

IT-Sicherheitsrichtlinie nach § 390 SGB V – Checkliste zur Umsetzung

Die aktualisierte IT-Sicherheitsrichtlinie wurde am 1. Juli 2025 veröffentlicht und trat am 2. Juli 2025 in Kraft. Die neuen bzw. geänderten Anforderungen sind **ab dem 2. Januar 2026 verpflichtend** umzusetzen und betrifft die Praxisleitung einschließlich aller Mitarbeiter einer Zahnarztpraxis, welche sich ständig mit der Datenverarbeitung befassen.

Diese Checkliste „**Mittlere Praxis bis 20 Personen**“ hilft Ihnen zur Orientierung der Anlagen 1, Anlage 2 und Anlage 5. Die Anlagen 4 benötigen Sie nur bei der Nutzung von medizinischen Großgeräten. Detaillierte Hinweise finden Sie auf der Website der KZBV sowie in der o. g. Richtlinie.

Hinweis:

- Ⓛ Es besteht Handlungsbedarf
- ✓ Alle IT-Sicherheitsanforderungen erfüllt
- Ⓞ Nicht für die Zahnarztpraxis zutreffend

Praxisnummer:	
Praxisname:	
✉:	
☎:	

Anlage	Nr.	Anforderung	Erläuterung	
1	1	Geregelte Einarbeitung neuer Mitarbeitender	Mitarbeitende müssen zu Beginn ihrer Beschäftigung in ihre neuen Aufgaben eingearbeitet werden. Die Mitarbeitenden müssen über bestehende Regelungen, Handlungsanweisungen und Verfahrensweisen informiert werden.	
		Umsetzung		
		Einarbeitung der neuen Mitarbeiter in neue Aufgaben:		
		Mit welchen IT-Systemen arbeiten wir?		
		Wer hat im Bereich der IT-Systeme welche Aufgaben?		
		Ist mein Personal über die Handlungsanweisungen informiert?		
		Ist mein Personal über die Regelungen informiert?		
		Ist mein Personal über Verfahrensweisen informiert?		
Anlage	Nr.	Anforderung	Erläuterung	
1	2	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 ausscheidenden Mitarbeitenden bekannt waren oder von diesen genutzt wurden, müssen geändert oder vernichtet werden. Vor der Verabschiedung muss noch einmal auf die fortdauernden Verschwiegenheitsverpflichtungen hingewiesen werden.	
		Umsetzung		
		Rücknahme aller betrieblichen Unterlagen:	Diensttelefon Zutrittskarte Praxisschlüssel Schrankschlüssel Sonstige:	
		Änderung Passwörter folgender Geräte:	PIN für Serverschrank Räume mit Zahlenschloss Allgemeine Benutzerkonten, z.B. an Geräten Sonstige:	
Fortdauernde Erinnerung an Verschwiegenheitspflicht:		Schriftliches Dokument überreicht, das auf Vertragsregelung und deren Fortdauer hinweist		

Anlage	Nr.	Anforderung	Erläuterung
1	3	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 Zugangsberichtigungen sind so restriktiv wie möglich zu halten.
		Umsetzung	
		Regelung der Belehrung zur Verpflichtung externer Dienstleister auf Gesetze, Vorschriften und interne Regelungen:	Unterschrift Belehrungsbogen Unterschrift Arbeitsschutz Unterschrift Gesundheitsschutz Unterschrift Datenschutz Sonstige:
		Regelung der Beaufsichtigung:	Arbeitsraum zuweisen Regelmäßige Prüfung der vereinbarten Tätigkeitsausführung des externen Dienstleisters
		Regelung der minimalen Berechtigungen:	Regelmäßige Prüfung der Tätigkeitsausführung des externen Dienstleisters, dass er keine sensiblen Daten einsehen kann
Anlage	Nr.	Anforderung	Erläuterung
1	4	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.
		Umsetzung	
		Vorbereitete Vertraulichkeitsvereinbarung unterschreiben lassen und belehren:	Unterschrift Vertraulichkeitsvereinbarung Belehrung Vertraulichkeitsvereinbarung
Anlage	Nr.	Anforderung	Erläuterung
1	5	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.
		Umsetzung	
		Vereinbarung treffen über die Verpflichtung aller Mitarbeiter auf Gesetze, Vorschriften und Regelungen	Unterschrift Standard-Dokument, mit dem Hinweis, welcher Rechtsrahmen gilt und das dieser einzuhalten ist Als Anlage zum Arbeitsvertrag beigefügt Sonstige:
		Dokumentation der Aufgaben und Zuständigkeiten:	Stellenbeschreibung um Zuständigkeiten in der Praxis-IT ergänzt
		Hinweis auf interne Nutzung der erhaltenen Informationen:	Verschwiegenheitsvereinbarung als Anlage zum Arbeitsvertrag, Geltung über das Vertragsende hinaus aus, siehe Anlage 1-2
Anlage	Nr.	Anforderung	Erläuterung
1	6	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.

zu Nr. 6	Umsetzung			
	Regelmäßige Schulungen zu IT-Themen organisieren:	Schulungsplan mit Turnus festlegen (z. B. mit Hilfe der von der KZV Sachsen angebotenen Mitarbeiterschulungen) Sonstige:		
	Kenntnisstand mit geeigneten Mitteln absichern:	IT-Wissen regelmäßig in Kurzschulungen auffrischen Bei Veränderungen (z. B. gesetzlich, neue Technik in der Praxis, ...) gezielt schulen		
	Weiterbildung im Rahmen der Tätigkeit anbieten:	Auf externe Schulungen zurückgreifen (z. B. mit Hilfe der von der KZV Sachsen angebotenen Schulungen zur Telematik, IT-Sicherheit) Sonstige Schulungen der Hersteller und Onlinekurse nutzen		
Anlage	Nr.	Anforderung	Erläuterung	
1	7	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.	
		Umsetzung		
		Vertrauenswürdigkeit anhand der Unterlagen prüfen:	Auswertung Arbeitszeugnisse Auswertung Beurteilungen und ggf. Führungszeugnis Sonstige:	
	Abstimmung, ob Angaben glaubhaft sind:	Alle Beteiligten kennen alle Unterlagen Gemeinsame Bewertung aller Unterlagen Protokoll angefertigt und abgelegt		
Anlage	Nr.	Anforderung	Erläuterung	
1	8	Sensibilisierung der Praxisleitung für Informationssicherheit	Die Praxisleitung muss ausreichend für Sicherheitsfragen sensibilisiert werden. Sicherheitskampagnen oder andere Schulungsmaßnahmen müssen von der Praxisleitung unterstützt werden.	
		Umsetzung		
		Regelmäßige Schulungen für die Praxisleitung organisieren:	Schulungen aus dem Fortbildungskalender der KZV Sachsen Sonstige:	
	Unterstützung für Schulungen und Kampagnen:	Teamschulungen von der KZV Sachsen Teamschulungen externer Partner		
Anlage	Nr.	Anforderung	Erläuterung	
1	9	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.	
		Umsetzung		
	Einweisung in sicheren Umgang mit IT-Komponenten:	Einweisung in Passwort- und Anmeldeeregeln Einweisung zur Sperrung ungenutzter Geräte Einweisung bei der Entnahme von Dokumenten aus dem Drucker Sonstige:		

Anlage	Nr.	Anforderung	Erläuterung		
1	10	Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit	Alle Mitarbeitenden sollten entsprechend ihren Aufgaben und Verantwortlichkeiten zu Informationssicherheitsthemen geschult werden.		
		Umsetzung Durchführung regelmäßiger Schulungen für Informationssicherheit: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Schulungen aus dem Fortbildungskalender der KZV Sachsen durchgeführt Schulungen externer Partner (online) durchgeführt Sonstige:</td> </tr> </table>			Schulungen aus dem Fortbildungskalender der KZV Sachsen durchgeführt Schulungen externer Partner (online) durchgeführt Sonstige:
	Schulungen aus dem Fortbildungskalender der KZV Sachsen durchgeführt Schulungen externer Partner (online) durchgeführt Sonstige:				
Anlage	Nr.	Anforderung	Erläuterung		
1	11	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.		
		Umsetzung Prüfen, ob eine Firewall vorhanden ist: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Physischer Konnektor in Reihenanbindung geprüft <i>oder</i> separate Hardware-Firewall geprüft</td> </tr> </table>			Physischer Konnektor in Reihenanbindung geprüft <i>oder</i> separate Hardware-Firewall geprüft
			Physischer Konnektor in Reihenanbindung geprüft <i>oder</i> separate Hardware-Firewall geprüft		
Dokumentierte Konfiguration mit ein- und ausgehenden Regeln einrichten: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Betreuung durch Dienstleister (<i>dringend angeraten</i>) Sichere Regeln mit minimaler Durchlässigkeit eingerichtet</td> </tr> </table>			Betreuung durch Dienstleister (<i>dringend angeraten</i>) Sichere Regeln mit minimaler Durchlässigkeit eingerichtet		
	Betreuung durch Dienstleister (<i>dringend angeraten</i>) Sichere Regeln mit minimaler Durchlässigkeit eingerichtet				
Anlage	Nr.	Anforderung	Erläuterung		
1	12	Dokumentation des Netzes	Das interne Netz ist inklusive eines Netzplanes zu dokumentieren.		
		Umsetzung Dokumentation des Netzplanes: <i>Empfehlung: Mit Dienstleister gemeinsam erarbeiten</i> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Alle Geräte erfasst und dokumentiert Standort dokumentiert VLAN dokumentiert IP-Adresse dokumentiert Sonstige:</td> </tr> </table>			Alle Geräte erfasst und dokumentiert Standort dokumentiert VLAN dokumentiert IP-Adresse dokumentiert Sonstige:
	Alle Geräte erfasst und dokumentiert Standort dokumentiert VLAN dokumentiert IP-Adresse dokumentiert Sonstige:				
Anlage	Nr.	Anforderung	Erläuterung		
1	13	Grundlegende Authentisierung für den Netzmanagement-Zugriff	Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden.		
		Umsetzung Absicherung des Management-Zugriffs: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Rollen und Nutzer angelegt Active Directory Anbindung geprüft</td> </tr> </table>			Rollen und Nutzer angelegt Active Directory Anbindung geprüft
			Rollen und Nutzer angelegt Active Directory Anbindung geprüft		
Änderung der Standard-Zugangsdaten: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"></td> <td>Standardkennwörter geändert Standardkennwörter sicher dokumentiert</td> </tr> </table>			Standardkennwörter geändert Standardkennwörter sicher dokumentiert		
	Standardkennwörter geändert Standardkennwörter sicher dokumentiert				
Anlage	Nr.	Anforderung	Erläuterung		
1	14	Installation von Updates	Updates müssen zeitnah nach ihrer Veröffentlichung installiert werden.		

	zu Nr. 14	Umsetzung	
		Festlegung fester Prüfzyklen:	Prüfzeitraum festgelegt Prüfung auf aktuelle Software von Rechner und Geräten
		Prüfen der Lizenzen und Verträge:	Wartungs- und Lizenzverträge geprüft, um Updates zu erhalten
Anlage	Nr.	Anforderung	Erläuterung
1	15	Verantwortlichkeit für Updates	Es muss festgelegt werden, wer die Updates installiert. Das ausgewählte Personal muss geschult und entsprechend berechtigt werden.
		Umsetzung	
		Festlegung der Zuständigkeit für Updates:	Aufgabenübertragung per vertraglicher Vereinbarung
		Schulungen zu Updates:	Wahl eines externen Anbieters oder Online-Kurses (<i>falls Aufgabe intern erfüllt wird</i>)
		Vergabe von Berechtigungen:	Berechtigungen dokumentiert Berechtigungen werden regelmäßig geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	16	Identifizierung ausbleibender Updates	Hardware, eingesetzte Betriebssysteme, eingesetzte Anwendungen und Dienste, die keine Sicherheitsupdates mehr erhalten, müssen identifiziert werden.
		Umsetzung	
		Inventarisierung der Hardware und Software:	Bestandverzeichnis angelegt Bestandsverzeichnis verfügbar gemacht
		Erstellung einer Liste aller Geräte mit Support-Enddatum:	Liste erstellt und gesichert
		Regelmäßige Prüfung:	Systeme, welche noch Sicherheitsupdates erhalten, wurden geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	17	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.
		Umsetzung	
		Identifizierung der Altsysteme:	In Bestandsverzeichnis übernommen Vermerk der Support-Ende-Daten
		Ausmusterung oder Netztrennung:	Entscheidung dokumentiert wird regelmäßig geprüft
		Nutzung eines eigenen Netzsegmentes:	Geräte erfasst und dokumentiert Adressen erfasst und dokumentiert Daten erfasst und dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	18	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.

	zu Nr. 18	Umsetzung	
		Deaktivieren von Mikrofon und Kamera am Rechner:	In BIOS/UEFI deaktiviert oder physisch abgeklebt Auf aktuelle Software von Rechner und Geräten geprüft
		Überprüfen von Mikrofon und Kamera:	Deaktivierung aller vorhandenen Mikrofone und Kameras an Geräten geprüft Überprüfung dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	19	Abmelden nach Aufgabenerfüllung	Nach Ende der Nutzung immer den Zugang zum Gerät sperren oder abmelden.
		Umsetzung	
		Festlegung einer klaren Regelung zum Abmelden:	Abmelderegulung festgelegt und dokumentiert Sonstige:
		Überprüfung der klaren Regelung zum Abmelden:	Abmelderegulung wird regelmäßig geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	20	Einsatz von Virenschutzprogrammen	Aktuelle Virenschutzprogramme sind einzusetzen.
		Umsetzung	
		Installation eines aktuellen Virenschutzprogrammes auf allen Rechnern:	Installation und Versorgung mit Updates geprüft
		Verwaltung und Erkennung:	Alle Rechner mit zentraler Plattform oder Web-Plattform erkannt/verwaltet Protokollierung geprüft
		Prüfung von Funden:	Festgelegt, wer / wann / wie Protokolle der Virenprüfung auswertet
Anlage	Nr.	Anforderung	Erläuterung
1	21	Regelmäßige Datensicherung	Sämtliche relevante Daten sind regelmäßig zu sichern.
		Umsetzung	
		Datensicherungsziel festlegen:	Auf separates Gerät oder NAS bzw. Cloud Externe Festplatte NAS bzw. Cloud Sonstige:
		Definieren, welche Daten gesichert werden:	Alle Praxisabläufe auf anfallende Daten geprüft <input type="checkbox"/> Geprüft, wo diese abgelegt sind Geprüft, wie sie zu sichern sind
Anlage	Nr.	Anforderung	Erläuterung
1	22	Schutz der Datensicherung	Die Datensicherung muss vor unbefugtem Zugriff gesichert werden.
		Umsetzung	
		Schutz der Datensicherung vor unbefugtem Zugriff:	Backups verschlüsselt <i>oder</i> Backups an sicheren Standorten abgelegt

Anlage	Nr.	Anforderung	Erläuterung
1	23	Art der Datensicherung	Es muss festgelegt werden, wie die Daten gesichert werden.
		Umsetzung	
		Festlegung der Sicherungsart von Daten:	Sicherung der Daten Full/Incremental dokumentiert Sicherung der lokalen/externen Daten dokumentiert Sicherungsmedien dokumentiert Sonstige:
		Schriftliche Ablage der Sicherungsart:	Sicherungsart dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	24	Verantwortliche der Datensicherung	Es muss festgelegt werden, wer für die Datensicherung zuständig ist.
		Umsetzung	
		Festlegung der Zuständigkeit für die Datensicherung:	IT-Dienstleister Zahnmedizinische Fachangestellte, o.ä. Praxisleitung Sonstige Personen:
		Festlegung der Vertretungsregelung:	Vertretungsregelung festgelegt, vereinbart und dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	25	Test der Datensicherung	Es sollte getestet werden, ob gesicherte Daten funktionsfähig und vollständig vorhanden sind.
		Umsetzung	
		Regelmäßiger Test der Datensicherung:	Test monatlich <i>oder</i> Test quartalsweise Testwiederherstellung durchgeführt
		Dokumentation des Testergebnisses:	Testergebnis dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	26	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.
		Umsetzung	
		Konfiguration der Benutzer und Rollen in der Praxissoftware:	Benutzerkonten mit restriktiven Rollen eingerichtet eHBA-Nutzung einschränkt
		Dokumentation und regelmäßige Prüfung der Zugriffe:	Zugriffe dokumentiert Zugriffe regelmäßig geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	27	Konfiguration von Synchronisationsmechanismen	Die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten sollte vollständig deaktiviert werden.

	zu Nr. 27	Umsetzung	
		Deaktivierung der Cloud-Synchronisierung:	Deaktivierung durchgeführt (Windows: Einstellungen > Konten > Cloud-Synchronisierung deaktivieren)
Anlage	Nr.	Anforderung	Erläuterung
1	28	Datei- und Freigabeberechtigungen	Berechtigungen und Zugriffe sind pro Personengruppe und pro Person zu regeln.
		Umsetzung	
		Anlage der Matrix mit Mitarbeitern und Berechtigungen zu Ordnern/Dateien:	Matrix mit Mitarbeitern und Berechtigungen zu Ordnern/Dateien angelegt
		Vergabe der Berechtigungen pro Gruppe oder Person sowie die Dokumentation:	Berechtigungen pro Gruppe oder Person vergeben Berechtigungen dokumentiert
		Regelmäßige Prüfung der Berechtigungen:	Berechtigungen regelmäßig geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	29	Datensparsamkeit	So wenige personenbezogene Daten wie möglich sind zu verwenden.
		Umsetzung	
		Überprüfung der Erfassung von notwendigen Patientendaten:	Erfassung der notwendigen Patientendaten geprüft
		Löschen von nicht mehr benötigten Daten:	Nicht mehr benötigte Daten gelöscht
Anlage	Nr.	Anforderung	Erläuterung
1	30	Verwendung der SIM-Karten-PIN	SIM-Karten sind durch eine PIN zu schützen. Super-PIN/PUK sind nur durch Verantwortliche anzuwenden.
		Umsetzung	
		Schutz der SIM-Karten mit PIN:	SIM-Karte mit PIN geschützt
		Standard-PIN ändern, Super-PIN/PUK sicher verwahren:	Standard-PIN geändert Super-PIN/PUK sicher verwahrt
Anlage	Nr.	Anforderung	Erläuterung
1	31	Sichere Grundkonfiguration für mobile Geräte	Auf mobilen Endgeräten sollten die strengsten bzw. sichersten Einstellungen gewählt werden, weil auch auf mobilen Geräten das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss.
		Umsetzung	
		Optimierung der Sicherheitseinstellungen auf mobilen Geräten:	Sicherheitseinstellungen auf mobilen Geräten optimiert
		Durchführung und Dokumentation der Sicherheits-Checkliste:	Sicherheits-Checkliste durchgeführt Ergebnisse der Sicherheits-Checkliste dokumentiert
Anlage	Nr.	Anforderung	Erläuterung
1	32	Verwendung eines Zugriffsschutzes	Geräte sind mit einem komplexen Gerätesperrcode zu schützen.
		Umsetzung	
		Schutz aller Smartphones und Tablets mit Gerätesperre:	Sicherheitseinstellungen auf mobilen Geräten optimiert
		Festlegung eines komplexen Codes (mind. 6-stellig) oder über Biometrie zum Schutz:	Schutz mit mind. 6-stelligem Code eingerichtet <i>und/oder</i> Schutz über Biometrie eingerichtet

Anlage	Nr.	Anforderung	Erläuterung
1	33	Datenschutz-Einstellungen	Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen der Endgeräte sollte in den Einstellungen restriktiv auf das Notwendigste eingeschränkt werden.
		Umsetzung	
		Restriktive Konfiguration der Datenschutz-Einstellungen:	Einstellungen der restriktiven Konfiguration überprüft (Einstellungen > Datenschutz und Sicherheit > Apps prüfen)
Anlage	Nr.	Anforderung	Erläuterung
1	34	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.
		Umsetzung	
		Dokumentation Kontaktdaten des Mobilfunkanbieters:	Kontaktdaten des Mobilfunkanbieters dokumentiert: Liste mit Anbieter Kundenservice Kontonummern an sicherer Stelle verwalten
		Planung eines Notfall-Prozesses (Bsp. Handyverlust):	Notfall-Prozess geplant Notfalldokument abgelegt
Anlage	Nr.	Anforderung	Erläuterung
1	35	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden.
		Umsetzung	
		Aktivierung der Sicherheitsmechanismen auf Mobiltelefonen:	Sicherheitsmechanismen auf Mobiltelefonen aktiviert: Gerätesperre Verschlüsselung Fernlöschung automatische Sperre
		Dokumentation der Standard-Konfiguration für neue Geräte:	Standard-Konfiguration für neue Geräte dokumentiert (Überprüfung bei Ausgabe)
Anlage	Nr.	Anforderung	Erläuterung
1	36	Schutz vor Schadsoftware	Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden.
		Umsetzung	
		Festlegung einer Regelung zum Schutz:	Anweisung an Mitarbeiter – informiert/festgelegt: Träger vor Nutzung mit Virenschutz scannen
Anlage	Nr.	Anforderung	Erläuterung
1	37	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.
		Umsetzung	
		Erfassung und Bereitstellung der Vorgaben zur Kennzeichnung:	Versand-ID vergeben Versand-ID im Ausgangsbuch dokumentiert

Anlage	Nr.	Anforderung	Erläuterung	
1	38	Sichere Versandart und Verpackung	Zum Versand von Datenträgern sollten Versandanbieter mit sicherem Nachweis-System und eine möglichst manipulationssichere Versandart und Verpackung gewählt werden.	
		Umsetzung		
		Verwendung einer sicheren Versandart:	Nutzung einer sicheren Versandart: Versand mit Nachweis (Einschreiben, DHL, o. ä.) manipulationssichere Verpackung	
		Erfassung der Sendungen im Ausgangsbuch:	Sendungen im Ausgangsbuch erfasst Sendungsverfolgung dokumentiert	
Anlage	Nr.	Anforderung	Erläuterung	
1	39	Sicheres Löschen der Datenträger vor und nach der Verwendung	Alle Datenträger müssen nach ihrer Verwendung durch die jeweiligen Mitarbeitenden sicher und vollständig gelöscht werden.	
		Umsetzung		
		Sicheres Löschen der Wechseldatenträger:	Verwendung von Festplattenlöschprogrammen (DBAN, Secure Erase)	
Anlage	Nr.	Anforderung	Erläuterung	
1	40	Sichere Konfiguration der E-Mail-Clients	Bei der Konfiguration der E-Mail-Clients muss mindestens Folgendes berücksichtigt werden: <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 	
		Umsetzung		
		Sicheres Konfigurieren der E-Mail-Clients:	E-Mail-Clients sicher konfiguriert: Anhang-Scanning aktiviert HTML deaktiviert TLS erzwungen	
Anlage	Nr.	Anforderung	Erläuterung	
1	41	Umgang mit Spam durch Benutzende	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.	
		Umsetzung		
		Schulung der Mitarbeiter im Spam-Umgang:	Mitarbeiterschulung: Keine Antwort auf Spam Mitarbeiterschulung: Links nicht anklicken	
		Festlegung des Umgangs mit verdächtigen Mails:	Verdächtige E-Mails werden archiviert Verdächtige E-Mails werden dem IT-Dienstleister zur Verfügung gestellt	
Anlage	Nr.	Anforderung	Erläuterung	
1	42	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.	
		Umsetzung		
		Installation der Apps nur aus offiziellen Stores:	Einschränkung auf App Store Einschränkung auf Play Store Fremde Quellen deaktiviert	

Anlage	Nr.	Anforderung	Erläuterung
1	43	Sichere Speicherung lokaler App-Daten	Es sollten nur Apps genutzt werden, die Dokumente verschlüsselt und lokal abspeichern.
		Umsetzung	
		Nur Nutzung der Apps mit verschlüsselter Speicherung:	App-Dokumentation geprüft Store-Beschreibungen geprüft
Anlage	Nr.	Anforderung	Erläuterung
1	44	Verhinderung von Datenabfluss	Der Zugriff von Apps auf vertrauliche Daten muss durch restriktive Datenschutz-Einstellungen soweit wie möglich eingeschränkt werden.
		Umsetzung	
		Beschränkung der Zugriffe von Apps auf sensible Daten:	Datenschutz-Einstellungen: Nur notwendige Apps erlauben
		Einrichtung minimaler App-Berechtigungen:	Apps-Berechtigungen eingerichtet Apps greift nur auf nötige Daten zu
Anlage	Nr.	Anforderung	Erläuterung
1	45	Authentisierung bei Webanwendungen	Sollten Sie als Praxis einen Webdienst anbieten: 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.
		Umsetzung	
		Konfiguration der Authentisierung für Webanwendungen:	Angemessene Authentisierungsmethode ausgewählt (Zugriff nicht nur durch Klick auf einen Link möglich oder durch Eingabe einfach zugänglicher Daten) Auswahlprozess dokumentiert Grenzwert für fehlgeschlagene Anmeldeversuche festgelegt
Anlage	Nr.	Anforderung	Erläuterung
1	46	Schutz vertraulicher Daten	Sollten Sie als Praxis einen Webdienst anbieten: 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.
		Umsetzung	
		Verschlüsselte Speicherung der Zugangsdaten:	Passwörtern mit salted hash gespeichert Aktuelle Hash-Algorithmen werden genutzt
Anlage	Nr.	Anforderung	Erläuterung
1	47	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.
		Umsetzung	
		Implementierung einer Web Application Firewall (WAF):	Web Application Firewall (WAF) implementiert
		Testung und Anpassung der Web Application Firewall (WAF):	Web Application Firewall (WAF) getestet Web Application Firewall (WAF) angepasst Im Protokoll erfasst und ausgewertet

Anlage	Nr.	Anforderung	Erläuterung
2	1	Alarmierung und Logging	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.
		Umsetzung	
		Aktivierung der Log-Funktion auf allen Geräten:	Funktion, Ziel und Log Levels geprüft
		Zentrale Organisation der Log-Erfassung:	Server-Dienst aktiv und abgesichert
2	2	Nutzung von verschlüsselten Kommunikationsverbindungen	Benutzende sollten darauf achten, dass zur Verschlüsselung von Kommunikationsverbindungen kryptografische Algorithmen nach dem Stand der Technik wie z.B. TLS verwendet werden.
		Umsetzung	
		Prüfung der externen Datenverbindungen:	Schützenswerte Daten werden nur über gesicherte Verbindungen übertragen
2	3	Restriktive Rechtevergabe	Rechte sollten so restriktiv wie möglich nach dem Need-to-know Prinzip vergeben werden.
		Umsetzung	
		Prüfung der Übereinstimmung von Rollen, Aufgaben und Berechtigungen:	Übereinstimmung von Rollen geprüft Aufgaben geprüft Berechtigungen geprüft
2	4	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.
		Umsetzung	
		Konfiguration von Kerberos in Windows-Netzen:	Konfiguration durchgeführt
2	5	Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeitende zur Benutzung von mobilen Geräten erstellt werden.
		Umsetzung	
		Mobile Geräte - Erstellung einer verbindlichen Nutzervereinbarung für Mitarbeiter:	Vereinbarung erstellt und unterzeichnet
2	6	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.
		Umsetzung	
		Mobile Geräte - Erstellung einer verbindlichen Sprachsteuerungs-Nutzervereinbarung für Mitarbeiter:	Vereinbarung erstellt und unterzeichnet

Anlage	Nr.	Anforderung	Erläuterung
2	7	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.
		Umsetzung	
		Mobiltelefon - Erstellung einer Nutzungs- und Sicherheitsrichtlinie:	Vereinbarung erstellt und unterzeichnet
Anlage	Nr.	Anforderung	Erläuterung
2	8	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.
		Umsetzung	
		Mobiltelefon – Erstellung von Regelungen zur verschlüsselten und sicheren Datenübertragung:	Vereinbarung erstellt und unterzeichnet
Anlage	Nr.	Anforderung	Erläuterung
2	9	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.
		Umsetzung	
		Wechseldatenträger – Erstellung von Nutzerregelung:	Vereinbarung erstellt und unterzeichnet Festgelegt, wie Wechseldatenträger mitgenommen werden Festgelegt, zu welchem Anlässen Wechseldatenträger mitgenommen werden
Anlage	Nr.	Anforderung	Erläuterung
2	10	Minimierung und Kontrolle von App-Berechtigungen	Die Berechtigungen von Apps sind auf das notwendige Minimum einzuschränken bzw. zu vergeben.
		Umsetzung	
		Explizite Prüfung und Dokumentation der App-Berechtigungen:	Abgleich der Berechtigungen mit dem Zweck der App App-Berechtigungen dokumentiert
		Regelmäßige Nachprüfung der App-Berechtigungen:	App-Berechtigungen nach Updates auf Änderungen geprüft

Anlage	Nr.	Anforderung	Erläuterung
5	1	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.
		Umsetzung	Informationen der gematik GmbH für die Installation der TI-Komponenten berücksichtigt Planung der Installation der TI-Komponenten, gemäß den geltenden technischen sowie gesetzlichen Vorgaben Durchführung der Installation der TI-Komponenten, gemäß den geltenden technischen sowie gesetzlichen Vorgaben
5	2	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.
		Umsetzung	Anwender- und Administrationsdokumentationen der gematik GmbH und Hersteller der IT-Komponenten wurden berücksichtigt Sicherer Betrieb der TI-Komponenten wird gewährleistet
5	3	Schutz vor unberechtigtem physischem Zugriff	Die TI-Komponenten in der Praxis müssen entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter geschützt werden.
		Umsetzung	Schutz des Zugriffs Unberechtigter auf TI-Komponenten wird gewährleistet
5	4	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.
		Umsetzung	Maßnahmen ergriffen, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen Maßnahmen dokumentiert Maßnahmen werden regelmäßig auf Aktualität geprüft
5	5	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.
		Umsetzung	VPN-Tunnel zwischen Praxis und Konnektor eingerichtet Schutz vor unberechtigtem Zugriff wird gewährleistet
5	6	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.
		Umsetzung	Konfiguration der TI-Komponenten entsprechend den Vorgaben des TI-Gateway-Anbieters angepasst Konfigurationseinstellung geprüft

Anlage	Nr.	Anforderung	Erläuterung
5	7	Geschützte Kommunikation mit dem Konnektor/TI-Gateway	Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden.
		Umsetzung	Authentisierungsmerkmale für die Clients erstellt Einstellungen und Konfiguration angepasst Konfigurationseinstellung geprüft Geschützte Kommunikation mit dem Konnektor/TI-Gateway wird gewährleistet
Anlage	Nr.	Anforderung	Erläuterung
5	8	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.
		Umsetzung	TI-Komponenten werden regelmäßig geprüft und aktualisiert verfügbare Aktualisierungen der TI-Komponenten werden zeitnah installiert Funktion für automatische Updates ist aktiviert
Anlage	Nr.	Anforderung	Erläuterung
5	9	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 die Praxis auch ohne ihre Dienstleister die Daten kennt.
		Umsetzung	Administrationsdaten/Passwörter für den Administrator-Zugang dokumentiert Administrationsdaten/Passwörter für den Administrator-Zugang sicher aufbewahrt Zugriff auf Administrationsdaten/Passwörter, ohne Unterstützung des Dienstleisters, ist gewährleistet

Ort:	_____
Datum:	_____
Praxisstempel/ Unterschrift:	_____