# **Checkliste zur Umsetzung der IT-Sicherheitsrichtlinie für Großpraxen (Anlagen 1, 2, 3 & 5) (Über 20 ständig mit Datenverarbeitung betraute Personen oder Datenverarbeitung in erheblichem Umfang)**

**Symbolerklärung:** 🗶 = nichtzutreffend **|** ? = unbekannt **|** ! = in Planung **|** 🡪 = Umsetzung hat begonnen **|** **✓** = Umsetzung ist abgeschlossen

**Anlagen 1, 2 & 3:**

| Nr. | Zielobjekt | Anforderung | gilt ab | 🗶 | ? | ! | 🡪 | ✓ |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Mobile Anwendungen (Apps) | Es werden nur Apps aus den offiziellen Stores runtergeladen und genutzt.  Nicht mehr benötigte Apps werden restlos gelöscht. | 01.04.2021 |  |  |  |  |  |
|  | Mobile Anwendungen (Apps) | Updates werden immer zeitnah installiert, um Schwachstellen zu vermeiden. | 01.04.2021 |  |  |  |  |  |
|  | Mobile Anwendungen (Apps) | Es werden nur Apps genutzt, die Dokumente verschlüsselt und lokal abspeichern. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Anwendungen (Apps) | Es werden keine vertraulichen Daten über Apps versendet. | 01.04.2021 |  |  |  |  |  |
|  | Mobile Anwendungen (Apps) | App-Berechtigungen sind minimiert | 01.04.2021 |  |  |  |  |  |
|  | Office-Produkte | Der in Office- Produkte integrierte Cloud- Speicher wird nicht zur Speicherung personenbezogener Informationen genutzt. | 01.04.2021 |  |  |  |  |  |
|  | Office-Produkte | Vertrauliches aus Dokumenten wird vor einer Weitergabe an Dritte gelöscht. | 01.04.2021 |  |  |  |  |  |
|  | Internet-Anwendungen | Es werden nur Internet-Anwendungen genutzt, die meine Zugänge (Login-Seite und - Ablauf, Passwort, Benutzerkonto etc.) strikt absichern. | 01.04.2021 |  |  |  |  |  |
|  | Internet-Anwendungen | Mein Internet- Browser ist gem. Hersteller-Anleitung so eingestellt, dass keine vertraulichen Daten im Browser gespeichert werden. | 01.04.2021 |  |  |  |  |  |
|  | Internet-Anwendungen | Es wird eine Web App Firewall verwendet und regelmäßig upgedatet. | 01.01.2022 |  |  |  |  |  |
|  | Internet-Anwendungen | Es werden nur verschlüsselte Internet-Anwendungen genutzt. | 01.04.2021 |  |  |  |  |  |
|  | Internet-Anwendungen | Es werden keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen  eingerichtet oder zugelassen | 01.01.2022 |  |  |  |  |  |
|  | Internet-Anwendungen | Zugriffskontrolle bei Webanwendungen: Berechtigungen sind sichergestellt | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte | Mikrofon und Kamera am Rechner werden grundsätzlich deaktiviert und nur bei Bedarf temporär direkt am Gerät aktiviert und danach wieder deaktiviert. | 01.04.2021 |  |  |  |  |  |
|  | Endgeräte | Nach Ende der Nutzung wird der Zugang zum Gerät immer gesperrt bzw. der Nutzer abgemeldet. | 01.04.2021 |  |  |  |  |  |
|  | Endgeräte | Alle Daten werden regelmäßig gesichert. | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte | Es werden aktuelle Virenschutzprogramme eingesetzt. | 01.04.2021 |  |  |  |  |  |
|  | Endgeräte | Es wird darauf geachtet, dass zur Verschlüsselung von Webseiten TLS verwendet wird | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte | Rechte werden restriktiv vergeben | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte mit dem Betriebssystem Windows | Die Synchronisierung von Nutzerdaten mit Microsoft- Cloud-Diensten wurde  vollständig deaktiviert. | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte mit dem Betriebssystem Windows | Die Berechtigungen und Zugriffe pro Personengruppe und pro Person sind geregelt. | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte mit dem Betriebssystem Windows | Es werden so wenige persönliche Daten wie möglich verwendet. | 01.01.2022 |  |  |  |  |  |
|  | Endgeräte mit dem Betriebssystem Windows | In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single-Sign-On (SSO) ausschließlich Kerberos eingesetzt werden. | 01.01.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Es werden aktuelle Schutzprogramme vor Phishing und Schadprogrammen im Browser genutzt. | 01.04.2021 |  |  |  |  |  |
|  | Smartphone und Tablet | SIM-Karten werden durch PIN geschützt. Super-PIN/PUK werden nur durch Verantwortliche angewandt. | 01.04.2021 |  |  |  |  |  |
|  | Smartphone und Tablet | Auf mobilen Endgeräten werden die strengsten bzw. sichersten Einstellungen gewählt, weil auch auf mobilen Geräten das erforderliche Schutzniveau für die verarbeiteten Daten sichergestellt werden muss. | 01.01.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Geräte werden mit einem komplexen Gerätesperrcode geschützt. | 01.04.2021 |  |  |  |  |  |
|  | Smartphone und Tablet | Updates des Betriebssystems und der eingesetzten Apps werden bei Hinweis auf neue Versionen immer zeitnah installiert, um Schwachstellen zu vermeiden. Zusätzlich ist ein fester Turnus festgelegt, in dem das Betriebssystem und alle genutzten Apps auf neue Versionen geprüft werden. | 01.04.2021 |  |  |  |  |  |
|  | Smartphone und Tablet | Der Zugriff von Apps und Betriebssystem auf Daten und Schnittstellen der Geräte sind Sie in den Einstellungen restriktiv auf das Notwendigste eingeschränkt. | 01.01.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten wurde erstellt. | 01.07.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Sprachassistenten werden nur eingesetzt, wenn sie zwingend notwendig sind. | 01.01.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. | 01.01.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Apps aus öffentlichen App-Stores werden durch die Verantwortlichen geprüft und freigegeben. | 01.07.2022 |  |  |  |  |  |
|  | Smartphone und Tablet | Es wurde festgelegt, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen. | 01.01.2022 |  |  |  |  |  |
|  | Mobiltelefon | Bei Verlust eines Mobiltelefons wird die darin verwendete SIM-Karte zeitnah gesperrt. Die dafür notwendigen Mobilfunkanbieter- Informationen sind hinterlegt, um sie bei Bedarf im Zugriff zu haben. | 01.01.2022 |  |  |  |  |  |
|  | Mobiltelefon | Alle auf den Mobiltelefonen verfügbaren Sicherheitsmechanismen werden genutzt und als Standard-Einstellung vorkonfiguriert. | 01.01.2022 |  |  |  |  |  |
|  | Mobiltelefon | Es wird regelmäßig geprüft, ob es Softwareupdates für die Mobiltelefone gibt. | 01.04.2021 |  |  |  |  |  |
|  | Mobiltelefon | Für die Verwendung von Mobiltelefonen für dienstliche Zwecke wurde eine Nutzungs- und Sicherheitsrichtlinie erstellt. | 01.07.2022 |  |  |  |  |  |
|  | Mobiltelefon | Es ist geregelt, welche Daten über Mobiltelefone übertragen werden dürfen. Diese werden verschlüsselt. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Die Verbindung der mobilen Endgeräte zum MDM ist angemessen abgesichert. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Für das MDM wurde ein Berechtigungskonzept erstellt, dokumentiert und wird angewendet. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät werden zentral über das MDM installiert, deinstalliert und aktualisiert. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Das MDM stellt sicher, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können. | 01.01.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden. | 10.07.2022 |  |  |  |  |  |
|  | Mobile Device Management (MDM) | Es ist festgelegt, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen. | 01.01.2022 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Wechseldatenträger werden bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft. | 01.01.2022 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Für Empfänger erfolgt eine eindeutige Kennzeichnung, die aber keine Rückschlüsse für andere ermöglicht. | 01.04.2021 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Es werden ausschließlich Versand-Anbieter mit sicherem Nachweis-System gewählt. Versandart und Verpackung sind manipulationssicher. | 01.04.2021 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Datenträger werden nach Verwendung immer sicher und vollständig gelöscht. | 01.01.2022 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Es gibt klare schriftliche Regeln, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. | 01.01.2022 |  |  |  |  |  |
|  | Wechseldatenträger / Speichermedien | Integritätsschutz durch Checksummen oder digitale Signaturen: Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen wird eingesetzt. | 01.01.2022 |  |  |  |  |  |
|  | Netzwerksicherheit | Der Übergang zu anderen Netzen, insbesondere das Internet wird durch eine  Firewall geschützt. | 01.04.2021 |  |  |  |  |  |
|  | Netzwerksicherheit | Das interne Netz ist inklusive eines Netzplanes dokumentiert. | 01.04.2021 |  |  |  |  |  |
|  | Netzwerksicherheit | Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen wird eine geeignete Authentisierung verwendet. | 01.01.2022 |  |  |  |  |  |
|  | Netzwerksicherheit | Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen werden automatisch an ein zentrales Management-System übermittelt und dort protokolliert. | 01.01.2022 |  |  |  |  |  |
|  | Netzwerksicherheit | Schützenswerte Informationen werden über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird. | 01.01.2022 |  |  |  |  |  |

**Anlage 5: Dezentrale Komponenten der Telematik Infrastruktur**

| Nr. | Zielobjekt | Anforderung | gilt ab | 🗶 | ? | ! | 🡪 | ✓ |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Dezentrale Komponenten der Telematik Infrastruktur | Planung und Durchführung der Installation:  Die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten wurden berücksichtigt. | 01.01.2022 |  |  |  |  |  |
|  | Dezentrale Komponenten der Telematik Infrastruktur | Betrieb: Die Anwender- und Administrationsdokumentationen der gematik GmbH und der Hersteller der TI-Komponenten, insbesondere die Hinweise zum sicheren Betrieb der Komponenten, müssen berücksichtigt werden. | 01.01.2022 |  |  |  |  |  |
|  | Dezentrale Komponenten der Telematik Infrastruktur | Die TI-Komponenten in der Praxis werden entsprechend den Vorgaben im Handbuch vor dem Zugriff Unberechtigter geschützt. | 01.01.2022 |  |  |  |  |  |
|  | Konnektor | Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk eingebracht, werden zusätzliche Maßnahmen ergriffen, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen. | 01.01.2022 |  |  |  |  |  |
|  | Primärsysteme | Geschützte Kommunikation mit dem Konnektor: Es sind Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden. | 01.01.2021 |  |  |  |  |  |
|  | Dezentrale Komponenten der Telematik Infrastruktur | Zeitnahes Installieren verfügbarer Aktualisierungen:  Die TI-Komponenten in der Praxis werden regelmäßig auf verfügbare Aktualisierungen geprüft und verfügbare Aktualisierungen werden zeitnah installiert bzw. die Funktion für automatische Updates wurde aktiviert. | 01.01.2022 |  |  |  |  |  |