Checkliste zum Datenschutz in Ihrer Praxis

Vorlage von

Benjamin Dick, Fachberater für Datenschutz und IT-Sicherheit,
Bautzner Straße 149, 01099 Dresden

Tel: 0151 420 931 43

Web: www.bedi-datenschutz.de

Mail: hallo@bedi-datenschutz.de

Liebe Praxisinhaberin, lieber Praxisinhaber,

das Thema Datenschutz ist auch in ambulanten Praxen nicht neu. Viele InhaberInnen handeln in der guten Überzeugung, alle gesetzlichen Vorgaben und Bestimmungen einzuhalten. Ohne ihr Wissen tun sie das dennoch selten und sind Haftungsrisiken ausgesetzt, die sie sicher fühlen können, aber nicht lokalisieren.

Datenschutz bestimmt auch meine tägliche Arbeit, denn ich unterstütze speziell ambulante ärztliche und therapeutische Praxen als Datenschutzbeauftragter und IT-Sicherheitsberater. Daher weiß ich um die tatsächliche Situation im ambulanten Gesundheitswesen.
Auch Praxen, die eine MitarbeiterIn als Datenschutzbeauftragten bestellt haben, erfüllen oft die Vorgaben nicht. Eine kurze Weiterbildung zu diesem Thema ersetzt einfach nicht die organisatorischen, rechtlichen und vor allem technischen Aspekte, die Datenschutz wirklich ausmachen. Im Alltag haben diese Mitarbeiter auch oft nicht die nötige Zeit für diese Verantwortung- hier kann man mindestens 15h pro Woche ansetzen.

Damit Sie eine Vorstellung davon bekommen, welche Aspekte Ihrer Praxis eine Relevanz für den Datenschutz haben, stelle ich Ihnen gern eine Checkliste zur Verfügung. Sie dient Ihrer kurzen Positionsbestimmung.
Bitte haben Sie Mut und beantworten die Fragen aufrichtig. Jede verdeckte Problemzone ist Ihr persönliches Haftungsrisiko. Keine Angst, genau wie ich verurteilt die Checkliste Sie nicht 😉.
Haben Sie alle Punkte erfüllt? Glückwunsch! Sie oder Ihr Dienstleister leisten wirklich gute Arbeit.
Erfüllen Sie nicht alle Punkte? Dann sollten Sie sich mit Ihrem Datenschutz-beauftragten dringend zusammensetzen. „Das machen andere Praxen auch so“ ist kein Freibrief. Jede InhaberIn muss das eigene Haftungsrisiko selbst einschätzen und tragen. Vielleicht wissen die anderen ja nicht was sie tun…?

Wenn Sie bislang keinen Beauftragten bestellt haben, vereinbaren Sie gern über meine Website ein Kennenlerngespräch. Ich helfe immer.

Herzliche Grüße,
Benjamin Dick

	Ja	Nein	Unbekannt
Organisationskontrolle			
Ist ein Datenschutzbeauftragter bestellt worden?			
Existiert ein vollständiges Verzeichnis der Verarbeitungs-tätigkeiten, das regelmäßig aktualisiert wird?			
Sind alle Mitarbeiter schriftlich zum Datengeheimnis verpflichtet?			
Ist in den letzten 12 Monaten eine Mitarbeiterschulung zum Datenschutz erfolgt?			
Wurde bereits ein Datenschutzkonzept erarbeitet?			
Wird die Einhaltung des Datenschutzkonzeptes geprüft und dokumentiert?			
Ist in der Praxis mehr als ein Arzt oder Therapeut beschäftigt?			
Zutrittskontrolle			
Ist der Zutritt zu Geschäftsräumen auf einen bekannten Personenkreis beschränkt?			
Ist die IT-Hardware nur für befugtes Personal zugänglich?			
Sind Server und PC sicher aufgestellt? (Einsicht durch Unbefugte, Diebstahlschutz)			
Ist der Zutritt zu Räumen beschränkt, in denen Datenmaterial verwahrt wird (Akten, Datenträger, IT-Komponenten, ...)?			
Zugangskontrolle			
Sind auf jedem Gerät Bildschirmsperren eingerichtet?			
Wurde eine Hardware Firewall oder vergleichbare Software-Appliance installiert, aktiviert, aktualisiert?			
Ist Software zum Schutz vor Schadsoftware installiert, aktiviert und aktualisiert?			
Ist auf jedem Endgerät eine Benutzeridentifikation/Authentifizierung eingerichtet?			
Verwenden alle Nutzer (eigene) sichere Passwörter?			
Zugriffskontrolle			
Liegt ein Konzept für Zugriffsberechtigungen vor?			
Wurden gemäß eines definierten Rollenkonzepts unterschiedliche Zugriffsrechte eingeteilt?			
Werden Verstöße und Verletzungen der Zugriffsbeschränkungen protokolliert?			
Werden Datenträger/Datenblätter sicher entsorgt?			
Wurde wo nötig ein Kopierschutz/Bearbeitungsschutz eingerichtet?			

Weitergabekontrolle			
Ist auf allen Endgeräten eine Datenverschlüsselung eingerichtet und aktiv?			
Finden eine regelmäßige Wartung und Prüfung der Datenverarbeitungssysteme statt?			
Nutzen Sie Facebook, WhatsApp oder andere soziale Medien?	Nein	Ja	
Vertragsmanagement			
Wurden mit allen relevanten Dienstleistern, Softwareanbietern und sonstigen Datenverarbeitern Verträge zur Auftragsdatenverarbeitung erarbeitet?			
Wird die Einhaltung der Verpflichtungen aus den Auftragsdatenverarbeitungsverträgen (stichprobenartig) kontrolliert?			
Wurde mit jedem Patienten ein Behandlungsvertrag geschlossen, in dem auf die Datenspeicherung, evtl. Online-Dienste und die Rechte der Betroffenen eingegangen wird?			
KBV IT-Sicherheitsrichtlinie			
Erfüllen Sie alle auf Ihre Praxis zutreffenden Anforderungen und prüfen das regelmäßig?			
Wird die Einhaltung der initial getroffenen Vorkehrungen und Einstellungen regelmäßig kontrolliert?			
Ist der Konnektor vor unbefugten Zugriffen geschützt?			
Werden die relevanten Systeme regelmäßig durch eine Datensicherung geschützt?			
Ist sichergestellt, dass auf allen Endgeräten und Servern ausschließlich Software/Apps betrieben werden, die unter aktuellem Herstellersupport stehen (Kein End-Of-Life)?			
Qualitätssicherung			
Wurden alle Prozesse dokumentiert, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen?			
Wird die Einhaltung der Prozesse (stichprobenartig) kontrolliert?			
Notfallmanagement			
Sind für verschiedene Notfallszenarien Abläufe und Informationswege definiert und allen relevanten Personen bekannt?			
Werden die hinterlegten Kontaktinformationen aktuell gehalten?			