Alles Gute.
KVBW
Kassenärztliche Vereinigung Baden-Württemberg

Ihr KVBW-Referententeam

- Frau Nina Hitzelberger
- Herr Bernd Gemeinder

Datenschutz in der Arztpraxis

Schweigepflicht und Datenschutz:
Schon immer ein bisschen mehr

- Strafgesetzbuch
- Ärztliches Berufsrecht
- Bundesdatenschutzgesetz
- EU Datenschutzgrundverordnung
- Bürgerliches Gesetzbuch
- Sozialgesetzbuch

ITSRL

IT-Sicherheits richtlinie

Hintergrund
IT-Sicherheitsrichtlinie

Gesetz
für eine bessere Versorgung durch Digitalisierung und Innovation
(Digitale-Versorgung-Gesetz – DVG)

Vom 9. Dezember 2019

„§ 75b

Richtlinie zur
IT-Sicherheit in der vertragsärztlichen
und vertragszahnärztlichen Versorgung

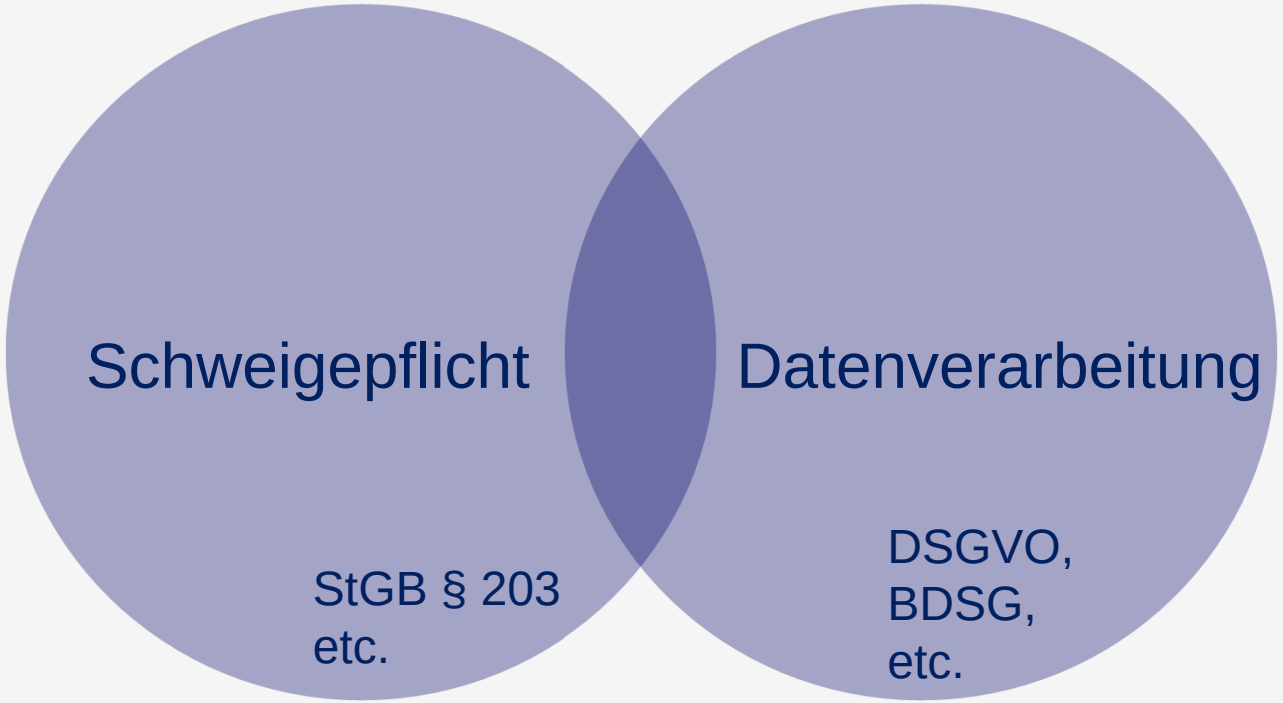
(1) Die Kassenärztlichen Bundesvereinigungen legen bis zum 30. Juni 2020 in einer Richtlinie die Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung fest. Die Richtlinie umfasst auch Anforderungen an die sichere Installation und Wartung von Komponenten und Diensten der Telematikinfrastruktur, die in der vertragsärztlichen und vertragszahnärztlichen Versorgung genutzt werden.

und an das Gefährdungspotential anzupassen. Die in der Richtlinie festzulegenden Anforderungen sowie deren Anpassungen erfolgen im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik sowie im Benehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesärztekammer, der Bundeszahnärztekammer, der Deutschen Krankenhausgesellschaft und den für die Wahrnehmung der Interessen der Industrie maßgeblichen Bundesverbänden aus dem Bereich der Informationstechnologie im Gesundheitswesen. Die Anforderungen nach Absatz 1 Satz 2 legen die Kassenärztlichen Bundesvereinigungen zusätzlich im Benehmen mit der Gesellschaft für Telematik fest.

Nutzen der IT-Sicherheitsrichtlinie (ITSRL)

- soll die Praxisleitung dabei unterstützen
  alle nötigen Sicherheitsvorkehrungen zu treffen,
  um einen Datenmissbrauch zu verhindern
- soll IT-Systeme und sensible Daten noch besser schützen
- sie „erfindet“ keine zusätzlichen Vorgaben
- sondern macht bestehende Regeln praxistauglich
- gibt verlässlichen Rahmen

Datenschutz-Schnittmengen



Praxisinterne Datenschutz-Richtlinie

Was tun wir alles um Datenschutz und Schweigepflicht einzuhalten?

- Verhaltensregeln
- Organisationsregeln
- IT-Sicherheitskonzept
- Dokumentation

Organisationsregeln

- Schweigepflichtserklärungen (Mitarbeiter, etc.) einholen
- Patientenunterlagen unzugänglich aufbewahren
  (ggf. Räume, Schränke abschließen)
- **Beim Arbeiten: Bildschirme nicht einsehbar machen**
- **Beim Verlassen: Bildschirme sperren mit Passwortschutz**
- Aktenvernichter mind. Sicherheitsstufe 4 benutzen
- Dokumentations- und Aufbewahrungspflichten umsetzen
- Löschkonzept (nach Ablauf der Aufbewahrungsfristen) umsetzen
- Patienteneinsichts- (und Auskunfts-) Recht umsetzen
- Meldepflicht für Datenpannen organisieren
- ggf. Datenschutzbeauftragten einsetzen

Dokumentationspflichten

- Datenschutz-Information bei der Datenerhebung - Mustervorlage
- Datenschutz-Information auf der Homepage - Mustervorlage
- Verzeichnis der Verarbeitungstätigkeiten - Mustervorlage
  einschl. **Beschreibung:**
- aller **technischen und organisatorischen Maßnahmen (TOMs)**
- Einwilligungserklärungen - Mustervorlage
- Schweigepflichtserklärungen - Mustervorlage
- Verträge für Auftragsverarbeitung (AV-Verträge)
  (EDV-Firma, externe Aktenvernichtung, Lohnbüro, PVS, etc.)
- ggf. Ernennungsurkunde DSB - Mustervorlage
- (ggf. und selten) Datenschutz-Folgenabschätzung

IT-Sicherheitskonzept – bisher

Dazu gehören z. Bsp.:

- Archivsicheres Dokumentieren und Scannen
- Automatische Updates im Betriebssystem aktivieren
- Automatische Updates des Browsers aktivieren
- Backups ausführen
- Aktueller Virenscanner/Sicherheitssoftware einsetzen
- PVS und Recherche-PC trennen
- Zugriffs- und Berechtigungskonzept festlegen
- Passwortschutz einsetzen
- Ende-zu-Ende und Transportverschlüsselung bei Onlineterminbuchung
- …

Art. 32 DSGVO

Artikel 32

Sicherheit der Verarbeitung

EG 83

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

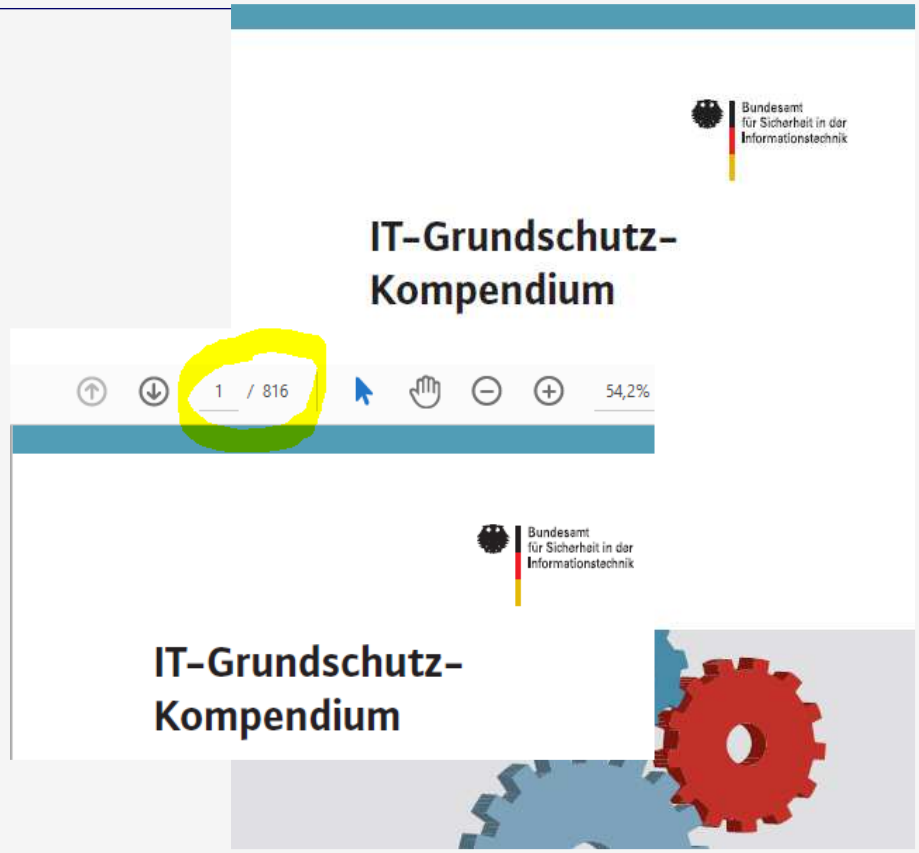
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Unternehmer und Dokumentation

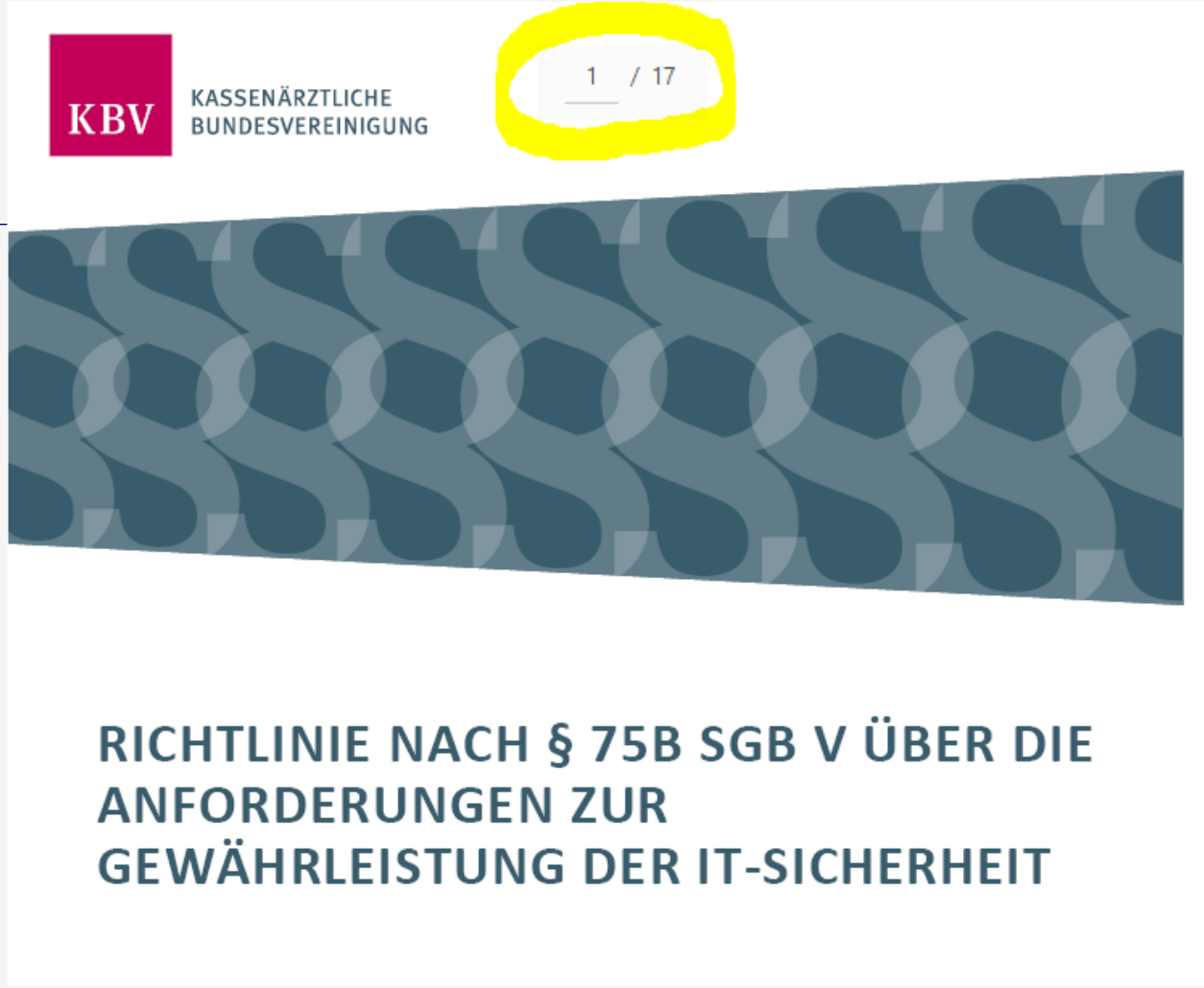
Jeder Unternehmer muss zur Umsetzung der IT-Sicherheit technische und organisatorische Maßnahmen (TOMs) umsetzen

Basis:
Das IT-Grundschutzkompendium des BSI



ITSRL

IT-Sicherheits richtlinie



Nutzen der ITSRL

- Konkretisiert die Maßnahmen zur Umsetzung der EU-DSGVO
- Unterstützt die Praxisleitung dabei alle nötigen Sicherheitsvorkehrungen zu treffen, um einen Datenmissbrauch zu verhindern
- Gibt einen Handlungsrahmen
- Abgestimmt mit dem BSI
- Stand der Technik
- Aktuelle Vorgaben - Jährliche Aktualisierungen
- Anwendungskriterien in 5 Anlagen auf 17 Seiten

Struktur der ITSRL

- Stand der Technik der technisch-organisatorischen Maßnahmen im Sinne von Artikel 32 DSGVO
- Darstellung in 5 getrennten Anlagen
- Legt technische Anforderungen fest
- Beschreibt das Mindestmaß
- Differenziert nach Größe der Praxis
- Zeitenvorgabe für die Umsetzung je Anforderung/Maßnahme
- Betrifft Hard- und Software / Zielobjekte

Die ITSRL unterscheidet 3 Praxisgrößen

Wie wird gezählt?

Einfach nach Köpfen

Jeder IT-Anwender ist
ein IT-Risiko

ITSRL

I. PRÄAMBEL

Die Kassenärztliche Bundesvereinigung hat nach § 75b SGB V den Auftrag, Anforderungen zur Gewährleistung der IT-Sicherheit in der vertragsärztlichen Versorgung zu regeln. Sie hat damit den Auftrag, den Stand der Technik der technisch-organisatorische Maßnahmen im Sinne von Artikel 32 Datenschutz-Grundverordnung zu standardisieren. Die hier getroffenen Richtlinien erfüllen diesen Auftrag und dienen damit dem Zweck, die Handhabung der Vorgaben der Datenschutz-Grundverordnung im Zusammenhang mit der elektronischen Datenverarbeitung für die vertragsärztliche Praxis zu vereinheitlichen und zu erleichtern.

Die Richtlinie adressiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme in der vertragsärztlichen –psychotherapeutischen Praxis. Die Richtlinie legt technischen Anforderungen fest und beschreibt das Mindestmaß der zu ergreifenden Maßnahmen, um die Anforderungen der IT-Sicherheit zu gewährleisten. Mit der Umsetzung der Anforderungen werden die Risiken der IT-Sicherheit minimiert. Bei der Umsetzung können Risiken auch an Dritte, wie IT-Dienstleister oder Versicherungen, übertragen oder durch den Verantwortlichen akzeptiert werden.

II. GELTUNGSBEREICH

1. Diese Richtlinie legt die in einer vertragsärztlichen bzw. vertragspsychotherapeutischen Praxis erforderlichen Anforderungen an die IT-Sicherheit fest.
2. Der/die Praxisinhaber ist/sind verantwortlich für die Einhaltung der Anforderungen dieser Richtlinie.

Die ITSRL hat 5 Anlagen

ANLAGE 1

Anforderungen für Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Software: Rechner-Programme, mobile Apps und Internet-Anwendungen			
1.	Mobile Anwendungen (Apps)	Sichere Apps nutzen	Nur Apps aus den offiziellen Stores runterladen und	01.04.2021
2.	Mobile Anv (Apps)			
3.	Mobile Anv (Apps)			
4.	Mobile Anv (Apps)			
5.	Office-Prod			

ANLAGE 2

Zusätzliche Anforderungen für mittlere Praxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	ner-Programme, mobile Apps und Internet-Anwendungen			
	lungen	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.	01.04.2021
		Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.	01.01.2022
	geräte und IT-Systeme			
		Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von	01.01.2022

ANLAGE 3

Zusätzliche Anforderungen für Großpraxen

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
	Hardware: Endgeräte und IT-Systeme			
1.	Smartphone und Tablet	Festlegung einer Richtlinie für den Einsatz von Smartphones und Tablets	Be Sm be eir	

ANLAGE 4

ıngen bei der Nutzung medizinischer Großgeräte

	Anforderung	Erläuterung	Geltung ab
	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen	Es muss sichergestellt werden, dass nur zuvor festgelegte berechtigte Mitarbeiter auf Konfigurations- und Wartungsschnittstellen von medizinischen Großgeräten zugreifen können. Standardmäßig eingerichtete	01.07.2021

ANLAGE 5

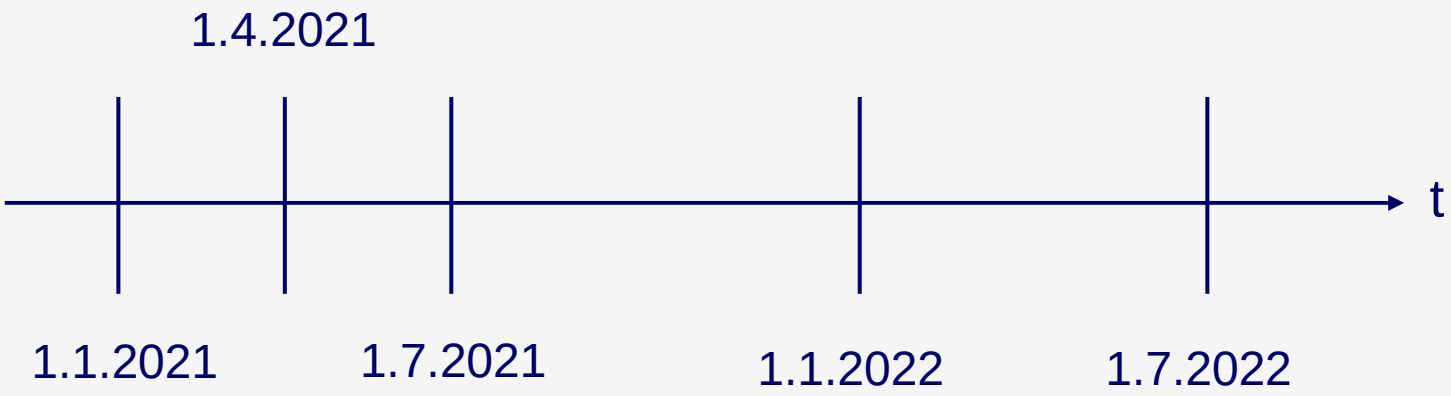
DEZENTRALE KOMPONENTEN DER TELEMATIKINFRASTRUKTUR

	Zielobjekt	Anforderung	Erläuterung	Geltung ab
1.	Dezentrale Komponenten der TI	Planung und Durchführung der Installation	Die von der gematik GmbH auf Ihrer Website zur Verfügung gestellten Informationen für die Installation der TI-Komponenten müssen berücksichtigt werden.	01.01.2022

Mitgeltende Anlagen in Abhängigkeit der Praxisgröße

Praxis-Typ	Anzahl der Personen	umzusetzende Anlage
(Klein)Praxis	1 bis 5	1, 5
mittlere Praxis	6 bis 20	1, 2, 5
Großpraxis	ab 21	1, 2, 3, 5
alle Praxen mit medizinischen Großgeräten (z. Bsp. CT)	unabhängig von der Personenanzahl	4
alle Praxen	unabhängig von der Personenanzahl	5

Zeitvorgaben



Nur eine einzige Aufgabe zum 1.1.2021 für alle

Eine Aufgabe zum TI-Konnektor

Anlage 5 Nummer 5

Primärsysteme	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.

Anforderungen aus Anlage 1 für **alle** Praxen

mit der ersten Frist
ab
1.4.2021

Anlage 1 Nummer 1 / **Sichere Apps nutzen:** Apps werden nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.

Anlage 1 Nummer 4 / **Verhinderung von Datenabfluss:** Es werden keine vertraulichen Daten über Apps versendet.

Anlage 1 Nummer 8 / **Schutz vertraulicher Daten:** Der Internet-Browser ist so eingestellt, dass in dem Browser keine vertraulichen Daten gespeichert werden.

Anlage 1 Nummer 10 / **Kryptografische Sicherung vertraulicher Daten:** Es werden NUR verschlüsselte Internet-Anwendungen genutzt.

Anlage 1 Nummer 13 / **Abmelden oder Sperren:** Nach der Nutzung eines Gerätes meldet sich die Person ab oder sperrt es.

Anlage 1 Nummer 15 / **Einsatz von Virenschutzprogrammen:** In der Praxis werden aktuelle Virenschutzprogramme eingesetzt.

Anlage 1 Nummer 22 / **Zugriffsschutz verwenden:** Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt.

Anlage 1 Nummer 33 / **Dokumentation des Netzes:** Das interne Netzwerk ist anhand eines Netzplanes dokumentiert. *Musterdokument online verfügbar*

Anlage 1 Nummer 12 / **Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras:** Kamera und Mikro sollten grundsätzlich deaktiviert sein und nur bei Bedarf aktiviert und danach wieder deaktiviert werden.

Anlage 1 Nummer 27 / **Updates von Mobiltelefonen:** Regelmäßig prüfen, ob es Updates gibt.

Anforderungen aus Anlage 1 für **alle** Praxen

mit der ersten Frist
ab
1.4.2021

Anlage 1 Nummer 1 / **Sichere Apps nutzen:** Apps werden nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.

Anlage 1 Nummer 4 / **Verhinderung von Datenabfluss:** Es werden keine vertraulichen Daten über Apps versendet.

Anlage 1 Nummer 8 / **Schutz vertraulicher Daten:** Der Internet-Browser ist so eingestellt, dass in dem Browser keine vertraulichen Daten gespeichert werden.

Anlage 1 Nummer 10 / **Kryptografische Sicherung vertraulicher Daten:** Es werden NUR verschlüsselte Internet-Anwendungen genutzt.

Anlage 1 Nummer 13 / **Abmelden oder Sperren:** Nach der Nutzung eines Gerätes meldet sich die Person ab oder sperrt es.

Anlage 1 Nummer 15 / **Einsatz von Virenschutzprogrammen:** In der Praxis werden aktuelle Virenschutzprogramme eingesetzt.

Anlage 1 Nummer 22 / **Zugriffsschutz verwenden:** Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt.

Anlage 1 Nummer 33 / **Dokumentation des Netzes:** Das interne Netzwerk ist anhand eines Netzplanes dokumentiert. *Musterdokument online verfügbar*

Anlage 1 Nummer 12 / **Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras:** Kamera und Mikro sollten grundsätzlich deaktiviert sein und nur bei Bedarf aktiviert und danach wieder deaktiviert werden.

Anlage 1 Nummer 27 / **Updates von Mobiltelefonen:** Regelmäßig prüfen, ob es Updates gibt.

Anforderungen aus Anlage 1 für **alle** Praxen

mit der ersten Frist
ab
1.4.2021

Anlage 1 Nummer 1 / **Sichere Apps nutzen:** Apps werden nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden.

Anlage 1 Nummer 4 / **Verhinderung von Datenabfluss:** Es werden keine vertraulichen Daten über Apps versendet.

Anlage 1 Nummer 8 / **Schutz vertraulicher Daten:** Der Internet-Browser ist so eingestellt, dass in dem Browser keine vertraulichen Daten gespeichert werden.

Anlage 1 Nummer 10 / **Kryptografische Sicherung vertraulicher Daten:** Es werden NUR verschlüsselte Internet-Anwendungen genutzt.

Anlage 1 Nummer 13 / **Abmelden oder Sperren:** Nach der Nutzung eines Gerätes meldet sich die Person ab oder sperrt es.

Anlage 1 Nummer 15 / **Einsatz von Virenschutzprogrammen:** In der Praxis werden aktuelle Virenschutzprogramme eingesetzt.

Anlage 1 Nummer 22 / **Zugriffsschutz verwenden:** Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt.

Anlage 1 Nummer 33 / **Dokumentation des Netzes:** Das interne Netzwerk ist anhand eines Netzplanes dokumentiert. *Musterdokument online verfügbar*

Anlage 1 Nummer 12 / **Verhinderung der unautorisierten Nutzung von Rechner-Mikrofonen und Kameras:** Kamera und Mikro sollten grundsätzlich deaktiviert sein und nur bei Bedarf aktiviert und danach wieder deaktiviert werden.

Anlage 1 Nummer 27 / **Updates von Mobiltelefonen:** Regelmäßig prüfen, ob es Updates gibt.

Anforderung aus Anlage 2 für **mittlere und große** Praxen

mit erster Frist
ab
01.04.2021

Anlage 2 Nummer 1 / Minimierung und Kontrolle von App-Berechtigungen: Bevor eine App eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält; weitere müssen hinterfragt und gegebenenfalls unterbunden werden.

Anforderung aus Anlage 3 nur für **Großpraxen**

mit erster Frist
ab
01.04.2021

Anlage 3 Nummer 10

Wechseldatenträger / Speichermedien	Datenträgerverschlüsselung	Wechseldatenträger sollten vollständig verschlüsselt werden.

DSB online melden/abmelden/löschen | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

Anlage 4
Medizinische Großgeräte

mit erster Frist
ab
01.07.2021

Anlage 4 Nummer 5

5.¤	Medizinische·Großgeräte¤	Deaktivierung·nicht·genutzter·Benutzerkonten¤	Nicht·genutzte·und·unnötige·Benutzerkonten·müssen·deaktiviert·werden.¤

Anlage 5
Dezentrale Komponenten der TI

mit erster Frist
ab
01.01.2021

Anlage 5 Nummer 5

Primärsysteme	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.

Serviceseite der KBV

https://hub.kbv.de/site/its
https://www.kbv.de

KBV

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

Unterseite der KBV

https://hub.kbv.de/display/itsrl

Dienstleister?

- Sie „können“ einen Dienstleister zur Unterstützung einbeziehen
- Dienstleister „können“ sich nach der Richtlinie zur Zertifizierung (§ 75 b Absatz 5 SGB V) zertifizieren lassen
- Zertifizierte Dienstleister finden Sie über die KBV-Seite: https://www.kbv.de/media/sp/KBV_ISAP_Dienstleister_ZERT_P75b_SGB V.pdf

DSGVO > ITSRL

Was ist wenn…?

… etwas schief geht? → „Datenpanne“ → Meldepflicht

Meldepflicht → Aufsichtsbehörde
Meldepflicht → ggf. betroffene Person/en

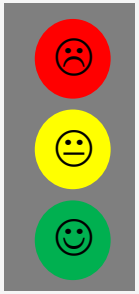
Aufsichtsbehörde → Untersuchung/Analyse

Untersuchung/Analyse → Strafbar? Mitwirkung? → Bußgeld
DSGVO

Vorgehensweise

1. Selbstbewertung:

   - Welche Praxisgröße gilt?
   - Welche Anlagen sind für mich relevant?
   - Diese Anlagen lesen
   - Welche Anforderungen sind schon umgesetzt?
   - Welche Anforderungen sind noch offen?
     „Ampelprinzip“



1 PRAXISTYP FESTLEGEN

Welcher Praxistyp sind wir?
Je nach Praxistyp müssen die Anforderungen nach den entsprechenden Anlagen erfüllt werden:

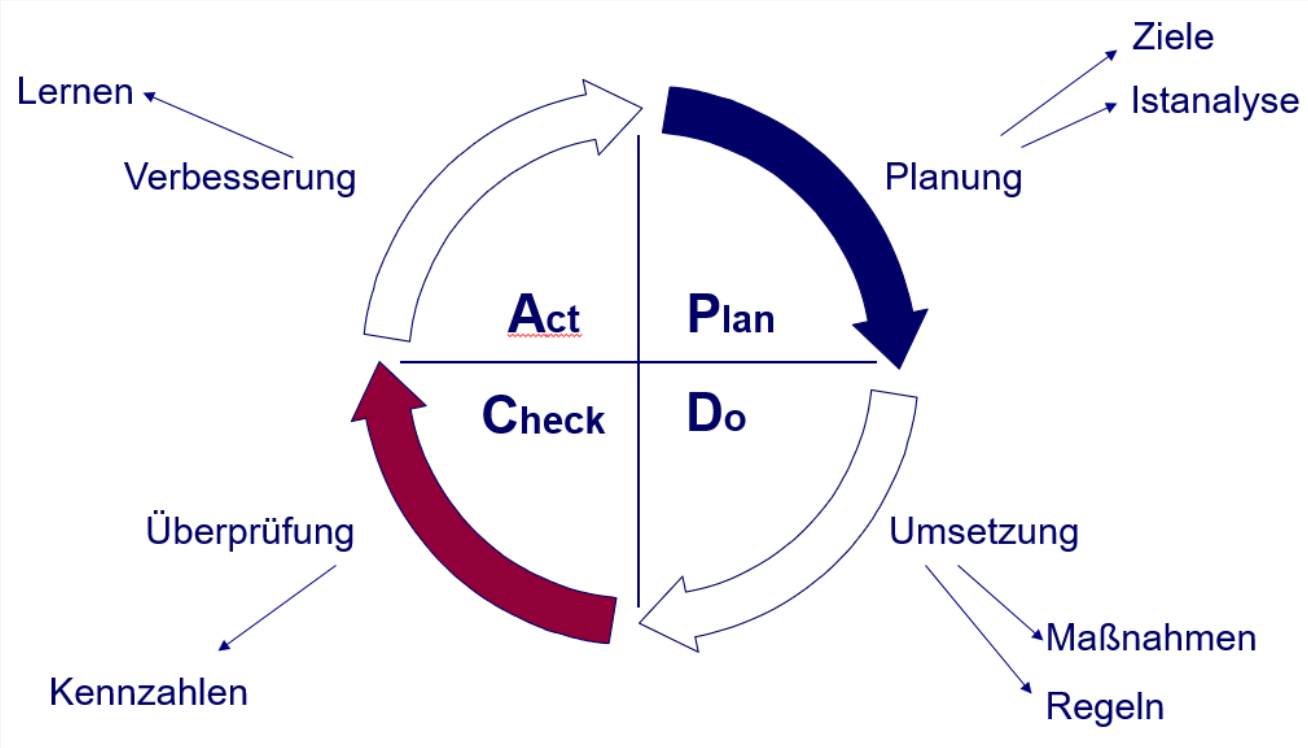
Praxis mit 1 bis 5 Personen*
Anlage 1, 5 (und 4 bei medizinischen Großgeräten)

Mittlere Praxis mit 6 bis 20 Personen*
Anlage 1, 2, 5 (und 4 bei medizinischen Großgeräten)

Große Praxis mit mehr als 21 Personen*
oder sehr vielen Daten
Anlage 1, 2, 3, 5 (und 4 bei medizinischen Großgeräten)

* ständig mit der Datenverarbeitung betraute Personen

Offene Aufgaben umsetzen
Managementprinzip



Neue Aufgaben/Änderungen nachhaltig umsetzen

1. Auftrag festlegen
2. Brainstorming
   - Idee 1
   - Idee 2
   - Idee 3
   - …
3. Entscheidung und Festlegung:

   Maßnahme oder Regel?

   ↓ ToDo-Liste

   ↓ QMH
4. Check:

   Maßnahmen umgesetzt? Regeln eingehalten?

Maßnahmenplan / Todo-Liste

Nr.	Was?	Wer?	Mit?	Bis wann?
1	Selbstbewertung ITSRL	PL alleine Oder mit Team Oder mit IT-ler	ITSRL	Ende April
2	Besprechung	PL mit bisherigem IT-ler/DvO		
3	…			
4	Netzplan		Muster KBV	

Informationen und Quellen u.a.m.

- KBV Themenseite zur ITSRL:
  https://www.kbv.de/html/it-sicherheit.php
- Sonderseite der KBV zur ITSRL:
  https://hub.kbv.de/display/itsrl
- Broschüre PraxisWissen:
  IT-Sicherheit
- Ansprechpartner der KBV
  Dezernat Digitalisierung und IT
  030 40 05 - 21 21 und/oder servicedesk@kbv.de
- Homepage KVBW: Infos und Ansprechpartner
  http://www.kvbawue.de/praxis/unternehmen-praxis/datenschutz-schweigepflicht/

Kurze Zusammenfassung Informations-Video der KBV

Vielen Dank für Ihre Aufmerksamkeit!