Checkliste für Praxen zur Umsetzung der IT-Sicherheitsrichtlinie der KBV

§75b SGB V IT-Sicherheitsrichtlinie der KBV, Anlage 1

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			
	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	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
Internet-Anwendungen	Authentisierung bei Webanwendungen	Nutzen Sie nur Internet-Anwendungen, die ihre Zugänge (Login-Seite und -Ablauf, Passwort, Benutzerkonto etc.) strikt absichern.	01.04.2021	• auf sichere 2 Faktor Authentisierung achten oder hinreichend komplexe Passwörter oder Passwortmanager 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	☐	☐	
	Kryptografische 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	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				https://www.kbv.de verwenden • dies wird durch ein "Schloss" als Icon im Webbrowser visualisiert • durch Anklicken des Schlosses lassen sich die Informationen zu dem Zertifikat und dem Herausgeber des Zertifikats einsehen			
	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 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	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				der Firewall, ggf. die Härtung der zugrunde liegenden Hardware und des Betriebssystems und die regelmäßige Wartung und Updates			
	Schutz vor unerlaubter automatisierter/Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen 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	☐	☐	
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	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
	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 unberechtigtem physischem Zugriff	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.	01.01.2022	• Informationen dazu auf der Webseite der gematik und von den Herstellern der TI-Komponenten	☐	☐	
	Betriebsart „parallel“	Wird der Konnektor in der	01.01.2022	• bei einer parallelen Installation des Konnektors, muss das	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		Konfiguration „parallel“ ins Netzwerk des Leistungser-bringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.		Netz durch eine Firewall ausreichend geschützt sein			
	Geschützte Kommuni-kation mit dem Konnektor	Es müssen Authentisie-rungsmerk-male für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend	01.01.2021	• TLS-Verbindung vom PVS-System zum Konnektor und die Authentisierungsmöglich keit 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,	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		konfiguriert werden.		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. Automatische Updates aktivieren.	01.01.2022	• auf Updates der TI-Komponenten prüfen und zeitnah installieren	☐	☐	
	Sicheres Aufbewahren von Administra-tionsdaten	Eingerichtete Administra-tionsdaten, insbesondere auch Pass-wörter für den Administrator-Zugang, müssen sicher aufbewahrt	01.01.2022	• notwendige Informationen vom Dienstleister aus-händigen lassen und sicher aufbewahren • wenn der Dienstleister die Informationen nicht zur Verfügung stellen möchte, auf eine ver-traglich angemessene	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		werden. Jedoch muss gewährleistet sein, dass der Leistungser-bringer auch ohne seinen Dienstleister die Daten kennt.		kurze Reaktionszeit und eine Herausgabe der Informationen am Ende des Vertrages achten • oder Administrations-daten 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			

Ort, Datum

Unterschrift