeführt.

Sie haben ferner das Recht, der Verarbeitung Ihrer Daten, die zur Wahrung der berechtigten Interessen von IBM erfolgt, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, nach Maßgabe der gesetzlichen Bestimmungen zu widersprechen (Widerspruchsrecht - Art. 21 DSGVO).

Soweit Sie Zweifel an der Rechtmäßigkeit der Erhebung und Verarbeitung der Sozialdaten haben, besteht das Recht der Beschwerde beim

Bundesbeauftragten für Datenschutz und die Informationsfreiheit (BfDI), Graurheindorfer Str. 15, 53117 Bonn, poststelle@bfdi.bund.de oder poststelle@bfdi.de-mail.de.

Zur Ausübung Ihrer datenschutzrechtlichen Betroffenenrechte wenden Sie sich bitte direkt an die TK.

wichtiger Hinweis:
Da IBM keinen Zugriff auf etwaige Identifikationsmerkmale von Ihnen hat, ist IBM bei Kontaktaufnahme eine Überprüfung Ihrer Berechtigung und eine Zuordnung zu den von Ihnen gespeicherten Daten nicht möglich.

6. Datenschutzbeauftragte

Die verantwortliche Datenschutzbeauftragte der TK ist unter Bramfelder Straße 140, 22305 Hamburg oder per E-Mail unter datenschutz@tk.de erreichbar.

7. Künftige Anpassungen der ePA-Datenschutzerklärung

Die TK behält sich vor, an dieser Datenschutzerklärung Anpassungen vorzunehmen.

Als Nutzer von TK-Safe werden Sie über einen entsprechenden Hinweis in der TK-App und in der Desktop-Anwendung im Vorfeld informiert, sofern Anpassungen oder Ergänzungen an dieser Datenschutzerklärung vorgenommen werden.

Des Weiteren finden Sie die aktuelle Datenschutzerklärung auf www.tk.de unter Datenschutz und Informationsfreiheit.