ANLAGE 3: ZUSÄTZLICHE ANFORDERUNGEN FÜR GROSSE PRAXEN

HARDWARE: ENDGERÄTE UND IT-SYSTEME

NR.	ZIELOBJEKT	ANFORDERUNG	ERLÄUTERUNG	GELTUNG AB	WEITERE HINWEISE ETC.
1.	Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Bevor eine Praxis Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden.	01.01.2022	– Bevor eine Institution Smartphones oder Tablets bereitstellt, betreibt oder einsetzt, muss eine generelle Richtlinie im Hinblick auf die Nutzung und Kontrolle der Geräte festgelegt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich im Bereich Musterdokumente. – Hierbei muss unter anderem festgelegt werden, wer auf welche Informationen der Institution zugreifen darf.
2.	Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	01.07.2022	– Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden. – Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. – Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden.
3.	Smartphone und Tablet	Definition der erlaubten Informationen und Applikationen auf mobilen Geräten	Die Praxis sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen.	01.01.2022	– Die Institution sollte festlegen, welche Informationen auf den mobilen Endgeräten verarbeitet werden dürfen. – Grundlage für die Regelung sollte einerseits die Klassifikation der Institutionsdaten sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden. – Die Benutzer der mobilen Endgeräte sollten nur freigegebene und geprüfte Apps aus als sicher klassifizierten Quellen installieren dürfen.
4.	Mobile Device Management (MDM)	Sichere Anbindung der mobilen Endgeräte an die Institution	Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden.	01.01.2022	– Die Verbindung der mobilen Endgeräte zum MDM sollte angemessen abgesichert werden. Dies bieten kommerzielle MDM-Lösungen in der Regel out-of-the-box an. – Die Verbindung der mobilen Endgeräte ins Netz der Institution sollte angemessen abgesichert werden. – Wenn Daten zwischen den mobilen Endgeräten und dem IT-Netz der Institution übertragen werden, sollte durch geeignete Maßnahmen (z. B. VPN) verhindert werden, dass Unbefugte sie verändern oder einsehen können.
5.	Mobile Device Management (MDM)	Berechtigungsmanagement im MDM	Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden.	01.01.2022	– Für das MDM sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden. – Den Benutzergruppen und Administratoren sollte das MDM nur so viele Berechtigungen einräumen wie für die Aufgabenerfüllung notwendig sind (Minimalprinzip). – Es sollte regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind und den Aufgaben entsprechen.
6.	Mobile Device Management (MDM)	Verwaltung von Zertifikaten	Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden.	01.01.2022	– Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät sollten zentral über das MDM installiert, deinstalliert und aktualisiert werden. – Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch den Benutzer sollte durch das MDM verhindert werden. – Das MDM sollte Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen.
7.	Mobile Device Management (MDM)	Fernlöschung und Außerbetriebnahme von Endgeräten	Das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können.	01.01.2022	– Das MDM sollte sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können (Remote Wipe bei bestehender Datenverbindung). – Werden in dem mobilen Endgerät externe Speicher genutzt, sollte geprüft werden, ob diese bei einem Remote Wipe ebenfalls gelöscht werden können. Diese Funktion sollte vom MDM unterstützt werden. – Der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) sollte sicherstellen, dass keine schutzbedürftigen Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies sollte insbesondere dann gelten, wenn das Unenrollment aus der Ferne ausgeführt wird.
8.	Mobile Device Management (MDM)	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	10.07.2022	– Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden. – Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. – Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden und dort für die Benutzer verfügbar sein. – Apps sollten gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden. – Das MDM sollte die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht.
9.	Mobile Device Management (MDM)	Festlegung erlaubter Informationen auf mobilen Endgeräten	Die Praxis sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen.	01.01.2022	– Die Institution sollte festlegen, welche Informationen die mobilen Endgeräte unter welchen Bedingungen verarbeiten dürfen. Grundlage für die Regelung sollten einerseits die Klassifikation bzw. der Schutzbedarf der Informationen sein und andererseits die Bedingungen, unter denen die Daten auf den Geräten verarbeitet werden, etwa in abgeschotteten Containern. – Die Verantwortlichen sollten das MDM auf Basis dieser Regeln konfigurieren, sodass es diese auf allen mobilen Endgeräten durchsetzen kann. – Den Benutzern sollten die Regeln in geeigneter Weise bekannt gegeben werden.
10.	Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.	01.04.2021	– Wechseldatenträger sollten vollständig verschlüsselt werden. Es sollte ein sicheres Verschlüsselungsverfahren eingesetzt werden. Empfehlungen zu geeigneten Algorithmen und Schlüssellängen bieten die Technischen Richtlinien des BSI BSI-TR-02102. Mittels Open-Source Lösungen wie VeraCrypt können entsprechende verschlüsselte Container angelegt werden.
11.	Wechseldatenträger / Speichermedien	Integritätsschutz durch Checksummen oder digitale Signaturen	Ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen sollte eingesetzt werden.	01.01.2022	– Um beim Datenaustausch mittels mobiler Datenträger die Integrität von vertraulichen Informationen sicherzustellen, sollte ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden. – Die Verfahren zum Schutz vor Veränderungen sollten dem aktuellen Stand der Technik entsprechen.
12.	Netzwerksicherheit	Absicherung von schützenswerten Informationen	Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.	01.01.2022	– Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. – Können solche Protokolle nicht genutzt werden, muss nach Stand der Technik angemessen verschlüsselt und authentisiert werden.

JETZT KOMMENTIEREN

Ein Service der Kassenärztlichen Bundesvereinigung (KBV)
Dezernat Digitalisierung und IT

Ansprechpartner

Telefon: 030 40 05 - 21 21
E-Mail: servicedesk@kbv.de

Weitere Informationen

Nutzungsbedingungen
Datenschutz
Impressum