Digitalisierung und IT

Weitere Informationen

Online-Plattform zur Sicherheitsrichtlinie

IT-Sicherheitsrichtlinie (Infoseite KBV)

Datensicherheit (Infoseite KBV)

IT-Sicherheit

Mit der IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung (KBV) gelten für Praxen seit 2021 verbindliche Anforderungen an die IT-Sicherheit. Diese Themenseite gibt einen Überblick über die Anforderungen –sortiert nach den Objekten auf die sich Anforderungen beziehen.

Die IT-Sicherheitsrichtlinie enthält Sicherheitsanforderungen, die sich am aktuellen Stand der Technik orientieren und die das Ziel haben, den Datenschutz in den Praxen mit der europäischen Datenschutzgrundverordnung (DSGVO) in Einklang zu bringen. Es geht um Punkte wie Sicherheitsmanagement, Organisation und Personal, IT-Systeme, Anwendungen und Dienste sowie das Aufspüren von Sicherheitsvorfällen.

Der Gesetzgeber hatte die KBV im Digitale-Versorgung-Gesetz mit der Entwicklung der IT-Sicherheitsrichtlinie beauftragt. Sie wird jährlich im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Bundesgesundheitsministerium aktualisiert.

Anforderungen unterscheiden sich hinsichtlich Praxisgröße und Umsetzungszeitpunkt
Je nach Größe der Praxis gelten die in der Richtlinie definierten Anforderungen in unterschiedlichem Umfang. Es werden drei Praxisgrößen unterschieden:

1. Praxis: bis zu fünf ständig mit der Datenverarbeitung betrauten Personen.
2. Mittlere Praxis: 6 bis 20 ständig mit der Datenverarbeitung betraute Personen.
3. Großpraxis oder Praxis mit Datenverarbeitung im erheblichen Umfang:
    - über 20 Personen, die ständig mit der Datenverarbeitung betraut sind
    - eine Praxis, die in über die normale Datenübermittlung hinausgehenden Umfang in der Datenverarbeitung tätig ist (z. B. Groß-MVZ mit krankenhausähnlichen Strukturen, Labore).

Viele der in der Richtlinie definierten Anforderungen müssen spätestens ab dem 1. April 2021 in den Praxen umgesetzt werden, andere Anforderungen gelten erst später.

Die Anforderungen im Überblick

Office (Apps)

Für alle Praxen

Was?	Ab wann?
Verzicht auf Cloud-Speicherung Nutzen Sie keine in Office-Produkte integrierte Cloud-Speicher, wie Microsoft 365 oder One Drive *IT-Sicherheitsrichtlinie, Anlage 1, Nr.5*	1. April 2021

Beseitigung von Rest-Informationen vor Weitergabe von Dokumenten Verwenden Sie für den Datenaustausch möglichst PDF-Dokumente. Bedenken Sie dabei, dass in den Metadaten Informationen zu Autor oder Erstellungsdatum gespeichert sind. Wenn Sie diese Informationen nicht weitergeben möchten, löschen Sie diese über Datei -> Einstellungen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 6*	1. April 2021

Internet-Anwendungen

Für alle Praxen

Was?	Ab wann?
Authentisierung bei Webanwendungen Ihre Zugänge zu Internet-Anwendungen müssen strikt abgesichert sein (mindestens Benutzername und Passwort). Noch sicherer ist der Zugang mit einer 2-Faktor-Authentisierung. Verwenden Sie hinreichend komplexe Passwörter, hierbei können Sie auch Passwortmanager nutzen, die sichere Passwörter generieren und speichern. Achten Sie außerdem darauf, dass die Verbindung Ihrer Anwendung verschlüsselt ist (HTTPS und Schloss im Webbrowser). *IT-Sicherheitsrichtlinie, Anlage 1, Nr.*	1. April 2021
Schutz vertraulicher Daten Stellen Sie Ihren Internet-Browser so ein, dass keine vertraulichen Daten im Browser gespeichert werden. Schalten Sie dafür Funktionen wie Passwortspeicherung und Formularvervollständigung ab. Löschen Sie außerdem regelmäßig Ihre Browserdaten oder nutzen Sie Einstellungen, die die Daten nach Schließen des Browsers automatisch löschen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 8*	1. April 2021
Kryptografische Sicherung vertraulicher Daten Nutzen Sie Internet-Anwendungen nur über das sichere HTTPS-Protokoll. Die Verschlüsselung ist in der URL an https:// (nicht „http://) zu erkennen und wird im Webbrowser durch ein vorangestelltes Schloss visualisiert. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 10*	1. April 2021
Firewall benutzen Betreiben Sie Anwendungen auf einem eigenen Webserver, können Sie diese über eine Web Application Firewall absichern. Hierbei handelt es sich um eine spezielle Firewall für das HTTP-Protokoll. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 9*	1. Januar 2022
Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen Betreiben Sie Anwendungen auf einem eigenen Webserver, sollten Sie diese vor automatisierten Eingaben schützen. Dafür können Sie Captcha-Mechanismen oder zeitlich verzögerte Anmeldeversuche nutzen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 11*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Zugriffskontrolle bei Webanwendungen Betreiben Sie Anwendungen auf einem eigenen Webserver, müssen den Benutzern Zugriffsrechte zugewiesen werden können. Nur so ist sichergestellt, dass jeder Benutzer nur Aktionen durchführen kann, zu denen er berechtigt ist bzw. die zur Bewältigung der Aufgaben nötig sind. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 2*	1. Januar 2022

Mobile Anwendungen (Apps)

Für alle Praxen

Was?	Ab wann?
Sichere Apps nutzen Laden Sie nur Apps aus offiziellen Stores (z.B. App Store oder Google Play) herunter. Löschen Sie die Apps restlos vom Gerät, wenn Sie diese nicht mehr benötigen. Zur Überprüfung der Sicherheit der Apps können Sie bereits vor dem Herunterladen der App die entsprechenden Informationen im jeweiligen App Store ansehen. Diese finden Sie i.d.R. unter „Über diese App“, „App-Berechtigungen“ oder „Datenschutzinformationen zur App“. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 1*	1. April 2021
Aktuelle App-Versionen Sie vermeiden Sicherheitslücken, wenn Sie Updates für Apps immer zeitnah installieren. Das geht am einfachsten, wenn Sie Autoupdates aktivieren. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 2*	1. April 2021
Verhinderung von Datenabfluss Achten Sie darauf, dass Apps keine vertraulichen Daten an Dritte senden. Dafür müssen Sie in den Einstellungen den Datenversand entsprechend einschränken. Überprüfen Sie vor der App-Benutzung auch, ob eine App ungeschützte Protokollierungs- oder Hilfsdateien schreibt, die vertrauliche Informationen enthalten. Um diese nach Herunterladen der App zu überprüfen und ggf. anzupassen gehen Sie auf die Einstellungen – Apps – App auswählen – Berechtigungen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 4*	1. April 2021
Sichere Speicherung lokaler App-Daten Nutzen Sie nur Apps, die Dokumente verschlüsseln und lokal abspeichern. Aktivieren Sie dafür die Verschlüsselung auf Ihrem Gerät (Android: PIN oder Passwort einrichten; IOS: Code-Sperre) *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 3*	1. Januar 2021

Für mittlere und große Praxen

Was?	Ab wann?
Minimierung und Kontrolle von App-Berechtigungen Erteilen Sie einer App nur die minimal notwendigen Berechtigungen (z.B. Zugriff auf Kamera, Mikrofon etc.). Sicherheitsrelevante Berechtigungseinstellungen sollten so fixiert sein, dass sie nicht durch Benutzer oder Apps geändert werden können. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 1*	1. April 2021

Endgeräte allgemein

Für alle Praxen

Was?	Ab wann?

Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras Deaktivieren Sie Mikrofon und Kamera grundsätzlich am Rechner und aktivieren Sie diese nur temporär bei Bedarf. Achten Sie bei der Anschaffung neuer Geräte darauf, dass die Kamera abgedeckt und das Mikrofon ausgestellt werden kann. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 12*	1. April 2021
Abmelden nach Aufgabenerfüllung Melden Sie sich vom Endgerät ab oder sperren Sie den Bildschirm, wenn Sie die Nutzung beendet haben. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 13*	1. April 2021
Einsatz von Virenschutzprogrammen Setzen Sie aktuelle Virusschutzprogramme ein. Hierfür gibt es eine Reihe an kommerziellen Programmen auf dem Markt. Bei Windows 10 können Sie den mitgelieferten „Windows Defender“ nutzen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 15*	1. April 2021
Regelmäßige Datensicherung Schützen Sie Ihre Daten durch regelmäßige Backups vor Ausfällen von Hard- und Software sowie Verschlüsselungstrojanern. Prüfen Sie regelmäßig, ob sich die Backups fehlerlos zurückspielen lassen und schützen Sie die Backups selbst vor Verlust oder ungewollten Überschreiben. Empfehlenswert ist die 3-2-1-Regel (3 Kopien auf 2 unterschiedlichen Medien, 1 außer Haus) *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 15*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Nutzung von TLS Nutzen Sie alle Internetverbindungen nur über das sichere HTTPS-Protokoll, das auf Transport Layer Security (TLS) basiert. Die Verschlüsselung ist in der URL an https:// (nicht „http://) zu erkennen und wird im Webbrowser durch ein vorangestelltes Schloss visualisiert. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 3*	1. Januar 2022
Restriktive Rechtevergabe Das verwendete IT-System muss es ermöglichen, dass Benutzern unterschiedliche Zugriffsrechte zugewiesen werden können. Nur so ist sichergestellt, dass jeder Benutzer nur Aktionen durchführen kann, zu denen er berechtigt ist bzw. die zur Bewältigung der Aufgaben nötig sind. Achten Sie darauf, den Kreis zugriffsberechtigter Administratoren möglichst klein zu halten. Prüfen Sie regelmäßig, ob die Berechtigungen den Vorgaben der Sicherheitsrichtlinie entsprechen. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 4*	1. Januar 2022

Endgeräte mit dem Betriebssystem Windows

Für alle Praxen

Was?	Ab wann?
Konfiguration von Synchronisationsmechanismen Auf Cloud-Speicher bei Office-Produkten soll komplett verzichtet werden (vgl. Anlage 1, Nr. 5). In diesem Zusammenhang ist auch die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten vollständig zu deaktivieren. Dafür deinstallieren Sie insbesondere die Anwendung „OneDrive“. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 16*	1. Januar 2022

Datei- und Freigabeberechtigungen Jede Person sollte nur so viel Berechtigungen auf Programm-, Datei und Verzeichnisebene erhalten, wie zur Bewältigung der Aufgaben nötig sind. Die Berechtigungen lassen sich mittels Gruppen und Rechte für mehrere Personen einrichten. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 17*	1. Januar 2022
Datensparsamkeit Verwenden Sie generell so wenig personenbezogene Daten wie möglich. Jede Verwendung dieser Daten muss begründet und im "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Beachten Sie auch die einzuhaltenden Löschfristen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 18*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Sichere zentrale Authentisierung in Windows-Netzen In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 5*	1. Juli 2022

Smartphone und Tablet, Mobile Device Management (MDM)

Für alle Praxen

Was?	Ab wann?
Konfiguration von Synchronisationsmechanismen Auf Cloud-Speicher bei Office-Produkten soll komplett verzichtet werden (vgl. Anlage 1, Nr. 5). In diesem Zusammenhang ist auch die Synchronisierung von Nutzerdaten mit Microsoft-Cloud-Diensten vollständig zu deaktivieren. Dafür deinstallieren Sie insbesondere die Anwendung „OneDrive“. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 16*	1. Januar 2022
Datei- und Freigabeberechtigungen Jede Person sollte nur so viel Berechtigungen auf Programm-, Datei und Verzeichnisebene erhalten, wie zur Bewältigung der Aufgaben nötig sind. Die Berechtigungen lassen sich mittels Gruppen und Rechte für mehrere Personen einrichten. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 17*	1. Januar 2022
Datensparsamkeit Verwenden Sie generell so wenig personenbezogene Daten wie möglich. Jede Verwendung dieser Daten muss begründet und im "Verzeichnis von Verarbeitungstätigkeiten" nach Artikel 30 DSGVO dokumentiert werden. Beachten Sie auch die einzuhaltenden Löschfristen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 18*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Sichere zentrale Authentisierung in Windows-Netzen In reinen Windows-Netzen SOLLTE zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 5*	1. Juli 2022

Mobiltelefon

Für alle Praxen

Was?	Ab wann?
Updates von Mobiltelefonen Prüfen Sie regelmäßig, ob Softwareupdates für Ihre Mobiltelefone zur Verfügung stehen und führen Sie diese aus. Stellen Sie nachher sicher, dass keine unterwünschten Funktionen wie Cloud-Speicher aktiviert wurden. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 27*	1. April 2021
Sperrmaßnahmen bei Verlust eines Mobiltelefons Bei Verlust eines Mobiltelefons sperren Sie die darin verwendete SIM-Karte zeitnah. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 25*	1. Januar 2022
Nutzung der Sicherheitsmechanismen von Mobiltelefonen Alle verfügbaren Sicherheitsmechanismen sollten auf den Mobiltelefonen genutzt und als Standard-Einstellung vorkonfiguriert werden. Dazu gehören PIN, Geräte-Code und SIM-Lock. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 26*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Sichere Datenübertragung über Mobiltelefone Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Außerdem sollte beschlossen werden, wie die Daten bei Bedarf zu verschlüsseln sind. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 9*	1. Januar 2022
Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung Eine Nutzungs- und Sicherheitsrichtlinie ist notwendig, wenn Mobiltelefone für dienstliche Zwecke verwendet werden. Die KBV stellt hierfür ein Musterdokument zur Verfügung. Die Richtlinie sollte Bestandteil von Sicherheitsschulungen sein, die Einhaltung der Richtlinie muss regelmäßig überprüft werden. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 8*	1. Juli 2022

Wechseldatenträger / Speichermedien

Für alle Praxen

Was?	Ab wann?
Angemessene Kennzeichnung der Datenträger beim Versand Der Datenträger sollte für den Empfänger eindeutig gekennzeichnet sein, es sollten aber keine Rückschlüsse für andere möglich sein. Sender und Empfänger sollten sich hier auf eine entsprechende Systematik verständigen. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 29*	1. April 2021
Sichere Versandart und Verpackung Nutzen Sie einen Versand-Anbieter, der ein sicheres Nachweis-System, eine manipulationssichere Versandart und Verpackung nutzt. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 30*	1. April 2021
Schutz vor Schadsoftware Überprüfen Sie Wechseldatenträger bei jeder Verwendung mit einem Antiviren- bzw. Anti-Malware-Programm auf Schadsoftware. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 28*	1. Januar 2022

Sicheres Löschen der Datenträger vor und nach der Verwendung Bevor wieder beschreibbare Datenträger weitergegeben, wiederverwendet oder entsorgt werden, sollten sie in geeigneter Weise gelöscht (mit spezieller Software mehrmals mit Zufallswerten überschrieben) werden. Diese Funktionalität bieten verschieden kommerzielle Anti-Viren und spezielle Open Source Programme an. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 31*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?
Regelung zur Mitnahme von Datenträgern Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. Die KBV stellt hierfür ein Musterdokument zur Verfügung. *IT-Sicherheitsrichtlinie, Anlage 2, Nr.10*	1. Januar 2022

Für große Praxen

Was?	Ab wann?
Datenträgerverschlüsselung Wechseldatenträger sollten vollständig verschlüsselt 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. *IT-Sicherheitsrichtlinie, Anlage 3, Nr. 10*	1. April 2021
Integritätsschutz durch Checksummen oder digitale Signaturen Um beim Datenaustausch mittels mobiler Datenträger die Integrität von vertraulichen Informationen sicherzustellen, sollte ein Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen eingesetzt werden. *IT-Sicherheitsrichtlinie, Anlage 3, Nr. 11*	1. Januar 2022

Netzwerksicherheit

Für alle Praxen

Was?	Ab wann?
Dokumentation des Netzes Dokumentieren Sie die logische Struktur Ihres Netzes, insbesondere Subnetze und wie das Netz zoniert und segmentiert wird. *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 33*	1. April 2021
Grundlegende Authentisierung für den Netzmanagement-Zugriff Verwenden Sie für den Management-Zugriff auf Netzkomponenten und Managementinformationen hinreichend komplexe und starke Passwörter (Es sollten mind. 3 verschiedene Zeichenarten verwendet werden, z. B. Buchstaben, Zahlen und Sonderzeichen). Die Länge eines Passworts sollte mind. 12 Zeichen betragen). *IT-Sicherheitsrichtlinie, Anlage 1, Nr. 34*	1. Januar 2022

Für mittlere und große Praxen

Was?	Ab wann?

Umfassende Protokollierung, Alarmierung und Logging von Ereignissen Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden. *IT-Sicherheitsrichtlinie, Anlage 2, Nr. 11*	1. Januar 2022

Für große Praxen

Was?	Ab wann?
Absicherung von schützenswerten Informationen Übertragen Sie schützenswerte Informationen über vertrauenswürdige dedizierte Netzsegmente oder über nach dem derzeitigen Stand der Technik sichere Protokolle. *IT-Sicherheitsrichtlinie, Anlage 3, Nr. 12*	1. Januar 2022

Medizinische Großgeräte

Für alle Praxen

Was?	Ab wann?
Protokollierung Es müssen alle sicherheitsrelevanten Systemereignisse protokolliert und bei Bedarf ausgewertet werden. In diesem Zusammenhang muss auch festgelegt werden, welche Daten und Ereignisse protokolliert werden sollen, wie lange die Protokolldaten aufbewahrt werden und wer diese einsehen darf. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 3*	1. Januar 2022
Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen Alle nicht genutzten Dienste, Funktionen und Schnittstellen der medizinischen Großgeräte müssen soweit möglich deaktiviert oder deinstalliert werden. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 4*	1. Januar 2022
Netzsegmentierung Trennen Sie medizinische Großgeräte von der weiteren IT. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 6*	1. Januar 2022
Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeitende auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Passwörter müssen gewechselt werden. Der Wechsel muss dokumentiert und das Passwort sicher hinterlegt werden. Standardmäßig eingerichtete bzw. herstellerseitig gesetzte Benutzerkonten sollten gewechselt werden. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 1*	1. Juli 2022
Nutzung sicherer Protokolle für die Konfiguration und Wartung Für die Konfiguration und Wartung von medizinischen Großgeräte müssen verschlüsselte Protokolle wie HTTPS genutzt werden. Die Daten müssen beim Transport vor unberechtigtem Mitlesen und Veränderungen geschützt werden. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 2*	1. Juli 2022
Deaktivierung nicht genutzter Benutzerkonten Nicht genutzte und unnötige Benutzerkonten müssen deaktiviert werden. *IT-Sicherheitsrichtlinie, Anlage 4, Nr. 5*	1. Juli 2022

Dezentrale Komponenten der TI

Für alle Praxen

Was?	Ab wann?
Planung und Durchführung der Installation Berücksichtigen Sie die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten. Lassen sie sich von Ihrem Dienstleister, der die Installation durchführt, Installationsprotokoll und Dokumentation aushändigen. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 1*	1. Januar 2022
Betrieb Berücksichtigen Sie die Anwender- und Administrationsdokumentationen der gematik GmbH und der Hersteller der TI-Komponenten, insbesondere die Hinweise zum sicheren Betrieb der Komponenten. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 2*	1. Januar 2022
Schutz vor unberechtigtem physischem Zugriff Schützen Sie die TI-Komponenten in der Praxis entsprechend den Vorgaben im jeweiligen Handbuch vor dem Zugriff Unberechtigter. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 3*	1. Januar 2022
Betriebsart „parallel“ Wird der Konnektor in der Konfiguration „parallel“ ins Netzwerk des Leistungserbringers eingebracht, müssen zusätzliche Maßnahmen ergriffen werden, um die mit dem Internet verbundene Praxis auf Netzebene zu schützen. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 4*	1. Januar 2022
Geschützte Kommunikation mit dem Konnektor Es müssen Authentisierungsmerkmale für die Clients (Zertifikate oder Username und Passwort) erstellt und in die Clients eingebracht bzw. die Clients entsprechend konfiguriert werden. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 5*	1. Januar 2022
Zeitnahes Installieren verfügbarer Aktualisierungen Prüfen Sie die TI-Komponenten in der Praxis regelmäßig auf verfügbare Aktualisierungen und installieren Sie verfügbare Aktualisierungen zeitnah. Bei Verfügbarkeit einer Funktion für automatische Updates sollte diese aktiviert werden. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 6*	1. Januar 2022
Sicheres Aufbewahren von Administrationsdaten Bewahren Sie die im Zuge der Installation der TI-Komponenten eingerichteten Administrationsdaten sicher auf, insbesondere auch Passwörter für den Administrator-Zugang. Es muss gewährleistet sein, dass der Leistungserbringer auch ohne seinen Dienstleister die Daten kennt. *IT-Sicherheitsrichtlinie, Anlage 5, Nr. 7*	1. Januar 2022

Hinweise zur Umsetzung:

Bitte achten Sie darauf, Ihre Bewertungen, Entscheidungen und Umsetzungen als Nachweis entsprechend zu dokumentieren. Die KV Berlin empfiehlt hierfür, die Anlagen der KBV mit den Prüfpunkten als Checkliste zu verwenden. Hier sollte je Punkt dokumentiert werden, wie dieser umgesetzt ist und welche Referenzdokumentation dazugehört (beispielsweise Passwortrichtlinie, Richtlinie

zur Nutzung mobiler Endgeräte, Benutzerkonzept usw.).
Bei Fragen zur Umsetzung der technischen Rahmenbedingungen, sollten Sie Rücksprache mit Ihrem IT-Dienstleister halten.

Beachten Sie auch das umfassende Schulungs- und Informationsangebot zur IT-Sicherheitsrichtlinie:
Online-Plattform der KBV
Die Online-Veranstaltung der KV Berlin zur IT-Sicherheitsrichtlinie vom 12. März 2021 gibt es als Mitschnitt im Mitgliederbereich
Die KBV bietet eine Online-Fortbildung „IT-Sicherheit in der Praxis“ auf dem KBV-Fortbildungsportal an.

Kontakt für Ärzt:innen und Psychotherapeut:innen

Service-Center der KV Berlin

FAQ: Hier finden Sie Antworten auf häufig gestellte Fragen

Kontakt für Patient:innen

Wann hilft die KV Berlin?

Terminservice:

Weitere Informationen und Termine buchen

Kontakt für Presseanfragen

presse@kvberlin.de

KV BERLIN

Kassenärztliche Vereinigung Berlin
Masurenallee 6A
14057 Berlin

030 / 31 003-0
030 / 31 003-380
Kontakt