



KASSENÄRZTLICHE
BUNDESVEREINIGUNG

IT-SICHERHEIT IN DER PRAXIS FORTBILDUNG



➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



➤ **EINLEITUNG**

➤ **GESETZLICHE RAHMENBEDINGUNGEN**

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ **§ 390 SGB V**

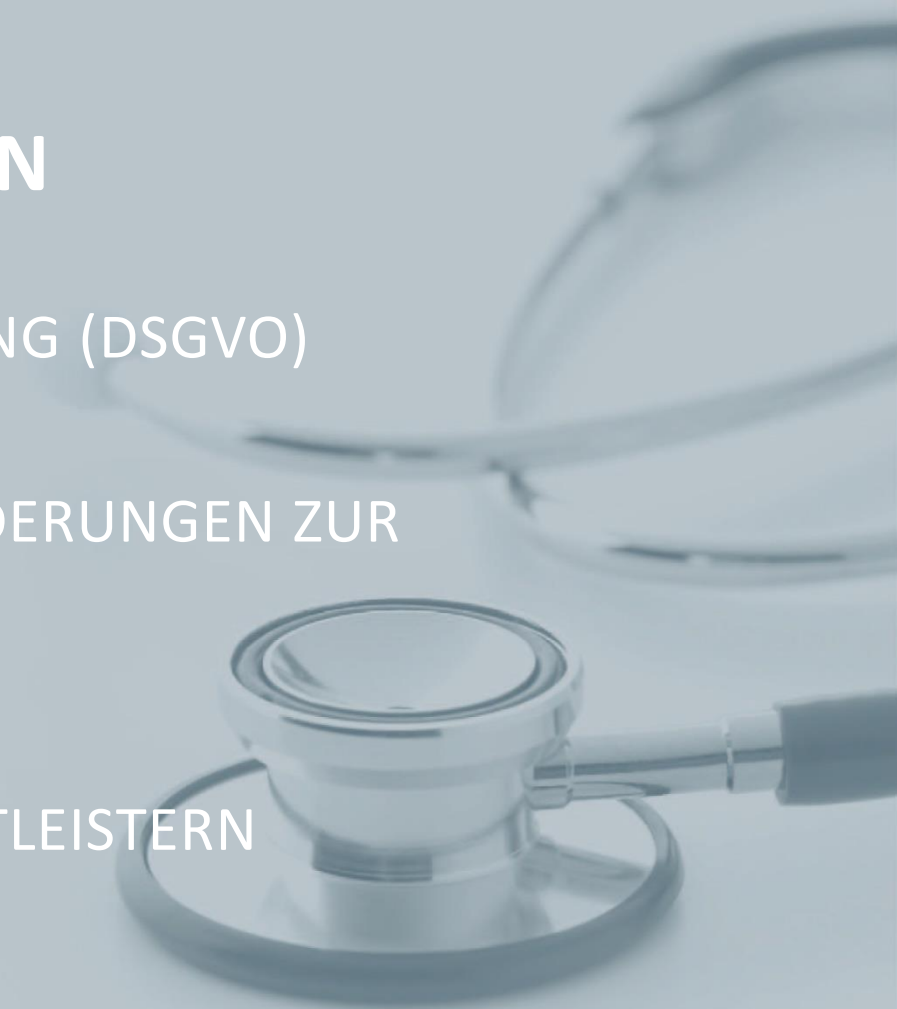
➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ **ABSCHLUSS**



Motivation für IT-Sicherheit in der Praxis

- › Patienten vertrauen Praxen besonders schutzbedürftige Informationen an
- › Bereits vor der IT-Sicherheitsrichtlinie existierten empfindliche Strafen bei Datenschutzverstößen oder Verletzung der Schweigepflicht (z. B. § 9 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte, § 203 Strafgesetzbuch)
- › Zur Konkretisierung der abstrakten Anforderungen der DSGVO hat der Gesetzgeber einheitliche und verbindliche Vorgaben für Praxen in einer zu erstellenden Richtlinie gefordert:
 - Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit



Ziele der Fortbildung

- › Herstellung eines Grundverständnisses der im Zusammenhang stehenden gesetzlichen Regelungen bzgl. Datenschutz und Informationssicherheit
- › Wissensvermittlung zu Aufbau und Inhalt der nach § 390 SGB V festgelegten Anforderungen zur Gewährleistung der IT-Sicherheit an Praxen, mittlere Praxen und große Praxen
- › Unterstützung in der Bewertung der Maßnahmen und Anforderungserfüllung der eigenen Praxis
- › Unterstützung der praktischen Umsetzung der Anforderungen durch Hinweise, Tipps und Beispiele

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Ärztliche Schweigepflicht (§ 9 MBO-Ä)

- › Geregelt in § 9 Abs. 1 (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) beziehungsweise den entsprechenden Bestimmungen der Berufsordnungen der Landesärztekammern
- › Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, auch nach dem Tod des Patienten, zu schweigen
- › Nebenpflicht aus dem zwischen Arzt und Patient geschlossenen Behandlungsvertrag
- › Seit Inkrafttreten des Patientenrechtegesetzes in den §§ 630a ff. Bürgerliches Gesetzbuch (BGB) geregelt (26. Februar 2013)

Ärztliche Schweigepflicht (§ 203 StGB)

- › § 203 des Strafgesetzbuches (StGB) „Verletzung von Privatgeheimnissen“ regelt strafrechtliche Sanktionen
- › behandelt u. a. Verstöße eines Arztes gegen die Verschwiegenheitspflicht (Schutz des Patientengeheimnisses)
- › Freiheitsstrafe bis zu einem Jahr oder Geldstrafe (§ 203 Abs. 1 StGB) sind möglich

→ Ein Verstoß gegen die ärztliche Schweigepflicht kann neben berufsrechtlichen oder berufsgerichtlichen Maßnahmen auch Schadensersatzansprüche und sogar strafrechtliche Konsequenzen zur Folge haben.

Achtung

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Europäische Datenschutzgrundverordnung (DSGVO)

- › Seit 25. Mai 2018 angewendet

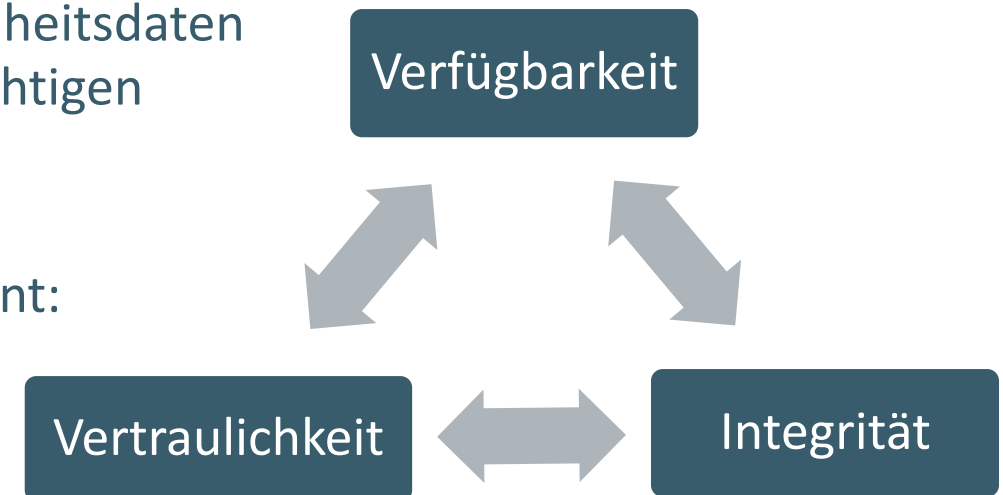
- › Ziele:
 - › Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten
 - › Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten
 - › weitgehende Vereinheitlichung europäischen Datenschutzrechts

- › betrifft alle gesellschaftlichen Bereiche mit Umgang von personenbezogenen Daten – so auch Praxen, die in der Regel Gesundheitsdaten als „besondere Kategorie personenbezogener Daten“ gem. Art. 9 Abs. 1 DSGVO verarbeiten und dies auch im Rahmen der ärztlichen Behandlung dürfen

Europäische Datenschutzgrundverordnung (DSGVO)

Technische und organisatorische Maßnahmen

- › Müssen vom Arzt im Interesse des Datenschutzes in seiner Praxis umgesetzt werden
- › Müssen zur Sicherstellung einer hinreichenden Datensicherheit geeignet sein
- › Sollten sowohl die bezweckte Verarbeitung von Gesundheitsdaten als auch mögliche Risiken für Patientenrechte berücksichtigen
- › Ebenfalls zu berücksichtigende Schutzziele der Informationssicherheit werden in Art. 32 DSGVO benannt:
 - › Vertraulichkeit
 - › Integrität
 - › Verfügbarkeit



Europäische Datenschutzgrundverordnung (DSGVO)

Sanktionen bei Verstößen

- › bis zu 20.000.000 € bzw. bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs u.a. bei:
 - › Verstoß bei einer Verarbeitung von Gesundheitsdaten ohne Rechtsgrundlage
 - › Verstoß im Hinblick auf die Einwilligung
 - › Missachtung von Betroffenenrechten
 - › ...

- › Materielle und immaterielle (Schäden aus schweren Persönlichkeitsrechtsverletzungen) Schadensersatzansprüche von Patienten sind außerdem möglich

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ **§ 390 SGB V**

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

- › Betrifft Leistungserbringer der vertragsärztlichen Versorgung
- › Setzt einen klaren Handlungsrahmen zur Umsetzung von IT-Sicherheit in Praxen
- › Wurde unter anderem im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt

Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

› Es gibt zwei Richtlinien für unterschiedliche Aspekte:

- 1. Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit**
Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich anzupassen. Die Richtlinie ist für die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich.
- 2. Zertifizierung vertrauenswürdiger Dienstleister**
IT-Dienstleister können sich auf Basis der o. g. Richtlinie bei der KBV zertifizieren lassen und ihre Kompetenz gegenüber Dritten mittels des ausgestellten Zertifikates vorweisen.

1. Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

- › Beschreibt das Mindestmaß der zu ergreifenden Maßnahmen für IT-Sicherheit
- › Gilt für vertragsärztliche bzw. vertragspsychotherapeutische Praxen
- › Praxisinhaber sind für die Einhaltung der Anforderungen verantwortlich

RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

A. ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 390 Sozialgesetzbuch (SGB) Fünftes Buch (V) den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung und –psychotherapeutischen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorischen Maßnahmen im Sinne des Artikel 32 Datenschutz-Grundverordnung (DSGVO) zu standardisieren. Die hier getroffene Richtlinie erfüllt diesen Auftrag und dient damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche und –psychotherapeutische Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen und –psychotherapeutischen Praxis. Die Richtlinie legt technische und organisatorische 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 IT-Sicherheit der Praxis und für die Einhaltung der Anforderungen dieser Richtlinie. Dies umfasst insbesondere auch, die erforderlichen Festlegungen und Regelungen gemäß dieser Richtlinie vorzugeben. Der/die Praxisinhaber kann/können die Umsetzung der einzelnen Anforderungen delegieren.

III. PRAXISGRÖSSEN UND ANFORDERUNGSKATEGORIEN

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

Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit – Anlagen

- › Anforderungen sind gestaffelt nach stattfindender Datenverarbeitung bzw. Praxistyp:
 - › Anlage 1 „Anforderungen für Praxen“
 - › Anlage 2 „Zusätzliche Anforderungen für mittlere Praxen“
 - › Anlage 3 „Zusätzliche Anforderungen für Großpraxen“
- › Bei Einsatz medizinischer Großgeräte müssen (unabhängig vom Praxistyp) die Anforderungen der Anlage 4 „Zusätzliche Anforderungen bei der Nutzung medizinischer Großgeräte“ erfüllt werden
- › Anforderungen der Anlage 5 „Dezentrale Komponenten der Telematikinfrastuktur“ müssen immer (unabhängig vom Praxistyp) erfüllt werden

→ Viele der Anforderungen können in den Vertragsbedingungen mit Dritten (z. B. IT-Dienstleistern, die den Betrieb von Software oder Infrastruktur übernehmen) genutzt werden.

Tipp

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ **§ 390 SGB V**

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Die Praxis als Patient

› Idee

Die Praxis wird mit einem Patienten verglichen, dem mit Hilfe von IT-Sicherheitsmaßnahmen geholfen werden kann.



› Beispielsituation

Die Praxis wird beim Arzt vorstellig: Ihr geht es nicht gut. Sie ist in absehbarer Lebensgefahr und ihr muss dringend geholfen werden. Nach einem ersten Gespräch stellt sich heraus, dass die akute Symptomatik auf einer chronischen Krankheit beruht. Der Praxis kann durch geeignete, dauerhafte Therapie ein Leben in Normalität ermöglicht werden.



Die Praxis als Patient – Umsetzung § 390 SGB V

1. **Anamnese:** Praxistyp festlegen
2. **Diagnose:** Anzuwendende Anlagen festlegen
3. **Behandlungsplan:** Anzuwendende Anforderungspunkte festlegen
4. **Therapie:** Maßnahmen festlegen und umsetzen
5. **Mitbehandlung:** Dienstleister beauftragen/anweisen
6. **Verlaufskontrolle:** Anforderungsumsetzung prüfen
7. **Folgetermin:** auf Änderungen reagieren



→ Die hier aufgelisteten Schritte werden auf den folgenden Seiten den Umsetzungsschritten der Richtlinie nach § 390 SGB V und mit dem Symbol  rechts oben gekennzeichnet.

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ VORBEREITUNG

➤ HILFESTELLUNGEN ZUR DURCHFÜHRUNG




➤ NACHBEREITUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS






Praxistyp auswählen

Praxistyp	Definition
 Praxis	Praxis mit bis zu fünf ständig mit der Datenverarbeitung betrauten Personen
 Mittlere Praxis	Praxis mit 6 bis 20 ständig mit der Datenverarbeitung betraute Personen
 Großpraxis	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 krankenhaushähnlichen Strukturen, Groß-Labore).

Anlagen auswählen

- › Anlagen 1, 2 und 3 korrelieren mit der Praxisgröße und bauen aufeinander auf
- › Anlage 4 ist verpflichtend bei Einsatz von medizinischen Großgeräten (Computertomograph, Magnetresonanztomograph, Positronenemissionstomograph, Linearbeschleuniger, o. ä.)
- › Anlage 5 ist für alle Praxen verpflichtend (und somit genauso anzuwenden wie Anlage 1)

Praxistyp	Ständig mit Datenverarbeitung betraute Personen	Anlage				
		1	2	3	4	5
 Praxis	Weniger als 5	x			ggf.	x
 Mittlere Praxis	Zwischen 6 und 20	x	x		ggf.	x
 Großpraxis	über 20 – oder – Datenverarbeitung in erheblichem Umfang	x	x	x	ggf.	x

Anforderungsauswahl

- › Anforderungen beziehen sich immer auf ein Zielobjekt
- › Anforderungen von Zielobjekten, die in der Praxis nicht genutzt werden, **müssen nicht** umgesetzt werden
- › Insgesamt werden 15 Zielobjekte in den fünf Anlagen referenziert:

Personal	Sensibilisierung und Schulung zur Informationssicherheit	Netzwerksicherheit
Patch- und Änderungsmanagement	Endgeräte	Endgeräte mit dem Betriebssystem Windows
Smartphone und Tablet	Mobile Device Management (MDM)	Mobiltelefon
Wechseldatenträger / Speichermedien	E-Mail-Client und -Server	Mobile Anwendungen (Apps)
Internet-Anwendungen/ Cloud Anwendungen	Medizinische Großgeräte	Dezentrale Komponenten der TI

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ VORBEREITUNG

➤ HILFESTELLUNGEN ZUR DURCHFÜHRUNG

➤ NACHBEREITUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Anforderungsumsetzung (I)

› Folienaufbau:

- › Anforderungen der Anlagen werden pro Zielobjekt und pro Anlage mit detaillierteren Hilfestellungen dargestellt

› Folienstruktur:

(VI) Smartphone und Tablet – Anlage 1, 2 & 3

Zu erfüllende Anforderungen in Anlage

	1	2	3	4	5	Gesamt
Zielobjekt: Smartphone und Tablet	6	-	-	-	-	6
	6	2	-	-	-	8
	6	2	3	-	-	11

Anforderung betrifft Hardware: Smartphone und Tablet

- › 6 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 2 Anforderungen müssen ab mittleren Praxen umgesetzt werden
- › 3 Anforderungen müssen ab großen Praxen umgesetzt werden

Übersichtsseite pro Zielobjekt/Anlage

(VI) Smartphone und Tablet - Anlage 2

Anforderung Nr. 6 & 7

Zielobjekt	Anforderung	Erfüllung
Smartphone und Tablet	6: Aktiviere für Mobiltelefone zur Benutzung von mobilen Geräten Sprachassistenten	Es sollte eine verlässliche Methode für Mobiltelefone zur Benutzung von mobilen Geräten Sprachassistenten aktiviert werden, wenn sie vorrangig notwendig sind.
Smartphone und Tablet	7: Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie vorrangig notwendig sind.

- › Eine Nutzungs- und Sicherheitsrichtlinie für mobile Geräte
- › Sollte Nutzungs-, Pflege-, Aufbewahrungs- und Verlustmeldungsorgaben machen
- › Sollte Deinstallation von Verwaltungssoftware und Rooten von Geräten verboten
- › Sollte Teil der Schulung zu Sicherheitsmaßnahmen sein
- › Muss jedem Benutzer ausgehändigt und regelmäßig auf Einhaltung überprüft werden
- › Nur solange der Sprachassistent genutzt wird, sollte er aktiviert und ansonsten grundsätzlich deaktiviert sein

Anlage x und Anforderungen pro Zielobjekt und Anlage mit Hinweisen auf der selben Seite

(VI) Smartphone und Tablet - Anlage 1 cont.

Anforderung Nr. 2, 3 & 4

Zielobjekt	Anforderung	Erfüllung
Smartphone und Tablet	2: Updates von Betriebssystem und Apps	Updates des Betriebssystems und der eingesetzten Apps bei Hinweis auf neue Versionen immer aktuell installieren, und Schwachstellen zu vermeiden. Legen Sie ausschließlich einen festen Termin (z.B. monatlich) fest, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden.
Smartphone und Tablet	3: Datensicherheits-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen ihrer Geräte sollte bei den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.

(VI) Smartphone und Tablet - Anlage 1 Details

- › Funktion „Safe Browsing“ bzw. die Funktion zur Warnung vor schädlichen Inhalten von Browsern
- › Anonyme Browserfunktion bei einigen Browsern wie Chrome/ Firefox oder Firefox Klar
- › Schutz durch achtsamen Umgang mit Zugangsdaten:
 - › Überprüfen der URL, auf der die Zugangsdaten eingabegeben werden
 - › Misstrauen gegenüber E-Mails mit einem Link und der Aufforderung, Zugangsdaten dort einzugeben
- › Nutzung von Browser-Leisteichen um auf der korrekten Webseite zu landen
- › Die Nutzung der SIM-Karte der Institution sollte durch eine PIN geschützt werden
- › Alle mobilen Endgeräte müssen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen.
 - › Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden.

Anlage y und Anforderungen pro Zielobjekt und Anlage mit Hinweisen auf der folgenden Seite

Anforderungsumsetzung (II)




- › Weitere Hinweise und konkrete Maßnahmen zur Umsetzung der Anforderungen können von unterschiedlichen Stellen herausgegeben werden:
 - › Hersteller eines Produktes selbst
 - › Verbände wie der Allianz für Cybersicherheit
 - › Behörden wie dem BSI
- › Auch eigenständig entwickelte technische und/oder organisatorische Maßnahmen können zur Erfüllung der Anforderungen genutzt werden

→ Eine ständig aktualisierte Liste von Hilfsmitteln zur Umsetzung kann auf einer Webseite der KBV unter <https://hub.kbv.de/display/itsrl> gefunden werden.

Tipp

(I) Personal Anlagen 1 & 3

Zielobjekt:
Personal

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		7	-	-	-	
	7	-	-	-	-	7
	7	1	-	-	-	8

- › Anforderung betrifft: Personal
- › 7 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 1 Anforderung muss ab großen Praxen umgesetzt werden

(I) Personal - Anlage 1

Anforderung Nr. 1 & 2

Zielobjekt	Anforderung	Erläuterung
Personal	Geregelte Einarbeitung neuer Mitarbeitenden	Mitarbeitende müssen zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeitenden müssen über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden.
Personal	Geregelte Verfahrensweise beim Weggang von Mitarbeitenden	Ausscheidende Mitarbeitende müssen alle im Rahmen ihrer Tätigkeit erhaltenen Unterlagen, Schlüssel und Geräte sowie Ausweise und Zutrittsberechtigungen zurückgeben. Zugangsdaten (bspw. Passwörter), die dem ausscheidendem Mitarbeiter bekannt waren oder von ihm genutzt wurden, müssen geändert oder vernichtet werden. Vor der Verabschiedung muss noch einmal auf die fortdauernden Verschwiegenheitsverpflichtungen hingewiesen werden.

(I) Personal - Anlage 1 cont.

Anforderung Nr. 3 & 4

Zielobjekt	Anforderung	Erläuterung
Personal	Festlegung von Regelungen für den Einsatz von Fremdpersonal	Externes Personal muss wie alle eigenen Mitarbeitenden dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Kurzfristig oder einmalig eingesetztes Fremdpersonal muss in sicherheitsrelevanten Bereichen beaufsichtigt werden. Ggf. notwendige Zugangsberechtigungen sind so restriktiv wie möglich zu halten.
Personal	Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal	Bevor externe Personen Zugang und Zugriff zu vertraulichen Informationen erhalten, müssen mit ihnen Vertraulichkeitsvereinbarungen in schriftlicher Form geschlossen werden.

(I) Personal - Anlage 1 cont.

Anforderung Nr. 5, 6 & 7

Zielobjekt	Anforderung	Erläuterung
Personal	Aufgaben und Zuständigkeiten von Mitarbeitenden	Alle Mitarbeitenden müssen dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Die Mitarbeitenden müssen auf den rechtlichen Rahmen ihrer Tätigkeit hingewiesen werden. Die Aufgaben und Zuständigkeiten von Mitarbeitenden müssen in geeigneter Weise dokumentiert sein. Dabei sollte ebenfalls dokumentiert werden, welche Berechtigungen und Zugänge für die Mitarbeitenden bereitgestellt/genutzt werden. Außerdem müssen alle Mitarbeitenden darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind.
Personal	Qualifikation des Personals	Mitarbeitende müssen regelmäßig geschult bzw. weitergebildet werden, insbesondere auch im Bezug auf die eingesetzte Technik/IT. Es müssen betriebliche Regelungen vorhanden sein, welche mit geeigneten Mitteln sicherstellen, dass die Mitarbeitenden auf einem aktuellen Kenntnisstand sind. Weiterhin sollte den Mitarbeitenden während ihrer Beschäftigung die Möglichkeit gegeben werden, sich im Rahmen ihres Tätigkeitsfeldes weiterzubilden.
Personal	Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden	Bei der Einstellung neuer Mitarbeitenden sollte besonders auf ihre Vertrauenswürdigkeit, beispielsweise bei der Prüfung vorliegender Arbeitszeugnisse, geachtet werden. Soweit möglich, sollten alle an der Personalauswahl Beteiligten kontrollieren, ob die Angaben der Bewerbenden, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind.

(I) Personal - Details




- › Alle neuen Mitarbeitende sollten in die Benutzung der für den Arbeitsplatz wesentlichen IT-Systeme und Anwendungen eingewiesen bzw. geschult werden.
- › Von dem Ausscheidenden sind sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene Geräte zurückzufordern.
- › Es sind sämtliche für den Ausscheidenden eingerichteten Zugangsberechtigungen und Zugriffsrechte zu entziehen bzw. zu löschen. Dies betrifft auch die externen Zugangsberechtigungen via Datenübertragungseinrichtungen.
- › Wurde in Ausnahmefällen eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt (z. B. mittels eines gemeinsamen Passwortes), so ist nach Weggang einer der Personen die Zugangsberechtigung zu ändern.
- › Externe Mitarbeitende, die eventuell Zugang zu vertraulichen Unterlagen und Daten bekommen könnten, sind schriftlich auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten.

(I) Personal – Details cont.

- › Werden Stellen besetzt, müssen die erforderlichen Qualifikationen und Fähigkeiten genau formuliert sein. Anschließend sollte geprüft werden, ob diese bei den Bewerbenden für die Stelle tatsächlich vorhanden sind. Es muss sichergestellt sein, dass Stellen nur von Mitarbeitenden besetzt werden, für die sie qualifiziert sind.
- › Grundsätzlich sollte vor der Übernahme von neuen oder externen Mitarbeitenden überprüft werden, ob
 - › diese hinreichende Referenzen haben, z. B. aus anderen, bisherigen Projekten, und
 - › der vorgelegte Lebenslauf des Bewerbenden aussagekräftig und vollständig ist.

(II) Sensibilisierung und Schulung – Anlage 1

Zielobjekt:
Sensibilisierung und Schulung zur Informationssicherheit

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		3	-	-	-	
	3	-	-	-	-	3
	3	-	-	-	-	3

- › Anforderung betrifft: Sensibilisierung und Schulung zur Informationssicherheit
- › Muss von allen Praxistypen umgesetzt werden

(II) Sensibilisierung und Schulung - Anlage 1

Anforderung Nr. 8, 9 & 10

Zielobjekt	Anforderung	Erläuterung
Sensibilisierung und Schulung zur Informationssicherheit	Sensibilisierung der Praxisleitung für Informationssicherheit	Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.
Sensibilisierung und Schulung zur Informationssicherheit	Einweisung des Personals in den sicheren Umgang mit IT	Alle Mitarbeitenden und externen Benutzenden müssen in den sicheren Umgang mit IT-Komponenten eingewiesen und sensibilisiert werden, soweit dies für ihre Arbeitszusammenhänge relevant ist.
Sensibilisierung und Schulung zur Informationssicherheit	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Alle Mitarbeitenden sollten entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.




(II) Sensibilisierung und Schulung - Details



- › Es ist für den Sicherheitsprozess wichtig, dass dieser aktiv von der Praxisleitung unterstützt wird. Hierfür muss die Praxisleitung den Wert von Informationssicherheit erkannt und verinnerlicht haben.
- › Um Sicherheitsprobleme durch fehlerhafte Benutzung bzw. Konfiguration der IT zu vermeiden, sollten alle Mitarbeitende in den sicheren Umgang mit den IT-Komponenten der Praxis eingewiesen und geschult werden, soweit dies ihre Arbeitszusammenhänge betrifft.

(III) Netzwerksicherheit - Anlage 1, 2 & 3

Zielobjekt:
Netzwerksicherheit

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		3	-	-	-	
	3	1	-	-	-	4
	3	1	2	-	-	6

- › Anforderung betrifft Hardware: Netzwerksicherheit
- › 3 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 1 Anforderung muss ab mittleren Praxen umgesetzt werden
- › 1 Anforderung muss ab großen Praxen umgesetzt werden

(III) Netzwerksicherheit - Anlage 1

Anforderung Nr. 11, 12 & 13

Zielobjekt	Anforderung	Erläuterung
Netzwerksicherheit	Absicherung der Netzübergangspunkte	Der Übergang zu anderen Netzen insbesondere dem Internet muss durch eine Firewall geschützt werden. Primäres Ziel ist es, keine unerlaubten Verbindungen von außen in das geschützte Netz zuzulassen. Zusätzlich sollten nur erlaubte Verbindungen aus dem geschützten Netz nach außen aufgebaut werden können.
Netzwerksicherheit	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.
Netzwerksicherheit	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.

- › Nur erlaubte Kommunikationsziele (IP-Adressen und Ports) und –protokolle zulassen (eingehend und ausgehend)
- › Besonders sensible Systeme innerhalb des Praxisnetzes isolieren (vgl. Anlage 4 – Anforderung 6)
- › Dokumentieren der logischen Struktur des Netzes (insbesondere Subnetze, Zonen und Segmente) und Änderungen dieser Struktur
- › Geeignete Authentisierung ist beispielsweise eine 2-Faktor-Authentifizierung mit Passwort (Wissen) und einem zugeschickten Code auf einem zweiten Endgerät (Besitz)

(III) Netzwerksicherheit - Anlage 2

Anforderung Nr. 1

Zielobjekt	Anforderung	Erläuterung
Netzwerksicherheit	Alarmierung und Logging	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.

- › Mindestens folgende Ereignisse protokollieren:
 - › unautorisierte Zugriffe bzw. Zugriffsversuche
 - › Leistungs- oder Verfügbarkeitsschwankungen des Netzes
 - › Fehler in automatischen Prozessen (z. B. bei der Konfigurationsverteilung)
 - › eingeschränkte Erreichbarkeit von Netzkomponenten

(III) Netzwerksicherheit - Anlage 3






Anforderung Nr. 2

Zielobjekt	Anforderung	Erläuterung
Netzwerksicherheit	Planung des internen Netzwerkes	Bei der Planung des internen Netzwerkes soll eine Netzwerksegmentierung erfolgen, die berücksichtigt, welche Daten in dem jeweiligen Segment verarbeitet und kommuniziert werden. Hierbei soll eine Trennung zwischen Gesundheitsdaten und weniger kritischen Daten erfolgen.
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.

- › Konfiguration und Einsatz sicherer und sichernder Protokolle bei Übertragung vertraulicher Informationen in einer nicht vertrauenswürdigen Umgebung
 - › Alternativ: angemessene Verschlüsselung der Informationen

(IV) Patch- und Änderungsmanagement – Anlage 1

Zielobjekt:
Patch- und Änderungsmanagement

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		4	-	-	-	
	4	-	-	-	-	4
	4	-	-	-	-	4

- › Anforderung betrifft: Patch- und Änderungsmanagement
- › Muss von allen Praxistypen umgesetzt werden

(IV) Patch- und Änderungsmanagement 1



Anforderung Nr. 14, 15, 16 & 17




Zielobjekt	Anforderung	Erläuterung
Patch- und Änderungsmanagement	Installation von Updates	Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.
Patch- und Änderungsmanagement	Verantwortlichkeit für Updates	Es muss festgelegt werden, wer die Updates installiert. Das ausgewählte Personal muss geschult und entsprechend berechtigt werden.
Patch- und Änderungsmanagement	Identifizierung ausbleibender Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.
Patch- und Änderungsmanagement	Ausmusterung oder Separierung bei ausbleibenden Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert oder separiert in einem eigenen Netzwerksegment betrieben werden.

(IV) Patch- und Änderungsmanagement - Details

- › Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.
- › Die Verantwortlichkeiten für das Patch- und Änderungsmanagement sollten festgelegt werden. Die Verantwortlichen müssen das notwendige Wissen und die entsprechenden Berechtigungen besitzen.
- › Häufig kündigen die Hersteller an, ab wann sie ein Produkt nicht mehr unterstützen, bzw. stellen die Information bereit, dass sie ein Produkt nicht mehr unterstützen.
- › Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen ausgemustert oder separiert in einem eigenen Netzwerksegment betrieben werden.

(V) Endgeräte - Anlage 1 & 2

Zielobjekt:
Endgeräte

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		9	-	-	-	
	9	2	-	-	-	9
	9	2	-	-	-	9

- › Anforderung betrifft Hardware: Endgeräte
- › 9 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 2 Anforderungen müssen ab mittleren Praxen umgesetzt werden

(V) Endgeräte - Anlage 1

Anforderung Nr. 18, 19, 20, 21, 22, 23 & 24

Zielobjekt	Anforderung	Erläuterung
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.
Endgeräte	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.
Endgeräte	Einsatz von Viren-Schutzprogrammen	Aktuelle Virenschutzprogramme sind einzusetzen.
Endgeräte	Regelmäßige Datensicherung	Sämtliche relevante Daten sind regelmäßig zu sichern.
Endgeräte	Schutz der Datensicherung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.
Endgeräte	Art der Datensicherung	Es muss festgelegt werden, wie die Daten gesichert werden.
Endgeräte	Verantwortliche der Datensicherung	Es muss festgelegt werden, wer für die Datensicherung zuständig ist.


(V) Endgeräte - Anlage 1 cont.

Anforderung Nr. 25 & 26

Zielobjekt	Anforderung	Erläuterung
Endgeräte	Test der Datensicherung	Es sollte getestet werden, ob gesicherte Daten funktionsfähig und vollständig vorhanden sind.
Endgeräte	Der Zugriff auf Geräte und Software muss abgesichert werden.	Es sollten Benutzer und Rollen in der Praxissoftware zum Steuern der Zugriffe auf Patientendaten oder zur Nutzung von Sicherheitskarten wie z.B. den eHBA für den Inhaber der Karte eingerichtet werden.

(V) Endgeräte - Anlage 1 Details

- › Mikrofon- oder Kameradeaktivierung (abhängig vom Gerät, vor einem Kauf informieren) über:
 - › Entsprechende Softwarefunktionen
 - › Entzug von Zugriffsberechtigungen
 - › physische Abdeckung, Ausschaltung oder Trennung

- › Unbeaufsichtigte Geräte sperren:
 - › Windows-Rechner: Windows-Taste  + L
 - › Mobile Geräte: Sperrtaste

- › Daten sind durch ein Backup vor Ausfällen von Hard- und Software sowie Verschlüsselungstrojaner zu schützen.
 - › Erstellen eines Planes, der festlegt welche Daten wie oft gesichert werden sollen. Kombinieren von vollständigen Backups und inkrementellen Backups.
 - › Festlegung der Verantwortlichkeit für das Backup
 - › Regelmäßiges Prüfen, ob sich die Backups fehlerlos wieder zurückspielen lassen.

(V) Endgeräte - Anlage 1 Details cont.

- › Ein aktuell gehaltener Virenschanner für Geräte im Praxisnetz sollte:
 - › Dateizugriffe prüfen, um die Ausführung schadhafter Dateien zu verhindern
 - › Versendete und empfangene Dateien prüfen, um die Ausführung schadhafter Dateien zu verhindern
 - › Den gesamten Datenbestand regelmäßig prüfen, um vergangene Infektionen mittels neuer Signaturen zu finden
 - › Änderungen am Virenschanner von Benutzern (z. B. Deinstallation oder Konfigurationsänderungen) verhindern
- › Realisierung des Zugriffs auf Geräte und Software durch ein Berechtigungskonzept mit unterschiedlichen Rechten für unterschiedliche Benutzer und Rollen.

(V) Endgeräte - Anlage 2






Anforderung Nr. 3 & 4

Zielobjekt	Anforderung	Erläuterung
Endgeräte	Nutzung von verschlüsselten Kommunikationsverbindungen	Benutzer sollten darauf achten, dass zur Verschlüsselung von Kommunikationsverbindungen kryptografische Algorithmen nach dem Stand der Technik wie z. B. TLS verwendet werden.
Endgeräte	Restriktive Rechtevergabe	Rechte sollten so restriktiv wie möglich nach dem Need-to-know Prinzip vergeben werden.

- › Ein Schlüsselsymbol und das S im „https“ einer Webseiten-Adresse weisen auf die TLS Verschlüsselung hin (vgl. Anlage 1 – Anforderung 49)
- › Benutzer und Programme sollten nur benötigte Berechtigungen erhalten, und Berechtigungen sollten regelmäßig geprüft werden

(VI) Endgeräte mit dem Betriebssystem Windows - Anlage 1 & 2

Zielobjekt:
Endgeräte mit dem Betriebssystem Windows

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		3	-	-	-	
	3	1	-	-	-	4
	3	1	-	-	-	4

- › Anforderung betrifft Hardware: Endgeräte mit dem Betriebssystem Windows
- › 3 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 1 Anforderung muss ab mittleren Praxen umgesetzt werden

(VI) Endgeräte mit dem Betriebssystem Windows - Anlage 1

Anforderung Nr. 27, 29 & 29

Zielobjekt	Anforderung	Erläuterung
Endgeräte mit dem Betriebssystem Windows	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.
Endgeräte mit dem Betriebssystem Windows	Datei- und Freigabeberechtigungen	Berechtigungen und Zugriffe sind pro Personengruppe und pro Person zu regeln.
Endgeräte mit dem Betriebssystem Windows	Datensparsamkeit	So wenige personenbezogene Daten wie möglich sind zu verwenden.

(VI) Endgeräte mit dem Betriebssystem Windows - Anlage 1 Details

- › Deinstallation von "OneDrive". Dazu klicken Sie auf den Windowsbutton, dann auf Einstellungen. Klicken Sie in dem geöffneten Fenster auf "Apps", in der angezeigten App-Liste auf "OneDrive" und deinstallieren Sie die App über den Button "deinstallieren".
- › Regelung der Berechtigungen nach dem Need-to-know-Prinzip. D. h. jede Person sollte nur so viel Berechtigungen, wie zur Bewältigung der Aufgaben nötig sind, auf Programm-, Datei und Verzeichnisebene erhalten. Mittels Gruppen und Rollen lassen sich Berechtigungen für mehrere Personen für Netzfreigaben einrichten.
- › Jede Verwendung von personenbezogenen Daten muss begründet (Zweckbindung) und in einem "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Dies schließt auch die einzuhaltenden Löschfristen mit ein.

(VI) Endgeräte mit dem Betriebssystem Windows - Anlage 2





Anforderung Nr. 4

Zielobjekt	Anforderung	Erläuterung
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.

- › Veraltete Protokolle zur Authentisierung sollten blockiert werden.

(VII) Smartphone und Tablet – Anlage 1, 2 & 3

Zielobjekt:
Smartphone
und Tablet

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		4	-	-	-	
	4	2	-	-	-	6
	4	2	3	-	-	9

- › Anforderung betrifft Hardware: Smartphone und Tablet
- › 4 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 2 Anforderungen müssen ab mittleren Praxen umgesetzt werden
- › 3 Anforderungen müssen ab großen Praxen umgesetzt werden

(VII) Smartphone und Tablet - Anlage 1

Anforderung Nr. 30, 31, 32 & 34

Zielobjekt	Anforderung	Erläuterung
Smartphone und Tablet	Verwendung der SIM-Karten-PIN	SIM-Karten sind durch eine PIN zu schützen. Super-PIN/PUK sind nur durch Verantwortliche anzuwenden.
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.
Smartphone und Tablet	Verwendung eines Zugriffsschutzes	Geräte sind mit einem komplexen Gerätesperrcode zu schützen.
Smartphone und Tablet	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen der Endgeräte sollte in den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.

(VII) Smartphone und Tablet - Anlage 1 Details

- › Die Nutzung der SIM-Karte der Institution sollte durch eine PIN geschützt werden.
- › Alle mobilen Endgeräte müssen so konfiguriert sein, dass sie das erforderliche Schutzniveau angemessen erfüllen.
 - › Dafür muss eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammengestellt und dokumentiert werden. Nicht benötigte Funktionen sollten deaktiviert werden.
- › Smartphones und Tablets müssen mit einem angemessen komplexen Gerätesperrcode geschützt werden.
 - › Die Nutzung der Bildschirmsperre muss vorgeschrieben werden.
 - › Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm muss deaktiviert sein.
- › Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen muss angemessen eingeschränkt werden.

(VII) Smartphone und Tablet - Anlage 2

Anforderung Nr. 5 & 6

Zielobjekt	Anforderung	Erläuterung
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.
Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.

- › Eine Nutzungs- und Sicherheitsrichtlinie für mobile Geräte:
 - › Sollte Nutzungs-, Pflege-, Aufbewahrungs- und Verlustmeldungsvorgaben machen
 - › Sollte Deinstallation von Verwaltungssoftware und Rooten von Geräten verbieten
 - › Sollte Teil der Schulung zu Sicherheitsmaßnahmen sein
 - › Muss jedem Benutzer ausgehändigt und regelmäßig auf Einhaltung überprüft werden
- › Nur solange der Sprachassistent genutzt wird, sollte er aktiviert und ansonsten grundsätzlich deaktiviert sein

(VII) Smartphone und Tablet - Anlage 3






Anforderung Nr. 4, 5 & 6

Zielobjekt	Anforderung	Erläuterung
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.
Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.
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.

- › Es muss geregelt sein:
 - › wer auf welche Informationen zugreifen darf
 - › welche Informationen auf mobilen Geräten verfügbar sind (Bewertungsgrundlage: Vertraulichkeit und Umstände der Datenverarbeitung)
- › Apps aus öffentlichen App-Stores vor Benutzung prüfen und erst dann freigeben.
- › Nur freigegebene und geprüfte Apps aus sicheren Quellen (vgl. Anlage 1 – Anforderung 42) sollten installiert werden dürfen.

(VIII) Mobiltelefon - Anlage 1 & 2

Zielobjekt:
Mobiltelefon

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		2	-	-	-	
	2	4	-	-	-	5
	2	4	-	-	-	5

- › Anforderung betrifft Hardware: Mobiltelefon
- › 2 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 2 Anforderungen müssen ab mittleren Praxen umgesetzt werden

(VIII) Mobiltelefon - Anlage 1

Anforderung Nr. 34 & 35

Zielobjekt	Anforderung	Erläuterung
Mobiltelefon	Sperrmaßnahmen bei Verlust eines Mobiltelefons	Bei Verlust eines Mobiltelefons muss die darin verwendete SIM-Karte zeitnah gesperrt werden. Die dafür notwendigen Mobilfunkanbieter-Informationen sind zu hinterlegen, um bei Bedarf darauf zugreifen zu können.
Mobiltelefon	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.

(VIII) Mobiltelefon - Anlage 1 Details

- › SIM-Karte durch PIN (vgl. Anlage 1 – Anforderung 30) und Mobiltelefon durch Geräte-Code schützen
- › Gerät wenn möglich an SIM-Karte binden (SIM-Lock).
- › Benutzer über Sicherheitsmechanismen informieren

(VIII) Mobiltelefon - Anlage 2




Anforderung Nr. 7 & 8

Zielobjekt	Anforderung	Erläuterung
Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.
Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.

- › Eine Nutzungs- und Sicherheitsrichtlinie für Mobiltelefone:
 - › Sollte Nutzungs-, Pflege-, Aufbewahrungs- und Verlustmeldungsvorgaben machen
 - › Sollte Deinstallation von Verwaltungssoftware und Rooten von Geräts verbieten
 - › Sollte Teil der Schulung zu Sicherheitsmaßnahmen sein
 - › Muss jedem Benutzer ausgehändigt und regelmäßig auf Einhaltung überprüft werden
- › Ist die Datenübertragung über Mobiltelefone erlaubt, müssen Informationen durch Verschlüsselung angemessen geschützt werden.

(IX) Mobile Device Management (MDM) - Anlage 3

Zielobjekt:
Mobile Device Management (MDM)

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		-	-	-	-	
	-	-	-	-	-	-
	-	-	6	-	-	6

- › Anforderung betrifft Hardware: Mobile Device Management (MDM)
- › 6 Anforderungen müssen ab großen Praxen umgesetzt werden

(IX) Mobile Device Management (MDM) - Anlage 3



Anforderung Nr. 7, 8, 9, 10, 11 & 12




Zielobjekt	Anforderung	Erläuterung
Mobile Device Management (MDM)	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden.
Mobile Device Management (MDM)	Berechtigungsmanagement im MDM	Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.
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.
Mobile Device Management (MDM)	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM muss sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.
Mobile Device Management (MDM)	Auswahl und Freigabe von Apps	Nur durch die Verantwortlichen geprüfte und freigegebene Apps dürfen über das MDM zur Installation angeboten werden.
Mobile Device Management (MDM)	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis muss festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.

(IX) Mobile Device Management (MDM) - Anlage 3 Details

- › Verbindungen mobiler Endgeräte angemessen (z. B. durch ein VPN zum Praxisnetz) schützen
- › Berechtigungskonzept nach Minimalprinzip erstellen, anwenden und regelmäßig Vergabe und Dokumentation überprüfen
- › Nicht vertrauenswürdige/verifizierbare Zertifikate blockieren und Zertifikatsgültigkeitsprüfungen durchführen lassen
- › Bei der Außerbetriebnahme des mobilen Endgerätes (aus der Ferne: „Remote Wipe“) nach Möglichkeit schutzbedürftigen Daten auf dem Gerät oder externen Speichermedien (z. B. SD-Karte) löschen
- › Folgendes muss geregelt, kommuniziert und sollte über MDM auf allen Geräte umgesetzt werden:
 - › wer auf welche Informationen zugreifen darf
 - › welche Apps gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden
 - › welche Informationen auf mobilen Geräten verfügbar sind (Bewertungsgrundlage: Vertraulichkeit und Umstände der Datenverarbeitung, z. B. in abgeschotteten Containern)

(X) Wechseldatenträger / Speichermedien - Anlage 1, 2 & 3

Zielobjekt:
Wechseldatenträger / Speichermedien

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		4	-	-	-	
	4	1	-	-	-	5
	4	1	2	-	-	7

- › Anforderung betrifft Hardware: Wechseldatenträger / Speichermedien
- › 4 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 1 Anforderung muss ab mittleren Praxen umgesetzt werden
- › 2 Anforderung muss ab großen Praxen umgesetzt werden

(X) Wechseldatenträger / Speichermedien - Anlage 1

Anforderung Nr. 28, 29, 30 & 31

Zielobjekt	Anforderung	Erläuterung
Wechseldatenträger / Speichermedien	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.
Wechseldatenträger / Speichermedien	Angemessene Kennzeichnung der Datenträger beim Versand	Beim Versand von Datenträgern sollte der Absender diese für den Empfänger eindeutig kennzeichnen. Dabei sollte die Kennzeichnung möglichst keine Rückschlüsse auf den Inhalt für andere ermöglichen.
Wechseldatenträger / Speichermedien	Sichere Versandart und Verpackung	Zum Versand von Datenträgern sollten Versandanbieter mit sicherem Nachweis-System und eine möglichst manipulationssichere Versandart und Verpackung gewählt werden.
Wechseldatenträger / Speichermedien	Sicheres Löschen der Datenträger vor und nach der Verwendung	Alle Datenträger müssen nach ihrer Verwendung durch den jeweiligen Mitarbeiter/Mitarbeiterin sicher und vollständig gelöscht werden.

(X) Wechseldatenträger / Speichermedien - Anlage 1 Details

- › Mittels Virens Scanner Wechseldatenträger automatisch vor der Verwendung auf Schadsoftware prüfen lassen
- › Datenträgerkennzeichnungen könnten erfolgen durch:
 - › Liste, die eine Kennzeichnung eines Datenträgers eindeutig zuordenbar macht
 - › Zwischen Sender und Empfänger abgestimmte Systematik, für Dritte keine Rückschlüsse ermöglicht. Z.B. Datenträger: "dd2bbeab-d901-4043-b543-0ce74ce57aae" statt "onkologischer Befund Patient XY".
- › Nutzung eines abgesicherten Versands einer oder mehrerer Postunternehmen.
- › Vor Weitergabe, Wiederverwendung oder Aussonderung wiederbeschreibbare Datenträger Informationen auf geeignete Weise löschen, sodass vertrauliche Daten nicht wiederherstellbar sind

(X) Wechseldatenträger / Speichermedien - Anlage 2

Anforderung Nr. 9

Zielobjekt	Anforderung	Erläuterung
Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.

- › Schriftlich festlegen, welche Datenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei umgesetzt werden müssen

(X) Wechseldatenträger / Speichermedien - Anlage 3



Anforderung Nr. 13 & 14




Zielobjekt	Anforderung	Erläuterung
Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.
Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.

- › Sichere und nicht veraltete Verschlüsselungsverfahren einsetzen
 - › Das BSI beschreibt in der ständig aktualisierten Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1) sichere Verfahren.

- › Datenaustausch vor (un)bewusster Manipulation mit aktuellen („Stand der Technik“) Checksummen oder Signaturen absichern
 - › Hinweise zum Stand der Technik: z. B. „Handreichung zum ‚Stand der Technik‘“ der TeleTrust

(XI) E-Mail-Client und -Server - Anlage 1 & 3

Zielobjekt:
E-Mail-Client
und -Server

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		2	-	-	-	
	2	-	-	-	-	2
	2	-	3	-	-	5

- › Anforderung betrifft: E-Mail-Client und -Server
- › 2 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 3 Anforderung muss ab großen Praxen umgesetzt werden

(XI) E-Mail-Client und -Server - Anlage 1

Anforderung Nr. 40 & 41

Zielobjekt	Anforderung	Erläuterung
E-Mail-Client und -Server	Sichere Konfiguration der E-Mail-Clients	<p>Bei der Konfiguration der E-Mail-Clients muss mindestens Folgendes berücksichtigt werden:</p> <ul style="list-style-type: none"> • Dateianhänge von E-Mails sollten vor dem Öffnen auf Schadsoftware geprüft werden • die automatische Interpretation von HTML-Code und anderen aktiven Inhalten in E-Mails sollte deaktiviert werden • zur Kommunikation mit E-Mail-Servern über nicht vertrauenswürdige Netze sollte eine sichere Transportverschlüsselung eingesetzt werden
E-Mail-Client und -Server	Umgang mit Spam durch Benutzende	<p>Grundsätzlich sollten die Benutzenden alle Spam-E-Mails ignorieren und löschen. Die Benutzenden sollten auf unerwünschte E-Mails nicht antworten. Sie sollten Links in diesen E-Mails nicht folgen.</p>

(XI) E-Mail-Client und -Server - Anlage 1 Details

- › Angriffe erfolgen oft initial über E-Mails. Daher ist eine sichere Konfiguration der E-Mail-Clients unerlässlich.
- › Als Spam werden unerwünschte, massenhafte E-Mails bezeichnet, die dem Empfänger unverlangt zugestellt werden.

(XI) E-Mail-Client und -Server - Anlage 3



Anforderung Nr. 15, 16 & 17




Zielobjekt	Anforderung	Erläuterung
E-Mail-Client und -Server	Sicherer Betrieb von E-Mail-Servern	<p>Bei dem Betrieb von E-Mail-Servern muss mindestens Folgendes berücksichtigt werden:</p> <ul style="list-style-type: none"> • es muss eine sichere Transportverschlüsselung für das Senden und Empfangen von E-Mails ermöglicht werden • es sollten Schutzmechanismen gegen Denial-of-Service (DoS)-Attacken ergriffen werden • E-Mail-Server müssen so konfiguriert werden, dass sie nicht als Spam-Relay missbraucht werden können
E-Mail-Client und -Server	Datensicherung und Archivierung von E-Mails	Die Daten der E-Mail-Server und -Clients sind regelmäßig und verschlüsselt zu sichern.
E-Mail-Client und -Server	Spam- und Virenschutz auf dem E-Mail-Server	Eingehende und ausgehende E-Mails und deren Anhänge sind auf Spam-Merkmale und schädliche Inhalte zu überprüfen.

(XI) E-Mail-Client und -Server - Anlage 3 Details

- › Der Empfang von E-Mails über unverschlüsselte Verbindungen sollte deaktiviert werden.
- › Der E-Mail-Server sollte so konfiguriert werden, dass E-Mail-Clients nur über eine sichere Transportverschlüsselung auf Postfächer zugreifen können, wenn dies über nicht vertrauenswürdige Netze passiert.
- › Es sollte beachtet werden, dass E-Mails möglicherweise nur lokal auf Clients gespeichert sind.
- › Es muss festgelegt werden, wie mit verschlüsselten E-Mails zu verfahren ist, wenn diese nicht durch das Virenschutzprogramm entschlüsselt werden können.

(XII) Mobile Anwendungen (Apps) Anlagen 1 & 2

Zielobjekt:
Mobile
Anwendungen
(Apps)

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		3	-	-	-	
	3	1	-	-	-	4
	3	1	-	-	-	4

- › Anforderung betrifft Software: mobile Apps
- › 3 Anforderungen müssen von allen Praxistypen umgesetzt werden
- › 1 Anforderung muss ab mittleren Praxen umgesetzt werden

(XII) Mobile Anwendungen (Apps) - Anlage 1

Anforderung Nr. 42, 43 & 44

Zielobjekt	Anforderung	Erläuterung
Mobile Anwendungen (Apps)	Sichere Apps nutzen	Apps sollten nur aus den offiziellen Stores geladen werden. Sofern Apps nicht mehr benötigt werden, ist der Benutzeraccount in der App / das Benutzerkonto zu löschen und danach die App inkl. aller enthaltenen Daten auf dem Gerät zu deinstallieren.
Mobile Anwendungen (Apps)	Sichere Speicherung lokaler App-Daten	Es sollten nur Apps genutzt werden, die Dokumente verschlüsselt und lokal abspeichern.
Mobile Anwendungen (Apps)	Verhinderung von Datenabfluss	Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.

(XII) Mobile Anwendungen (Apps) - Anlage 1 Details

- › Apps nur aus vertrauenswürdigen Hersteller-App-Stores installieren (z. B. „Google Play Store“, „App Store“ oder „Microsoft Store“)
- › Android: keine Apps aus externen Quellen zulassen
- › „Automatische Updates“-Funktion unterstützt bei einer zeitnahen Installation aktueller App Versionen
- › Verschlüsselung von Android (PIN oder Passwort einrichten)/ IOS ("Code-Sperre") aktivieren.
- › Alle vertraulichen Informationen (z. B. Dokumente, personenbezogene Daten, Schlüsselinformationen) sind zu schützen
- › Datenversand einschränken (z. B. über die Einstellungen der App):
 - › Verhindert den ungewollten Versand vertraulicher Daten von Apps
 - › Verhindert die ungewollte Erstellung von Benutzerprofilen
- › Wenn möglich vor der App-Benutzung prüfen:
 - › Werden ungeschützte Protokollierungs- oder Hilfsdateien geschrieben, die vertrauliche Informationen preisgeben

(XII) Mobile Anwendungen (Apps) - Anlage 2






Anforderung Nr. 10

Zielobjekt	Anforderung	Erläuterung
Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken bzw. zu vergeben.

- › Vor der Nutzung einer App sicherstellen, dass nur für die Funktionen benötigte Berechtigungen erlaubt sind
- › Weitere Berechtigungen hinterfragen und gegebenenfalls unterbinden
- › Änderungen sicherheitsrelevante Berechtigungseinstellungen durch Benutzer oder Apps technisch verhindern oder regelmäßig auf Korrektheit überprüfen

(XIII) Internet-Anwendungen - Anlage 1

Zielobjekt:
Internet-Anwendungen

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		5	-	-	-	
	5	-	-	-	-	5
	5	-	-	-	-	5

- › Anforderung betrifft Software: Internet-Anwendungen
- › 5 Anforderungen müssen von allen Praxistypen umgesetzt werden

(XIII) Internet-Anwendungen - Anlage 1

Anforderung Nr. 45 & 46

Zielobjekt	Anforderung	Erläuterung
Internet-Anwendungen – Anbieter	Authentisierung bei Webanwendungen	<p>Sollten Sie als Praxis einen Webdienst anbieten:</p> <p>Der IT-Betrieb muss Webanwendungen und Webservices so konfigurieren, dass sich Clients gegenüber der Webanwendung oder dem Webservice authentisieren müssen, wenn diese auf geschützte Ressourcen zugreifen wollen. Dafür muss eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess sollte dokumentiert werden. Der IT-Betrieb muss geeignete Grenzwerte für fehlgeschlagene Anmeldeversuche festlegen.</p>
Internet-Anwendungen – Anbieter	Schutz vertraulicher Daten	<p>Sollten Sie als Praxis einen Webdienst anbieten:</p> <p>Der IT-Betrieb muss sicherstellen, dass Zugangsdaten zur Webanwendung oder zum Webservice serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden. Dazu müssen Salted Hash-Verfahren verwendet werden. Die Dateien mit den Quelltexten der Webanwendung oder des Webservices müssen vor unerlaubten Abrufen geschützt werden.</p>

(XIII) Internet-Anwendungen - Anlage 1 cont.

Anforderung Nr. 47, 48, & 49




Zielobjekt	Anforderung	Erläuterung
Internet-Anwendungen – Anbieter	Einsatz von Web Application Firewalls	Sollten Sie als Praxis einen Webdienst anbieten: Institutionen sollten eine Web Application Firewall (WAF) einsetzen. Die Konfiguration der eingesetzten WAF sollte auf die zu schützende Webanwendung oder den Webservice angepasst werden. Nach jedem Update der Webanwendung oder des Webservices sollte die Konfiguration der WAF geprüft werden.
Internet-Anwendungen - Anwender	Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen	Sollten Sie als Praxis einen Webdienst anbieten: Der IT-Betrieb muss sicherstellen, dass Webanwendungen und Webservices vor unberechtigter automatisierter Nutzung geschützt werden. Dabei muss jedoch berücksichtigt werden, wie sich die Schutzmechanismen auf die Nutzungsmöglichkeiten berechtigter Clients auswirken. Wenn die Webanwendung RSS-Feeds oder andere Funktionen enthält, die explizit für die automatisierte Nutzung vorgesehen sind, muss dies ebenfalls bei der Konfiguration der Schutzmechanismen berücksichtigt werden.
Internet-Anwendungen – Anbieter	Kryptografische Sicherung vertraulicher Daten	Bei der Nutzung von Webanwendungen ist darauf zu achten, dass eine verschlüsselte Kommunikation zum Einsatz kommt (z.B. https statt http).

(XIII) Internet-Anwendungen - Anlage 1 Details

- › Es sollte eine 2 Faktor Authentisierung angeboten werden oder hinreichend komplexe Passwörter eingefordert werden.
- › Die Webanwendung sollte verschlüsselte Verbindungen bereitstellen.
- › Falls Benutzernamen und Passwörter als Authentisierungsmethode angeboten werden, so dürfen die Passwörter nicht im Klartext sondern mittels dem Salted Hash-Verfahren gespeichert werden.
- › 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 sie entweder eine open source Lösungen (wie ModSecurity, Waf2Py oder OctopusWAF) oder eine spezielle kommerzielle Appliance verwenden
- › Nur <https://...> Webseiten nutzen
- › Mittels des sogenannten "Captcha-Mechanismus" lassen sich automatisierte Zugriffe begrenzen. Durch zeitlich verzögerte Anmeldeversuche bei Falscheingaben lassen sich missbräuchliche Anmeldeversuche erschweren.

(XIV) Cloud-Anwendungen - Anlage 1

Zielobjekt:
Cloud-Anwendungen

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
	1	-	-	-	-	1
	1	-	-	-	-	1
	1	-	-	-	-	1

- › Anforderung betrifft Software: Cloud-Anwendungen
- › 1 Anforderung muss von allen Praxistypen umgesetzt werden

(XIV) Cloud-Anwendungen - Anlage 1






Anforderung Nr. 50

Zielobjekt	Anforderung	Erläuterung
Cloud-Anwendungen – Anbieter	Sicherheit von Cloud-Dienstleistern	Soweit Sozial- oder Gesundheitsdaten im Wege des Cloud-Computing verarbeitet werden sollen, muss der Anbieter der eingesetzten Cloud-Anwendung über ein aktuelles C5-Testat entsprechend § 393 SGB V in Verbindung mit § 384 SGB V verfügen.

- › Fragen Sie den Anbieter nach dem Testat der Cloud-Anwendung.
- › Beachten Sie die in dem Testat aufgeführten "korrespondierende Kriterien für Kunden".
- › Beachten Sie die Anforderungen aus § 393 Abs. 3 Satz 1 Nr. 1 SGB V über die notwendigen "angemessen technische und organisatorische Maßnahmen zur Gewährleistung der Informationssicherheit". In der vertragsärztlichen und vertragszahnärztlichen Versorgung können die die Anforderungen nach § 390 SGB V sein.

(XV) - Medizinische Großgeräte - Anlage 4

Zielobjekt:
Medizinische Großgeräte

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		-	-	-	ggf. 6	
	-	-	-	ggf. 6	-	ggf. 6
	-	-	-	ggf. 6	-	ggf. 6

- › Anforderung betrifft Medizinische Großgeräte
- › Muss von allen Praxistypen umgesetzt werden, die medizinische Großgeräte einsetzen

(XV) Medizinische Großgeräte - Anlage 4

- › Medizinische Großgeräte sind beispielweise:
 - › Röntgengeräte, Computertomograph (CT), Magnetresonanztomograph (MRT), Positronenemissionstomograph (PET)
 - › Linearbeschleuniger /Telecobalt-Gerät
 - › Herzkatheter-Messplätze
 - › Dialysegeräte
 - › Gammakameras
 - › Herz-Lungen-Maschinen

- › Geltende gesetzliche Vorgaben für Medizinprodukte:
 - › Medizinproduktegesetz (nach Richtlinie 93/42/EWG bzw. Verordnung (EU) 2017/745)
 - › Datenschutzgrundverordnung (DSGVO)
 - › Medizinprodukte-Betreiberverordnung (MPBetreibV)

(XV) Medizinische Großgeräte - Anlage 4

Anforderung Nr. 1, 2, 3, ...

Zielobjekt	Anforderung	Erläuterung
Medizinische Großgeräte	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechnigte 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.
Medizinische Großgeräte	Nutzung sicherer Protokolle für die Konfiguration und Wartung	Für die Konfiguration und Wartung von medizinischen Großgeräten müssen sichere Protokolle genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden.
Medizinische Großgeräte	Protokollierung	<p>Es muss festgelegt werden:</p> <ul style="list-style-type: none"> • welche Daten und Ereignisse protokolliert werden sollen, • wie lange die Protokolldaten aufbewahrt werden und <ul style="list-style-type: none"> • wer diese einsehen darf. <p>Generell müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden.</p>

(XV) Medizinische Großgeräte - Anlage 4 cont.

Anforderung Nr. 4, 5 & 6




Zielobjekt	Anforderung	Erläuterung
Medizinische Großgeräte	Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen	Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden.
Medizinische Großgeräte	Deaktivierung nicht genutzter Benutzerkonten	Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden.
Medizinische Großgeräte	Netzsegmentierung	Medizinische Großgeräte sollten von der weiteren IT getrennt werden.

(XV) Medizinische Großgeräte - Anlage 4 - Details

- › Protokollfunktionalitäten der medizinischen Großgeräte richtig konfigurieren und auswerten um Fehlfunktionen und mögliche Sicherheitsvorfälle zu erkennen
- › Verifizieren, dass der Zugriff auf die vernetzte Medizintechnik von außerhalb der Praxis nicht möglich ist
- › Verhindern des Zugriffs durch Deaktivierung ungewollter Dienste und Konfiguration der Firewall
- › Zum Schutz der medizinischen Großgeräte (z.B. bei ausbleibenden Sicherheitsupdates der Hersteller) Isolierung der Geräte von der weiteren IT durch Netzwerksegmente oder -Zonen
- › Die erlaubten Kommunikationsverbindungen auf das notwendige Maß beschränken
- › Trennung der medizinischen Großgeräte im Netzplan (vgl. Anlage 1 – Anforderung 33) nachvollziehbar dokumentieren

(XVI) Dezentrale Komponenten der TI - Anlage 5

Zielobjekt:
Dezentrale
Komponenten
der TI

	Zu erfüllende Anforderungen in Anlage					Gesamt
	1	2	3	4	5	
		-	-	-	-	
	-	-	-	-	9	9
	-	-	-	-	9	9

- › Anforderung betrifft „Dezentrale Komponenten der TI“
- › Muss von allen Praxistypen umgesetzt werden

(XVI) Dezentrale Komponenten der TI - Anlage 5

Anforderung Nr. 1, 2, 3, 4, 5, 6, 7,

Zielobjekt	Anforderung	Erläuterung
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.
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.
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.
Dezentrale Komponenten der TI	Internet Verbindung parallel zur TI Anbindung	Existiert zusätzlich zur TI-Anbindung eine Internet Verbindung, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen.
gehosteter Konnektor	Verbindung absichern	Um die Verbindung zu einem gehosteten Konnektor vor unberechtigtem Zugriff zu schützen, muss ein VPN-Tunnel zwischen Praxis und Konnektor eingerichtet und aufgebaut werden.
TI-Gateway	Beachtung der Vorgaben des TI-Gateway-Anbieters	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch des TI-Gateway-Anbieters konfiguriert und betrieben werden.
Dezentrale Komponenten der TI	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.

(XVI) Dezentrale Komponenten der TI - Anlage 5 cont.

Anforderung Nr. 8 & 9

Zielobjekt	Anforderung	Erläuterung
Dezentrale Komponenten der TI	Zeitnahes Installieren verfügbarer Aktualisierungen	Die TI-Komponenten 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.
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.

(XVI) Dezentrale Komponenten der TI - Anlage 5 - Details

- › Informationen von der Webseite der gematik und von den Herstellern der TI-Komponenten nutzen
- › Installationsprotokoll, die vom Dienstleister erstellten Dokumentation und ggf. weitere relevante Informationen wie Administrationsdaten aushändigen lassen und aufbewahren
- › Konnektor an einem zutrittsgeschützten Ort aufstellen (z. B. (Server-)Raum oder abschließbarer Schrank)
- › Schutz z. B. durch Aktivierung
 - › der verschlüsselnden TLS-Verbindung vom PVS-System zum Konnektor
 - › der Authentisierungsmöglichkeit am Konnektor
- › Bei **paralleler** Installation des Konnektors, ausreichende Funktionen (Firewall, UTM etc.) anderer für die Internetanbindung zuständigen Geräte (Router, etc.) sicherstellen und konfigurieren
- › Regelmäßig auf Updates der TI Komponenten prüfen und zeitnah installieren

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ VORBEREITUNG

➤ HILFESTELLUNGEN ZUR DURCHFÜHRUNG

➤ NACHBEREITUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS





Umsetzungsprozess: Maßnahmenkontrolle

- › Regelmäßige Überprüfung der Maßnahmen auf:
 - › **Umsetzungsstand**
z. B.:
„Können alle anwendbaren Anforderungen bis zum jeweiligen Fristtermin umgesetzt werden?“
 - › **Wirksamkeit**
z. B.:
„Halten sich Angestellte an die Vorgaben und Richtlinien, z. B. den Regelungen zur Nutzung mobiler Geräte?“

Umsetzungsprozess: Gesamtkontrolle

› Regelmäßige Überprüfung der IT-Sicherheit der Praxis aufgrund:

› **Richtlinienaktualisierung**

„Bedarf es aufgrund der (jährlichen) Anpassung der Richtlinie für IT-Sicherheit in der Praxis einer Angleichung der Vorgaben oder Maßnahmen?“

› **Umfeldwandel**

„Bedarf es aufgrund von Änderungen im Praxisalltag, in der Praxis-IT, zusätzlichen Aufgaben oder einer geänderten Rechtslage einer Angleichung der Vorgaben oder Maßnahmen?“

➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ **§ 390 SGB V**

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS



Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

› Es gibt zwei Richtlinien für unterschiedliche Aspekte:

- 1. Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit**
Die in der Richtlinie festzulegenden Anforderungen müssen dem Stand der Technik entsprechen und sind jährlich anzupassen. Die Richtlinie ist für die an der vertragsärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich.
- 2. Zertifizierung vertrauenswürdiger Dienstleister**
IT-Dienstleister können sich auf Basis der o. g. Richtlinie bei der KBV zertifizieren lassen und ihre Kompetenz gegenüber Dritten mittels des ausgestellten Zertifikates vorweisen.



2. Zertifizierung vertrauenswürdiger Dienstleistern (§ 390 Abs. 5 SGB V)

- › Zweiter Aspekt des § 390 SGB V und in Absatz 7 von diesem geregelt
- › Erstellt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
- › Erstellt im Benehmen mit maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen

→ Dank dieser Personenzertifizierung können qualifizierte Dienstleister zur Unterstützung der anforderungsgerechten Umsetzung der „Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ in Anspruch genommen werden.



2. Zertifizierung vertrauenswürdiger Dienstleistern (§ 390 Abs. 7 SGB V)

„Richtlinie zur Zertifizierung nach § 75b Absatz 5 SGB V“
(zukünftig § 390 Absatz 7 SGB V)

- › Veröffentlichung zertifizierter Antragsteller von der KBV und der KZBV

Zertifikatsausstellung

- › Bestehen einer Prüfung zur Umsetzung der Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

oder

- › Anerkennung von Zertifikatsinhabern anderer IT-Sicherheitsstandards



➤ EINLEITUNG

➤ GESETZLICHE RAHMENBEDINGUNGEN

➤ ÄRZTLICHE SCHWEIGEPFLICHT

➤ EUROPÄISCHE DATENSCHUTZGRUNDVERORDNUNG (DSGVO)

➤ § 390 SGB V

➤ RICHTLINIE NACH § 390 SGB V ÜBER DIE ANFORDERUNGEN ZUR
GEWÄHRLEISTUNG DER IT-SICHERHEIT

➤ DIE PRAXIS ALS PATIENT

➤ ANFORDERUNGSUMSETZUNG

➤ ZERTIFIZIERUNG VERTRAUENSWÜRDIGER DIENSTLEISTERN

➤ ABSCHLUSS





Die Praxis als Patient - Durchführung

1. **Anamnese:** Praxistyp festlegen
2. **Diagnose:** Anzuwendende Anlagen festlegen
3. **Behandlungsplan:** Anzuwendende Anforderungspunkte festlegen
4. **Therapie:** Maßnahmen festlegen und umsetzen
5. **Mitbehandlung:** Dienstleister beauftragen/anweisen
6. **Verlaufskontrolle:** Maßnahmenwirksamkeit prüfen
7. **Folgetermin:** auf Änderungen reagieren; spätestens nach einem Jahr eine überarbeitete Richtlinie



Take-Home-Message Fortbildung „IT-Sicherheit in der Praxis“

1. Geltende Anforderungen aufgrund der Praxisgröße und den genutzten Systemen identifizieren
2. Umgesetzte Maßnahmen dokumentieren und fehlende Maßnahmen umsetzen
3. Eine ständig aktualisierte Liste von Hilfsmitteln zur Umsetzung kann auf der Webseite der KBV gefunden werden.

→ Beauftragen Sie einen qualifizierten Dienstleister, der Sie bei bestimmten Punkten unterstützt (z. B. der Aufstellung der erforderlichen Anforderungen und möglichen Maßnahmen) oder den kompletten Prozess für Sie übernimmt.

Tipp

Autoren

Kontakt

Kassenärztliche Bundesvereinigung
Dezernat Digitalisierung und IT
Herbert-Lewin-Platz 2
10623 Berlin



Alle Informationen auch unter
<https://www.kbv.de/html/it-sicherheit.php>

und
<https://hub.kbv.de/display/itsrl>



***Wir sind
für Sie nah.***

rettet-die-praxen.de