

Checkliste

(Stand: 26.04.2018)

Europäische Datenschutzgrundverordnung (EU-DSGVO) in der Arztpraxis

Ab dem 25.05.2018 müssen Ärzte und Psychotherapeuten nach der EU-DSGVO nicht nur die datenschutzrechtlichen Vorgaben einhalten, sondern diese auch nachweisen.

Insbesondere in Bezug auf die Überwachung, Sicherung und Pflege Ihrer EDV-Anlage können wir Ihnen viel Arbeit abnehmen. Sie finden bei den entsprechenden Punkten einen Vermerk.

Sicherheit

Quelle: (KBV)

Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten, die in der Praxis anfallen

Zusammenstellung der technischen und organisatorischen Maßnahmen, die die Praxis zum Schutz von personenbezogenen Daten ergreift.

Bereitstellung einer Patienteninformation zum Datenschutz in der Praxis, zum Beispiel als Aushang in den Praxisräumen und auf der Praxis-Website

Verträge zur Auftragsverarbeitung mit Softwareanbietern und anderen Dienstleistern anpassen oder neu abschließen. Solche Verträge sind notwendig, wenn Auftragnehmer auf Patienten- oder Mitarbeiterdaten zugreifen können

Praxen, die mit Einwilligungserklärungen des Patienten arbeiten, zum Beispiel zur Weitergabe von Daten an eine privatärztliche Verrechnungsstelle, müssen die Erklärung um einen Hinweis auf Widerrufbarkeit ergänzen

Praxen, die eine Internet- oder Facebook-Seite anbieten, sollten die Datenschutzerklärung prüfen und gegebenenfalls anpassen; dies gilt ebenso, wenn personenbezogene Daten zum Beispiel über Kontaktformulare oder für einen Praxis-Newsletter erfasst und gespeichert werden

Praxen ab 10 Mitarbeiter und MVZ's

Beauftragen eines Datenschutzbeauftragten, wenn in der Praxis mindestens zehn Personen regelmäßig personenbezogene Daten automatisiert verarbeiten, zum Beispiel am Empfang oder bei der Abrechnung. Übernimmt ein Mitarbeiter diese Aufgabe, benötigt dieser eventuell eine Schulung

Melden der Kontaktdaten des Datenschutzbeauftragten der Praxis an die zuständige Aufsichtsbehörde.



EDV / Datenweitergabe

Ist der Zugang zum Computer durch Passwörter geschützt?

- e+e vor Ort individuell

Entsprechen Ihre Passwörter dem aktuellen Sicherheitsstandard (8 Stellen, bestehend aus Buchstaben, Zahlen und Sonderzeichen)?

- e+e vor Ort individuell

Werden mitgeteilte Passwörter zur EDV-Nutzung vertraulich behandelt und bei Verdacht der Kenntnisnahme durch Dritte sofort geändert?

Werden Passwörter in gewissen Zeitabständen geändert?

- e+e vor Ort individuell

Können Sie beim Verlassen des Arbeitsplatzes den Computer sperren?
Die Praxissoftware können Sie wie folgt sperren:

- x.isynet: Job anlegen: Direktbefehl „Fertig“ + „BW“ (Benutzerwechsel)
- medatixx: Direktbefehl „BW“ (Benutzerwechsel)

Sind Computer mit Patientendaten, die mit dem Internet verbunden sind, tatsächlich ausreichend geschützt („Firewall“)?

Wird täglich eine verschlüsselte Sicherung Ihrer Daten durchgeführt, kontrolliert und sicher außerhalb Ihrer Praxis aufbewahrt?

- e+e Online Backup
- e+e Datensicherung Crypt

Einsatz eines Antivirusprogramm und tägliche Kontrolle auf Aktualität?

- e+e Managed AntiVirus

Einsatz einer Sicherheitslösung ein, die den Internetzugriff absichert und schädliche Internetseiten blockiert?

- e+e Managed WebProtection

Regelmäßige Installation von Betriebssystem- und Programmupdates. Wöchentliche Kontrolle von automatischen Updateinstallationen.

- e+e VIP Wartungs- und Servicepaket

Regelmäßige Kontrolle der Ereignisprotokolle Ihrer Rechner, insbesondere Ihres Servers um Versuche von unberechtigtem Zugriff frühzeitig erkennen zu können.

- e+e VIP Wartungs- und Servicepaket

Achten Sie bei der Übermittlung von Patientendaten darauf, dass die Empfänger nicht mehr Informationen erhalten, als diese zur Erfüllung ihrer Aufgaben benötigen?

Bei der Übermittlung von Daten an Dritte überprüfen Sie vor der Übermittlung, ob die Auskünfte, Berichte oder Bescheinigungen nicht auch über den Patienten schriftlich weitergegeben werden können?

Liegt eine schriftliche Einwilligung des Patienten vor, falls Sie eine externe privatärztliche Verrechnungsstelle oder ein Labor beauftragt haben?

Wird geprüft, dass bei der Weiterleitung von Unterlagen an Dritte (z. B. Versicherungen, MDK, Ärzte etc.) eine schriftliche Zustimmung des Patienten vorliegt. Ein Versand ist mit Datum und Empfänger in der Patientenkartei zu dokumentieren.

Für Vollständigkeit und rechtlich übernehmen wir keine Gewähr. Wir empfehlen Ihnen ergänzend an den Informationsveranstaltungen Ihrer KV und der Aufsichtsbehörde teilzunehmen und sich ggf. durch einen externen Datenschutzbeauftragten beraten zu lassen.