Checkliste für Praxen zur Umsetzung der IT-Sicherheitsrichtlinie der KBV

§75b SGB V IT-Sicherheitsrichtlinie der KBV, Anlage 3

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und nutzen. Wenn nicht mehr benötigt, Apps restlos löschen.	01.04.2021	• für IOS: "App Store" • für Android: "Google Play" verwenden und in den Sicherheits-einstellungen keine Apps aus externen Quellen zulassen	☐	☐	
	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstell-en zu vermeiden.	01.04.2021	• Autoupdates aktivieren	☐	☐	
	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.	01.04.2021	• um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden, muss der Datenversand entsprechend eingeschränkt werden	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				• vor der App-Benutzung sollte überprüft werden, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten			
	Minimierung und Kontrolle von App-Berechti-gungen	Minimierung der App-Berechti-gungen.	01.04.2021	• bevor eine App eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält • nicht unbedingt notwendige Berechtigungen müssen hinterfragt und gegebenenfalls unterbunden werden • Sicherheitsrelevante Berechtigungseinstell-ungen müssen so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können • wo dies technisch nicht möglich ist, müssen die Berechtigungseinstell-ungen regelmäßig	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				geprüft und erneut gesetzt werden			
	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.	01.01.2022	• Verschlüsselung von Android (PIN oder Passwort einrichten)/ IOS ("Code-Sperre") aktivieren	☐	☐	
Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung des in Office-Produkten integrierten Cloud-Speichers zur Speicherung personen-bezogener Informationen.	01.04.2021	• kein Microsoft 365 (ehemals Office 365), OneDrive verwenden	☐	☐	
	Beseitigung von Rest-Information-en vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.	01.04.2021	• entfernen der Metadaten wie "Autor(en)", zuletzt "geändert von" der Dokumente unter → Datei -> Eigenschaften	☐	☐	
Internet-Anwendungen	Authentisier-ung bei Webanwen-dungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite	01.04.2021	• auf sichere 2 Faktor Authentisierung achten oder hinreichend komplexe Passwörter oder Passwortmanager	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.		mit generierten Passwörtern verwenden • auf verschlüsselte Verbindungen achten			
	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.	01.04.2021	• Löschen der Browserdaten: Chrome, Firefox, Edge mittels "Strg" + "Umschalt" + "Entf":, Safari: "cmd" + "alt" + "E" oder Browser wie "Firefox Klar" verwenden, die diese Daten mit einem Klick oder nach Beendigung der Anwendung automatisch löschen	☐	☐	
	Krypto-grafische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.	01.04.2021	• auf https achten, Plug-In/ Erweiterung wie HTTPS Everywhere verwenden • Beispielsweise statt http://www.kbv.de besser https://www.kbv.de verwenden • dies wird durch ein "Schloss" als Icon im Webbrowser visualisiert • durch Anklicken des Schlosses lassen sich	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				die Informationen zu dem Zertifikat und dem Herausgeber des Zertifikats einsehen			
	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen	01.01.2022	• es muss durch die Entwickler einer Internet-Anwendung mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur Aktionen durchführen können, zu denen sie berechtigt sind • jeder Zugriff auf geschützte Inhalte und Funktionen muss kontrolliert werden, bevor er ausgeführt wird • sollte es nicht möglich sein, Zugriffsrechte zuzuweisen, muss dafür ein zusätzliches Sicherheitsprodukt eingesetzt werden	☐	☐	
	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.	01.01.2022	• eine Web Application Firewall ist eine Spezialform einer Application Firewall für das HTTP-Protokoll, um die damit	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				verbundeneren Angriffe zu minimieren • bei der Bereitstellung einer web-Anwendung sollten entweder open source Lösungen (wie ModSecurity, Waf2Py oder OctopusWAF) oder eine spezielle kommerzielle Appliance verwendet werden • zu dem Einsatz einer Web Application Firewall gehört auch die richtige Konfiguration der Firewall, ggf. die Härtung der zugrunde liegenden Hardware und des Betriebssystems und die regelmäßige Wartung und Updates			
	Schutz vor unerlaubter automati-sierter/Nutz-ung von Weban-wendungen	Keine automati-sierten Zugriffe bzw. Aufrufe auf Web-anwendungen einrichten oder zulassen.	01.01.2022	• mittels des sogenannten "Captcha-Mechanismus" lassen sich automatisierte Zugriffe begrenzen • durch zeitlich verzögerte Anmeldeversuche bei Falscheingaben lassen sich missbräuchliche Anmeldeversuche erschweren	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
Dezentrale Komponenten der TI	Planung und Durchführung der Installation	Die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten müssen berücksichtigt werden.	01.01.2022	• das Installationsprotokoll und die vom Dienstleister erstellten Dokumentationen werden ausgehändigt und müssen sicher aufbewahrt werden	☐	☐	
	Betrieb	Die Anwender- und Administrationsdokumentationen der gematik GmbH und der Hersteller der TI-Komponenten, insbesondere die Hinweise zum sicheren Betrieb der Komponenten, müssen berücksichtigt werden.	01.01.2022	• Informationen dazu auf der Webseite der gematik und von den Herstellern der TI-Komponenten	☐	☐	
	Schutz vor unberechtig-	Die TI-Komponenten	01.01.2022	• Informationen dazu auf der Webseite der	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
	tem physischem Zugriff	in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.		gematik und von den Herstellern der TI-Komponenten			
	Betriebsart „parallel“	Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungser-bringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.	01.01.2022	• bei einer parallelen Installation des Konnektors, muss das Netz durch eine Firewall ausreichend geschützt sein	☐	☐	
	Geschützte Kommuni-	Es müssen Authentisie-	01.01.2021	• TLS-Verbindung vom PVS-System zum	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
	kation mit dem Konnektor	rungsmerk-male für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.		Konnektor und die Authentisierungsmöglichkeit am Konnektor muss aktiviert sein • für die Authentisierung mittels X.509 Clientauthentisierung, muss ein Zertifikat im Konnektor generiert, und das PVS System inklusive PIN und Zugriff auf den privaten Schlüssel konfiguriert, oder ein Konnektor-fremdes X.509 Zertifikat muss im PVS-System inklusive PIN und Zugriff auf den privaten Schlüssel und im Konnektor konfiguriert werden			
	Installieren verfügbarer Aktualisie-rungen	Die TI-Komponeten in der Praxis müssen regelmäßig auf verfügbare Aktualisierun-gen geprüft und zeitnah installiert werden.	01.01.2022	• auf Updates der TI-Komponenten prüfen und zeitnah installieren	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		Automatische Updates aktivieren.					
	Sicheres Aufbewahren von Administrationsdaten	Eingerichtete Administrationsdaten, insbesondere auch Passwörter für den Administrator-Zugang, müssen sicher aufbewahrt werden. Jedoch muss gewährleistet sein, dass der Leistungserbringer auch ohne seinen Dienstleister die Daten kennt.	01.01.2022	• notwendige Informationen vom Dienstleister aushändigen lassen und sicher aufbewahren • wenn der Dienstleister die Informationen nicht zur Verfügung stellen möchte, auf eine vertraglich angemessene kurze Reaktionszeit und eine Herausgabe der Informationen am Ende des Vertrages achten • oder Administrationsdaten in einem versiegelten Umschlag erhalten, um im Notfall auf die TI-Komponenten zugreifen zu können. Wenn der Umschlag geöffnet wurde, ist dies dem Dienstleister anzuzeigen	☐	☐	
Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von	Bevor eine Praxis Smartphones oder Tablets bereitstellt,	01.01.2022	• Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
	Smartphones und Tablets	betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.		Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.			
	Definition der erlaubten Information-en und Applikationen auf mobilen Geräten	Die Praxis sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.	01.01.2022	• die Institution sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen • Grundlage für die Regelung sollte einerseits die Klassifikation der Institutionsdaten sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden • die Benutzer der mobilen Endgeräte sollten nur freigegebene und geprüfte Apps aus als sicher klassifizierten	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				Quellen installieren dürfen			
	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwort-lichen geprüft und freigegeben werden.	01.07.2022	• Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden • dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind • alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden	☐	☐	
Mobile Device Management (MDM)	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden.	01.01.2022	• die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden • dies bieten kommerzielle MDM-Lösungen in der Regel out-of-the-box an • die Verbindung der mobilen Endgeräte ins Netz der Institution sollte angemessen abgesichert werden	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				• wenn Daten zwischen den mobilen Endgeräten und dem IT-Netz der Institution übertragen werden, sollte durch geeignete Maßnahmen (z. B. VPN) verhindert werden, dass Unbefugte sie verändern oder einsehen können			
	Berechtigungsmanagement im MDM	Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.	01.01.2022	• für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden • den Benutzergruppen und Administratoren sollte das MDM nur so viele Berechtigungen einräumen wie für die Aufgabenerfüllung notwendig sind (Minimalprinzip) • es sollte regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind und den Aufgaben entsprechen	☐	☐	
	Verwaltung von Zertifikaten	Zertifikate zur Nutzung von Diensten auf	01.01.2022	• Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.		sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden • die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch den Benutzer sollte durch das MDM verhindert werden. • das MDM sollte Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen			
	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.	01.01.2022	• das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können (Remote Wipe bei bestehender Datenverbindung) • werden in dem mobilen Endgerät externe Speicher genutzt, sollte geprüft werden, ob diese bei einem Remote Wipe ebenfalls gelöscht	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				werden können. Diese Funktion sollte vom MDM unterstützt werden • der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) sollte sicherstellen, dass keine schutzbedürftigen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies sollte insbesondere dann gelten, wenn das Unenrollment aus der Ferne ausgeführt wird			
	Festlegung erlaubter Information-en auf mobilen Endgeräten	Die Praxis sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.	01.01.2022	• festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen • Grundlage für die Regelung sollten einerseits die Klassifikation bzw. der Schutzbedarf der Informationen sein und andererseits die Bedingungen, unter	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				denen die Daten auf den Geräten verarbeitet werden, etwa in abgeschotteten Containern • die Verantwortlichen sollten das MDM auf Basis dieser Regeln konfigurieren, sodass es diese auf allen mobilen Endgeräten durchsetzen kann • Den Benutzern sollten die Regeln in geeigneter Weise bekannt gegeben werden			
	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlich-en geprüft und freigegeben werden.	10.07.2022	• Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind • alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				und dort für die Benutzer verfügbar sein • Apps sollten gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden • das MDM sollte die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht			
Wechseldaten-träger / Speicher-medien	Integritäts-schutz durch Check-summen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätz-liche Veränderung-en sollte eingesetzt werden.	01.01.2022	• um beim Datenaustausch mittels mobiler Datenträger die Integrität von vertraulichen Informationen sicherzustellen, sollte ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden • die Verfahren zum Schutz vor Veränderungen sollten	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				dem aktuellen Stand der Technik entsprechen			
	Datenträger-verschlüsse-lung	Wechseldatent räger sollten vollständig verschlüsselt werden.	01.04.2021	• Wechseldatenträger sollten vollständig verschlüsselt werden. Es sollte ein sicheres Verschlüsselungsverfah ren eingesetzt werden. Empfehlungen zu geeigneten Algorithmen und Schlüssellängen bieten die Technischen Richtlinien des BSI BSI-TR-02102. Mittels Open-Source Lösungen wie VeraCrypt können entsprechende verschlüsselte Container angelegt werden	☐	☐	
Netzwerk-sicherheit	Absicherung von schützens-werten Information-en	Schützenswer-te Informa-tionen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über	01.01.2022	• schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		vertrauens-würdige dedizierte Netzsegmente kommuniziert wird.		Managementnetzes) kommuniziert wird • können solche Protokolle nicht genutzt werden, muss nach Stand der Technik angemessen verschlüsselt und authentisiert werden			

Ort, Datum

Unterschrift