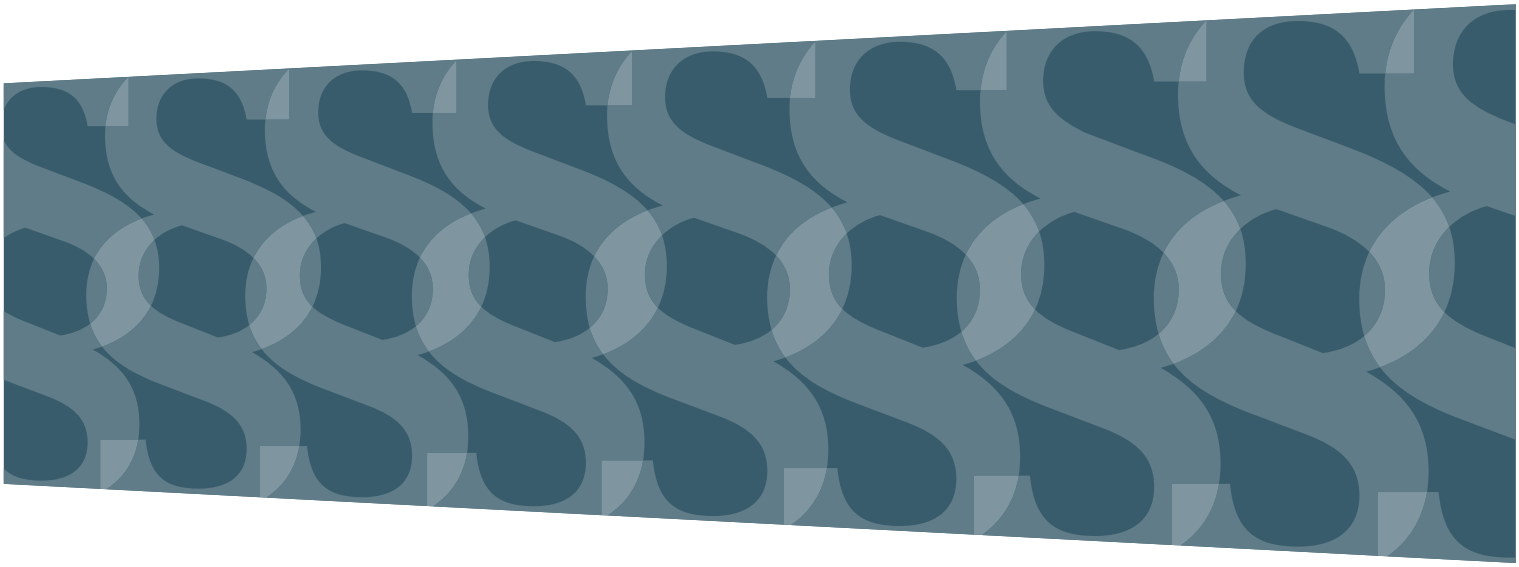
KBV
KASSENÄRZTLICHE
BUNDESVEREINIGUNG



RICHTLINIE NACH § 75B SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

16. Dezember 2020

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

II. GELTUNGSBEREICH

1. Diese Richtlinie legt die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest.
2. Der/die Praxisinhaber ist/sind verantwortlich für die Einhaltung der Anforderungen dieser Richtlinie.

III. PRAXISGRÖSSEN UND ANFORDERUNGSKATEGORIEN

Die umzusetzenden Anforderungen richten sich nach der Größe der Praxis. Dabei gilt Folgendes:

1. Praxis: Eine Praxis ist eine vertragsärztliche Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen.

2. Mittlere Praxis: Eine mittlere Praxis ist eine vertragsärztliche Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen.

3. Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang: Eine Großpraxis oder Praxis mit Datenverarbeitung im erheblichem Umfang ist eine Praxis mit über 20 ständig mit der Datenverarbeitung betrauten Personen oder eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore).

IV. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT IN PRAXEN

1. Praxen nach A. III. 1. haben die Anforderungen aus Anlage 1 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

2. Praxen nach A. III. 2. haben die Anforderungen aus Anlage 1, 2 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

3. Praxen nach A. III. 3. haben die Anforderungen aus Anlage 1, 2, 3 und 5 umzusetzen, soweit die Zielobjekte in der Praxis genutzt werden.

4. Sofern in der Praxis medizinische Großgeräte, wie Computertomograph, Magnetresonanztomograph, Positronenemissionstomograph und Linearbeschleuniger, eingesetzt werden, sind ergänzend die Anforderungen aus Anlage 4 umzusetzen.

Die in dieser Richtlinie formulierten Anforderungen unterliegen einem kontinuierlichen Verbesserungsprozess mit einer jährlichen Evaluationspflicht. Die erforderliche Evaluation richtet sich an der jeweiligen Informationssicherheitslage aus.

B. INKRAFTTRETEN UND GELTUNG

Diese Richtlinie tritt am Tag nach der Veröffentlichung in Kraft. Die Anforderungen gelten ab den in den Anlagen angegebenen Zeitpunkten.

ANLAGE 1

Anforderungen für Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen			
1.	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
2.	Mobile Anwendungen (Apps)	Aktuelle App-Versionen	Updates immer zeitnah installieren, um Schwachstellen zu vermeiden.	01.04.2021
3.	Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Nur Apps nutzen, die Dokumente verschlüsselt und lokal abspeichern.	01.01.2022
4.	Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Keine vertraulichen Daten über Apps versenden.	01.04.2021
5.	Office-Produkte	Verzicht auf Cloud-Speicherung	Keine Nutzung der in Office-Produkte integrierte Cloud-Speicher zur Speicherung personenbezogener Informationen	01.04.2021
6.	Office-Produkte	Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten	Vertrauliches aus Dokumenten löschen vor einer Weitergabe an Dritte.	01.04.2021
7.	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
8.	Internet-Anwendungen	Schutz vertraulicher Daten	Stellen Sie ihren Internet-Browser gem. Hersteller-Anleitung so ein, dass keine vertraulichen Daten im Browser gespeichert werden.	01.04.2021
9.	Internet-Anwendungen	Firewall benutzen	Verwendung und regelmäßiges Update einer Web App Firewall.	01.01.2022
10.	Internet-Anwendungen	Kryptografische Sicherung vertraulicher Daten	Nur verschlüsselte Internet-Anwendungen nutzen.	01.04.2021
11.	Internet-Anwendungen	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen einrichten oder zulassen.	01.01.2022

	Hardware: Endgeräte und IT-Systeme			
12.	Endgeräte	Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras	Mikrofon und Kamera am Rechner sollten grundsätzlich deaktiviert sein und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert werden.	01.04.2021
13.	Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder Abmelden.	01.04.2021
14.	Endgeräte	Regelmäßige Datensicherung	Sichern Sie regelmäßig Ihre Daten.	01.01.2022
15.	Endgeräte	Einsatz von Viren-Schutzprogrammen	Setzen Sie aktuelle Virenschutzprogramme ein.	01.04.2021
16.	Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.	01.01.2022
17.	Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Regeln Sie Berechtigungen und Zugriffe pro Personengruppe und pro Person.	01.01.2022
18.	Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	Verwenden Sie so wenige persönliche Daten wie möglich.	01.01.2022
19.	Smartphone und Tablet	Schutz vor Phishing und Schadprogrammen im Browser	Nutzen Sie aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser.	01.04.2021
20.	Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten durch PIN schützen. Super-PIN/PUK nur durch Verantwortliche anzuwenden.	01.04.2021
21.	Smartphone und Tablet	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräte das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.	01.01.2022
22.	Smartphone und Tablet	Verwendung eines Zugriffschutzes	Schützen Sie Ihre Geräte mit einem komplexen Gerätesperrcode.	01.04.2021
23.	Smartphone und Tablet	Updates von Betriebssystem und Apps	Updates des Betriebssystems und der eingesetzten Apps bei	01.04.2021

			Hinweis auf neue Versionen immer zeitnah installieren, um Schwachstellen zu vermeiden. Legen Sie zusätzlich einen festen Turnus (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.	
24.	Smartphone und Tablet	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen Ihrer Geräte sollten Sie in den Einstellungen restriktiv auf das Notwendigste einschränken.	01.01.2022
25.	Mobiltelefon	Sperrmaßnahmen bei Verlust eines Mobiltelefons	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Hinterlegen Sie die dafür notwendigen Mobilfunkanbieter-Informationen, um sie bei Bedarf im Zugriff zu haben.	01.01.2022
26.	Mobiltelefon	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.	01.01.2022
27.	Mobiltelefon	Updates von Mobiltelefonen	Es sollte regelmäßig geprüft werden, ob es Softwareupdates für die Mobiltelefone gibt.	01.04.2021
28.	Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.	01.01.2022
29.	Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Eindeutige Kennzeichnung für Empfänger, aber keine Rückschlüsse für andere ermöglichen.	01.04.2021
30.	Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Versand-Anbieter mit sicherem Nachweis-System, Manipulationssichere Versandart und Verpackung.	01.04.2021

31.	Wechseldatenträger / Speichermedien	Sicheres Löschen der Datenträger vor und nach der Verwendung	Datenträger nach Verwendung immer sicher und vollständig Löschen. Ihr Rechner bietet dafür verschiedene Möglichkeiten.	01.01.2022
32.	Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere das Internet muss durch eine Firewall geschützt werden.	01.04.2021
33.	Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.	01.04.2021
34.	Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.	01.01.2022
35.				

ANLAGE 2

Zusätzliche Anforderungen für mittlere Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen			
1.	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.	01.04.2021
2.	Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.	01.01.2022
	Hardware: Endgeräte und IT-Systeme			
3.	Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.	01.01.2022
4.	Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.	01.01.2022
5.	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
6.	Smartphone und Tablet	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
7.	Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.	01.01.2022
8.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	01.07.2022
9.	Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.	01.01.2022
10.	Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.	01.01.2022
11.	Netzwerksicherheit	Umfassende Protokollierung, Alarmierung und Logging von Ereignissen	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-	01.01.2022

			Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.	

ANLAGE 3

Zusätzliche Anforderungen für Großpraxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Hardware: Endgeräte und IT-Systeme			
1.	Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.	01.01.2022
2.	Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	01.07.2022
3.	Smartphone und Tablet	Definition der erlaubten Informationen und Applikationen auf mobilen Geräten	Die Praxis sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.	01.01.2022
4.	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
5.	Mobile Device Management (MDM)	Berechtigungsmanagement im MDM	Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.	01.01.2022
6.	Mobile Device Management (MDM)	Verwaltung von Zertifikaten	Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.	01.01.2022
7.	Mobile Device Management (MDM)	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
8.	Mobile Device Management (MDM)	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	10.07.2022
9.	Mobile Device Management (MDM)	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.	01.01.2022

10.	Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.	01.04.2021
11.	Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.	01.01.2022
12.	Netzwerksicherheit	Absicherung von schützenswerten Informationen	Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.	01.01.2022

ANLAGE 4

Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
1.	Medizinische Großgeräte	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten sollten gewechselt werden.	01.07.2021
2.	Medizinische Großgeräte	Nutzung sicherer Protokolle für die Konfiguration und Wartung	Für die Konfiguration und Wartung von medizinischen Großgeräte müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.	01.07.2021
3.	Medizinische Großgeräte	Protokollierung	Es muss festgelegt werden: • welche Daten und Ereignisse protokolliert werden sollen, • wie lange die Protokolldaten aufbewahrt werden und • wer diese einsehen darf. Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.	01.01.2022
4.	Medizinische Großgeräte	Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen	Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte	01.01.2022

			müssen soweit möglich deaktiviert oder deinstalliert werden.	
5.	Medizinische Großgeräte	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.	01.07.2021
6.	Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden.	01.01.2022

ANLAGE 5

DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
1.	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
2.	Dezentrale Komponenten der TI	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
3.	Dezentrale Komponenten der TI	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
4.	Konnektor	Betriebsart „parallel“	Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungserbringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.	01.01.2022
5.	Primärsysteme	Geschützte Kommunikation mit dem Konnektor	Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.	01.01.2021

6.	Dezentrale Komponenten der TI	Zeitnahes Installieren verfügbarer Aktualisierungen	Die TI-Komponeten in der Praxis müssen regelmäßig auf verfügbare Aktualisierungen geprüft werden und verfügbare Aktualisierungen müssen zeitnah installiert werden. Bei Verfügbarkeit einer Funktion für automatische Updates sollte diese aktiviert werden.	01.01.2022
7.	Dezentrale Komponenten der TI	Sicheres Aufbewahren von Administrationsdaten	Die im Zuge der Installation der TI-Komponenten eingerichteten 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

ANLAGE 6

Quellensammlung, informatorische Quellen des BSI zu den Anforderungen:

1. BSI-Empfehlung für sichere Web-Browser v2.0

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_071.html

2. Sichere Konfiguration von Microsoft Office 2013/2016/2019 v1.1

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_135.html

3. Sichere Konfiguration von Microsoft Outlook 2013/2016/2019 v.1.1

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_139.html

4. Android - Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit v2.0

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_109.html

Ihre Ansprechpartner:

Stabsbereich Recht
Jakob Strüve, Tel.: 030 4005-1724, jstrueve@kbv.de

Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
politik@kbv.de, www.kbv.de

Die Kassenärztliche Bundesvereinigung (KBV) vertritt die politischen Interessen der rund 170.000 an der vertragsärztlichen Versorgung teilnehmenden Ärzte und Psychotherapeuten auf Bundesebene. Sie ist der Dachverband der 17 Kassenärztlichen Vereinigungen (KVen), die die ambulante medizinische Versorgung für 70 Millionen gesetzlich Versicherte in Deutschland sicherstellen. Die KBV schließt mit den gesetzlichen Krankenkassen und anderen Sozialversicherungsträgern Vereinbarungen, beispielsweises zur Honorierung der niedergelassenen Ärzte und Psychotherapeuten sowie zum Leistungsspektrum der gesetzlichen Krankenkassen. Die KVen und die KBV sind als Einrichtung der ärztlichen Selbstverwaltung Körperschaften des öffentlichen Rechts.