FAQ

EU-DSGVO-Paket

Datenschutz in der Praxis

Mitarbeiter

Umgang mit Mitarbeiterdaten

- Dürfen Mitarbeiterdaten in einem System (z.B. CRM) verwaltet werden?
  Datentrennung ist hier das Motto. Es muss sicher gestellt werden, dass Funktionen für die Kunden und die Aufbewahrungsfristen nicht mit den von den Mitarbeitern vermischt werden. Daher klare Trennung.

Verschwiegenheitsverpflichtung

- Eine Praxisgemeinschaft aus mehreren Heilpraktikern hat einen Mitarbeiter, der für alle Heilpraktiker arbeitet. Reicht es, wenn der Mitarbeiter eine gebündelte Verschwiegenheitserklärung unterschreibt, in der alle Heilpraktiker der Praxisgemeinschaft benannt sind oder muss der Mitarbeiter jedem einzelnen Heilpraktiker seine Verschwiegenheit in einem separaten Dokument erklären?
  Gebündelt reicht hier aus.

- Müssen unterstützende Familienmitglieder auch eine Verschwiegenheitsverpflichtungserklärung unterschreiben?
  Nur weil es Familienmitglieder sind, brauchen Sie nicht verschwiegen sein. Alle, die Zugriff auf personenbezogene Daten haben, sollten unterschreiben.

- Müssen freie Mitarbeiter die Verschwiegenheitserklärung für Externe oder diese für Mitarbeiter ausfüllen?
  Da freie Mitarbeiter „frei" sind, bitte hier die für Externe nutzen.

Patienten/Kunden

Umgang mit Patientendaten

- Wie müssen Patientendaten bei mobiler Tätigkeit geschützt werden (Patientenakten im Auto)?
  So, dass kein Zugriff auf diese Daten erfolgen kann. Es gibt drei Arten des Zugriffs:
  1. *Nur mit den Augen, ohne Nutzung der Hände*
  2. *Nutzung der Hände um an Informationen zu kommen*
  3. *Vorsätzliche Kraftanwendung (Einbruch)*

Bei den Patientendaten handelt es sich um besonders schützenswerte Daten. Wenn sie im Auto transportiert werden müssen, dann so, dass keine sieht, dass da welche sind, um durch Einbruch an die Daten zu kommen.

- Gehört ein KFZ-Kennzeichen zu den personenbezogenen Daten?
  Kommt drauf an. Wenn
  - *die Buchstaben den Besitz erkennen lassen*
  - *der Kfz-Betrieb meines Vertrauens die Pseudonymisierungstabelle hat*

  dann ja.

- dürfen Kunden im Geschäft mit Namen angesprochen werden?
  Es ist nicht verboten. Sie übernehmen die Verantwortung, dafür, ob er es möchte oder nicht.

- Wie muss man mit Patientendaten umgehen, die in elektronischer und analoger Form vorliegen? Schutz, Speicherung und Back-Up?
  Dem Schutzniveau entsprechend muss das die Datenhaltung erfolgen. Egal ob Papier oder elektronisch: Vor Zugriff Unberechtigter schützen, Verfügbar halten und so sichern, dass die Rechte der Betroffenen umgesetzt werden können.

- Sollten Behandlerverträge um eine Erklärung zu Patientendaten und Aufbewahrungsfristen erweitert werden?
  Ja, ein Hinweis dazu gibt es 4. Video.

- Können / Müssen Erziehungsberechtigte eine Patientenerklärung unterschreiben? Dürfen Daten von Kinder / Erziehungsberechtigten in einer Akte sein?
  Ja, da die Erziehungsberechtigten für die Kinder handeln/entscheiden.

- Für welche Datennutzung und zu welchem Zeitpunkt müssen Kunden aufgeklärt werden?
  Immer bevor Sie die Daten erheben/verarbeiten. Damit der Kunde entscheiden kann.

- Mit welchen Besonderheiten sind besonders schützenswerte Daten zu verarbeiten und zu speichern?
  Die besonders schützenswerte Daten sind deshalb so deklariert, da Sie bei einer Datenpanne eine besondere Gefahr für den Betroffenen bedeuten. Daher sind sie angemessen Ihres Schutzniveaus zu verwalten. Einfach sicherer.

- Sind Bilder / Fotos / Videos personenbezogene Daten?
  Ja, denn eine Person ist da häufig zu identifizieren.

- Muss oder kann ich alle Daten der Patienten nach 10 Jahren löschen?
  Jein, hängt von den individuellen Aufbewahrungsfristen aus den entsprechenden Regelungen, z.B. SGB ab.

- Wie muss mit bereits erhobenen Kundendaten (Altdaten) umgegangen werden?
  Gibt es einen Vertrag noch? Gibt es eine Aufbewahrungsfrist? Hat der Kunde aktiv zugestimmt? Wenn alles nein, dann dürfen Sie die Daten nicht mehr aufbewahren.

- Müssen die Daten nach einem gewissen Zeitraum gelöscht werden, wenn mit dem Betroffenen keine Interaktion erfolgt ist?
  Ja, nach Ablauf der Aufbewahrungsfrist.

Einwilligung und Informationspflicht

- Müssen Patienten eine Einverständniserklärung für die Nutzung Ihrer Daten unterschreiben? (Muster)
  Siehe 4. Video.

- Müssen Patienten darüber informiert werden, dass ihre Daten an ein externes Inkassobüro weitergeleitet werden?
  Wenn Sie mit dem externen Dienstleister einen AV-Vertrag geschlossen haben, dann nein.

- Ist es wichtig den Kunden / potentiellen Kunden schon am Telefon darüber zu informieren was mit den aufgenommenen Daten passiert? Wird vor Kontaktaufnahme eine Einwilligung benötigt?
  Wenn Sie Daten am Telefon schon erheben, dann brauchen Sie die Zustimmung, oder aber es gilt bereits ein Vertrag.

Praxis

Notwendige Konzepte

<u>Verzeichnis der Verarbeitungstätigkeiten (vormals Verfahrensverzeichnis)</u>

- Wann und in welchem Umfang müssen Lieferanten im Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden?
  Wenn Sie von Ihnen personenbezogene Daten erhalten.

- Muss ich nur ein Verzeichnis der Verarbeitungstätigkeit ausfüllen oder mehrere?
  Ein „Verzeichnis“. Das gibt das Wort schon wieder.

- Ist ein verkürztes Verfahrensverzeichnis auf der Internetseite verpflichtend, anzuraten oder nur auf Anfrage zu überlassen?
  Ab der Einführung der DSGVO braucht ein Verzeichnis nicht mehr online gestellt werden.

- Wenn rechtlich zwei Praxen (zwei isolierte GbR Verträge) sich in den gleichen Räumlichkeiten befinden, müssen dann auch unterschiedliche Verzeichnisse der Verarbeitungstätigkeit angelegt werden oder können diese in ein Verzeichnis zusammengefasst werden?
  Je Organisation ein Verzeichnis.

- Was verbirgt sich hinter den Begrifflichkeiten Vertraulichkeit und Integration und Authentizität und Transparenz?
  Vertraulichkeit – Stillschweigen über geheime und personenbezogene Daten
  Integration – Das IT- System muss in den Ablauf integriert sein. Nicht für die agieren.
  Authentizität – Die Daten die Sie bekommen müssen unverändert vorliegen.
  Transparenz – Die Verfahren in Ihrem Unternehmen darf nicht Ihr Geheimnis sein. Damit kann keine Kontrolle und Prüfung stattfinden.

- Muss das Verzeichnis der Verarbeitungstätigkeiten proaktiv an die Betroffenengruppen übergeben werden?
  Nein, bei Nutzen des Betroffenenrechts auf Auskunft

- Was bedeuten die Begriffe Eingabekontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und Belastbarkeit der Systeme sowie Art der Gewährleistung?
  Eingabekontrolle – Wie stellen Sie sicher, dass die Daten, die erfasst wurde, richtig sind?
  Verfügbarkeitskontrolle – Wie stellen Sie sicher, das die Daten dann zur Verfügung stehen, wenn sie gebraucht werden.
  Trennungskontrolle – Funktionstrennung
  Belastbarkeit – Läuft Ihr System mit einem Maß an Puffer (Speicher).
  Gewährleistung – Was passiert, wenn etwas passiert ist.

- Wie konkret muss der Zweck der Datenverarbeitung formuliert werden?
  So konkret, dass ein Externe Ihre Entscheidung für dieses Verfahren nachvollziehen kann.

- Müssen externe Stellen (Steuerberater, Finanzamt, Krankenversicherung, Berufsgenossenschaft, Betriebsversicherung) Berücksichtigung finden, wenn an dieser Stelle ein Datenaustausch erfolgt?
  JA

- Seit April diesen Jahres arbeite ich mit einer neuern Praxisverwaltungssoftware. Vorher wurden die Daten von mir mit Excel verarbeitet und lokal gesichert. Müssen beide „Verarbeitungswege“ in das Verzeichnis der Verarbeitungstätigkeit oder nur der aktuelle?
  Entweder beide oder aber Sie erstellen versionisierte Verzeichnisse

<u>Löschkonzept</u>

- Muss man ein Löschkonzept haben?
  Ja, sonst können Sie den Grundsatz der Transparenz nicht umsetzen.

- Muss das Löschkonzept auf der Internetseite veröffentlicht werden?
  Nein

Verschwiegenheitsverpflichtung

- Muss man einen externen IT-Spezialisten eine Verschwiegenheitsverpflichtungserklärung unterzeichnen lassen?
  Mindestens diese. Wenn er Zugriff hat auf Ihren Datenbestand, dann ein AV-Vertrag.

Notwendige Festlegungen

Passwortregeln

- Benötigen nur Endgeräte einen Passwortschutz oder müssen auch Software, Bereiche einer Software und Dateien geschützt werden?
  Wenn mit dem Passwort auch die Berechtigung gesteuert wird, dann reicht ein zentrales Passwort.

- Braucht jeder Mitarbeiter sein eigenes Passwort für den gleichen Rechner? Oder reicht der Schutz mit einem „Gemeinschafts-Passwort“?
  Die Vergabe von verschiedenen Passwörtern wird angewendet, um ein Funktionstrennung z.B. zwischen Geschäftsführung und Buchhaltung, zwischen Einkauf und Verkauf, zwischen Einkauf und Buchhaltung sicher zu stellen. Entscheidende Begriffe sind: Interessenkonflikt und Datensparsamkeit. Wenn alle Mitarbeiter die gleichen Daten benötigen und kein Interessenkonflikt besteht, dann kann aus Gründen der Wirtschaftlichkeit auf einen unterschiedlichen Account verzichtet werden.

- Dürfen Mitarbeiter auch von Zuhause auf Daten zugreifen? Muss dieser Zugriff geschützt werden?
  Ja, wenn Sie den Zugriff sichern können.

- Dürfen Familienmitglieder Endgeräte und Software nutzen mit dem selben Passwort?
  Wenn Sie angestellt sind, dann unter Beachtung 2 Fragen vorher.

Meldepflichten

- Muss die Meldung innerhalb von 72 durchgeführt werden oder auch zugegangen sein?
  Da es ein Portal für die Meldungen gibt, ist Durchführung und Zugang gleich.

- Was muss bei Verlust von mobilen Endgeräten getan werden?
  Maßnahmen der Widerbeschaffung, Sperrung des illegalen Zugriff, Meldung

- Trifft die DSGVO auch Privatpersonen - muss bei Handyverlust der Kontaktkreis informiert werden?
  Frage zurück: Darf man Privat schlecht mit den Daten anderer umgehen?

Datenschutzfolgeabschätzung (vormals Vorabkontrolle)

- Was bedeutet der Erwägungsgrund Artikel 91?
  Ein Erwägungsgrund ist die Grundlage vor der Entstehung des eigentlichen Artikels. In ihr wird beschrieben, was der zukünftige Artikel hergeben soll. Im Nachgang ist es eine gute Basis um zu verstehen, was die Autoren des Artikels meinen. Der 91 ist exemplarisch dafür.

Löschung

- Wie und mit welchen Angaben muss eine durchgeführte Löschung dokumentiert werden?
  Meine Meinung: Eine Dokumentation einer Löschung ist doof. Die richtige Antwort auf die Frage, ob mein Datenschutz gelöscht worden ist, kann nur sein: Wer sind Sie?

- Gibt es Vorgaben für die Löschung, wenn ein Patient über einen bestimmten Zeitraum nicht mehr in der Praxis war?
  Ja, dies geben die Aufbewahrungsfristen vor.

Kommunikation per E-Mail

- Wie muss eine E-Mail-Archivierung aufgebaut sein?
  So dass sie dem Datenschutz, der Unveränderbarkeit, der Vollständigkeit und der Betroffenenrechte genüge tut.

- Darf man Rechnungen per E-Mail verschicken? Welche Schutzmaßnahmen müssen getroffen werden?
  Angemessen zum Schutzniveau. Nur eine Rechnung ohne sensible Daten oder besonders schützenswerte Daten?

- Muss ich mit meinem Host eine Verschwiegenheitsverpflichtungserklärung abstimmen?
  Mindestens. Wenn er auf Ihre Daten zugreifen kann, dann sogar ein AV-Vertrag.

Datenschutzbeauftragter

- Wann ist ein Datenschutzbeauftragter erforderlich?
  - *Mehr als 9 Personen (Köpfe), die Zugriff auf personenbezogene Daten haben*
  - *Wenn mehrere Personen besonders schützenswerte Daten verarbeiten. Das ist zur Zeit noch in der Klärung, da dies nicht umsetzbar ist.*

- Kann ein Mitarbeiter Datenschutzbeauftragter sein?
  Ja, wenn er keinen Interessenkonflikt hat (kein Entscheider, kein IT-Admin) und die anderen Voraussetzungen vorliegen.

- Weichen die Vorgaben in den einzelnen Bundesländern voneinander ab?
  Bei nichtöffentlichen Stellen -> Nein.

- Muss ich generell einen Datenschutzbeauftragten auf meiner Website benennen?
  Nur wenn Sie auch einen haben.

Datenschutz Online

Internetseite

- Die Domain einer Homepage erlaubt keine verschlüsselte Verbindung (z. B. bei der Nutzung eines Kontaktformulars). Ist es ausreichend, in der Datenschutzerklärung auf die fehlende Verschlüsselung hinzuweisen? Oder ist eine Datenverschlüsselung zwingend erforderlich?
  Nur wenn es das Datenniveau verlangt. Das heißt, wenn es um Namen und Vorname geht, und der Host in Deutschland, gehe ich davon aus, dass es angemessen ist.

- Gehören IP-Adressen zu den personenbezogenen Daten?
  Ja.

- Unterliegt das Impressum der DSGVO? Muss ich im Impressum etwas ändern?
  Nein

- Ist ein Vertrag mit Google verpflichtend, wenn Google benutzt wird?
  Ja. Wenn Google Daten verarbeitet (z.B. Analytics).

- Muss mit Anbietern von Analyse-Tools von Webseiten-Inhalten eine vertragliche Regelung getroffen werden?
  Ja, unbedingt.

- Dürfen Formulare auf der Internetseite zur Verfügung gestellt werden?
  Ja, klar. Am besten als pdf zum Download. So wie diese FAQ Liste.

- Müssen Verweise immer als aktive Links anklickbar sein (z.B. im Impressum) oder ist die reine Textinformation mit Nennung der Adresse auch in Ordnung?
  Das kann zu umständlich sein. Somit fehlt eine angemessene Unterstützung.

- Kann eine Internetseite ohne die Erhebung von personenbezogenen Daten genutzt werden? Besteht dann eine Pflicht zur Vorhaltung einer Datenschutzerklärung?
  Ja, denn der Browser verarbeitet meistens die IP-Adresse.

Datenschutzerklärung

- Was ist der Inhalt und Auftrag einer Datenschutzerklärung?
  Grundlage ist § 13 TMG. Der Besucher Ihrer Website hat das Recht einfach und schnell zu erfahren, welche Daten Sie von ihm verarbeiten und was Sie damit machen.

- Müssen Datenschutzerklärungen von externen Dienstleistern auf der Internetseite veröffentlicht werden?
  Nein

- Die Domain unterstützt die Verschlüsselung. Muss in diesem Fall in der Datenschutzerklärung auf die Verschlüsselung explizit hingewiesen werden?
  Ja.

- Dürfen Datenschutzerklärung und Impressum zusammen ein Button sein?
  Jein. Wenn mir als Besucher schnell und einfach mitgeteilt wird, wie Sie mit dem Datenschutz umgehen, ohne dass ich lange scrolle.

Einbindung externer Inhalte

- Sind Verlinkung, Plug-Ins und Like-Buttons auf Internetseiten datenschutzkonform nutzbar?
  Ja, wenn ich dessen Nutzung in meiner Datenschutzerklärung erläutere.

- Darf man Verlinkungen verwenden?
  Dürfen ja, man trägt aber die Verantwortung.

- Darf man Videos und Bilder externer Anbieter einbinden? Was ist datenschutzrechtlich zu beachten?
  Haben Sie das Recht diese zu veröffentlichen? Dann ja.

Social Media

- Welche Auswirkungen hat die DSGVO auf die Nutzung von Social Media?
  Das besonders hier mit der Würde der Person umgegangen wird.

- Ist bei der Nutzung solcher Plattformen etwas besonders zu beachten?
  Evtl. eigene Datenschutzerklärung. Keine Daten anderer veröffentlichen.

- Können Messenger Dienste wie WhatsApp zur Kommunikation mit Patienten genutzt werden?
  Ich würde mich als Patient abwenden, wenn mein Arzt dies nutzt. Die Daten sind in Amerika und fast ausschließlich frei zugänglich.

Stand 22.05.2018

- Reichen die Datenschutzerklärungen der Social Media Anbieter (z.B. Facebook) aus oder benötigt man eine eigene bei der Nutzung?
  Die sind richtig gut.

Nutzung Online Tools

E-Mails

- Sollte die E-Mail-Signatur einen Link auf die Datenschutzerklärung der Homepage enthalten? Müssen solche Links anklickbar sein?
  Finde ich richtig gut. Wenn Sie dann noch in weiterleiten, dann erst recht.

Doodle

- Ist die Nutzung von Doodle zur Terminkoordination datenschutzkonform möglich?
  Problem bei Doodle: Ich erkenne nicht, wie die mit Datenschutz umgehen.

Teamviewer

- Kann Teamviewer datenschutzkonform genutzt werden?
  Ja, wenn ein AV-Vertrag mit denen abgeschlossen wurde.

Datenschutz im Verhältnis zu Externen

Auftragsverarbeitung (ehemals Auftragsdatenverarbeitung)

Lieferanten

- Mit wem muss man einen AV-Vertrag abschließen (Apotheken, Labore, Finanzdienstleister, Onlineshops)?
  Mit allen, die im Auftrag von Ihnen Daten Ihrer Kunden verarbeiten.

- Kann man das Musterformular zur Auftragsdatenverarbeitung auch als vollständigen Vertrag für die Unternehmen die personenbezogene Daten verarbeiten nutzen oder ist er nur eine Ergänzung?
  Ich würde immer trennen, da die Orientierung eine andere ist.

- Muss zusätzlich zum AV-Vertrag auch eine Verschwiegenheitsverpflichtungserklärung abgeschlossen werden?
  Nein

Steuerberater

- Muss man mit Steuerberatern einen AV-Vertrag abschließen?
  Nein, er ist über die Berufsordnung vergattert.