DATA*privat*
Datenschutz für die Praxis

Praxis-Check Datenschutz

Ist meine Praxis auf die DSGVO vorbereitet?

Ein Schnelltest…

Dieser Schnelltest soll Ihnen eine Hilfe sein, um einzuschätzen, wie fit Ihre Praxis im Datenschutz aktuell ist. Versuchen Sie alle Fragen möglichst gewissenhaft und ehrlich zu beantworten, machen Sie bei jeder Frage immer nur 1 Kreuz und nehmen Sie bei jeder Frage die Antwort, die auf Ihre Praxis am ehesten zutrifft. Seien Sie hier vorsichtig und wählen Sie, wenn Sie sich nicht sicher sind, lieber Antwort 2 als Antwort 1 bzw. Antwort 3 als Antwort 2; Safety first! Nur wenn die Frage für Ihre Praxis keine Relevanz hat, wählen Sie Antwort 4.

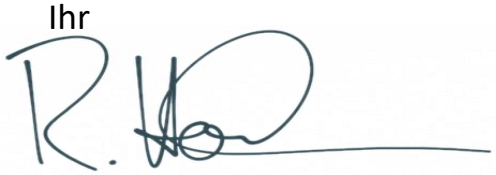
Der Test ist geeignet für alle Praxen von Heilmittelerbringern und Ärzten.

Eine Anleitung zur Auswertung finden Sie im Anschluss an diesen Test.

Es ist sehr einfach! Der Test dauert ca. 25 Minuten.

Viel Spaß!

Ihr



Rainer Horbach
DATA*privat*
Rechtsanwalt
Datenschutzbeauftragter (extern)

Achtung! ***Bitte beachten Sie, dass dieser Test Ihnen nur eine sehr grobe Einschätzung geben und nicht alle möglichen Risiken und Bedrohungsszenarien abbilden kann. Eine abschließende Auskunft über den Stand des Datenschutzes in Ihrer Praxis erhalten Sie nur durch eine fachkundige Prüfung vor Ort. Nehmen Sie das Ergebnis dieses Tests keinesfalls als einzige Beratungsgrundlage für Entscheidungen zum Datenschutz.***

Frage Nr. 1
Welche Maßnahmen haben Sie in Ihrer Praxis, damit papierhafte Patientenakten und Rezepte nicht einfach offen herumliegen und von unberechtigten Personen gelesen werden können?

1. Es besteht eine schriftliche Anweisung für das gesamte Praxispersonal, wie mit den papierhaften Patientenakten umzugehen ist. Alle Patientenakten werden in abschließbaren Schränken gelagert. Die für das Tagesgeschäft erforderlichen Akten werden in einem sicheren Behältnis im Anmeldetresen aufbewahrt. Die Therapeutinnen und Therapeuten sind schriftlich angewiesen, Patientenakten aus den Schränken nur unmittelbar für die Behandlung herauszunehmen und nach der Behandlung wieder im Schrank einzuschließen. Der Karteikasten mit den Patientenakten für das Tagesgeschäft wird nach Dienstschluss und wenn die Anmeldung nicht besetzt ist, in den Aktenschrank eingeschlossen. Rezepte unterschreiben Patienten auf einem verdeckten Klemmbrett in den Behandlungskabinen.

2. Es bestehen mit allen Mitarbeiterinnen und Mitarbeitern eine mündliche Abrede darüber, wie mit papierhaften Patientenakten umzugehen ist. Die Patientenakten werden grundsätzlich im abgeschlossenen Holzschrank aufbewahrt. Die Akten für das Tagesgeschäft befinden sich in einem Holzkasten auf dem Anmeldetresen. Rezepte unterschreiben die Patienten sowohl in den Kabinen, als auch am Anmeldetresen. Es wird dabei darauf geachtet, dass Rezepte nur unterschrieben werden, wenn keine anderen Patienten am Anmeldetresen stehen.

3. Alle Therapeutinnen und Therapeuten sowie die Bürokräfte sind sich der besonderen Verantwortung, die sich aus der Beziehung zu unseren Patienten ergibt, bewusst. Ausdrückliche Absprachen zum Umgang mit Patientenakten haben wir daher nicht getroffen, weil wir es für selbstverständlich halten, dass ein vertraulicher Umgang gepflegt wird. Die Patientenakten werden in einem offenen Register hinter dem Anmeldetresen außerhalb der Reichweite von Patienten geführt. Patienten unterschreiben die Rezepte grundsätzlich auf dem Anmeldetresen.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 2
Wie stellen Sie sicher, dass papierhafte Patientenunterlagen (Patientenakte, Rezepte, etc.) auf dem Weg zu Hausbesuchspatienten nicht verloren gehen?

1. Alle Therapeutinnen und Therapeuten, die bei uns in der Praxis Hausbesuche durchführen, erhalten eine eigene sicher verschließbare Umlaufmappe, welche mit dem Namen des Therapeuten bzw. seinem Kürzel gekennzeichnet ist. Es besteht die schriftliche Vereinbarung innerhalb der Praxis, dass papierhafte Patientenunterlagen ausschließlich in den dafür vorgesehen Umlaufmappen außerhalb der Praxisräume verbracht werden dürfen. Die Therapeutinnen und Therapeuten sind ferner gehalten, die Umlaufmappen wiederum in sicheren Transporttaschen zu befördern. Dies können Rucksäcke, Handtaschen oder Aktentaschen sein.

2. Es besteht innerhalb der Praxis die mündliche Abrede, dass papierhafte Patientenakten sicher transportiert werden sollen. Überprüft wird dies nur stichprobenhaft. Patientenakten transportieren unsere Therapeutinnen und Therapeuten überwiegend in der persönlichen Handtasche.

3. Wir überlassen unseren Therapeutinnen und Therapeuten selbst, wie sie papierhafte Patientenakten (Patientenakte, Rezepte, etc.) sicher transportieren und vertrauen darauf, dass sie hier ausreichende Vorsicht walten lassen. Konkrete Absprachen haben wir bisher nicht getroffen und kontrollieren auch nicht, wie Patientenakten transportiert werden. Es kann sein, dass Patientenakten auch lose, d.h. nicht in einer Tasche oder einem sonstigen Behältnis, bspw. frei auf dem Beifahrersitz eines Autos, zum Hausbesuch mitgenommen werden.

4. Wir machen keine Hausbesuche in unserer Praxis

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 3
Wie ist sichergestellt, dass Unbefugte keine Einsicht in den Praxiskalender/Terminkalender nehmen können?

1. Der Terminkalender der Praxis wird ausschließlich im PC geführt und alle Monitore sind so aufgestellt, dass ein Einsehen des Monitorbildes durch Patienten oder Besucher nicht möglich ist oder ist mit Sichtschutzfolie beklebt. Oder: Der Terminkalender befindet sich hinter dem Anmeldetresen und der Anmeldetresen bietet einen ausreichenden Sichtschutz, so dass auch sich über den Anmeldetresen hinüberlehnende Personen keine Einsicht nehmen können. Es besteht die (schriftliche) Anweisung an das gesamte Praxispersonal, den Terminkalender geschlossen zu halten, wenn dieser gerade nicht verwendet wird.

2. Der Terminkalender liegt hinter dem Anmeldetresen. Patienten können ihn zwar theoretisch einsehen, wenn sie sich über den Tresen hinüberbeugen. Wir sind jedoch bemüht, Patienten auf Diskretion hinzuweisen, wenn sie sich übe den Tresen beugen. Oder: Der im PC geführte Terminkalender kann auf dem Monitor durch Patienten eingesehen werden, wenn diese sich leicht über den Anmeldetresen hinüberbeugen.

3. Der papierhaft geführte Terminkalender der Praxis liegt eigentlich immer offen auf dem Anmeldetresen. Patienten können theoretisch hineinschauen. Wir gehen aber davon aus, dass in den Kalender grundsätzlich nicht hineingeschaut wird. Zudem ist unsere Handschrift weitestgehend unleserlich. Zudem weisen wir Patienten auf Diskretion hin, sollte uns auffallen, dass sie in den Kalender schauen.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 4
Ist Ihre Praxis ausreichend gegen Zugriffe von außen etwa gegen Einbrecher gesichert?

1. Alle Türen und Fenster der Praxis, an welche man von außen gelangen kann, entsprechen mindestens der Sicherheitsstufe RC3, d.h.: alle Fenster sind mit Getriebesperren (ein kleines Schloss am Handgriff) ausgestattet, Schließnocken und einbruchhemmender Verglasung. Die Praxis verfügt ferner über eine hochwertige Alarmanlage mit Glasbruchsensoren, Bewegungsmeldern und automatischer Alarmmeldung über Mobilfunk/GSM.
   Es besteht mit allen Mitarbeiterinnen und Mitarbeitern eine schriftliche Dienstanweisung, dass die Fenster bei Dienstschluss darauf zu kontrollieren sind, dass die Getriebesperren verriegelt und alle Fenster geschlossen sind.
   Es ist eine Schließanlage mit registrierten Schlüsseln vorhanden. Es wird eine Schlüsselliste geführt, aus der sich ergibt, wer welchen Schlüssel hat. Die Ausgabe der Schlüssel an Mitarbeiter erfolgt nur gegen Quittung.

2. Die Fenster der Praxis sind mit Getriebesperren ausgestattet (ein kleines Schloss am Handgriff) verfügen jedoch über einfache Zylinderschließnocken. Eine Alarmanlage ist in der Praxis nicht vorhanden. Es besteht die mündliche Absprache, dass der Letzte der abends geht, noch einmal überprüfen soll, ob alle Fenster auch geschlossen sind. Es sind registrierte Schlüssel für die Eingangstüre vorhanden.

3. Die Fenster der Praxis verfügen über einfache Schließmechanismen, Zylinderschließnocken und einfache Verglasung. Es handelt sich um einfache Fenster. Eine Alarmanlage ist nicht vorhanden und es bestehen keine konkreten Absprachen zum Schließen oder Kippen der Fenster. Wir vertrauen bislang darauf, dass Fenster bei Ende der Arbeitszeit schon von allen geschlossen werden. Bislang ist ja auch noch nichts passiert.
   Die Praxistür ist mit einem einfachen Zylinderschloss versehen.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 5
Wie stellen Sie sicher, dass keine Unbefugten die Praxis betreten oder sich im Wartebereich befindende Personen keinen unbefugten Zugriff auf Praxisunterlagen nehmen?

1. Unsere Anmeldung ist zu den Öffnungszeiten durchgehend besetzt und alle Besucher werden persönlich in Empfang genommen. Ist die Anmeldung nicht besetzt, ist die Praxistüre nur durch einen elektrischen Türöffner zu öffnen, den wir in die Behandlungskabinen mitnehmen oder wir gehen kurz selbst die Tür öffnen. Der Anmeldebereich ist zudem videoüberwacht und das Videobild wird auf Bildschirme in den Behandlungskabinen übertragen, in denen wir gerade arbeiten.

2. Die Anmeldung ist nur halbtags besetzt. Zu den Zeiten, in denen die Anmeldung nicht besetzt ist, kann die Praxis frei betreten werden. Allerdings haben wir einen Sensor an der Tür oder ein Glockenspiel, welches ein lautes Signal abgibt, wenn die Tür geöffnet wird. Wir haben mit allen Mitarbeiterinnen und Mitarbeiter die Absprache, dass wenn die Türe aufgeht, nachzuschauen ist, wer da kommt. Eine Videoüberwachung machen wir nicht.

3. Die Anmeldung ist nur halbtags besetzt oder eine Anmeldekraft gibt es in unserer Praxis nicht. Patienten können die Praxis einfach so betreten; die Tür ist laut genug, als dass wir sie auch noch in der letzten Kabine hören. Da wir ja wissen, wer kommt, gehen wir nicht extra gucken, damit wir die Behandlung nicht unterbrechen müssen. Bislang ist auch noch nie etwas weggekommen.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 6
Welche Maßnahmen haben Sie getroffen, damit Besucher und Patienten die Anzeigebilder der Monitore zu Ihren PCs in der Praxis nicht einsehen können?

4. Alle Monitore der Praxis sind so aufgestellt, dass ein Einsehen des Anzeigebildes für Besucher und Patienten unmöglich ist. Die Monitore sind entweder fest in den Anmeldetresen integriert, so dass nur dahinterstehendes Personal darauf schauen kann oder die Monitore sind mit einer Sichtschutzfolie beklebt. Monitore und Computer haben eine automatische Inaktivitätssperre, welche den Bildschirm nach 3 Minuten Inaktivität abschaltet.

5. Die Monitore in der Praxis sind so aufgestellt, dass ein Einsehen des Monitorbildes für Besucher und Patienten schwierig ist. Die Monitore stehen möglicherweise auf dem Anmeldetresen, sind aber so gedreht, dass sie zu den Anmeldekräften hinzeigen. Über den Anmeldetresen hinüberbeugende Personen können aber schon darauf gucken. Eine Sichtschutzfolie haben wir nicht aufgeklebt. Die Monitore schalten sich nach einer Inaktivität des Computers von ungefähr 5 Minuten selbst ab.

6. Die Monitore sind so aufgestellt, dass die Anmeldekräfte hieran gut arbeiten können. Ein Einsehen durch Besucher und Patienten ist zwar möglich, wenn diese sich über den Tresen beugen, kommt jedoch nicht häufig vor. Schauen Patienten oder Besucher über den Tresen auf das Monitorbild, weisen wir diese freundlich aber bestimmt darauf hin, einen diskreten Abstand zu wahren.

7. Wir haben bislang keinen PC in der Praxis

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 7
Wie stellen Sie sicher, dass Patientengespräche nicht von anderen mitgehört werden können?

1. Unsere Praxis verfügt über einen großzügigen Anmeldebereich, an welchem diskrete Gespräche mit Patienten ohne weiteres möglich sind oder es besteht die Anweisung, keine Patientengespräche am Anmeldetresen zu führen. Zudem besteht mit allen Mitarbeiterinnen und Mitarbeitern eine schriftliche Dienstanweisung, sensible Patientengespräche – insbesondere zur Befunderhebung und zur Klärung von anderen gesundheitlichen Fragen – ausschließlich in einer geschlossenen Behandlungskabine zu führen. Alle Behandlungskabinen in unserer Praxis sind festumschlossene Räume, ein Mithören von Gesprächen ist nicht möglich. Vor dem Anmeldetresen steht ein gut lesbares Schild, welches auf die Wahrung des Diskretionsabstandes hinweist.

2. Unser Anmeldebereich ist klein und wartende Patienten könnten Gespräche am Anmeldetresen mithören, wenn sie gut zuhören. Wir vertrauen aber darauf, dass eine entsprechende Diskretion gewahrt wird.
   In unserer Praxis haben wir teilweise umschlossene Behandlungskabinen und teilweise Behandlungskabinen, welche noch durch Vorhänge voneinander abgetrennt sind. Wir vertrauen darauf, dass die Therapeutinnen und Therapeuten zur Führung von Patientengesprächen – insbesondere für Gespräche zur Befunderhebung oder Anamnese von sektoralen Heilpraktikern – einen umschlossenen Behandlungsraum wählen.

3. Unser Anmeldebereich ist sehr klein. Wenn hier Patienten warten, könnten diese ohne weiteres mithören, was ein anderer Patient mit den Anmeldekräften oder einem Therapeuten an der Anmeldung bespricht. Wir versuchen aber Patientengespräche zu vermeiden, wenn wartende Patienten da sind. Unsere Behandlungskabinen sind entweder alle oder weitüberwiegend durch Vorhänge voneinander abgegrenzt. Man kann gut hören, was in der benachbarten Kabine gesprochen wird. Wir geben uns allerdings Mühe, mit gedämpfter Stimme zu sprechen, damit nicht alle mithören und vertrauen insgesamt auf die Diskretion von allen Patienten und Therapeuten.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 8
Ist Ihre EDV ausreichend vor unbefugtem Zugriff geschützt?

1. Für unsere EDV besteht eine differenzierte Nutzerstruktur. Zum Anmelden am PC ist ein Nutzername und ein Passwort einzugeben. Zum Öffnen des Praxisverwaltungsprogrammes (Theorg, Tim, Protea, etc.) ist wieder ein Nutzername und ein Passwort einzugeben. Jede Mitarbeiterin und jeder Mitarbeiter, der Zugriff auf die Praxis-EDV hat, verfügt über einen eigenen Benutzer-Account und ein eigenes Passwort mit ausreichender Schlüssellänge von mindestens 8 Zeichen, Groß- und Kleinbuchstaben sowie Zahlen und einem Sonderzeichen. Die Rechte sind nach Nutzern differenziert. Jeder Nutzer darf an dem PC nur das, was er für seine Arbeit tatsächlich braucht.

2. Wir haben bei der Praxis-EDV ein einheitliches Benutzerpasswort. Dies ist für alle Mitarbeiterinnen und Mitarbeiter gleich und alle können den PC gleichermaßen nutzen.

3. Schaltet man den PC in der Praxis ein, kommt keine Passwortabfrage. Der PC kann einfach so genutzt werden.

4. Wir haben bislang keinen PC in der Praxis

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 9
Haben Sie Ihr WLAN ausreichend gesichert?

1. Das WLAN in unserer Praxis ist vollständig abgeschaltet oder mit einem WPA2-Schlüssel mit ausreichender Schlüssellänge und Zeichenfolge ausgestattet. Der Schlüssel ist mindestens zwölf Zeichen lang und enthält sowohl Groß- als auch Kleinbuchstaben, Zahlen und Sonderzeichen. WPS und broadcasting ist ausgeschaltet. Der MAC-Filter ist eingeschaltet und erlaubt nur Verbindungen von bekannten Geräten. Die Nutzeroberfläche des Routers ist mit einem Passwort geschützt.

2. Wir haben das WLAN eigentlich seit der Installation nicht verändert. Es ist durch den voreingestellten Schlüssel gesichert. Dieser entspricht dem Standard WPA2.

3. Unser WLAN hat z. Zt. entweder gar kein Kennwort oder nur ein sehr einfaches, da wir auch Patienten manchmal Zugriff auf unseren WLAN-Hotspot geben, damit diese ins Internet können.

4. Wir haben kein WLAN-Gerät in der Praxis

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 10
Haben Sie Ihre Mitarbeiterinnen und Mitarbeiter ausreichend und nachvollziehbar im Datenschutz geschult und auf das Datengeheimnis verpflichtet?

1. Wir haben mit unserem gesamten Team an einer Datenschutz-Schulung teilgenommen oder ein Datenschutzexperte hat bei uns in der Praxis eine Schulung durchgeführt oder einer aus unserem Team hat ein mehrtägiges Datenschutzseminar gemacht und uns danach alle im Datenschutz geschult. Nachschulungen führen wir in regelmäßigen Abständen (jährlich) durch und dokumentieren, wer teilgenommen hat.
   Alle Mitarbeiterinnen und Mitarbeiter werden jährlich an ihre Datenschutzpflichten hingewiesen. Dies dokumentieren wir. Alle Mitarbeiterinnen und Mitarbeiter haben zudem eine Verpflichtungserklärung auf das Datengeheimnis unterschrieben.

2. Wir haben unseren Mitarbeiterinnen und Mitarbeitern über den Datenschutz gesprochen und sie ermahnt mit Patientendaten sorgsam umzugehen. Eine Verpflichtung zur Einhaltung des Datenschutzes haben wir als Klausel in allen Arbeitsverträgen.

3. Wir haben bislang mit unseren Mitarbeitern nicht ausdrücklich über den Datenschutz gesprochen, da wir es für selbstverständlich halten, dass alle Therapeuten mit Patientendaten sorgsam und vertraulich umgehen. Bei uns plaudert keiner Patientengeheimnisse aus, darum haben wir eine ausdrückliche Verpflichtung auf das Patientengeheimnis bislang nicht für nötig gehalten.

4. Ich arbeite alleine und habe keine Mitarbeiter

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 11
Wie haben Sie sichergestellt, dass auch externe Dienstleister (z.B. Computerfachmann, IT-Dienstleister, Firma zur Aktenvernichtung, etc.) ein angemessenes Maß an Datensicherheit gewährleisten und den Datenschutz beachten?

1. Wir haben mit allen Dienstleistern einen Artikel 28 DSGVO konformen Vertrag über die Auftragsverarbeitung geschlossen, der alle Rechte und Pflichten in Bezug auf den Datenschutz abschließend regelt.

2. Wir haben mit unserem IT-Dienstleister vor Jahren mal einen Vertrag geschlossen, wissen aber nicht mehr genau, wo der ist und haben den auch nicht aktualisiert. Wir vertrauen aber darauf, dass unser IT-Dienstleister den Datenschutz beachtet, da wir schon seit vielen Jahren vertrauensvoll mit ihm zusammenarbeiten.

3. Wir haben mit unserem IT-Dienstleister keinen Vertrag über die Auftragsverarbeitung geschlossen, arbeiten mit ihm aber schon seit vielen Jahren sehr gut zusammen und vertrauen darauf, dass er alle Bestimmungen des Datenschutzes einhält und mit Patienteninformationen vertrauensvoll umgeht.

4. Wir haben keine externen Dienstleister (Keine IT-Firma, etc.)

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Frage Nr. 12
Haben Sie in Ihrer Praxis ein Konzept Löschung und sicheren Vernichtung von sensiblen Unterlagen/Patientenakten?

1. Die Löschfristen für in der Praxis gespeicherte Daten sind den gesetzlichen Anforderungen entsprechend, schriftlich festgelegt und allen Verantwortlichen gegenüber bekannt gegeben. Die Aktenvernichtung erfolgt zu festgelegten Intervallen. Zur Aktenvernichtung steht ein Aktenvernichter der Sicherheitsstufe 4 gemäß DIN 32757 (D.h. Kreuzschnitt bzw. Partikelschnitt) oder wir übergeben zu vernichtende Akten einem auf Aktenvernichtung spezialisierten und zertifizierten Unternehmen. Mit diesem Unternehmen ist ein mit Art. 28 DSGVO konformer Auftragsverarbeitungsvertrag geschlossen.

2. Wir bewahren alle Akten 10 Jahre auf, weil wir dazu verpflichtet sind. Aktenvernichtungen führen wir in unregelmäßigen Abständen aber meistens schon ein bis alle zwei Jahre durch. Hierfür steht uns ein Aktenvernichter zur Verfügung, der einen Streifenschnitt macht und der Sicherheitsstufe 3 DIN 32757 entspricht. Löschfristen haben wir nicht festgelegt.

3. Über die Vernichtung von Akten haben wir uns bislang keine Gedanken gemacht, entweder weil unsere Praxis noch keine 10 Jahre besteht oder weil wir einfach alle Patientenakten aufheben wollten, für den Fall, dass man auch nach 10 Jahren nochmal etwa nachschlagen muss oder ein Patient nach langer Zeit doch nochmal in die Behandlung kommt. Sollten doch mal Unterlagen vernichtet werden müssen, werden diese in kleine Stücke gerissen und in den Papiermüll geworfen oder eine unserer Mitarbeiter nimmt diese mit nach Hause und verbrennt sie im heimischen Kachelofen oder wir haben einen einfachen Schredder, der Streifen macht.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 13
Erfüllen Sie alle Transparenzpflichten gemäß Artikel 12 FF. DSG-VO?

1. Unsere Patienten werden differenziert über alle Datenverarbeitungsvorgänge in unserer Praxis informiert. Wir haben eine umfassende Datenschutzerklärung in unseren schriftlichen Behandlungsverträgen, in welchen wir den Patienten gegenüber offenlegen, welche Daten wir zu welchen Zwecken speichern und verarbeiten, und wem gegenüber wir Daten von Patienten ggfs. offenlegen.
   Dies umfasst insbesondere die Abrechnungsstelle und Ärzte. Zudem liegen für unsere Patienten Datenschutzinformationsblätter an der Anmeldung aus, welche wir bei Nachfragen aushändigen. Diese Informationsblätter geben genaue Auskunft darüber, welche Daten erhoben werden, welche Löschfristen bestehen, für welche Zwecke Daten verarbeitet werden und an welche Empfänger Daten ggfs. weitergegeben werden.

2. Wir weisen unsere Patienten in den schriftlichen Behandlungsverträgen auf den Datenschutz kurz hin und insbesondere lassen wir uns unterschreiben, dass wir die Daten zur Abrechnung an die Abrechnungsstelle weitergeben dürfen.

3. Bislang haben wir in unserer Praxis keine schriftlichen Behandlungsverträge und auch sonst keine ausdrücklichen Hinweise auf den Datenschutz. Unsere Patienten vertrauen uns, dass wir sorgsam und angemessen mit ihren Daten umgehen.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 14
Führen Sie in Ihrer Praxis ein Verzeichnis von Verarbeitungstätigkeiten

1. Wir führen ein Verzeichnis von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO, in welchem alle Verfahren und Verarbeitungstätigkeiten, welche wir in unserer Praxis durchführen, geordnet festgehalten sind. Alle Verarbeitungszwecke sind dargelegt und auf Legitimität geprüft. Die Kategorien von in unserer Praxis verarbeiteten Daten sind einer Schutzbedarfsanalyse unterzogen worden und das Ergebnis ist im Verzeichnis festgehalten. Das Verzeichnis enthält ferner eine abschließende Auflistung aller Kategorien Betroffener von Datenverarbeitung und Empfänger von Daten.
   An das Verzeichnis schließt sich eine differenzierte Beschreibung der verfahrensübergreifenden technischen und organisatorischen Maßnahmen zur Datensicherheit gem. Art. 32 DSGVO (TOMs) an.
   Es bestehen schriftlich fixierte Prozesse zur regelmäßigen Überprüfung und Aktualisierung des Verzeichnisses von Verarbeitungstätigkeiten.

2. In unserer Praxis besteht ein internes und externes Verfahrensverzeichnis nach BDSG. Dieses aktualisieren wir aber nicht regelmäßig. Wir führen eine Übersicht über die verfahrensübergreifenden technischen und organisatorischen Maßnahmen zur Datensicherheit gem. Art. 32 DSGVO (TOMs).

3. Wir führen in unserer Praxis bislang kein Verzeichnis von Verarbeitungstätigkeiten und auch kein Verfahrensverzeichnis nach BDSG.

Antwort 1	Antwort 2	Antwort 3	

Frage Nr. 15
Wie setzen Sie die Sicherung Ihrer Daten um?

1. Sicherungen unserer Praxis-EDV erfolgen zu festgelegten Intervallen nach dem sog. 3-Generationen-Prinzip. Die Sicherungen erfolgen etwa täglich, wöchentlich und monatlich. Zur Datensicherung steht ein redundantes System an Festplatten (RAID) oder ein netzwerkgebundener Datenserver (NAS) zur Verfügung. Zusätzlich erfolgt eine manuelle Sicherung über eine Externe USB-Festplatte. Die Festplatte ist verschlüsselt.
   Unser Serverraum ist mit einer unterbrechungsfreien Stromversorgung (USV) und einer Klimaüberwachung versehen. Der Serverraum ist stets abgeschlossen und der Schlüssel liegt nur bei der Praxisleitung.

2. Die Datensicherung machen wir jeden Abend über externe Datenträger. Hierfür kommen zwei externe USB-Festplatten zum Einsatz, die abwechselnd zur Datensicherung eingesetzt und anschließend bei der Praxisleitung zu Hause gelagert werden oder die Datensicherung erfolgt auf unserem Server über ein System redundanter Festplatten (RAID).

3. Eine Datensicherung führen wir nur selbst über einen einzigen Datenträger (z.B. USB-Stick) aus. Der Datenträger wird anschließend im Schrank hinter der Anmeldung eingeschlossen

4. Wir haben in unserer Praxis keinen Computer.

Antwort 1	Antwort 2	Antwort 3	Antwort 4

Auswertung

So nehmen Sie die Auswertung vor:

1. Wenn Sie bei jeder Frage ein Kreuz gemacht haben, tragen Sie die Kreuze in nachfolgende Tabelle ein.
2. Zählen Sie die Kreuze jeder Spalte und tragen Sie die Anzahl der Kreuze in die unterste Zeile ein.

		Antwort 1	Antwort 2	Antwort 3	Antwort 4
Frage Nr. 1	Herumliegende Akten				
Frage Nr. 2	Akten bei Hausbesuchen				
Frage Nr. 3	Terminkalender				
Frage Nr. 4	Sicherung der Fenster und der Praxistür				
Frage Nr. 5	Sicherung gegen unbefugtes Betreten				
Frage Nr. 6	Monitore				
Frage Nr. 7	Mithören von Patientengesprächen				
Frage Nr. 8	Passwortschutz PC				
Frage Nr. 9	WLAN Sicherheit				
Frage Nr. 10	Schulung der Mitarbeiter im Datenschutz				
Frage Nr. 11	Externe Dienstleister				
Frage Nr. 12	Sichere Aktenvernichtung				
Frage Nr. 13	Transparenzpflichten				
Frage Nr. 14	Verzeichnis von Verarbeitungstätigkeiten				
Frage Nr. 15	Datensicherung				
	Anzahl				

3. Tragen Sie nun die Anzahl der Kreuze in die nachstehende Tabelle ein, nehmen Sie mal und addieren Sie dann. Nehmen Sie wenn nötig einen Taschenrechner zur Hand. (Achtung: Die Anzahl der Antwort 4 brauchen wir erst im nächsten Schritt!):

Anzahl Kreuze Antwort 1		x	4	=	
					+
Anzahl Kreuze Antwort 2		x	2	=	
					+
Anzahl Kreuze Antwort 3		x	1	=	
					=
Ergebnis:					

4. Schauen Sie nun, wo hoch die Anzahl Antwort 4 ist und gehen Sie in die entsprechende Zeile. Vergleichen Sie Ihr Ergebnis mit den in der Zeile gegebenen Zahlen. Je höher Ihr Ergebnis, desto weiter nach rechts kommen Sie. Haben Sie zum Beispiel **3x** Antwort 4 und ein Ergebnis von **39**, dann sind Sie in der Spalte „Sehr gut“. Haben Sie bspw. **2x** Antwort 4 und ein Ergebnis von **48,** dann sind Sie in der Spalte „Ausgezeichnet!“.

Anzahl Antwort 4	Kritisch	Verbesserungswürdig	Sehr Gut	Ausgezeichnet
0	**0 – 28**	**29 – 38**	**38 – 53**	**54 – 60**
1	**0 – 26**	**27 – 35**	**36 – 49**	**50 – 56**
2	**0 – 24**	**25 – 32**	**33 – 46**	**47 – 52**
3	**0 – 22**	**23 – 30**	**31 – 42**	**43 – 48**
4	**0 – 20**	**21 – 27**	**28 – 39**	**40 – 44**
5	**0 – 19**	**20 – 25**	**26 – 35**	**36 – 40**
6	**0 – 17**	**18 – 22**	**23 – 31**	**32 – 36**
7	**0 – 15**	**16 – 20**	**21 – 28**	**29 – 32**
8	**0 – 13**	**14 – 17**	**18 – 24**	**25 – 28**

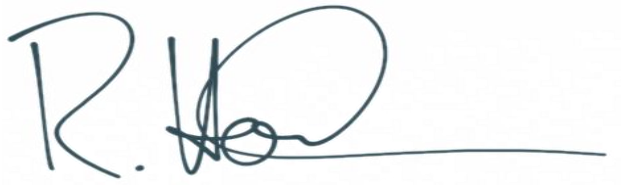
Ausgezeichnet Ihre Praxis ist aller Voraussicht nach auf die DSGVO sehr gut vorbereitet. Das Prinzip ‚privacy by Design' ist in Ihrer Praxis wahrscheinlich durchgehend umgesetzt und Sie erfüllen wahrscheinlich alle wesentlichen neuen Pflichten, die auf Sie zukommen. Seien Sie jedoch dennoch wachsam und insbesondere kritisch mit sich selbst. Überprüfen Sie auch noch einmal, ob im Verzeichnis von Verarbeitungstätigkeiten alle Verfahren auf dem neuesten Stand sind und ob alle technischen und organisatorischen Maßnahmen TOM's verzeichnet sind.
Sehr gut Sie haben Datenschutz in Ihrer Praxis bereits zum Thema gemacht und es sind wahrscheinlich bereits zahlreiche wichtige Maßnahmen zur Herstellung eines angemessenen Datenschutzniveaus in Ihrer Praxis umgesetzt. Sie sollten jedoch kritisch hinterfragen, ob alle Maßnahmen auch den neuen Anforderungen der DSGO gerecht werden. Insbesondere sollten Sie schauen, dass Ihre Datenschutzdokumentation dem Stand der DSGVO entspricht.
Verbesserungswürdig In Ihrer Praxis sind bereits zahlreiche Maßnahmen des Datenschutzes vorhanden. Wahrscheinlich fehlt Ihnen aber bislang ein einheitliches Konzept. Insbesondere die Datenschutzdokumentation sollten Sie schleunigst anlegen oder – falls Sie bereits eine führen – Ihre Datenschutzdokumentation auf die Anforderungen an die DSGVO anpassen. Sie sollten zudem dringend schauen, welche Datenschutzmaßnahmen Sie in Ihrer Praxis noch einführen oder anpassen müssen, um ein angemessenes Datenschutzniveau zu erreichen.
Kritisch Datenschutz hat in Ihrer Praxis bislang wahrscheinlich keine tragende Rolle gespielt. Sie sollte sich schleunigst mit dem neuen Datenschutzrecht vertraut machen, und gegebenenfalls fachkundige Beratung einholen. Nehmen Sie sich ausreichend Zeit und Muße, um am besten mit ihrem gesamten Team zu besprechen, welche Datenschutzmaßnahmen in Ihrer Praxis umzusetzen und einzuführen sind. Machen Sie sich einen Fahrplan, in dem Sie festhalten, wann Sie welche Maßnahmen umsetzen und wir innerhalb Ihres Teams die Umsetzung kontrolliert. Legen Sie auch so bald wie möglich eine Datenschutzdokumentation und ein Verzeichnis von Verarbeitungstätigkeiten einschließlich einer Übersicht über die technischen und organisatorischen Maßnahmen der Datensicherheit (TOMs) an.

Schlusswort

Ich hoffe Ihnen hat dieser Schnelltest einen Eindruck davon vermitteln können, wie weit die Umsetzung des Datenschutzes in Ihrer Praxis ist. Ich würde mich freuen, wenn Ihnen der Test auch dazu verholfen hat, Ihr Verständnis für den Datenschutz etwas zu schärfen.
Bitte nehmen Sie diesen Test nur als eine grobe Orientierung und machen Sie bitte das Ergebnis nicht zur alleinigen Grundlage von Entscheidungen bezüglich des Datenschutzes in Ihrer Praxis. Natürlich kein so ein starrer Test nicht alle möglichen Schwachstellen abdecken, die in jeder Praxis ganz individuell vorhanden sein können.
Ich würde mich sehr freuen, wenn Sie an meinem Test Gefallen gefunden haben.

Sollten Sie Fragen oder Beratungsbedarf zum Thema Datenschutz haben, stehe ich Ihnen natürlich jeder Zeit gerne zur Verfügung.

Ihr



Rainer Horbach
DATA*privat*
Rechtsanwalt
Datenschutzbeauftragter (extern)