

Datenschutzfolgenabschätzung TK-Safe - Zugang und Übertragung der TK-Daten

Bezeichnung [VVZ] GBVI.TK-Safe						
Verantwortliche Stelle(n) <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;">Fachverantwortliche Stelle</td> <td style="width: 50%; border: none;">Versorgungsmanagement Projekte</td> </tr> <tr> <td style="border: none;">Serviceverantwortliche Stelle</td> <td style="border: none;">IT - Onlineprojekte</td> </tr> </table>			Fachverantwortliche Stelle	Versorgungsmanagement Projekte	Serviceverantwortliche Stelle	IT - Onlineprojekte
Fachverantwortliche Stelle	Versorgungsmanagement Projekte					
Serviceverantwortliche Stelle	IT - Onlineprojekte					
Zweckbestimmung [VVZ] 1. Sicherer Zugang von TK-Versicherten in die elektronische Gesundheitsakte TK-Safe, die von der IBM Deutschland GmbH betrieben und gehostet wird. 2. Sicherstellung, dass es eine eindeutige Zuordnung zwischen Versicherten und Akte über einen willkürlich gewählten Schlüssel gibt, da der Versicherte die Möglichkeit hat, sich Abrechnungsdaten der TK in die Akte übertragen zu lassen. 3. Sicherstellung, dass der Versicherte gegenüber dem Aktenbetreiber anonym bleibt, damit seine Identität diesem zu keinem Zeitpunkt bekannt wird. 4. Sicherstellung, dass ausschließlich TK-Versicherte die Leistung in Anspruch nehmen, da die Lizenzgebühren von der Techniker Krankenkasse übernommen werden.						
Kontext & Rechtmäßigkeit <table style="width: 100%; border: none;"> <tr> <td style="width: 60%;">Kontext - Kranken- und Pflegekasse</td> <td style="width: 40%; text-align: center;">[X]</td> </tr> <tr> <td>Kontext - Allgemeiner Datenschutz</td> <td style="text-align: center;">[]</td> </tr> </table>			Kontext - Kranken- und Pflegekasse	[X]	Kontext - Allgemeiner Datenschutz	[]
Kontext - Kranken- und Pflegekasse	[X]					
Kontext - Allgemeiner Datenschutz	[]					
Rechtmäßigkeit (Lizensierung) [VVZ] Gesetzesgrundlage für die Leistung ist § 68 SGB V.						
Kategorien der Betroffenen [VVZ]						
	<i>(Kategorie)</i>	<i>(Anmerkungen, Erläuterungen)</i>				
1.	Versicherte	Nutzung der TK-App ist Voraussetzung				
Kategorien der datenschutzrelevanten Daten [VVZ]						
	<i>(Kategorie)</i>	<i>(Anmerkungen, Erläuterungen)</i>				
1.	Profildaten	Geburtsdatum, Geschlecht, Referenznummer				
2.	Abrechnungsdaten	Medikamente, Ärzte, Krankenhäuser				
3.	Arbeitsunfähigkeitsdaten	Datenquelle: Techniker Krankenkasse				

Darstellung des Verfahrens

(Hier erfolgt die Darstellung des Prozesses der Verarbeitung, inkl. beteiligte Stellen, technische Komponenten zur Verarbeitung/Anwendungen)

Zugang: Da ausschließlich ein Zugang zu TK-Safe über die TK-App möglich ist, ist sichergestellt, dass nur TK-Versicherte das Angebot nutzen. Der Versicherte gibt im Rahmen des Registrierungsprozesses der TK die Einwilligung, eine technische Referenznummer unverschlüsselt an den Anbieter der Akte zu übergeben. Daraufhin wird eine Akte beim Anbieter angelegt und die Erstellung des Sicherheitsschlüssels auf dem Smartphone des Nutzers initiiert.

Übertragung der TK-Daten: Der Nutzer kann für jeden Leistungsbereich (Ambulant ärztliche Abrechnungen, Arbeitsunfähigkeit, Krankenhausabrechnungen und Abrechnungen für Arzneimittel) seine Daten von der TK anfordern. Dafür ist immer eine Einwilligung notwendig, die direkt gegenüber der TK als Datenlieferant ausgesprochen werden muss.

Schutzbedarfsfeststellung

Durchgeführt am: 03.05.2016

Durchgeführt von: [REDACTED]

[Link/Verweis](#) (intern) auf Schutzbedarfsfeststellung

Schutzbedarf Schutzziele

Vertraulichkeit	Integrität & Authentizität	Verfügbarkeit	Datenschutz
3	3	3	3

Maßnahmen für die Schutzziele Nichtverkettung, Transparenz und Intervenierbarkeit

In Art. 5 der DSGVO werden wesentliche Grundsätze für die Verarbeitung personenbezogener Daten formuliert. Zu diesem Zweck strukturiert die Verfahrensbeschreibung die rechtlichen Anforderungen in Form der Gewährleistungsziele **Transparenz, Nichtverkettung und Intervenierbarkeit**. Mit Hilfe dieser Gewährleistungsziele überführt die Verfahrensbeschreibung der TK die rechtlichen Anforderungen der DSGVO in dem von der Verordnung geforderten Katalog sowohl die technischen als auch organisatorischen Maßnahmen.

Nichtverkettung

Die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden, ist insbesondere den einzelnen Verarbeitungsbefugnissen zu entnehmen, die die Geschäftszwecke, die Forschungszwecke etc. zum Maßstab machen und findet über den Zweckbindungsgrundsatz aus Art. 5 Abs. 1 c) DSGVO Eingang in die Grundverordnung.

Bei der Datenverarbeitung auf der Grundlage der Einwilligung ergibt sich aus Art. 7 Abs. 4 DSGVO, dass eine Einwilligung unwirksam sein kann, wenn die Daten zu Zweckerfüllung nicht erforderlich sind.

Nähere Beschreibung

Sind die Verarbeitungs-, Nutzungs- und Übermittlungsrechte eingeschränkt?	☒ Ja ☐ Nein	Die Abläufe sind automatisiert und werden nur für den fest definierten Zweck durch den Nutzer angestoßen.
Gibt es eine technische Überwachung der Nichtverkettung?	☒ Ja ☐ Nein	Ja, siehe oben.
Sind die Daten nach Organisations-/Abteilungsgrenzen getrennt?	☒ Ja ☐ Nein	Ja, das betrifft das grundsätzliche Datenschutzkonzept der Techniker

		Krankenkasse und ist unabhängig von TK-Safe.
Sind die Daten durch Rollenkonzepte mit abgestuften Zugriffsrechten getrennt?	☒ Ja ☐ Nein	Ja, siehe den vorgenannten Punkt.
Sind Regelungen zu Zweckänderungsverfahren vorhanden und dokumentiert?	☒ Ja ☐ Nein	Ja, jede Änderung muss von der umsetzenden Organisationseinheit hinsichtlich rechtlicher und datenschutzrechtlicher Auswirkungen mit den Organisationseinheiten Recht sowie Datenschutz abgestimmt werden.

Transparenz

Der Grundsatz der Transparenz ist in Art. 5 Abs. 1 lit. a DSGVO festgeschrieben. Er findet sich als tragender Grundsatz des Datenschutzrechts in zahlreichen Regelungen der DSGVO.

Die verantwortliche Stelle trifft geeignete Maßnahmen für den Betroffenen, sodass dieser alle relevanten Informationen zur Ausübung seiner Betroffenenrechte in präziser, transparenter, verständlicher Form und in einer einfachen Sprache zur Verfügung stellt.

Nähere Beschreibung

Werden die Informationen in einer Sprache zur Verfügung gestellt, sodass ein Großteil der Mitglieder der TK diese verstehen?	☒ Ja ☐ Nein	Ja, auf Deutsch
Können die Informationen gem. der Betroffenenrechte sowohl in schriftlicher als auch in elektronischer Form dem Betroffenen zur Verfügung gestellt werden?	☒ Ja ☐ Nein	Ja, die Abrechnungsdaten der TK werden auf Anforderung auch in schriftlicher Form an den Versicherten gesandt
Wurden Maßnahmen (Prozesse) initiiert, die die gesetzliche Bearbeitungsfrist von vier Wochen berücksichtigen?	☒ Ja ☐ Nein	Die Prozesse laufen automatisiert und in Echtzeit ab
Werden die Kontaktdaten des Fachbereichs, des Datenschutzbeauftragten (DSB) und der Aufsichtsbehörden benannt?	☒ Ja ☐ Nein	Ja, wird im Impressum der TK-App explizit ausgewiesen

Intervenierbarkeit

Die Interventionsrechte der Betroffenen ergeben sich explizit aus den Vorschriften zu Berichtigung, Löschung, Widerspruch und zur Einschränkung der Verarbeitung (Art. 16, 17, 18 DSGVO) sowie der Datenportabilität (Art. 20 DSGVO).

Wiederum muss der Verantwortliche gem. Art. 5 Abs. 1 lit. d DSGVO die Voraussetzung für die Gewährung dieser Rechte, sowohl auf organisatorischer als auch, soweit erforderlich, auf technischer Ebene schaffen.

Nähere Beschreibung

Stehen dem Betroffenen in dem geplanten Prozess die Rechte zu?	☒ Ja ☐ Nein	Der Nutzer initiiert selbst die Prozesse für seine Rechte. Er kann alle manuellen Eingaben löschen, er kann alle Leistungsbereiche der
--	---	--

		Abrechnungsdaten löschen, er kann seine Akte jederzeit kündigen und seine Daten in einem maschinenlesbaren und programmiersprachenunabhängigen Format speichern.
Kann der Betroffene jederzeit seine Rechte in Anspruch nehmen?	☒ Ja ☐ Nein	Ja, siehe oben.
Ist ein Prozess bei Wahrnehmung der Rechte etabliert worden?	☒ Ja ☐ Nein	Ja, siehe oben.
Wirkt der Betroffene auf den Prozess ein?	☒ Ja ☐ Nein	Ja, siehe oben.
Ist eine Korrektur im Hinblick auf die Verarbeitung seiner Daten für den Betroffenen mit einfachen Mitteln zu erreichen?	☐ Ja ☒ Nein	Nein, Urheber und damit verantwortlich für die Abrechnungsdaten ist der jeweilige Leistungserbringer. Die Techniker Krankenkasse wird diese Daten nicht ändern.
Kann die Verarbeitung eingeschränkt werden?	☒ Ja ☐ Nein	Die Übertragung der Abrechnungsdaten erfolgt ausschließlich nach expliziter Anforderung durch den Nutzer. Es ist ein freiwilliger Service, der nicht in Anspruch genommen werden muss.
Ist ein Single Point of Contact (SPoC) für den Betroffenen eingerichtet?	☒ Ja ☐ Nein	Ja, sämtliche Anfragen gehen direkt an die TK-Servicecenter.

Sicherheit in der Verarbeitung [VVZ]

Kurzdarstellung (Verweis) auf Standardmaßnahmen:

Der Betreiber von TK-Safe (IBM Deutschland GmbH) bekommt bei der Registrierung eines neuen Nutzers ausschließlich eine technische Referenznummer von der Techniker Krankenkasse übertragen. Der TK-Versicherte muss der Übertragung zustimmen. Die Referenznummer ist für den Betreiber willkürlich gewählt und lässt keine Rückschlüsse auf den Nutzer zu. Die Referenznummer dient der eindeutigen Zuordnung einer Akte zu einem TK-Versicherten, damit unter anderem die richtigen Abrechnungsdaten in die Akte übertragen werden können, wenn der Nutzer diese anfordert.

Die Akte selbst ist contentverschlüsselt (Ende-zu-Ende), so dass weder die TK noch der Betreiber selbst Zugriff auf die Dateninhalte haben. Nur die technische Referenznummer kennen beide Seiten im Klartextformat. Den Sicherheitsschlüssel für die Ver- / Entschlüsselung der Daten auf dem Smartphone besitzt nur der Nutzer.

Nur TK-Versicherte können TK-Safe nutzen. Dazu sind zwei Voraussetzungen notwendig: 1. Er muss die TK-App nutzen. Einen Freischaltcode für die Registrierung erhält der TK-Versicherte ausschließlich auf dem Postweg. 2. Registrierung für TK-Safe inklusive der Einwilligung, dass die TK dem Betreiber eine technische Referenznummer übermitteln darf.

Der Zugang zu TK-Safe erfolgt immer über die TK-App. Dazu ist eine 2-Faktor Authentifizierung notwendig: Besitz (= registriertes Smartphone) und Wissen (= Passwort) oder Biometrie (= Fingerabdruck, wenn gewünscht).

Die Übertragung der Daten erfolgt verschlüsselt (Transportverschlüsselung), gleiches gilt für die Speicherung (Speicherverschlüsselung), neben der bereits erwähnten Contentverschlüsselung. Dabei kommen Verfahren der asymmetrischen Public-Private-Key-Verschlüsselung und symmetrische Algorithmen zum Einsatz, die den BSI-Richtlinien für langfristige Datenablagen entsprechen (RSA 4096 Bit, AES-256).

Zusätzlich erfolgt ein automatischer Logout nach 10 Minuten Inaktivität.

Kurzdarstellung verfahrensspezifische Maßnahmen (public)

Jede Aktion innerhalb der Akte muss vom Nutzer initiiert werden. In der Akte wird nichts ohne die Eingabe, Aktivität oder Einwilligung des Versicherten ausgeführt.

Übermittlungen und Auftragsverarbeitungen [VVZ]**Übermittlungen an Dritte [VVZ]**

	(Kategorie)	(Anmerkungen, Erläuterungen)
1.	Partnernummer	willkürliche technische Referenznummer

Auftragsverarbeitungen [VVZ]

	(Kategorie)	(Anmerkungen, Erläuterungen)
1.	Findet nicht statt	

Aufbewahrungs- und Löschfristen [VVZ]

Grundsätzlich sind die Daten in TK-Safe frei von jeglichen Aufbewahrungs- und Löschfristen, weil sie dem Nutzer gehören.

In TK-Safe werden den TK-Versicherten die Abrechnungsdaten übertragen, die die Techniker Krankenkasse von den abrechnenden Akteuren des Gesundheitswesens erhält. Zum aktuellen Zeitpunkt sind das ambulante ärztliche Abrechnungen, Krankenhausabrechnungen und Arzneimittelabrechnungen. Zusätzlich werden Arbeitsunfähigkeitsdaten direkt von der TK zur Verfügung gestellt.

Diese Daten unterliegen gesetzlicher Aufbewahrungsfristen, für die es mehrere Rechtsgrundlagen gibt. Dazu gehört § 84 SGB X als Rahmenvorgabe für eine zweckgebundene Speicherung, § 292 SGB V für die Speicherung der Abrechnungsdaten, § 295 SGB V speziell für die ambulant ärztlichen Daten, § 304 SGB V für Aufbewahrungsfristen, sofern keine anderen gesetzlichen Regelungen greifen.

Automatisierte und terminierte Löschläufe bei der TK sorgen dafür, dass die gesetzlichen Fristen zur Löschung eingehalten werden.

Interner Verweis auf zugehöriges Löschkonzept

Liegt je verantwortlicher Fachabteilung vor (Arzneimittel, Ambulante Versorgung, Arbeitsunfähigkeit, Krankenhaus).

Stellungnahme des Datenschutzbeauftragten der TK

Prüfung durchgeführt am: 15.03.2019

Prüfung durchgeführt durch:

Stellungnahme Team DS

Aus Datenschutzsicht keine Anmerkungen.