Was Heilpraktiker über die DSGVO wissen ~~wollen~~ (sollten!)

Am 22.5.2018 hatte ich, Gabriele Ermen, Herrn Thomas Schulze in meine Webinar-Akademie eingeladen, damit er uns über darüber aufklärt, warum wir als Kleinunternehmer von der neuen Datenschutzgrundverordnung betroffen sind und was wir tun müssen. Die Teilnehmer stellten eine Menge Fragen, die während der Stunde gar nicht alle beantwortet werden konnten. Deshalb habe ich die Fragen gesammelt, nach Themen sortiert und Antworten aus dem von Herrn Schulze Gesagten sowie durch eigene Internetrecherche zusammengetragen.

Das Thema DSGVO bringt viele emotionale Reaktionen hervor. Ich habe mich zwar bemüht, auf die meisten Fragen sachlich zu antworten und nicht zu viele polemische Kommentare abzugeben. Nichtsdestotrotz gibt der gesamte Text nur meine persönliche Auffassung und Meinung wieder.

Oder noch mal als expliziter Haftungsausschluss: Meine Antworten sind sicherlich nicht vollständig und ersetzen keine Rechtsberatung durch einen Juristen. Ich habe die Fragen nach bestem Wissen und Gewissen beantwortet, gebe aber keine Garantie, dass alles korrekt ist!

Sie können dieses Dokument gerne an andere Therapeuten weitergeben, die sich über die Auswirkungen der neuen Gesetzgebung informieren wollen. Aber bitte nur im Ganzen mit diesem Vorwort. Ich verbitte mir, dass einzelne Auszüge aus diesem Text zitiert werden, weil ich nicht Gefahr laufen möchte, dass jemand denkt, ich würde mir anmaßen verbindliche rechtliche Auskünfte zu geben.

Ich bitte auch um Verzeihung, wenn sich durch die Antworten wieder neue Fragen auftun. Bei vielen Abläufen ist einfach noch nicht alles geklärt, wie sie in der Praxis überhaupt realisiert werden können.

Ich danke Herrn Schulze, dass er hier seine Folien vom Webinar zur Verfügung stellt!

Fragen, die uns in den Webinaren gestellt wurden:

Die europäische Datenschutz-Grundverordnung - DGSVO

- Was ist los?
  - ➡ *Am 25.05.2018 wird die neue Datenschutzgrundverordnung der EU rechtsbindend.*
- Worum geht es in dem Gesetz?
  - ➡ *Dem Gesetzgeber ist es wichtig, dass jede natürliche Person ein Recht auf ihre eigenen Daten (z.B. Name, Adresse, Geburtsdatum, Gesundheitsdaten, Recht am Bild, etc.) hat. Es gilt ein grundsätzliches „Verbot mit Erlaubnisvorbehalt“ bei jeder Datenverarbeitung (d.h. egal ob digital oder auf Papier). Zur Ausnahme kommt es nur, wenn es eine anderweitige Rechtsvorschrift gibt (z.B. Erhebung der Patientendaten)*
- Ab wann gilt das neue Gesetz?
  - ➡ *Das Gesetz gilt schon seit dem 24.05.2016. Es gab eine 2-jährige Übergangsfrist, damit jeder genügend Zeit hat, die Bestimmungen umzusetzen. Blöd für uns, dass wir es so lange aufgeschoben haben…*

- Wen betrifft das Gesetz?
  - ➞ *Es gilt für jeden Unternehmer, also auch für jede/n Heilpraktiker/in mit eigener Praxis.*
- Wer kontrolliert das alles?
  - ➞ *Dafür ist der Datenschutzbeauftragte Ihres Bundeslands zuständig. Sie finden seine Kontaktdaten hier: https://www.datenschutz-wiki.de/Aufsichtsbeh%C3%B6rden_und_Landesdatenschutzbeauftragte*
- Was passiert, wenn ich es ignoriere?
  - ➞ *Hoffentlich gar nichts, weil die Landesdatenschutzstellen zurzeit noch vollkommen überfordert sind. Grundsätzlich werden bei Nicht-Einhaltung Bußgelder von 4% des Jahresumsatzes, bis zu 20 Millionen Euro angedroht. Kommentar eines Webinar-Teilnehmers: „4% von 20 Tausend sind 800 Euro. Blöd, aber nicht tödlich. Und vielleicht sogar als aussergewöhnliche Belastung abzusetzen :-)“*
- Muss ich alles bis zum 25.5.18 fertig haben?
  - ➞ *Nein, Sie müssen nachweisen können, dass Sie rechtzeitig angefangen haben sich drum zu kümmern.*
- Woher weiß ich, welche Daten ich trotz Datenschutzgesetz aufbewahren/weitergeben darf/muss?
  - ➞ *Benutzen Sie das 3-stufige Prüfverfahren:*
    - ▸ *Muss ich hoheitliche Anforderungen erfüllen? (z.B. Meldepflicht nach dem Infektionsschutzgesetz oder Rechnungen dem Finanzamt zur Verfügung zu stellen) Diese Vorgänge fallen nicht unter den Datenschutz!*
    - ▸ *Muss ich betriebliche Aufgaben erfüllen (Daten der Finanzbuchhaltung 10 Jahre aufbewahren) Auch das fällt nicht unter den Datenschutz*
    - ▸ *Alle anderen personenbezogenen Daten fallen unter den Datenschutz*
- Was ist, wenn nur ich alleine Zugriff auf die Daten meiner Patienten habe?
  - ➞ *Dann schreiben Sie das so in Ihr Datenschutzkonzept rein*
- Ich bin ein Ein-Mann-Kleinstbetrieb - dafür dieser ganze Aufwand?
  - ➞ *Ja, sorry, grundsätzlich schon. Allerdings verlangt niemand von Ihnen, dass Sie sich so sehr ins Zeug für den Datenschutz legen, dass sie keine Zeit mehr für's Hauptgeschäft haben. Es wird im Gesetz immer wieder darauf hingewiesen, dass kein unverhältnismäßig großer Aufwand entstehen darf.*

Thema Homepage:

- Brauche ich bei einem Blog auch Hinweise im Impressum?
  - ➞ *Werfen Sie die Impressumpflicht und die Pflicht zur Datenschutzerklärung nicht durcheinander! Sie müssen sich an beides halten.*
- Was muss ins Impressum, was in die Datenschutzerklärung?
  - ➞ *Im Impressum steht, wer verantwortlich für die Webseite ist, in der Datenschutzerklärung wird erklärt, was mit den Daten der Benutzer geschieht, die durch diese Seite gesammelt werden. Am Impressum ändert sich durch die DSGVO nichts. Ich verweise immer gerne auf das Muster-Impressum vom UDH . Die Datenschutz-Seite darf nicht einfach mit im Impressum untergebracht sein!*
- Datenschutz Erklärung Homepage, Welche Module müssen in die Datenschutzerklärung auf meiner Homepage rein?
  - ➞ *Es muss ab dem 25.5.2018 auf jeder Seite Ihrer Homepage einen Button oder Link geben (z.B. Menüpunkt), der mit dem Wort „Datenschutz“ oder*

„Datenschutzerklärung“ versehen ist. Wenn man draufklickt, bekommt man Ihre Datenschutzerklärung angezeigt.

- Kann ich von Ihnen eine Datenschutzerklärung bekommen?
  - ➞ *Nein, überlassen Sie das besser einem Juristen. Benutzen Sie z.B. diesen kostenlosen Generator. Er deckt alle benötigten Module ab.*
- Ich habe im Internet Datenschutzerklärung von verschiedenen Homepages verglichen. Der Inhalt geht von 1 DIN A4-Seite bis zu 12 DIN A4-Seiten! Wie ausführlich muss die Erklärung denn sein?!?!
  - ➞ *Sie muss alle geforderten Punkte abdecken und sie muss vor allem in verständlicher Sprache geschrieben sein. Theoretisch geht sogar eine Seite Schaubild, das alle nötigen Informationen abbildet.*
- Was ist auf der Internetseite zu beachten / Was muss ich unbedingt tun
  - ➞ *Die größte Gefahr, die in näherer Zeit auf uns lauert, werden wahrscheinlich „Abmahnvereine" sein, die versuchen das schnelle Geld zu machen. Wenn Sie eine solche Abmahnung bekommen, zahlen Sie nicht sofort, sondern schalten Sie lieber einen Anwalt ein, der überprüft, ob der Verein überhaupt das Recht hat Sie abzumahnen. Vermutlich bekommen nur Unternehmen mit einer Internetseite eine Abmahnung. Wenn Sie eine haben, setzen Sie vor Freitag noch einen Link „Datenschutz“ auf jede Seite, der zu einer Seite führt, auf die Sie nach bestem Wissen und Gewissen eine (ggf. vorläufige) Datenschutzerklärung setzen. Wenn Sie auf der Seite ein Kontaktformular bzw. eine Kommentarfunktion haben, die noch nicht der DSGVO entspricht (Einverständnis-Checkbox und Double-opt-in-Verfahren), deaktivieren Sie diese erst einmal. Deaktivieren Sie sie auch, wenn Ihre Seite noch nicht SSL-verschlüsselt ist (http**s**://)*
  - ➞ *Tipp: Setzen Sie Ihre Datenschutz-Seite auf „noindex“, damit Abmahner, die auf der Suche nach willigen Opfern sind, Ihre Seite nicht von Google auf dem Präsentierteller vorgesetzt bekommen!*
- Was muss ich tun, um meine Datenschutzerklärung auch UMZUSETZEN?
- Wie muss das Kontaktformular in Zukunft aussehen?
  - ➞ *Allgemeine Aussage: Es muss zusätzlich zu den normalen Feldern eine Checkbox als Pflichtfeld haben mit einer verständlichen Beschriftung und einem Link zur Datenschutzseite. Wie die Beschriftung formuliert werden soll - da gibt es noch wilde Spekulationen. Irgendetwas in Richtung „Ich bestätige, dass ich die Datenschutzerklärung gelesen und verstanden habe und damit einverstanden bin, dass Sie mir Informationen schicken.“*
  - ➞ *In einem Webinar von Klick-Tipp hat Mario Wolosz die Strategie vorgestellt, die Rechtsanwalt Dr. Stefan Gärtner für ihn entwickelt hat: Schreiben Sie zum Eingabeformular: „Bevor Sie sich hier anmelden, lesen Sie bitte diese wichtigen Informationen zum Datenschutz und zur DSGVO.“ Mit Link auf eine Transparenzerklärung. Sie sollten auch in der Bestätigungsmail noch einmal den Link auf diese Transparenzerklärung schicken und sich selbst eine Kopie, damit Sie beweisen können, dass der Interessent diese Informationen direkt bei der Anmeldung bekommen hat. Aber Vorsicht, lassen Sie sich lieber selbst von einem Rechtsanwalt beraten, wenn Sie diese Strategie umsetzen wollen, damit Ihre Transparenzerklärung wasserfest ist! (Oder Sie steigen auf Klick-Tipp um, und bekommen die Strategie samt vom Rechtsanwalt formulierter Transparenzerklärung kostenlos dazu.)*
- Warum brauch ich das Häkchen bei einem Kontaktformular?
  - ➞ *Damit Sie die Bestätigung des Interessenten nachweisen können, dass er Sie darum gebeten hat, ihm Informationen zu schicken.*

- Muss meine Homepage auch sicher sein, wenn ich kein Kontaktformular habe?
  - ➞ *Ohne Kontaktformular braucht die Homepage m.W. nicht SSL-verschlüsselt zu sein. Allerdings werden SSL-Seiten bei Google besser gelistet. Einen Hinweis auf den Datenschutz braucht die Seite trotzdem.*
- Woher weiß ich, ob ich Cookies einsetze?
  - ➞ *Schauen Sie doch mal bei sich in den Browser! Z.B. Chrome: Rechts oben gibt es ein Menü, das durch 3 Punkte gekennzeichnet ist. Wählen Sie Einstellungen - erweitert - Sicherheit & Datenschutz - Inhaltseinstellungen - Cookies - Alle Webseitendaten und Cookies anzeigen. Suchen Sie nach Ihrer Webseite. Wird sie gefunden? Dann können Sie schauen, welche Cookies Ihre Seite speichert. (Das funktioniert natürlich nur, wenn Sie Ihrem Browser nicht das Speichern von Cookies verboten haben.) Ich setze übrigens mit meiner Webseite (noch) keine Cookies, habe es aber trotzdem schon einmal „für alle Fälle" in meine Datenschutzerklärung geschrieben, damit ich es nicht ändern muss, wenn ich irgendwann doch Cookies benutzen will oder ein neues Plugin installiere, von dem ich gar nicht weiß, dass es Cookies setzt.*
- Was muss ich bei der Verwendung von Social Media Buttons beachten?
  - ➞ *Buttons, die den Webseitenbesucher auffordern, die Seite in einem Social-Media-Portal zu teilen, sind noch umstritten. (Quelle: https://www.datenschutz.org/social-media-buttons/). Am besten, Sie entfernen Sie erst einmal von Ihren Webseiten. Wenn das ganze geklärt ist, wird der Kompromiss vermutlich auf eine 2-Klick-Lösung oder einen Shariff-Button hinauslaufen, damit die personenbezogenen Daten nicht schon an das Social Media Portal geschickt werden, bevor der Webseitenbesucher auf den Button klickt.*
- Wie kann ich diese Probleme lösen?
  - ➞ *Es ist davon auszugehen, dass die Software-Entwickler mit der Zeit genügend Möglichkeiten finden, die umstrittenen Funktionen datenschutzkonform abzubilden - es sei denn, der Hersteller ist außerhalb der EU und es kümmert ihn nicht, was seine EU-Kunden brauchen. Siehe dazu auch:*
- *Ist es problematisch, wenn ich auf meiner Website Empfehlungslinks auf die Seiten meiner Kollegen setze?*
  - ➞ *Nein, das Datenschutzgesetz gilt nur für persönliche Daten. Eine Webseiten-URL zählt nicht dazu. Wenn der Kollege private Daten von sich auf seiner Seite preisgibt, ist das seine Entscheidung… Wenn Sie neben den Link ein Foto des Kollegen auf Ihre Seite setzen wollen, brauchen Sie allerdings die Erlaubnis des Kollegen.*
- Meine Homepage läuft über Vistaprint. wie ist es da mit dem Kontaktformular?
  - ➞ *Ich fürchte, das könnte schwierig werden, weil Vistaprint amerikanisch ist und sich als Druck-Spezialist nicht unbedingt mit seinen Webseiten identifiziert: https://spadedesignlab.com/6-reasons-never-use-vistaprint-design-website/*
- Kann ich Websitetracker benutzen?
  - ➞ *Websitetracker sind Programme, die das Besucherverhalten auf einer Webseite beobachten und Auskunft z.B. darüber geben, von welcher Seite man auf diese gekommen ist, wie lange man geblieben ist usw. Der Webseitenbetreiber kann aus den Daten wichtige Informationen darüber ziehen, wie er seine Seite weiter optimieren kann. Wenn das Programm die IP-Adresse des Besuchers speichert, gehört das zu den personenbezogenen Daten und ist nicht gestattet. Deshalb ist es wichtig, dass der Websitetracker die IP-Adresse anonymisiert. Nachteil: Er kann dann nicht mehr so viele Erkenntnisse liefern. Außerdem brauchen Sie einen*

Auftragsdatenverarbeitungsvertrag mit dem Anbieter. Für Google Analytics finden Sie den Antrag hier.

- Ich bin Heilpraktiker, gebe jedoch vorwiegend Seminare in Sehtraining und Feldenkraiss. Muss ich dafür etwas extra in Datenschutzerklärung schreiben?
  ➞ *Wenn Sie die Zwecke Ihrer Datenerhebung angeben, erwähnen Sie einfach die Verwaltung der Seminaranmeldungen.*

Thema Emails / Newsletter:

- Wie verschicke ich Mails korrekt und muss ich sie gesondert speichern? Was muss bei Rundmails beachtet werden?
  ➞ *Eine persönliche Mail an einen einzelnen Patienten können Sie so schicken wir üblich. Wenn Sie Rundmails verschicken oder einen Newsletter herausgeben, reicht es nicht mehr darunter zu schreiben „schicken Sie mir eine Mail, wenn Sie sich austragen wollen". Die Mails müssen zwingend einen Link enthalten, durch den man sich automatisch abmelden kann. Das heißt: Sie kommen nicht mehr drumherum, einen Newsletter-Dienst wie Klick-Tipp, GetResponse o.ä. zu benutzen. Wichtig: Wählen Sie einen Anbieter, der die DSGVO unterstützt (englisch: GDPR) und mit dem Sie einen Auftragsdatenverarbeitungsvertrag abschließen können.) Ob Mailchimp inzwischen DSGVO-kompatibel ist, konnte ich nicht genau herausfinden. Ich persönlich würde immer einen europäischen Anbieter bevorzugen.*
- Wie soll ich einen Abmeldelink umsetzen wenn ich keine Homepage habe?
  ➞ *Der Abmeldelink hat nichts mit Ihrer Homepage zu tun, sondern mit Ihrem Newsletter-Verwaltungsprogramm. (Es wird allerdings schwer, ein double opt-in-Verfahren aufzubauen, wenn Sie keine Webseite haben.)*
- Was mache ich mit früher gesammelten Emailadressen für meinen Newsletter? Muss ich alle Newsletterempfänger, die ich schon habe, fragen, ob sie weiter Emails bekommen wollen? Darf ich für Newsletter Patienten anschreiben?
  ➞ *Also, Patienten dürfen Sie anschreiben, weil das Ihre Kunden sind und damit ein „*
- Ich habe kein double-opt-in
  ➞ *Double-opt-in bedeutet: wer Ihnen seine Email-Adresse mitteilt, bekommt erst eine Mail dorthin geschickt, die er bestätigen muss, bevor Sie das Recht haben, ihm weitere Emails zu schicken. Wenn Sie nicht Gefahr laufen wollen abgemahnt zu werden, sollten Sie eine Möglichkeit finden den double-opt-in-Prozess anzubieten.*
- Für Newsletter werden ja jetzt von vielen eine neu Anmeldung angefordert, ist das nötig, wenn man schon doppel opt-in hat?
  ➞ *Es gibt unterschiedliche Meinungen dazu. Laut Aussage von Herrn Schulze muss man sich wieder neue ops-ins holen bei denen gleichzeitig der Kontakt der Datenschutzordnung zustimmt. Theoretisch braucht man das nur bei Interessenten und nicht bei Kunden. Es reicht den Kunden (Patienten) einen Link auf die Datenschutzerklärung zuzuschicken.*
- Wenn ich keine Newsletter, sondern nur normale Mails versende, muss ich dann auch noch anfragen?
  ➞ *Grundsätzlich schon, aber Sie dürfen natürlich auf eine Email-Anfrage eines Interessenten antworten, weil man davon ausgehen kann, dass er damit einverstanden ist. Sonst würde er ja nicht zuerst schreiben. Oder wenn Sie mit jemandem ins Gespräch kommen und mündlich ausmachen, dass Sie ihn anschreiben. Der Gesetzgeber will nur nicht, dass Sie spontan wildfremde Menschen*

anschreiben und anbieten: „Fühlen Sie sich krank? Wollen Sie in meine Praxis kommen?“ Aber das würden wir ja schon allein aufgrund des HWG nicht tun!

- Was muss ich beachten, wenn mir Patienten über Whats App schreiben?
  - ➞ *Das ist weniger problematisch, weil die Patienten in diesem Fall eindeutig einen WhatsApp Account haben. Wenn Sie jedoch Menschen über WhatsApp kontaktieren, deren Mobilnummer Sie haben, und die Person ist selbst nicht WhatsApp-Nutzer, wird die Nummer damit an WhatsApp weitergegeben, was nicht erlaubt ist.*
- Darf ich meine Rechnung per Email verschicken? Kann ich mit Patienten über eine normale t-online. email-adresse kommunzieren? ist diese ausreichend verschlüsselt?
  - ➞ *Achten Sie bitte darauf, dass Ihre Emails verschlüsselt sind. (SSL, besser TLS) Sie können das an Ihrem Computer so einstellen.*
- Darf ich Klienten noch anschreiben zum Seminar
  - ➞ *Wenn sie schon Klienten sind, besteht ja eine Geschäftsbeziehung. Die normalen Geschäftsabläufe gehören nicht zum Datenschutz.*
- Wie lange muss/darf ich Mails von Interessenten / Klienten aufbewahren?
  - ➞ *https://www.datenschutzbeauftragter-info.de/loeschfristen-in-unternehmen-mehr-muss-als-kann/ Tut mir leid, ich finde keine Vorgaben. Vielleicht können Sie es selbst entscheiden? Auf jeden Fall müssen Sie eine Zahl in Ihr Datenkonzept schreiben und sich dann daran halten.*
- Was muss ich bei der Mail Archivierung beachten?
  - ➞ *Sie sind einerseits verpflichtet dafür zu sorgen, dass Ihre geschäftsbezogenen Emails (z.B. Rechnungen, die per Email verschickt werden) nicht verloren gehen. Deshalb brauchen Sie eine Strategie, wie Sie diese Emails regelmäßig sichern. Spannend wird es, wenn eine Person ihr „Recht auf Vergessen“ ausübt. Dann sind Sie verpflichtet, alle Daten zu löschen, auch aus der Archivierung, aber die Rechnung an sich dürfen Sie natürlich nicht löschen! Wie das die einzelnen Mail-Provider realisieren werden, wird die Zukunft zeigen…*
- Braucht man eine Unterschrift, um jemandem eine Mail zu senden? z.B. Seminareinladung?
  - ➞ *Ja, eine Unterschrift oder einen entsprechenden Klick, wenn die Erlaubnis online eingeholt wird. Achtung: Sie dürfen in Seminaren und Vorträgen keine Teilnehmerlisten mehr rumgehen lassen, in der Person A den Namen und/oder die Emailadresse von Person B lesen kann.*
- wie verschlüssle ich die Mails?
  - ➞ *Bei allen Email-Providern die ich kenne kann man die Mails über die Einstellungen auf SSL oder besser TSL setzen. Es ist normalerweise kein separates Verschlüsselungsprogramm notwendig.*

Thema Internet und Smartphone:

- Was muss ich bei Facebook beachten?
  - ➞ *Wenn Sie eine Facebook Fanpage haben, muss da jetzt nicht nur ein Impressum, sondern auch eine Datenschutzerklärung im Info-Teil angegeben werden. Auf meiner Seite habe ich das gelöst, indem ich bei „Impressum“ beide Links auf meine Homepage eingetragen habe.*
  - ➞ *Das typische „Like-Widget“, das man auf seiner Webseite einbauen kann und Besucher darum bittn, die Facebook-Seite zu like, kann jetzt datenschutzrechtlich Schwierigkeiten bereiten, weil es schon benutzerbezogene Daten zur Webseite*

schicken kann, bevor man draufklickt (Jedenfalls, wenn man gleichzeitig bei Facebook angemeldet ist.)

- Ist das jameda-Siegel auf meiner Website in Datenschutzproblem?
  - ➡ *Ich habe mit* **Jameda** *telefoniert und folgende Antwort bekommen:*
    Wenn Sie die automatische Terminvergabe nutzen und Sie tragen Daten Ihrer Patienten ein, brauchen Sie einen Auftragsdatenverarbeitungsvertrag mit Jameda. Wenn Sie die Patientendaten aus der Terminvergabe nur auslesen, nachdem die Patienten ihre Daten selbst eingetragen haben, brauchen Sie es nicht.
  - ➡ *Zur DSGVO konformen Nutzung der jameda Siegel / Widgets auf Ihrer Homepage empfiehlt Jameda Ihnen, diesen Passus in Ihre Datenschutzerklärung einzufügen:*
    Jameda Siegel und Widget
    Auf unserer Internetseite sind Siegel oder Widgets der jameda GmbH, St. Cajetan-Straße 41, 81669 München eingebunden. Ein Widget ist ein kleines Fenster, das veränderliche Informationen anzeigt. Auch unser Siegel funktioniert in ähnlicher Weise, d. h. es sieht nicht immer gleich aus, sondern die Anzeige ändert sich regelmäßig. Dabei wird der entsprechende Inhalt zwar auf unserer Internetseite dargestellt, er wird aber in diesem Moment von den jameda-Servern abgerufen. Nur so kann immer der aktuelle Inhalt gezeigt werden, vor allem die jeweils aktuelle Bewertung. Dafür muss eine Datenverbindung von dieser Internetseite zu jameda aufgebaut werden und jameda erhält gewisse technische Daten (Datum und Uhrzeit des Besuchs; die Seite, von der die Abfrage erfolgt; verwendete Internet Protokoll-Adresse (IP-Adresse), Browsertyp und -version, Gerätetyp, Betriebssystem und ähnliche technische Informationen), die nötig sind, damit der Inhalt ausgeliefert werden kann. Diese Daten werden aber nur für die Bereitstellung des Inhalts verwendet und nicht gespeichert oder anderweitig genutzt.
    Wir verfolgen mit der Einbindung den Zweck und das berechtigte Interesse, aktuelle und korrekte Inhalte auf unserer Homepage darzustellen. Rechtsgrundlage ist Art 6 Abs. 1 f) DSGVO. Eine Speicherung der genannten Daten erfolgt durch uns aufgrund dieser Einbindung nicht. Weitere Informationen zur Datenverarbeitung durch jameda können Sie der Datenschutzerklärung der Seite https://www.jameda.de/jameda/datenschutz.php entnehmen.

- Stimmt es, dass ich keine Patientendaten/-kontakte auf dem Handy haben darf?
  - ➡ *Nein, das Handy an sich ist kein Problem. Schwierig wird es, wenn auf dem Smartphone auch Apps wie Facebook oder WhatsApp installiert sind, die Zugriff auf die Kontaktliste oder andere Daten (z.B. Fotos von Patienten) haben. Dieser Tatbestand wird als „grob fahrlässig" eingestuft.*

- Wie kann ich Whatsapp noch nutzen, wenn in den Kontakten auch Klienten drin sind?
  - ➡ *Es ist kritisch irgendwelche Apps auf dem Praxis-Handy installiert zu haben, weil zumindest viele der amerikanischen Apps sich erlauben lassen, auf Kontaktdaten o.ä. zugreifen zu dürfen. Sie sind auf der sicheren Seite, wenn Sie ein reines Praxis-Handy mit Patientenkontaktdaten, aber ohne kritische Apps haben und ein weiteres privates Handy, auf dem Sie beliebig viele Apps haben können.*
    Falls Sie keine 2 Mobilverträge bezahlen wollen, können Sie diesen Trick von Thomas Schulze benutzen:
    - *Nehmen Sie ein altes Smartphone, für das Sie keine SIM-Karte mehr betreiben.*
    - *Legen Sie Ihre momentane SIM-Karte ein und installieren Sie WhatsApp.*
    - *Nehmen Sie die SIM-Karte wieder heraus und legen Sie sie wieder ins Praxishandy ein.*
    - *Jetzt können Sie mit dem Handy nicht mehr telefonieren, aber zuhause am WLAN funktioniert es noch!*

- *Löschen Sie aus der WhatsApp-Liste alle Patienten-Kontakte.*
- *Deinstallieren Sie WhatsApp auf dem Praxis-Handy.*
- *Und alles am besten vor dem 25.5.18!*

➡ *Ein Webinar-Teilnehmer empfahl die App Secure Contact pro, mit der man alle Geschäftsdaten auf dem Handy separieren und schützen kann. Ich hatte keine Zeit nachzuprüfen, ob die App allen DSGVO-Anforderungen auch für Gesundheitsdaten genügt.*

➡ *Der einfachste Weg ist natürlich, einen Auftragsdatenverarbeitungsvertrag mit WhatsApp abzuschließen…*

- Was muss ich bei Google beachten?
  - ➡ *Wenn Sie Google Analytics nutzen, brauchen Sie einen Auftragsdatenverarbeitungsvertrag mit Google.*
  - ➡ *Wenn Sie auf Google Drive personenbezogene Daten ablegen, …?*
  - ➡ *Wenn Sie in den Google-Kalender personenbezogene Daten eintragen, …?*
- Was ist ein zertifiziertes Programm? Reichen Windowsprogramme zur Erstellung der Rechnung? Wie ist es mit Programmen zur Rechnungserstellung? Windows? Darf ich überhaupt Officeprogramme verwenden?
-

➡ *Die Programme brauchen nicht zertifiziert sein, sondern es kommt darauf an, dass sich der Hersteller der DSGVO verpflichtet und allen Anforderungen nachkommt. Wenn Sie Office 365-Produkte benutzen (d.h. Cloud-basiert), brauchen Sie einen Auftragsdatenverarbeitungsvertrag mit Microsoft. (Ich habe vergeblich danach auf den Microsoft-Seiten gesucht und ihn letztendlich per Mail angefragt. Falls Sie einen Download-Link finden, sagen Sie mir bitte Bescheid.) Vertrauen wir Windows mal, dass es keine Patientendaten spioniert…*

- Darf man Daten in der Cloud auf dem PC speichern?
  - ➡ *Diese Frage widerspricht sich, weil „in der Cloud" bedeutet, dass die Daten gerade nicht auf auf dem PC (sprich auf einer Festplatte oder einem Speicherchip) gespeichert werden. Bei vielen gängigen Cloud-Lösungen (z.B. iCloud von Apple) werden die Daten auf Servern außerhalb der EU gespeichert, was datenschutzrechtlich kritisch ist. Erkundigen Sie sich, ob der Cloud-Anbieter die Möglichkeit eines Auftragsverarbeitungsvertrag anbietet. Wenn ja, schließen Sie ihn ab und listen Sie ihn in Ihrem Datenschutzkonzept auf. Wenn nein, lassen Sie lieber die Finger davon.*
- Terminvereinbarung via SMS etc.
  - ➡ *Ich bin mir nicht sicher, wie diese Frage gemeint war. Wir haben ja schon festgehalten, dass auf dem Handy, auf dem sich die Patiententelefonnummern befinden (spätestens, wenn die Person angerufen oder eine SMS geschickt hat, ist ihre Nummer ja erst einmal gespeichert), kein WhatsApp oder andere Apps installiert sein dürfen, die sich nicht an die DSGVO halten. Ansonsten hat SMS-Kommunikation die gleiche Bedeutung wie Telefonkommunikation.*
- Mein IT Anbieter hat mir gesagt ich müsste eine Firewall Hardware kaufen um Hacker auszuschliessen
  - ➡ *Ich kenne ja Ihre Verhältnisse nicht, aber es scheint, dass hier mal wieder mit Angst gearbeitet wird, damit Kunden mehr Geld ausgeben als nötig. Eine Hardware-Firewall ist dafür, zwei Netzwerke von einander zu trennen. Wenn Sie einen einsamen Praxis-PC haben, ist sie ungeeignet. Sie sollten jedoch einen Virenscanner und eine Software-Firewall auf Ihrem PC installieren.*

- Was muss ich beim Datenschutz beachten, wenn meine Patienten Termine online buchen können?
  - ➞ *Weil Patientendaten besonders schützenswert sind, brauchen Sie nicht nur eine Software, deren Hersteller einen Auftragsdatenverarbeitungsvertrag anbietet. Er muss auch Daten mit hoher Sicherheitsstufe abdecken!*

Tagesgeschäft:

- alles, was nicht-online Themen angeht: Heilpraktiker-Tagesgeschäft
  - ➞ *Um ehrlich zu sein: da können die Berufsverbände / Heilpraktiker-Schulen besser Auskunft geben. Sie sind ja seit längerem verpflichtet, vor der ersten Behandlung mit dem Patienten eine Behandlungsvertrag abzuschließen. In Zukunft bekommt er also noch einen Zettel mehr, auf dem er bestätigt, dass er damit einverstanden ist, dass Sie seine Daten aufnehmen und speichern. Wenn er das nicht ist, bekommt er keine Behandlung…*
- Muss beim Erstkontakt eine Einwilligungserklärung unterschrieben werden?
  - ➞ *Ja, sonst dürfen Sie nicht einmal den Namen notieren, geschweige denn der ersten Termin in Ihren Kalender schreiben.*
- Wie konkret kann der Erstkontakt zum Patienten funktionieren, also z.B. die Versendung von Patienten-Aufnahmebögen und die Honorarvereinbarung?
  - ➞ *Ja, wenn ich das wüsste! So, wie es der Gesetzgeber vorsieht, wird es nicht funktionieren können. Theoretisch müssten Sie einem anrufenden Interessenten erstmal Ihre Datenschutzerklärung vorlesen, bevor Sie überhaupt seinen Namen notieren oder ihn in einen Kalender eintragen können. Da Datenschutzerklärungen nicht nur ellenlang, sondern auch furchtbar langweilig sind, würden die Anrufer vermutlich auflegen, bevor Sie fertig sind. Warten wir ab, was in nächster Zeit für Regelungen gefunden werden…*
- Muss ich die Datenvereinbarung mit jedem Patienten vereinbaren? d.h. Muss ich auch das Einverständnis von meinen bestehenden Patienten einholen?
  - ➞ *Ja, das müssen Sie. Da ich davon ausgehe, dass Ihre Patienten Sie mögen und Ihnen nichts Böses wollen, ist das meiner Meinung nach aber nur Prio 2.*
- Was muss das Einverständnis mit dem Patienten enthalten?
  - ➞ *Ich hoffe, Ihre Berufsverbände können Ihnen dazu bald Vorschläge unterbreiten. Derweil habe ich hier ein Muster für Ärzte gefunden.*
- Müssen bei Kindern die gesetzlichen Vertreter beide unterschreiben wie bei den Banken?
  - *Nein, das ist nur notwendig, wenn größere ärztliche Eingriffe wie Operationen vorgenommen werden und ggf. bei Impfungen. Wir sind ja keine Gefahr für die Volksgesundheit! ;-)*
- Muss ich alle meine bestehende und ehemalige Patienten anschreiben um Datenschutz bekannt zu machen? und ob ich deren Daten aufbewahre darf?
  - ➞ *Bei Patienten geht es nicht darum, dass Sie um Erlaubnis bitten, die Daten aufbewahren und verarbeiten zu dürfen. Aber Sie müssen ihnen eine Ergänzungserklärung schicken und transparent machen, wenn Sie Daten an Dritte schicken (z.B. Webseiten-Hoster, Lohnbuchhalter, Labor, …)*
- Muss bzw. darf ich meine Akten aufbewahren?
  - ➞ *Als Unternehmer müssen Sie Ihre Buchhaltungsakten 10 Jahre aufheben, als Heilpraktiker genauso die Patientenakten. Das ist eine betriebliche Aufgabe und damit wichtiger als der Datenschutz.*

- Welche Unterlagen müssen den Patienten in der Praxis ausgehändigt werden
  - ➞ *Ein Informationsblatt , das die Art der Verarbeitung Ihrer Patientendaten für den Patienten transparent macht. Lassen Sie sich unterschreiben, dass der Patient die Informationen gelesen und verstanden hat. Sie erhalten entsprechende Muster vermutlich bei Ihrem Berufsverband. Wenn Sie keinen haben, können Sie sich z.B. hier erkundigen, was das Informationsblatt beinhalten muss.*
- Wie muss die Einverständniserklärung aussehen?
  - ➞ *Schauen Sie mal hier: https://www.mit-sicherheit-gut-behandelt.de/muster.html*
- Wieviele Daten kann man ohne Datenschutzerklärung am Telefon erfragen?
  - ➞ *Es gibt die Behauptung, dass Sie erst mal 10 Minuten Datenschutzbedingungen vorlesen, bevor Sie überhaupt den Namen notieren dürfen. Andererseits sagt das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (Anstalt des öffentlichen Rechts), dass Sie sich das Vorlesen sparen können, wenn die Informationen auf Ihrer Webseite leicht auffindbar sind.*
- welche Möglichkeiten gibt es mit meinen Patienten in Kontakt zu treten
  - ➞ *Alle, die Sie sich auf der Einverständniserklärung unterschreiben lassen.*
- Darf ich noch elektronische Rechnungen verschicken?
  - ➞ *Sie brauchen dafür einen Auftragsdatenverarbeitungsvertrag mit der Firma, die die Rechnungen verschickt.*
- Kassenbuch, Rechnungskopien aufbewahrung
  - ➞ *Sie haben und hatten ja schon immer die Pflicht, alles 10 Jahre aufzubewahren. Das müssen Sie auch dann aufheben, wenn ein Patient/Kunde Sie darum bittet, seine Daten zu löschen. Das Kassenbuch ist bekommt eine extra-Seite in Ihrem Datenschutzkonzept.*
- Müssen bei Kindern beide gesetzliche Vertreter ihre Einwilligung geben?
  - ➞ *Solch eine Forderung ist mir nicht bekannt. Sie schließen den Behandlungsvertrag ja sowieso mit einem Elternteil. Der kann dann gleich die Datenschutzerklärung mit unterschreiben.*
- Muss mein Aktenschrank, tatsächlich feuerfest sein?
  - ➞ *In der TOM werden die Maßnahmen aufgezählt, die Sie unternehmen um Datenverluste zu vermeiden und vor allem rückgängig zu machen. Es wird nicht speziell ein feuerfester Aktenschrank gefordert, aber schaden kann es nicht!*
- Muss ich meine Patientendaten in einem abschließbaren Schrank haben?
  - ➞ *Wenn niemand anderes hereinkommt, reicht es, wenn der Praxisraum abschließbar ist, oder die Flurtür der Praxis, oder die Haustür, wenn nur Sie im Haus wohnen. Irgendwo werden Sie schon eine abschließbare Tür haben, die verhindert, dass Sie Ihrer Patientenakten verlustig gehen… Dokumentieren Sie es einfach im Datenschutzkonzept.*
- Gilt das auch für die Labore, denen ich das Blut schicke, gilt mein Laborauftrag als Vertrag? Wie ist das mit Patientendaten und den Ergebnissen?
  - ➞ *Soweit ich das sehe, ist ein Labor kein Auftragsdatenverarbeiter, sondern es handelt sich um eine Funktionsübertragung. -> keine ADV im Datenschutzkonzept.*
- Ich arbeite manchmal mit einem Arzt zusammen und sende ihm Daten über Email von meinen Patienten. ich würde das gern weiter über Email machen. Muss ich verschlüsseln? Brauche ich AV?
  - ➞ *Ja, Sie sollten Ihre Email verschlüsseln (s.o.) Eine ADV brauchen Sie laut Thomas Schulze nicht, weil der Arzt selbst Geheimnisdatenträger ist.*

- Was gilt denn bei Arbeitskreisen mit Patientenvorstellung? Muss dort eine Verschwiegenheitserklärung ausgefüllt werden?
  - ➞ *Wenn der Patient zu dieser Veranstaltung kommt und vor den Augen Anderer behandelt wird, müssen diese eine Erklärung unterschreiben. (Analog muss ein Hospitant unterschreiben, der einen Patienten oder dessen Daten zu Gesicht bekommt.) Wird nur eine anonyme Fallvorstellung gemacht, aus der die Identität des Patienten nicht ableitbar ist, braucht man keine Erklärung.*
- Was muss ich noch beachten?
  - ➞ *Entwickeln Sie eine Sensibilität dafür, dass niemand die Daten Ihrer Patienten zu Gesicht bekommt. Lassen Sie also keine Karteikarten offen rumliegen und erlauben Sie es den Patienten nicht zuzuschauen, was (bzw. wer) in Ihrem Terminkalender steht.*
  - ➞ *Kaufen Sie einen Schredder, mit dem Sie alle Papiere mit personenbezogenen Daten fachgerecht entsorgen. (Wenn die Datenschutzbehörde zu einer Prüfung kommt, fängt der Beamte oft damit an, den Müll des geprüften Unternehmens zu durchforsten um einen Eindruck zu bekommen, wie gewissenhaft dort mit solchen Daten umgegangen wird.*
- Darf ich überhaupt noch Werbung an Interessenten schicken (Mail, Brief)?
  - ➞ *Erwägungsgrund 47 der DGSVO besagt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." Schreiben Sie also in Ihre Datenschutzerklärung: „Ich sammele, verarbeite und speichere Daten von Interessenten und Patienten zum Zwecke der Direktwerbung." Übertreiben Sie es aber nicht mit der Sammelwut! Art. 5 gebietet das Prinzip der Datenminimierung. Danach dürfen nur „dem Zweck der Speicherung angemessene" Daten gespeichert werden und nur solange dies erforderlich ist.*
- Was ist mit Menschen, die schon lange nicht mehr als Patient bei mir waren? Karteileichen darf ich ja nicht anschreiben.
  - ➞ *Denken Sie dran, dass Sie die Patientenakten und Rechnungen 10 Jahre aufbewahren müssen! Laut UWG (Gesetz gegen den unlauteren Wettbewerb) ist es in Deutschland gestattet, Bestandskunden ohne explizite Einwilligung Werbung zu senden.*

Datenschutzkonzept:

- Wer muss ein Datenschutzkonzept haben?
  ➞ *Jeder Unternehmer, egal wie viel oder wenig Umsatz die Person macht. Das Argument „Meine Patientenakten und meine Buchhaltung oder Rechnungen sieht ja keiner“ ist nicht ausreichend. Im Datenschutzkonzept muss drinstehen, dass es niemand sieht.*

- Woraus besteht das Datenschutzkonzept?
  ➞ *Hier ein grober (unvollständiger) Überblick auf das, was Sie benötigen.*
  Das Datenschutzkonzept ist aufgebaut aus diesen 4 Teilen:
  1. *Verzeichnis von Verarbeitungstätigkeiten für Verantwortliche (VVZ).*
     Hierin werden einzelne, vom Gesetzgeber ausgewählte Verarbeitungstätigkeiten aufgelistet und dazu angegeben, was der Zweck ist, wer dafür verantwortlich ist, welche Personengruppen davon betroffen sind, etc. Beispiele: Finanzbuchhaltung, elektronischer Zahlungsverkehr, Email-Kommunikation.
  2. *Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM)*
     Hierin wird beschrieben,
     - *welche Maßnahmen getroffen werden, um die Vertraulichkeit zu gewährleisten (z.B. Praxistür abschließbar, Firewall auf dem Rechner, Pseudonymisierung)*
     - *Wie dafür gesorgt wir, dass personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert werden*
     - *Wie gewährleistet wird, dass Daten nicht verloren gehen (z.B. Back-up-Strategie)*
     - *Welche Maßnahmen getroffen werden, wenn jemand sein „Recht auf Vergessenwerden“ einfordert.*
     - *Wie dafür gesorgt wird, dass die Maßnahmen regelmäßig überprüft, bewertet und evaluiert werden (z.B. Beschreibung interner Verhaltensregeln)*

     Alle beauftragten Auftragsdatenverarbeiter (z.B. Website-Hoster, Google Analytics, etc.) werden mit ihrer Firmenadresse und einer Angabe, in welche Kategorie die Verarbeitung fällt, aufgelistet.
  3. *Einschätzung, ob eine Datenschutz-Folgeabschätzung notwendig ist (Risikoanalyse)*
     Hier werden die Verarbeitungstätigkeiten noch einmal durchgegangen und für jede eingeschätzt, wie sensibel die Daten der Betroffenen sind, wie wahrscheinlich es ist, dass sie zweckentfremdet werden und ob eine Datenschutzfolgenabschätzung notwendig ist.
     Diese Risikoanalyse muss von jedem Unternehmer durchgeführt werden - auch wenn man sich nicht als Risikopotenzial wahrnimmt. Doch keine Angst: Obwohl die Sensibilität von Patientendaten (im Gegensatz zu normalen Kundendaten als „hoch“ gilt, werden Sie vermutlich keine Datenschutzfolgenabschätzung machen müssen, weil es recht unwahrscheinlich ist, dass durch ein Datenleck bei Ihnen in der Heilpraktikerpraxis dem Patienten nennenswerter Schaden zugefügt werden kann.
  4. *Die Sammlung von Auftragsdatenverarbeitungsverträgen mit den einzelnen Firmen, die von beiden Seiten unterschrieben sein müssen. (Die Bank und der Steuerberater sind von dieser Pflicht ausgenommen.)*

- Wo bekomme ich denn nun die Formulare für den Datenschutzordner her?
  ➞ *Ich danke Herrn Schulze, dass er hier die ganzen Vorlagen zur Verfügung stellt!*

- Wie macht man eine ADV?
  - ➞ *Theoretisch können Sie selbst so einen Vertrag aufsetzen und Ihrem Auftragsdatenverarbeiter vorlegen. Ich habe die entsprechenden Firmen um einen solchen Vertragsentwurf gebeten und von den meisten ohne Murren (höchstens etwas verspätet) bekommen. Ich habe für Sie bei verschiedenen bekannten Webhoster recherchiert:*
    - Strato: https://www.strato.de/faq/article/2763/Fragen-zur-Auftragsverarbeitungsvertrag-AVV-und-der-neuen-EU-Datenschutzgrundverordnung-DSGVO.html#avv_abschliessen
    - Jimdo: https://jimdo-legal.zendesk.com/hc/de/articles/360000782763-Auftragsverarbeitungsvertrag-Jimdo
    - 1&1: https://hosting.1und1.de/hilfe/datenschutz/allgemeineinformationen/auftragsverarbeitung/
    - WIX: noch keine Antwort
    - Beepworld: erst nach dem 25.5. Lösung in Sicht
- Was beinhaltet ein Auftragsdatenverarbeitungsvertrag (ADV)?
  - ➞ *Das ist eine Menge. Die Beschreibung finden Sie hier: https://www.datenschutz-wiki.de/Auftragsdatenverarbeitung*
- Für wen brauchen wir alles eine ADV? WO schickt man die hin?
  - ➞ *Sie brauchen eine ADV mit allen Dienstleistern, denen Sie personenbezogene Daten (bewusst oder unbewusst) übermitteln. Also Labore, Kollegen, mit denen Sie ein Computersystem teilen, Cloud-Services, Google-Analytics, etc. Die ADV wird nirgendwo hingeschickt, sondern in Ihren Ordner mit dem Datenverarbeitungskonzept geheftet.*
- Muss die ADV vom Patienten unterschrieben sein oder wäre es auch möglich, den Patienten anzuschreiben und darauf hinzuweisen, dass die ADV ab dem 25.5. gilt (ohne Rückmeldung)?
  - ➞ *Jetzt müssen wir aufpassen, dass wir keine Begrifflichkeit durcheinander werfen. Die ADV brauchen Sie „nur" für ihr Datenschutzkonzept. Ihre Patienten brauchen Ihnen nur Ihre Datenschutzerklärung unterschreiben. Soviel ich weiß, reicht es, wenn der Patient das beim nächsten Termin macht, aber fragen Sie lieber Ihren Berufsverband.*
- Was ist mit Telefonanbieter? Benötigt man für diesen auch eine ADV?
  - ➞ *Aus irgendeinem Grund sind Telefonanbieter genau wie Banken und Steuerberater von der Verpflichtung ausgenommen.*
- Ganz praktisch: Wie sieht so ein Verfahrensverzeichnis aus und gibt es eine Art Vordruck/Muster?
  - ➞ *Ein Teilnehmer empfahl das Buch Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine: Das Sofortmaßnahmen-Paket für 5,50€*
  - ➞ *einige Heilpraktikerverbände (auf alle fälle der BDH) haben diese Formulars auf ihrer Homepage Seite zum ausdrucken*
  - ➞ *Netterweise stellt und Thomas Schulze die Muster zur Verfügung.*
- Muss ich einen Ordner anlegen?
  - ➞ *Zurzeit ist die Rechtsprechung noch so, dass das Datenschutzkonzept in Papierform vorliegen muss. Es reicht nicht es irgendwo gespeichert zu haben. Deshalb ist ein Ordner die einfachste Art, die bis zu 200 Seiten aufzubewahren.*

- Gibt es Besonderheiten für Heilpraktiker?
  - ➞ *Laut DSGVO (Art. 4 Nr. 15) sind „Gesundheitsdaten“ personenbezogene Daten„die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“. Also das, was Sie in Ihre Patientenakte schreiben und die Diagnosen und Behandlungsmethoden, die auf der Rechnung stehen. Gesundheitsdaten werden in der Risiko-Bewertung als „hohes Risiko“ eingeschätzt. Für Ihr Datenschutzkonzept bedeutet es, dass Sie eine Seite mehr ausfüllen müssen als z.B. ich, die nur „normale“ Daten ihrer Kunden speichert. Eine Risiko-Folgeabschätzung würde nur bei besonders vielen oder sensiblen Daten nötig, z.B. genetische Informationen.*
- Was muss ich beachten, wenn mein Praxiszimmer in den Privaträumen unserer Familie ist?
  - ➞ *Sie müssen dafür sorgen, dass Sie Ihre Patientenakten und den Computer so wegschließen können, dass niemand darauf Zugriff hat. Die Art der Sicherung (z.B. abschließbarer Praxisraum oder abschließbarer Schrank) wird zusammen mit einem Schlüsselprotokoll im Datenschutzkonzept vermerkt.*
- Nicht-digitale Daten - Was mache ich mit den Patientendaten?
  - ➞ *Das kommt darauf an, was Sie früher damit gemacht haben. Wenn es die nur auf Karteikarten gibt, ist es einfach. Dann brauchen Sie nur in Ihr Datenschutzkonzept schreiben, wie Sie sie gegen unbefugten Zugriff schützen, z.B. dadurch, dass Ihre Praxis absperrbar ist. Wenn Sie ein Programm benutzen, sollten Sie darauf achten, dass es DSGVO-kompatibel ist (z.B. Soliprax ab Version 20.4) Den Programmnamen schreiben Sie bei der entsprechenden Frage in das Datenschutzkonzept. Wenn es eine (sichere) Cloudlösung ist, brauchen Sie noch einen Auftragsdatenverarbeitungs-Vertrag mit dem Anbieter.*
- Brauche ich als HP mit Angestellten einen externen Datenschutzbeauftragten?
  - ➞ *Es ist noch etwas umstritten, aber ziemlich wahrscheinlich gilt folgendes:*
    Sie brauchen nur dann einen Datenschutzbeauftragten, wenn Sie
    - *eine Gemeinschaftspraxis haben, die sich Infrastruktur teilt oder*
    - *mehr als 9 Angestellte haben, die Zugang zum Computer haben (die Reinigungskraft zählt also i.d.R. nicht) oder*
    - *wenn die Haupttätigkeit Ihrer Praxis ist, große Mengen an Gesundheitsdaten zu verarbeiten. (Ich glaube aber nicht, ob das Betreiben eine Bioresonanzcomputers damit gemeint ist… Vielleicht, wenn Sie in großem Stil Labordiagnosen durchführen?)*
- Verfahrensverzeichnis als Verein
  - ➞ *Vereine haben ein paar mehr Seiten in Ihrem Datenschutz-Konzept. Weil ich kein Verein bin, hat Herr Schulze diese Seiten bei mir übersprungen, deshalb kann ich dazu nichts sagen. Sein Program beherrscht aber auch das.*
- Brauche ich rückwirkend eine schriftliche Einwilligung für Fotos von Patienten auf meiner website, die sie schon vor langer Zeit mündlich gegeben haben im Beisein anderer?
  - ➞ *Meines Wissens nach ja. Allerdings: meiner persönlichen Meinung nach ist der Aufwand den Leuten hinterherzutelefonieren höher als der mögliche Schaden. Es sind ja keine Fremden. Damit ist es eher unwahrscheinlich, dass die Sie abmahnen wollen. Und woher soll ein Abmahnverein wissen, ob Sie die Erlaubnis schriftlich haben oder nicht?*

- Dieser Ordner, den man anlegen muss...wer schaut sich das denn regelmässig an? Kommt da tatsächlich so ein Mensch und überprüft das?
  - ➞ *Normalerweise verlässt sich der Gesetzgeber darauf, dass Sie den Ordner anlegen. Es gibt z.Zt. auch viel zu wenig Mitarbeiter in den Landesdatenschutzbehörden, als dass es überprüft werden könnte. Sollte jedoch jemand auf die Idee kommen, dass Sie mit Ihren Daten nicht gesetzeskonform umgehen und Sie deshalb beim Landesdatenschutzbeauftragten melden, bekommen Sie die Aufforderung nachzuweisen, dass*
- Braucht man einen Anwalt unbedingt?
  - ➞ *Niemand wird verpflichtet einen Anwalt hinzuzuziehen. Jeder hat das Recht, sich selbst in den Dingen schlau zu machen. Allerdings wäre man mir einem Anwalt auf der sicheren Seite, weil der dann dafür geradestehen muss, wenn er etwas falsches geraten hat. Dieses Risiko lassen sich die Anwälte gut bezahlen. Ich persönlich fand es ausreichend, mir die Hilfe von Herrn Schulze (datenschutz@webinarfahrschule.de) zu holen, weil ich ja nicht vorhabe, vorsätzliche oder grob fahrlässige Vergehen zu begehen.*
- muss man angeklagt werden um belangt zu werden?
  - ➞ *Nein, der Datenschutzbeauftragte Ihres Bundeslands kann Bußgelder verhängen ohne Sie vor Gericht zu zerren. Auch Abmahnvereine werden versuchen ohne Prozess an das von ihnen geforderte Geld zu kommen.*
- gilt das alles auch für die Schweiz?
  - ➞ *Naja, den Schweizer Unternehmen wird geraten, sich auch dran zu halten, weil die meisten auch Kunden aus EU-Ländern haben. Und das Gesetz ist nicht abhängig vom Hauptsitz des Unternehmens, sondern davon, ob es auch Zielgruppen in EU-Ländern als Kunden hat. Sie wissen am besten, ob Deutsche zu Ihnen in die Praxis kommen. Ob Sie sich wegen eines deutschen oder österreichischen Patienten schon an das EU-Gesetz halten müssen , kann Ihnen ein Schweizer Rechtsberater besser erklären als ich.*
- Muss das jedes Jahr gemacht werden oder nur einmal?
  - ➞ *Das Datenschutzkonzept muss regelmäßig auf den neuesten Stand gebracht werden, z.B. 1-mal pro Jahr. Das heißt, den großen Arbeitsaufwand zur Erstellung haben Sie nur 2018. Danach korrigieren Sie nur Eintragungen, die überholt sind und heften ein Protokoll ab, in dem Sie notieren, dass Sie die Eintragungen überprüft und ggf. korrigiert haben.*

Ein paar gefundene interessante Weblinks:

https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html
https://hootproof.de/cookie-hinweis/
https://www.emailtooltester.com/blog/dsgvo-email-marketing/
https://www.heilpraktikerrecht.com/2018/04/10/faktencheck-zur-dsgvo-was-fuer-heilpraktiker-wichtig-ist/
https://www.datenschutz-notizen.de/google-apps-fuer-die-unternehmensdatenverarbeitung-im-ernst-0412068/