Checkliste für Praxen zur Umsetzung der IT-Sicherheitsrichtlinie der KBV

§75b SGB V IT-Sicherheitsrichtlinie der KBV, Anlage 2

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	☐	☐	
Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüssel-	01.01.2022	• vgl. Anlage 1 - Anforderung Nr. 10 • Auf https achten, Plug-In/ Erweiterung wie	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		ung von Webseiten TLS verwendet wird.		HTTPS Everywhere verwenden			
	Restriktive Rechtever-gabe	Restriktive Rechtever-gabe.	01.01.2022	• der verfügbare Funktionsumfang des IT-Systems sollte für einzelne Benutzer oder Benutzergruppen so eingeschränkt werden, dass sie nur genau die Rechte besitzen und nur auf die Funktionen zugreifen können, die sie für ihre Aufgabenwahrnehmung benötigen („Need-to-know-Prinzip“). • Zugriffsberechtigungen sollten hierfür möglichst restriktiv vergeben werden • es sollte regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				• auf Systemdateien sollten möglichst nur die Systemadministratoren zugreifen können • der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden • auch System-Verzeichnisse sollten nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen			
Endgeräte mit dem Betriebssystem Windows	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.	01.07.2022	• in reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden • eine Gruppenrichtlinie sollte die Verwendung älterer Protokolle verhindern • der Schutz des Local Credential Store (LSA) sollte aktiviert werden	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				(PPL, Protected Mode Light) • die Speicherung der LAN-Manager-Hashwerte bei Kennwortänderungen sollte per Gruppenrichtlinie deaktiviert werden • die Überwachungsein-stellungen sollten gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informations-verbunds abgestimmt werden • es sollte eine Protokollierung auf Clientseite sichergestellt werden			
Smartphone und Tablet	Verwendung von Sprach-assistenten	Sprach-assistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.	01.01.2022	• Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind. Andernfalls sollten sie deaktiviert werden • Generell sollte ein Sprachassistent nicht genutzt werden können,	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				wenn das Gerät gesperrt ist			
	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden.	01.07.2022	• es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden • diese sollte festlegen, wie mobile Geräte genutzt und gepflegt werden sollen • darin sollten die Themen Aufbewahrung und Verlustmeldung behandelt werden • außerdem sollte verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten	☐	☐	
Mobiltelefon	Sichere Datenüber-tragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.	01.01.2022	• es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen • die dafür erlaubten Schnittstellen sollten festgelegt werden • außerdem sollte beschlossen werden,	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				wie die Daten bei Bedarf zu verschlüsseln sind			
	Sicherheits-richtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheits-richtlinie erstellt werden.	01.07.2022	• werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden • jedem Benutzer eines Mobiltelefons muss ein Exemplar der Sicherheitsrichtlinie ausgehändigt werden • es muss regelmäßig überprüft werden, ob die Sicherheitsrichtlinie eingehalten wird • die Sicherheitsleitlinie zur dienstlichen Nutzung von Mobiltelefonen sollte Bestandteil der Schulung zu Sicherheitsmaßnahmen sein	☐	☐	
Wechseldaten-träger / Speicher-medien	Regelung zur Mitnahme von Wechsel-datenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen	01.01.2022	• es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
		Anlässen Wechseldaten-träger mitgenommen werden dürfen.		mitgenommen werden dürfen • darin sollte festgelegt sein, welche Datenträger von wem außer Haus transportiert werden dürfen und welche Sicherheits-maßnahmen dabei zu beachten sind			
Netzwerk-sicherheit	Umfassende Protokoll-ierung, Alarmierung und Logging von Ereignissen	Wichtige Ereignisse auf Netzkomponen ten und auf den Netzmanage-ment-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort proto-kolliert werden.	01.01.2022	• es sollten mindestens folgende Komponenten und Ereignisse auf einem zentralen Protokoll-Server protokolliert werden: ○ Active Directory: ○ unautorisierte Zugriffe bzw. Zugriffsversuche , ○ Firewall: Ereignisse wie erlaubte und unterbundene Zugriffe ○ Virenscanner: ○ Start, Stop, Fehler bei Scannen ○ Erkannte Malware	☐	☐	

Anforderungen der KBV					Umsetzungsstand in der Praxis		
Zielobjekt	**Anforderung**	**Erläuterung**	**Umsetzung ab**	**Hinweise**	**Nicht zutreffend**	**Erledigt**	**Bemerkung**
				○ PVS:Anmeld-ungen, Verfüg-barkeit, etc. • wenn der Durchsatz und die Erreichbarkeit der Netzwerkkomponenten und Dienste überwacht werden soll, kann dies mit open source Tools wie Icinga erfolgen			

Ort, Datum

Unterschrift