Was bedeutet die IT-Sicherheitsrichtlinie für Praxen?

Jede Praxis hat mit sensiblen Gesundheitsdaten zu tun – gerade in Zeiten der fortschreitenden Digitalisierung müssen diese vor Fremdzugriffen geschützt werden. Damit alle Praxen die dazu notwendigen Maßnahmen ergreifen, hat der Gesetzgeber die Kassenärztlichen Bundesvereingung (KBV) im Digitale-Versorgungs-Gesetz mit der Entwicklung der IT-Sicherheitsrichtlinie beauftragt. Diese Richtlinie wurde im Einvernehmen mit dem Bundesamt für Sicherheit beschlossen und gilt seit dem 1. Januar 2021.

Standards für ein Mindestmaß an IT-Sicherheit

Die IT-Sicherheitsrichtlinie bildet das Mindestmaß der zu ergreifenden Maßnahmen ab, um IT-Sicherheit zu gewährleisten. Sie orientiert sich am aktuellen Stand der Technik und enthält Sicherheitsanforderungen zu Sicherheitsmanagement, IT-Systemen, Rechnerprogrammen, mobilen Apps und Internetanwendungen oder dem Aufspüren von Sicherheitsvorfällen.

Alle in der Richtlinie aufgeführten Anforderungen sind zu einem Stichtag, beginnend mit dem 1. April 2021, verpflichtend umzusetzen. Beim Umfang der Anforderungen wird hinsichtlich der Praxisgröße (bis 5 Personen, 6 bis 20 Personen, 20 oder mehr Personen) unterschieden.

Viele der Sicherheitsanforderungen sind Ihnen nicht fremd, denn sie ergaben sich bereits aus der seit Mai 2018 geltenden Datenschutzgrundverordnung (DSGVO). **Was Praxen konkret ab dem 1. April 2021 umgesetzt haben müssen, können Sie der Übersicht auf Seite 2 entnehmen.** Ab dem 1. Juli 2021 kommen verpflichtende Anforderungen im Umgang mit medizinischen Großgeräten hinzu und ab 2022 gelten weitere Anforderungen für alle Praxen.

Bitte beachten: Bei den definierten Anforderungen kann es Änderungen geben, denn die IT-Sicherheitsrichtlinie wird jährlich im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesgesundheitsministerium aktualisiert.

Wo gibt es weitere Informationen?

Informationen und Schulungen stellt die KBV bereit:

- Neue **Online-Plattform**: Hier finden Sie Begleitinformationen zur IT-Sicherheitsrichtlinie. Neben der Richtlinie selbst gibt es FAQ und Musterdokumente, wie einen Muster-Netzplan oder eine Muster-Richtlinie für Mitarbeitende zur Nutzung von mobilen Endgeräten. Die KBV baut das Informationsangebot kontinuierlich aus.
- **Infoseite** der KBV: Hier finden Sie alle Dokumente und Beschlüsse der KBV-Vertreterversammlung zum Thema.
- Online-Schulung auf dem **KBV-Fortbildungsportal**: Die Schulung soll ab Mitte Februar zur Verfügung stehen, voraussichtlich können 2 CME-Punkte erworben werden.

Im Überblick: Diese Anforderungen müssen Praxen ab dem 1. April 2021 erfüllen

Erläuterungen zu den Anforderungen finden Sie in den Anlagen der **IT-Sicherheitsrichtlinie** und auf der **Online-Plattform**.

Alle Praxen	
Zielobjekt	Anforderung
Mobile Anwendungen (Apps)	• sichere Apps nutzen • aktuelle Apps nutzen • Verhinderung von Datenabfluss
Office-Produkte	• Verzicht auf Cloud-Speicherung • Beseitigung von Restinformationen vor Weitergabe von Dokumenten
Internetanwendungen	• Authentisierung bei Webanwendungen • Schutz vertraulicher Daten • Kryptografische Sicherung vertraulicher Daten
Netzwerksicherheit	• Absicherung der Netzübergangspunkte • Dokumentation des Netzes
Endgeräte	• Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und -kameras • Abmelden nach Aufgabenerfüllung • Einsatz von Virenschutzprogrammen
Smartphone und Tablet	• Schutz vor Phishing und Schadprogrammen im Browser • Verwendung der SIM-Karten-PIN • Verwendung eines Zugriffschutzes • Updates von Betriebssystem und Apps
Mobiltelefon	• Updates von Mobiltelefonen
Wechseldatenträger/Speichermedien	• Angemessene Kennzeichnung der Datenträger beim Versand • Sichere Versandart und Verpackung
Zusätzliche Anforderungen für mittlere Praxen (6 bis 20 Personen)*	
Mobile Anwendungen (Apps)	• Minimierung und Kontrolle von App-Berechtigungen
Zusätzliche Anforderungen für Großpraxen (20 oder mehr Personen)* oder Praxen mit erheblichen Umfang an Datenverarbeitung	
Wechseldatenträger/Speichermedien	• Datenträgerverschlüsselung

*Personenzahl, die ständig mit Datenverarbeitung in der Praxis betraut ist

HINWEIS: Die rot hinterlegte Schrift (bzw. die roten Felder) ist verlinkt mit dem dort beschriebenen Dokument.

Datenschutzerklärung und Impressum: Datenschutzerklärung und Impressum: Der Newsletter „Praxisinformationsdienst“ (PID) ist eine monatliche Information der Kassenärztlichen Vereinigung (KV) Berlin (KdÖR) für die Vertragsärzte und Vertragspsychotherapeuten sowie deren Praxispersonal. Sie erhalten den kostenlosen Newsletter aufgrund Ihrer freiwilligen Eintragung. Möchten Sie diese Informationen zukünftig nicht mehr erhalten, senden Sie uns bitte eine formlose E-Mail an die Adresse **kvbe@kvberlin.de**. Selbstverständlich werden alle Ihre Daten vertraulich behandelt, die Einzelheiten dazu finden Sie in unserer **Datenschutzerklärung**. Hrsg.: Dr. Burkhard Ruppert (V. i.S.d.P.), Kassenärztliche Vereinigung Berlin, Masurenallee 6A, 14057 Berlin. Tel.: 030 / 31 003-0, **www.kvberlin.de**. Redaktion: Dörthe Arnold, Laura Vele – Tel. Newsletter-Redaktion: 030 / 31 003-483. Kontakt zum Service-Center der KV Berlin: Tel.: 030 / 31 003-999, Fax: 030 / 31 003-900, E-Mail: **service-center@kvberlin.de.**