Checkliste IT-Sicherheitsrichtlinie

nach § 390 SGB V für Zahnarztpraxen – Prüfgrundlage für den denkkontor § 390 Check

Praxis _____ Datum der Prüfung _____ Prüfer (denkkontor) _____

1. Praxisgröße bestimmen

Maßgeblich ist die Zahl der Personen, die ständig mit der Datenverarbeitung betraut sind. Daraus ergibt sich, welche Anlagen geprüft werden.

☐	**Praxis** – bis 5 Personen	Anlage 1 + Anlage 5
☐	**Mittlere Praxis** – 6 bis 20 Personen	Anlage 1 + 2 + 5
☐	**Großpraxis** – mehr als 20 Personen bzw. mit Datenverarbeitung im großen Umfang	Anlage 1 + 2 + 3 + 5
☐	**Zusätzlich:** Praxis betreibt medizinische Großgeräte (z. B. DVT, CT)	+ Anlage 4

So arbeiten Sie mit der Liste: Kreuzen Sie je Anforderung den Status und die Zuständigkeit an (DK = denkkontor, Praxis, Dritte = z. B. PVS-Hersteller). Wo eine denkkontor-Leistung genannt ist, kann diese die Anforderung ganz oder teilweise abdecken. Offene Punkte übernehmen wir im § 390 Check in Ihren Maßnahmenplan. Die geänderten Anforderungen sind seit 2. Januar 2026 verbindlich.

Anlage 1 Grundanforderungen

alle Praxen

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
Personal				
1.1	**Geregelte Einarbeitung neuer Mitarbeitender** Neue Mitarbeitende werden eingearbeitet und über Regeln und Abläufe informiert. denkkontor: Vorlage im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.2	**Geregeltes Vorgehen beim Weggang von Mitarbeitenden** Schlüssel, Geräte und Zugänge werden zurückgegeben bzw. gesperrt, bekannte Passwörter geändert. denkkontor: Zugänge sperren	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.3	**Regeln für den Einsatz von Fremdpersonal** Externe halten sich an dieselben Regeln, werden in sensiblen Bereichen begleitet und erhalten nur nötige Zugriffe.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.4	**Vertraulichkeitsvereinbarung mit Fremdpersonal** Externe unterschreiben eine Vertraulichkeitsvereinbarung, bevor sie Zugriff erhalten. denkkontor: Vorlage im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.5	**Aufgaben und Zuständigkeiten festgelegt** Aufgaben und Zugriffsrechte der Mitarbeitenden sind dokumentiert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.6	**Qualifikation des Personals** Mitarbeitende werden regelmäßig zur eingesetzten IT geschult. denkkontor: Beratung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.7	**Vertrauenswürdigkeit bei der Einstellung** Bei Neueinstellungen wird auf Vertrauenswürdigkeit geachtet, z. B. Zeugnisse prüfen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Sensibilisierung & Schulung				
1.8	**Praxisleitung ist für Informationssicherheit sensibilisiert** Die Praxisleitung kennt die Risiken und unterstützt Schulungsmaßnahmen. denkkontor: Beratung im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
1.9	**Einweisung in den sicheren Umgang mit IT** Alle Mitarbeitenden und Externen werden in die sichere Nutzung ihrer IT eingewiesen. denkkontor: Beratung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.10	**Schulungen zur Informationssicherheit** Mitarbeitende werden passend zu ihren Aufgaben geschult – z. B. zu Phishing. denkkontor: Beratung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
	Netzwerksicherheit			
1.11	**Absicherung des Internetzugangs (Firewall)** Eine Firewall blockiert unerlaubte Zugriffe von außen und lässt nur erlaubte Verbindungen zu. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.12	**Dokumentation des Netzes** Das interne Netz ist dokumentiert, inklusive Netzplan. denkkontor: Netzplan im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.13	**Geschützter Zugang zur Netzwerkverwaltung** Router, Switches & Co. sind nur mit Anmeldung administrierbar. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
	Patch- & Änderungsmanagement			
1.14	**Updates werden zeitnah installiert** Sicherheitsupdates werden kurz nach Erscheinen eingespielt. denkkontor: Managed Software Update	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.15	**Zuständigkeit für Updates geregelt** Es ist festgelegt, wer Updates installiert. denkkontor: Managed Software Update	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.16	**Geräte ohne Updates erkannt** Hard- und Software ohne Sicherheitsupdates (z. B. veraltetes Windows) ist bekannt. denkkontor: Systemüberwachung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.17	**Ausmustern oder Abtrennen veralteter Systeme** Systeme ohne Updates werden ersetzt oder in ein eigenes Netzsegment verschoben. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
	Endgeräte			
1.18	**Mikrofone und Kameras abgesichert** Mikrofone und Kameras sind standardmäßig aus und werden nur bei Bedarf eingeschaltet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.19	**Abmelden bzw. Sperren nach der Arbeit** Rechner werden nach der Nutzung gesperrt oder abgemeldet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.20	**Aktueller Virenschutz** Auf allen Geräten läuft ein aktueller Virenschutz. denkkontor: Managed Antivirus	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.21	**Regelmäßige Datensicherung** Alle relevanten Daten werden regelmäßig gesichert. denkkontor: Online Backup	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.22	**Schutz der Datensicherung** Sicherungen sind vor unbefugtem Zugriff geschützt (z. B. verschlüsselt). denkkontor: Online Backup	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.23	**Art der Datensicherung festgelegt** Es ist festgelegt, wie, wohin und wie oft gesichert wird. denkkontor: Online Backup	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.24	**Verantwortliche für die Datensicherung** Es ist festgelegt, wer für die Datensicherung zuständig ist. denkkontor: Systemüberwachung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.25	**Test der Datensicherung** Sicherungen werden auf Vollständigkeit und Wiederherstellbarkeit getestet. denkkontor: Feuerwehrübung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
1.26	**Zugriff auf Geräte und Software abgesichert** Benutzer und Rollen in der Praxissoftware regeln den Zugriff auf Patientendaten und z. B. den eHBA.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Windows-Geräte				
1.27	**Cloud-Synchronisation deaktiviert** Die Synchronisation von Benutzerdaten mit Microsoft-Clouddiensten ist abgeschaltet. denkkontor: Managed Software Update	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.28	**Datei- und Freigabeberechtigungen** Zugriffe auf Ordner und Freigaben sind je Gruppe bzw. Person geregelt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.29	**Datensparsamkeit** Es werden so wenige personenbezogene Daten wie möglich verwendet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Smartphone & Tablet				
1.30	**SIM-Karten-PIN** SIM-Karten sind mit PIN geschützt; PUK kennen nur die Verantwortlichen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.31	**Sichere Grundeinstellungen** Auf mobilen Geräten sind die sichersten Einstellungen gewählt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.32	**Gerätesperre** Geräte sind mit einem komplexen Code gesperrt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.33	**Datenschutz-Einstellungen** Apps haben nur die Zugriffe, die sie wirklich brauchen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Mobiltelefon				
1.34	**Sperrung bei Verlust** Bei Verlust wird die SIM-Karte sofort gesperrt; die nötigen Daten sind hinterlegt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.35	**Sicherheitsfunktionen genutzt** Vorhandene Sicherheitsfunktionen sind aktiviert und voreingestellt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Wechseldatenträger				
1.36	**Prüfung auf Schadsoftware** USB-Sticks & Co. werden bei jeder Nutzung auf Viren geprüft. denkkontor: Managed Antivirus	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.37	**Kennzeichnung beim Versand** Datenträger sind für den Empfänger gekennzeichnet, ohne den Inhalt zu verraten.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.38	**Sicherer Versand** Versand mit Zustellnachweis und manipulationssicherer Verpackung.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.39	**Sicheres Löschen** Datenträger werden nach der Nutzung sicher und vollständig gelöscht.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
E-Mail				
1.40	**Sichere Einstellungen im E-Mail-Programm** Anhänge werden geprüft, aktive Inhalte nicht automatisch ausgeführt, Verbindungen verschlüsselt. denkkontor: Managed Anti-Spam	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.41	**Umgang mit Spam** Spam wird gelöscht – nicht beantwortet, keine Links angeklickt. denkkontor: Managed Anti-Spam	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Apps				
1.42	**Nur sichere Apps** Apps nur aus offiziellen Stores; nicht benötigte Apps samt Daten werden entfernt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.43	**Sichere Speicherung von App-Daten** Apps speichern Dokumente nur verschlüsselt und lokal.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.44	**Kein unkontrollierter Datenabfluss** Restriktive Einstellungen verhindern den Zugriff von Apps auf vertrauliche Daten.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
Eigene Webanwendungen*				
1.45	**Anmeldung bei Webanwendungen** Bietet die Praxis selbst einen Webdienst an: sichere Anmeldung mit Begrenzung von Fehlversuchen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.46	**Schutz vertraulicher Daten** Zugangsdaten werden serverseitig geschützt gespeichert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.47	**Web Application Firewall** Für eigene Webdienste sollte eine Web Application Firewall eingesetzt werden.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
1.48	**Schutz vor automatisiertem Missbrauch** Eigene Webdienste sind gegen automatisierte Angriffe geschützt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Internet-Nutzung				
1.49	**Verschlüsselte Verbindungen (https)** Webanwendungen werden nur über verschlüsselte Verbindungen genutzt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Cloud-Dienste				
1.50	**Sicherheit von Cloud-Anbietern (C5-Testat)** Werden Gesundheitsdaten in der Cloud verarbeitet, braucht der Anbieter ein aktuelles C5-Testat. denkkontor: Prüfung im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

* Anforderungen 1.45–1.48 gelten nur, wenn die Praxis selbst Webanwendungen anbietet (z. B. eigenes Patientenportal).

Anlage 2 Zusätzlich für mittlere Praxen

ab 6 Personen

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
Netzwerksicherheit				
2.1	**Alarmierung und Protokollierung** Wichtige Ereignisse von Netzwerkgeräten werden zentral gemeldet und protokolliert. denkkontor: Systemüberwachung	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Endgeräte				
2.2	**Verschlüsselte Verbindungen** Es werden aktuelle Verschlüsselungsverfahren (z. B. TLS) verwendet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
2.3	**Restriktive Rechtevergabe** Rechte werden nur so weit vergeben, wie sie für die Arbeit nötig sind.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Windows-Geräte				
2.4	**Sichere zentrale Anmeldung** In reinen Windows-Netzen wird zur zentralen Anmeldung nur Kerberos genutzt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Smartphone & Tablet				
2.5	**Richtlinie zur Nutzung mobiler Geräte** Eine verbindliche Regelung für Mitarbeitende zur Nutzung mobiler Geräte liegt vor. denkkontor: Vorlage im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
2.6	**Sprachassistenten** Sprachassistenten werden nur genutzt, wenn unbedingt nötig.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Mobiltelefon				
2.7	**Regeln zur dienstlichen Handynutzung** Für dienstlich genutzte Mobiltelefone gibt es eine Nutzungsrichtlinie. denkkontor: Vorlage im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
2.8	**Sichere Datenübertragung** Geregelt ist, welche Daten per Handy übertragen werden dürfen – verschlüsselt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Wechseldatenträger				

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
2.9	**Regeln zur Mitnahme** Schriftlich geregelt, ob und wie Datenträger mitgenommen werden dürfen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Apps				
2.10	**App-Berechtigungen minimiert** Apps erhalten nur die nötigsten Berechtigungen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Anlage 3 Zusätzlich für Großpraxen

ab 21 Personen

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
Personal				
3.1	**Lernerfolg messen** Der Erfolg von Schulungen wird gemessen und ausgewertet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Netzwerksicherheit				
3.2	**Netzsegmentierung** Das Netz ist so aufgeteilt, dass Gesundheitsdaten von weniger kritischen Daten getrennt sind. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.3	**Schutz sensibler Informationen** Sensible Daten werden nur über sichere, aktuelle Protokolle übertragen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Smartphone & Tablet				
3.4	**Richtlinie für Smartphones und Tablets** Vor dem Einsatz liegt eine Regelung zu Nutzung und Kontrolle vor.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.5	**Auswahl und Freigabe von Apps** Apps werden vor der Installation geprüft und freigegeben.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.6	**Erlaubte Informationen definiert** Festgelegt, welche Informationen auf mobilen Geräten verarbeitet werden dürfen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Mobile Device Management				
3.7	**Sichere Anbindung mobiler Geräte** Die Verbindung zwischen Geräten, MDM und Praxisnetz ist abgesichert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.8	**Berechtigungskonzept im MDM** Ein Berechtigungskonzept für das MDM ist erstellt und dokumentiert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.9	**Zertifikatsverwaltung** Zertifikate werden zentral über das MDM verwaltet.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.10	**Fernlöschung** Daten auf mobilen Geräten können aus der Ferne gelöscht werden.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.11	**App-Freigabe über das MDM** Über das MDM werden nur geprüfte, freigegebene Apps angeboten.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.12	**Erlaubte Informationen im MDM** Festgelegt, welche Daten mobile Geräte unter welchen Bedingungen verarbeiten dürfen.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Wechseldatenträger				
3.13	**Datenträgerverschlüsselung** Wechseldatenträger sind vollständig verschlüsselt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.14	**Integritätsschutz** Prüfsummen oder Signaturen schützen vor Veränderung.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
E-Mail				
3.15	**Sicherer Betrieb von E-Mail-Servern** Mailserver verschlüsseln den Transport und sind gegen Missbrauch geschützt. denkkontor: Managed Anti-Spam	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
3.16	**Sicherung und Archivierung von E-Mails** E-Mails werden regelmäßig und verschlüsselt gesichert. denkkontor: Online Backup	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
3.17	**Spam- und Virenschutz auf dem Server** Ein- und ausgehende E-Mails werden zentral auf Spam und Schadsoftware geprüft. denkkontor: Managed Anti-Spam	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Anlage 4 Medizinische Großgeräte

nur bei Großgeräten

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
Medizinische Großgeräte				
4.1	**Zugriff auf Wartungsschnittstellen beschränkt** Nur Berechtigte haben Zugriff; Standardpasswörter sind geändert und dokumentiert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
4.2	**Sichere Protokolle für Wartung** Konfiguration und Wartung laufen nur über sichere Protokolle.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
4.3	**Protokollierung** Sicherheitsrelevante Ereignisse werden protokolliert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
4.4	**Unnötige Dienste abgeschaltet** Nicht genutzte Dienste und Schnittstellen sind deaktiviert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
4.5	**Unnötige Benutzerkonten deaktiviert** Nicht genutzte Konten sind deaktiviert.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
4.6	**Netzsegmentierung** Großgeräte sind von der übrigen IT getrennt. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Anlage 5 Telematikinfrastruktur

alle Praxen

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
TI-Komponenten				
5.1	**Installation nach gematik-Vorgaben** Die Installation berücksichtigt die Hinweise der gematik. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
5.2	**Betrieb nach Herstellerdokumentation** Hinweise zum sicheren Betrieb von gematik und Herstellern werden beachtet. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
5.3	**Schutz vor physischem Zugriff** Konnektor und Kartenterminals sind vor unbefugtem Zugriff geschützt.	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Konnektor				
5.4	**Internet parallel zur TI abgesichert** Besteht neben der TI ein Internetzugang, ist das Netz zusätzlich abgesichert. denkkontor: Managed Firewall	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Gehosteter Konnektor				
5.5	**Verbindung per VPN** Zwischen Praxis und gehostetem Konnektor besteht ein VPN-Tunnel. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
TI-Gateway				
5.6	**Vorgaben des Gateway-Anbieters** TI-Komponenten werden nach Handbuch des TI-Gateway-Anbieters betrieben. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
Praxisverwaltungssystem				
5.7	**Geschützte Kommunikation mit Konnektor** Die Verbindung zum Konnektor bzw. TI-Gateway ist per Zertifikat oder Passwort geschützt. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
TI-Komponenten				

Nr.	Anforderung	erfüllt · teilw. · offen	Zuständig	Notiz
5.8	**Updates zeitnah installiert** TI-Komponenten werden regelmäßig geprüft und aktualisiert. denkkontor: TI-Service	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	
5.9	**Administrationsdaten sicher verwahrt** Admin-Passwörter sind sicher hinterlegt – und der Praxis bekannt, unabhängig vom Dienstleister. denkkontor: Übergabe im Check	☐ ☐ ☐	☐ DK ☐ Praxis ☐ Dritte	

Ergebnis

Anforderungen erfüllt: _____ teilweise: _____ offen: _____

Wichtigste Maßnahmen / nächste Schritte:

Ort, Datum, Unterschrift Praxisleitung

Unterschrift denkkontor

Grundlage: Richtlinie nach § 390 SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit (KZBV, Version 1.1). Die Anforderungen sind sinngemäß und verkürzt wiedergegeben; verbindlich ist der Originaltext der Richtlinie. Die Checkliste ersetzt keine Rechtsberatung.
denkkontor.com – Inh. Alexander Teske e.K. · www.denkkontor.com