Fragen und Antworten zur Datenschutz-Grundverordnung (DS-GVO) und Datenschutz in der Arztpraxis

Stand: 03.01.2023

Inhalt

FAQs zum Datenschutz in der Arztpraxis

Wo finde ich Informationen und Hilfestellungen zum Thema Datenschutz in der Arztpraxis?

Basisinformationen zur DSGVO, Muster zur Patienteninformation nach Art. 13 DSGVO und Muster zum Verzeichnis der Verarbeitungstätigkeit finden Sie auf der Homepage der Kassenärztlichen Bundesvereinigung (http://www.kbv.de/html/datensicherheit.php).
Am Ende dieser Seite finden Sie auch Links zu den Hinweisen und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis sowie der technischen Anlage hierzu. Diese wurden im September 2021 neu überarbeitet und aktualisiert.

Auf unserer Homepage finden Sie ein Muster für eine datenschutzrechtliche Einwilligungserklärung, zur Bestellung eines Datenschutzbeauftragten, zur Verpflichtung der Mitarbeiter auf die Einhaltung der Vorgaben der DSGVO und ein Muster für Auskunftsersuchen nach Art. 15 DSGVO. Außerdem stellen wir Ihnen dort eine Hilfestellung zur Erfüllung der so genannten Rechenschaftspflicht zur Verfügung (https://www.kvb.de/praxis/praxisfuehrung/datenschutz/).

Weitere Informationen finden Sie auf der Homepage der Bayerischen Landesärztekammer, Informationen für Ärzte zum Datenschutz 2018 (EU-DSGVO) | Bayerische Landesärztekammer, in der Rubrik Arzt und Recht.

Mit welchen Maßnahmen sollte bei der Umsetzung der DSGVO begonnen werden?

Nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA) sollte bei der Umsetzung der DSGVO mit folgenden Maßnahmen begonnen werden:

- Erstellung des Verzeichnisses der Verarbeitungstätigkeit (Muster s. o.)
- Überprüfung vorhandener Einwilligungserklärungen im Hinblick auf die Bedingungen nach Art. 7 DSGVO (Einsichtsfähigkeit, freiwillig, informiert, nachweisbar, unmissverständlich, widerruflich)
- Umsetzungen der Informationspflichten nach Art.13 DSGVO (Muster s. o.)
- Datenschutzverpflichtung von Beschäftigten (Muster s. o.)
- Verfahren für Datenpannenmeldungen (Formular unter www.lda.bayern.de; Meldefrist grundsätzlich 72 Stunden)
- Verfahren für Betroffenenrechte (insbes. Auskunft und Löschen)

- Kontrolle von Verträgen zur Auftragsverarbeitung (Verträge vorhanden? Genügen diese den Anforderungen des § 28 DSGVO?)

Darüber hinaus sollten Sie ein Dokument zur Erfüllung der Rechenschaftspflicht erstellen (s. nachstehende Frage).

Was versteht man unter Rechenschaftspflicht und wie kann diese erfüllt werden?

Unter der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) versteht man den Nachweis des Verantwortlichen (der Arztpraxis), dass die Grundsätze zur Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DSGVO eingehalten werden. Dieser Nachweis muss in der Arztpraxis vorliegen.
Auf unserer Homepage haben wir Ihnen hierzu ein Dokument bereitgestellt, aus dem hervorgeht, welche Inhalte der Nachweis haben sollte.

Übermittlung von Patientendaten

Wann ist für die Übermittlung von Patientendaten eine Einwilligungserklärung (Schweigepflichtentbindungserklärung) erforderlich?

Eine Einwilligungserklärung ist immer dann erforderlich, wenn keine gesetzliche Übermittlungsverpflichtung oder -befugnis besteht. Sofern ein Fall der Mit-/Weiterbehandlung vorliegt (Überweisungsschein), sind die beteiligten Ärzte nach § 9 Abs. 4 der Berufsordnung Ärzte Bayerns von der ärztlichen Schweigepflicht befreit, soweit das Einverständnis des Patienten vorliegt oder anzunehmen ist. Dies gilt auch für Laborüberweisungen oder z. B. für die Auswertung eines Langzeit-EKG´s durch einen anderen Arzt. In diesen Fällen muss der Patient aber ausdrücklich über die Datenübermittlung informiert werden, vgl. KVB-FORUM, 4/2018, Seite 13 Mitte.
https://www.kvb.de/fileadmin/kvb/dokumente/Presse/Publikation/KVB-FORUM/Einzeldateien-FORUM/2018/KVB-FORUM-4-2018.pdf

§ 73 Abs. 1b SGB V regelt die Datenweitergabe der Leistungserbringer untereinander. Der Gesetzgeber geht dabei davon aus, dass die für die Behandlung eines Patienten erforderliche Verarbeitung von Behandlungsdaten auch durch mehrere an der Behandlung beteiligte Ärzte auf der Grundlage des § 22 Abs. 1 Nr. 1 Buchst. b BDSG grundsätzlich

ohne eine datenschutzrechtliche Einwilligung der Patienten erfolgen kann. Das in § 73 Abs. 1b SGB V geregelte Zustimmungserfordernis ergibt sich nicht aus datenschutzrechtlichen Vorgaben, sondern ist Ausdruck der Souveränität der Versicherten, sich entgegen der vom Gesetzgeber vorgegebenen Regelung dennoch für oder gegen eine Mitteilung von Behandlungsdaten im Rahmen der koordinierenden hausärztlichen Betreuung zu entscheiden (BeckOK SozR/Warner, SGB V, § 73 Rn. 16).

Äußert sich der Patient nicht, sind die Fachärzte grundsätzlich verpflichtet, die den Versicherten betreffenden Behandlungsdaten und Befunde zum Zwecke der bei dem Hausarzt durchzuführenden Dokumentation und der weiteren Behandlung zu übermitteln. Der Hausarzt wiederum ist grundsätzlich verpflichtet, die für die Behandlung erforderlichen Daten und Befunde an die den Versicherten behandelnden Leistungserbringer zu übermitteln (§ 73 Abs. 1b S. 2 SGB V).

Wo finde ich Informationen zur Übermittlung von Patientendaten aufgrund gesetzlicher Bestimmungen?

Personenbezogene Daten dürfen nur übermittelt werden, wenn eine Rechtsgrundlage die Datenübermittlung erlaubt oder der Patient in die Datenübermittlung eingewilligt hat (sog. Verbot mit Erlaubnisvorbehalt). Es gibt zahlreiche Rechtsgrundlagen in den unterschiedlichsten Gesetzen aufgrund derer Ärzte bzw. Psychotherapeuten Patientendaten an Dritte übermitteln dürfen bzw. müssen. Um nur einige beispielhaft zu nennen:

- Übermittlung nach dem Infektionsschutzgesetz an Gesundheitsämter:
  namentliche Meldung nach § 9 IfSG
- Übermittlung von Abrechnungsdaten an die Kassenärztliche Vereinigung:
  § 295 SGB V
- Übermittlung von Behandlungsdaten an den MDK:
  § 276 Abs. 2 S. 2 SGB V

Ausführlichere Informationen finden Sie im Handbuch Datenschutz in der Arzt-/Psychotherapeutenpraxis der KV Bayerns in Kapitel 4 „Übermittlung von Patientendaten aufgrund gesetzlicher Bestimmungen“.

Dürfen Anfragen des Versorgungsamtes und von Gerichten auch ohne Vorlage der Einwilligungserklärung des Patienten beantwortet werden?

Diese Fragen beantworten wir nach erfolgter Abstimmung mit dem Bayerischen Landesamt für Datenschutzaufsicht (am 30.01.19) wie folgt:

Versorgungsamt (Zentrum Bayern Familie und Soziales)
„Das Zentrum Bayern Familie und Soziales (ZBFS) informiert in Absprache mit dem Bayerischen Landesamt für Datenschutz, dass es genügt und der Arzt nicht gegen seine Schweigepflicht verstößt, wenn der Patient dem ZBFS gegenüber einwilligt, dass es bei den von ihm benannten Ärzten Befundberichte einholen darf und das ZBFS dem Arzt das Vorliegen dieser Einwilligungserklärung bestätigt. Auf Anforderung stellt das ZBFS dem Arzt die Einwilligungserklärung selbstverständlich ohne Weiteres zur Verfügung“ (Bayerisches Ärzteblatt 10/2018, S. 511).

Gerichte
Zur Beantwortung von Anfragen von Gerichten ist die Versicherung des Gerichts, dass für die gewünschte Auskunftserteilung eine entsprechende Einwilligungserklärung des Patienten vorliegt, ausreichend. Der Arzt hat keinen Anspruch auf die Vorlage der Schweigepflichtentbindungserklärung (s. a. https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 16.4).

Andere öffentliche Stellen
Für die Auskunftserteilung an andere öffentliche Stellen (Krankenkassen, Rentenversicherung, Behörden) ist bis auf weiteres die Vorlage entsprechender Einwilligungserklärungen erforderlich, es sei denn, es liegt eine gesetzliche Übermittlungsbefugnis vor.

Dürfen Rezepte Angehörigen ausgehändigt oder direkt an Apotheken übermittelt werden?

In beiden Fällen bedarf es hierzu einer Einwilligung des Patienten, die nachweisbar sein muss. In der Einwilligung sollten die zur Abholung berechtigten Angehörigen bzw. die empfangsberechtigte(n) Apotheke(n) konkret benannt werden (s. a. https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 16.5).

Dürfen Ärzte Rezepte in Rezeptsammelstellen sammeln?

Mit **Rezeptsammelstelle** bezeichnet das deutsche Apothekerrecht einen speziellen Briefkasten in Orten ohne eigene Apotheke, in den Kunden Rezepte einwerfen können, um diese von der Apotheke geliefert zu bekommen. In Arztpraxen dürfen solche Rezeptsammelstellen nicht eingerichtet werden (§ 24 Abs. 2 Apothekenbetriebsordnung).

Dürfen Rezepte an Altenheime ausgehändigt werden?

Auch hier gilt, dass die Rezepte Mitarbeitern des Altenheimes nur mit Einwilligung des Patienten ausgehändigt werden dürfen (siehe dazu auch die Veröffentlichung des Ärztlichen Kreisverbandes Ebersberg: https://www.aekv-ebersberg.de/aktuelles/162-versorgung-von-heimpatienten-rechtliche-fallstricke-und-empfehlungen.html). Soweit die Abholung durch Personal des Altenheims erfolgt, sollten die Rezepte insgesamt in einem verschlossenen, an das Altenheim adressierten Umschlag, übergeben werden. Das Altenheim ist dann dafür verantwortlich, dass dieser Umschlag nur von berechtigten Mitarbeitern geöffnet wird.

Soweit keine Patienteneinwilligung vorliegt, kann unter Berücksichtigung des Briefgeheimnisses das Rezept in einem an den Patienten adressierten Umschlag an Mitarbeiter des Altenheimes übergeben werden. In diesem Fall muss das Altenheim in eigener Verantwortung prüfen, ob es zur Öffnung des Briefumschlages berechtigt ist.

Dürfen Anfragen von Apotheken zu ausgestellten Rezepten beantwortet werden?

Nachfragen von Apotheken zu von der Arztpraxis ausgestellten Rezepten dürfen auch weiterhin beantwortet werden. Nähere Informationen hierzu finden Sie auf Seite 145 der KVB INFOS 10/2018.
https://www.kvb.de/fileadmin/kvb/dokumente/Presse/Publikation/KVB-FORUM/Einzeldateien-INFOS/2018/KVB-INFOS-10-2018.pdf

Dürfen Patientendaten per Fax übermittelt werden?

Der Faxversand wird vom Hessischen Landesdatenschutzbeauftragten aufgrund diverser technischer Veränderungen informationstechnisch als unsicheres Kommunikationsmittel eingestuft. Technologische Weiterentwicklungen haben dazu geführt, dass seit einiger Zeit die sog. Paketvermittlung als Grundlage der Datenübertragung beim Fax zum Einsatz kommt. Dabei werden die zu übertragenden Daten mittels des TCP/IP-Standards auf „Pakete“ aufgeteilt und über eine Vielzahl von Verbindungen zwischen mehreren vermittelnden Punkten zu den Endstellen übertragen. Die beteiligten Zwischenpunkte sind weltweit verteilt und werden von verschiedensten staatlichen oder privaten Akteuren betrieben. Diese haben die Möglichkeit auf die Pakete Zugriff zu nehmen. Personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, sollten daher grundsätzlich nicht per Fax übertragen werden, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-%C3%BCbermittlung-personenbezogener-daten-per-fax).

Der Hessische Landesbeauftragte für den Datenschutz empfiehlt Verantwortlichen daher zeitnah alternative Kommunikationsmittel zum Fax zu implementieren. In Betracht kommen insbesondere:

- Versand inhaltsverschlüsselter E-Mail-Nachrichten (PGP oder S/MIME)
- Portallösungen, bei denen die Kommunikationspartner Nachrichten und Inhalte verschlüsselt abrufen und bereitstellen können
- bereichsspezifischer digitaler Kommunikationsdienst:

  KIM
  KIM steht für Kommunikation im Medizinwesen und ist der einheitliche Standard für die elektronische Übermittlung medizinischer Dokumente. Durch diesen Kommunikationsdienst können Nachrichten und Dokumente (Arztbriefe, Befunde etc.) über die Telematik-Infrastruktur per Ende-zu-Ende verschlüsselter E-Mail-Nachricht übermittelt werden. Beim Abruf werden die Nachrichten automatisch für die Empfängerinnen und Empfänger entschlüsselt. So können auch sensible Gesundheitsdaten datenschutzkonform übermittelt werden. KIM wird von der Gesellschaft für Telematik aufgrund eines gesetzlichen Auftrags im SGB V betrieben. Über ein zentrales Adressbuch können die verschiedenen Akteure im Gesundheitswesen (Arztpraxen, Krankenhäuser, Apotheken, Kassenärztliche Vereinigungen, Krankenkassen) sicher erreicht werden.

Dürfen Patienten noch mit Namen aufgerufen werden?

Das Bayerische Landesamt für Datenschutzaufsicht bestätigt, dass Patienten auch nach dem Inkrafttreten der DSGVO noch mit Namen aufgerufen werden dürfen (s. a. https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 16.3).

Die Dokumentation der Ärzte/Psychotherapeuten („Patientenakte“)

Muss eine Einwilligungserklärung im Original aufbewahrt werden?

Nach Art. 7 Abs. 1 DSGVO muss eine Einwilligung nachweisbar sein. Die Schriftform ist hierfür nicht mehr vorgeschrieben, aber aus Gründen der Nachweisbarkeit zu empfehlen. Als Nachweis im datenschutzrechtlichen Sinne ist ein „Scan“ der Einwilligung ausreichend. Ggf. kann zur Dokumentation der Einwilligung auch ein Tablet verwendet werden.

Die Einwilligungen müssen nicht zwingend im Original aufbewahrt werden (https://www.lda.bayern.de/de/faq.html).

Wann müssen Patientendaten gelöscht werden?

Art. 17 Abs. 1 lit. a) DSGVO definiert auch für Patienten das „Recht auf Vergessenwerden". Personenbezogene Daten sind unverzüglich zu löschen, sofern diese für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Dennoch darf die Patientendokumentation nicht sofort nach Behandlungsende vernichtet werden.

Die Patientendokumentation muss aufbewahrt werden, wenn dies zur Erfüllung einer rechtlichen Pflicht erforderlich ist (Art. 17 Abs. 3 lit. b) DSGVO) oder einer Löschung satzungsgemäße oder vertragliche Aufbewahrungsfristen entgegenstehen (§ 35 Abs. 3 BDSG).

Aus § 630f Abs. 3 BGB bzw. § 10 Abs. 3 der Berufsordnung für die Ärzte Bayerns ergibt sich die Pflicht zur Aufbewahrung der Patientendokumentation grundsätzlich für einen Zeitraum von zehn Jahren nach Abschluss der Behandlung. Die zehnjährige Aufbewahrungsfrist beginnt erst mit der letzten Behandlung zu laufen. Ist die Zehnjahresfrist erfüllt, sollte der Verantwortliche prüfen, ob die Unterlagen vernichtet werden können. Grundsätzlich muss der Praxisinhaber die Daten – auch ohne, dass der Patient dies verlangt – nach Ablauf dieser Fristen löschen. Allerdings gibt es für bestimmte Patientenunterlagen längere Fristen. So sind z.B. Aufzeichnungen über ein Durchgangsarztverfahren 15 Jahre aufzubewahren.

Darüber hinaus dürfen die Patientenakten länger aufbewahrt werden, wenn Gründe für die Annahme vorhanden sind, dass einer Löschung berechtigte Interessen des Patienten entgegenstehen (§ 35 Abs. 2 BDSG) oder die Unterlagen zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Stichwort: Vorwurf Behandlungsfehler) erforderlich sind (Art. 17 Abs. 3 lit e) DSGVO).
https://www.lda.bayern.de/media/FAQ_Loeschen_von_Patientendaten.pdf und
https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 7.4.2, Punkt 9.2

Dürfen Patientenakten im Original an den Patienten herausgegeben werden?

Solange die berufsrechtliche Aufbewahrungsfrist nicht abgelaufen ist, darf keine Aushändigung der Originalakte an den Patienten erfolgen. Bei einem Hausarztwechsel ist die Weitergabe der Originalunterlagen an den neuen Hausarzt jedoch möglich (§ 73 Abs. 1b S. 4 SGB V).

Siehe dazu auch: https://www.datenschutzzentrum.de/artikel/42-Hat-ein-Patient-bei-einem-Arztwechsel-einen-Anspruch-auf-Heraus-oder-Weitergabe-der-Patientendokumentation.html#extended.

Der betriebliche Datenschutzbeauftragte

Wann muss eine Arztpraxis einen Datenschutzbeauftragten benennen?

Die Pflicht einen Datenschutzbeauftragten zu benennen kann sich für eine Arztpraxis aus verschiedenen Gründen bzw. Normen ergeben:

1. **In der Regel sind mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt**

Jede Arztpraxis, in der mindestens 20 Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten befasst sind, muss einen betrieblichen Datenschutzbeauftragten benennen. Die Inhaber der Arztpraxis und Auszubildende sind dabei zu berücksichtigen.

Was versteht man unter dem Begriff „ständig“ im Sinne des § 38 Abs. 1 BDSG?
Das BayLDA definiert den Begriff „ständig“ wie folgt:

„Wir vertreten dazu die Auffassung, dass das Merkmal „ständig“ zwar nicht bedeutet, dass eine Person während ihrer gesamten Arbeitszeit mit der automatisierten Verarbeitung personenbezogener Daten befasst ist. Ausreichend ist, dass dies ein Schwerpunkt der Tätigkeit der Person ist.
Wenn Ärzte oder Mitarbeitende in einer Arztpraxis zur Terminkalender- und Patientendatenverwaltung, für Behandlungszwecke, zur Erfüllung von Dokumentationspflichten und zu Zwecken der Abrechnung im Schwerpunkt Patientendaten automatisiert verarbeiten, sind diese also mitzuzählen.
Nicht ständig mit der automatisierten Verarbeitung befasst wäre dagegen in einer Zahnarztpraxis der Zahntechniker, wenn er in erster Linie handwerkliche Aufgaben erledigt, die Beschäftigten, die ausschließlich Zahnreinigungen durchführen oder Physiotherapeuten, wenn sie nur im automatisierten Kalender nachsehen, wer ihr nächster Patient ist.“

(Fundstelle: https://www.lda.bayern.de/media/FAQ_DSB_im_medizinischen_Bereich.pdf und https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 5.1; Aufgaben des DSB: Punkt 5.2.

Uns ist bewusst, dass auch mit diesen Hinweisen in der Praxis nicht immer zweifelsfrei festgestellt werden kann, ob ein Mitarbeiter/eine Mitarbeiterin bei der Prüfung der Bestellpflicht eines Datenschutzbeauftragten zu berücksichtigen ist. Bitte wenden Sie sich

in Zweifelsfällen unmittelbar an das BayLDA (Tel. 0981/53 1300, Mail: poststelle@lda.bayern.de).

In besonderen Fällen können Praxen auch bei einer Unterschreitung der o.g. Personenzahl zur Benennung eines Datenschutzbeauftragten verpflichtet sein (vgl. https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/95DSK_DSB_Bestellpflicht2.html;jsessionid=9E9DB820369F4C78F775942C6F86BB85.2_cid354?nn=5217016).

2. **Datenschutz-Folgenabschätzung**

Erfolgt in einer Arztpraxis eine Datenverarbeitung, die eine Datenschutz-Folgenabschätzung erfordert, dann ist ebenfalls ein Datenschutzbeauftragter zu benennen (§ 38 Abs. 1 S. 2 BDSG).
Wenn ein Praxisinhaber eine **Videosprechstunde** anbietet, muss dieser keine Datenschutz-Folgenabschätzung durchführen und damit nicht aufgrund des Einsatzes einer Videosprechstunde einen Datenschutzbeauftragten bestellen (Beratungsanfrage beim BayLDA; Stand: Dezember 2019). Begründet wird dies damit, dass eine ausreichende Risikoeindämmung beim Einsatz einer Videosprechstunde durch geeignete technische und organisatorische Maßnahmen erbracht werden kann. Eine individuelle Risikobeurteilung und Risikoeindämmung, die den Kern einer Datenschutz-Folgenabschätzung darstellt, wäre demnach nicht erforderlich.

Wann ist bei gemeinschaftlicher Berufsausübung ein Datenschutzbeauftragter zu benennen?

Praxisgemeinschaften bestehen aus rechtlich selbständigen Praxen. Jede Mitgliedspraxis muss für sich prüfen, ob sie einen Datenschutzbeauftragten benennen muss.
Überörtliche Berufsausübungsgemeinschaften sind rechtlich eine einheitliche Praxis d. h. diese müssen bei Erfüllung der o. g. Voraussetzungen einheitlich einen betrieblichen Datenschutzbeauftragten benennen.

Muss ein Datenschutzbeauftragter der Aufsichtsbehörde gemeldet werden bzw. müssen dessen Kontaktdaten veröffentlicht werden?

Soweit ein Datenschutzbeauftragter benannt werden muss, muss dieser der Datenschutzaufsichtsbehörde (www.lda.bayern.de) gemeldet werden (Online-Formular auf der Homepage). Außerdem müssen dessen Kontaktdaten veröffentlicht werden.

Ein Mitarbeiter unserer Praxis soll die Aufgabe des Datenschutzbeauftragten übernehmen. Benötigt er eine besondere Aus- oder Fortbildung?

Nach den gesetzlichen Vorgaben muss der Datenschutzbeauftragte die nötige Fachkunde und Zuverlässigkeit haben. Dies bedeutet, dass er die gesetzlichen Regelungen kennen und sicher anwenden muss. Eine rechtliche Vorgabe, wie sich Ihr Mitarbeiter das nötige Wissen aneignet, gibt es nicht.
Das BayLDA fordert seit Ende Juni 2018 für neue Datenschutzbeauftragte **nicht mehr** den Besuch eines mindestens zweitägigen Intensivseminars zum Erwerb der erforderlichen Kenntnisse.

Was unterscheidet interne und externe Datenschutzbeauftragte?

Wird ein Mitarbeiter der Arztpraxis mit der Aufgabe des Datenschutzbeauftragten betraut, spricht man von einem internen Datenschutzbeauftragten. Dem Mitarbeiter darf ab dem Zeitpunkt der Benennung nur noch außerordentlich gekündigt werden und er hat das Recht auf eine eigene Ausstattung und Fortbildung.

Praxisinhaber können aber auch einen externen Dienstleister beauftragen. Es handelt sich also – anders als bei einem internen Datenschutzbeauftragten – nicht um einen Mitarbeiter der Arztpraxis. Es besteht jedoch keine gesetzliche Verpflichtung zur Bestellung eines externen Datenschutzbeauftragten.
Bei dieser Variante fallen zusätzliche Kosten an. Welche Variante gewählt wird, muss der Praxisinhaber entscheiden.

Benötigen Gemeinschaftspraxen wie Einzelpraxen ab 20 Personen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten?

Ja, denn Gemeinschaftspraxen (Berufsausübungsgemeinschaften – BAG) bilden eine einheitliche Rechtspersönlichkeit. Deshalb sind auch datenschutzrechtlich dieselben Vorgaben zu beachten.

Ab 20 Personen, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, muss ein Datenschutzbeauftragter bestellt werden:
Müssen es Vollzeitstellen sein oder geht es um die Anzahl der Personen?

Entscheidend ist die Anzahl der Personen, die in der Praxis tätig sind. Somit ist unerheblich, ob die Personen in Voll- oder Teilzeit oder als Auszubildende beschäftigt sind.

Aufsichtsbehörde für den Datenschutz

Wer ist im Hinblick auf die freiberuflich Tätigen die zuständige (Datenschutz-) Aufsichtsbehörde?

Die zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich, das heißt u.a. für die freiberuflich Tätigen ist dies das Bayerische Landesamt für Datenschutzaufsicht, Promenade 18, 91522 Ansbach (www.lda.bayern.de).

Datenschutzverletzungen

Was ist eine Verletzung des Schutzes personenbezogener Daten (sog. Datenpanne) und was ist ggf. zu tun?

Der Begriff der „Verletzung des Schutzes personenbezogener Daten“ ist in Art. 4 Nr. 12 DSGVO definiert und ist grundsätzlich weit auszulegen. Hiernach versteht man unter einer „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
Der Praxisinhaber hat jede Verletzung (z. B. Diebstahl, Fehlentsorgung/-versendung, Hackerangriffe, Schadcode, Softwarefehler, Verlust, Vernichtung) bei der Aufsichtsbehörde zu melden, die ein Risiko für die Rechte und Freiheiten des Patienten darstellen. Die Meldepflicht wird aber erst dadurch ausgelöst, dass der Arztpraxis (bei der die Verletzung stattgefunden hat, d. h. z. B. die den Fehlversand verursacht hat) diese Verletzung auch bekannt wird (was die Arztpraxis nicht weiß kann sie auch nicht melden). Ein Verstoß gegen die Meldepflicht kann ein Bußgeld zur Folge haben. Bitte beachten Sie auch, dass nach Art. 33 Abs. 5 DSGVO jede „Verletzung“ dokumentiert werden muss. Zum Umfang der Dokumentation können Sie sich am Meldeformular des Bayer. Landesamtes für Datenschutzaufsicht (www.lda.bayern.de) orientieren (Datenschutzverletzung

durch Ransomware (Verschlüsselung der Festplatte durch Dritte): https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkte 4.9 und 21.8).

Welche Frist ist bei der Meldung der Datenschutzverletzung einzuhalten?

Der Praxisinhaber muss die Datenschutzverletzung unverzüglich und möglichst binnen 72 Stunden nach Kenntnisnahme an die Datenschutzaufsichtsbehörde melden (Art. 33 Abs. 1 S. 1 DSGVO).

Muss ich ein Verzeichnis von Verarbeitungstätigkeiten nur einmal erstellen oder in regelmäßigen Abständen?

Sie sollten Ihr Verzeichnis der Verarbeitungstätigkeit immer auf dem aktuellen Stand halten und hin und wieder prüfen, ob es angepasst werden muss. Treten Sie zum Beispiel einem neuen Versorgungsvertrag bei, bei dem Daten von Patienten erhoben, gespeichert oder an Dritte weitergeleitet werden, prüfen Sie, ob Sie Ihr Verzeichnis um diese Tätigkeit ergänzen müssen. So sind Sie immer auf der sicheren Seite, falls die Datenschutzbehörde sich Ihr Verzeichnis vorlegen lässt.

Ein Muster für ein bereits ausgefülltes Verarbeitungsverzeichnis finden Sie hier: https://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Verarbeitungsverzeichnis_Ausfuellbeispiel.pdf

Auftragsverarbeitung - Datenverarbeitung im Auftrag durch externe Dritte

Ist die KVB Auftragsverarbeiter für Ärzte?

Soweit Sie Patientendaten an Dritte (also auch die KVB) aufgrund von Rechtsvorschriften zur Aufgabenerfüllung des Dritten übermitteln, liegt kein Fall der Auftragsverarbeitung vor. Eine Auftragsverarbeitung setzt vielmehr voraus, dass der Auftragsverarbeiter für den Arzt/die Arztpraxis Dienstleistungen erbringt, die diese bei der Erfüllung ihrer Aufgaben unterstützen. Typische Fälle einer Auftragsverarbeitung sind z. B. die Wartung und Pflege Ihres PVS-Systems durch einen Dienstleister oder die Löschung (= Vernichtung) von Patientenakten durch eine Fremdfirma.

Ist eine Laborpraxis ein Auftragsverarbeiter?

Eine Laborpraxis erbringt eine eigene Leistung und ist selbst Verantwortlicher für seine Datenverarbeitung und damit kein Auftragsverarbeiter (siehe dazu auch: „Ist ein Steuerberater ein Auftragsverarbeiter?“ und „Wann ist für die Übermittlung von Patientendaten eine Einwilligungserklärung (Schweigepflichtentbindungserklärung) erforderlich?“).
s. a. https://www.lda.bayern.de/media/FAQ_Auftragsverarbeitung_Arzt.pdf

Ist ein Steuerberater ein Auftragsverarbeiter?

Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DSGVO gegeben sein muss, sind beispielsweise die Einbeziehung eines

- Berufsgeheimnisträgers (Steuerberater, Rechtsanwälte, externe Betriebsärzte, Wirtschaftsprüfer),
- Inkassobüros mit Forderungsübertragung,
- Bankinstituts für den Geldtransfer,
- Postdienstes für den Brieftransport,

und vieles mehr.
https://www.lda.bayern.de/media/FAQ_Steuerberater_keine_ADV.pdf
https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf
https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 9.1

Ist das „Hosten“ einer Website Auftragsverarbeitung?

Die meisten Websites werden auf Web-Servern externer Anbieter (Website-Hoster) gehostet. Zu den Service-Leistungen eines Website-Hosters **kann** das Entgegennehmen und Archivieren von E-Mails der Kunden (Patienten) oder Interessenten oder von Kontaktformulareintragungen auf der Website, das Tracking des Verhaltens der Website-Nutzer usw. gehören. Betreffen die Leistungen des Website-Hosters (auch) den Umgang mit personenbezogenen Daten des Unternehmens, so ist dies eine Auftragsverarbeitung nach Art. 28 DSGVO.

Die Tätigkeit sog. Access-Provider, d. h. Anbieter, die bloße Internet-Zugangsdienste (Zugangsvermittlung, Datentransportleistung, Website Hosting ohne weitere Leistungen mit personenbezogenen Daten) anbieten, sind dagegen keine Auftragsverarbeiter.

Einige Website-Hoster informieren auf ihrer Homepage zu dieser Thematik und bieten auch Vereinbarungen zur Auftragsverarbeitung an. Soweit solche Informationen nicht verfügbar sein sollten, empfiehlt es sich mit dem Website-Hoster Kontakt aufzunehmen.

Ist die Verwahrung von Patientenakten bei einer Praxisübernahme eine Auftragsverarbeitung?

Im Rahmen von Praxisübernahmen übergibt der Praxisabgeber i. d. R. seine Patientenakten dem Praxisübernehmer in gehörige Obhut (§ 10 Abs. 4 der Berufsordnung für die Ärzte Bayerns). Die Verwahrung der Patientenakten durch den Praxisübernehmer stellt - nach Abstimmung mit dem Bayerischen Landesamt für Datenschutzaufsicht - keine Auftragsverarbeitung dar. Es ist daher ausreichend, diesen Sachverhalt im Praxisübernahmevertrag zu regeln.

Was versteht man unter dem sog. Zwei – Schrank – Modell?

Gibt ein Arzt seine Praxis ab, so stellt sich die Frage, ob und unter welchen Voraussetzungen die vorhandenen Patientenakten vom Nachfolger übernommen werden dürfen.

Der Arzt, dem bei einer Praxisübergabe ärztliche Aufzeichnungen über Patienten in Obhut gegeben werden, muss diese Aufzeichnungen unter Verschluss halten und darf sie nur mit Einwilligung des Patienten einsehen oder weitergeben.

Ein gängiges Modell zur Übergabe stellt danach das sog. Zwei-Schrank-Modell dar. Bei einer im Zeitpunkt der Praxisveräußerung noch nicht vorliegenden Einwilligung der Patienten in eine Weitergabe ihrer Daten kann für eine Übergangszeit, bis die Einwilligung abgegeben wurde, nach der sog. „Zwei-Schrank“-Methode verfahren werden. Im Rahmen der Übergabe einer Arztpraxis an den Nachfolger hat sich in Bezug auf die Patientendokumentation aus datenschutzrechtlicher Sicht das sogenannte „Zwei-Schrank-Modell“ bewährt. Dies bedeutet, dass die Patientenakten in einem Schrank übergeben werden, für den der Praxisnachfolger zwar einen Schlüssel besitzt, sich aber gleichzeitig vertraglich dazu verpflichtet, auf eine Patientenakte aus diesem Schrank nur dann Zugriff zu nehmen, wenn er die Einwilligung des Patienten hat.

Sobald die Einwilligung vorliegt, kann die Patientenakte in den zweiten Schrank mit den „Altbestands“-Patientenakten übernommen werden und steht ab dann für den normalen Praxisbetrieb zur Verfügung. Bei digital geführten Patientenakten sind die Datensätze zu sperren und mit einem Kennwort zu schützen.

Weitere Informationen zum Zwei-Schrank-Modell finden Sie auf den Seiten der Aufsichtsbehörde in Schleswig-Holstein: Hinweise zur datenschutzgerechten Übergabe einer Arztpraxis mit Patientenakten und zum Wechsel von Betriebsärzten - ULD (datenschutzzentrum.de).

Wir planen einen Terminerinnerungsservice per sms, was ist dabei zu beachten?

Antwort BayLDA:
Sofern dafür externe Dienstleister eingesetzt werden, ist in der Regel ein Vertrag zur Auftragsverarbeitung nötig. Die Erinnerung als solche sollte nur mit Einwilligung des Patienten erfolgen.

Wie wirkt sich die Neufassung des § 203 StGB auf Verträge zur Auftragsverarbeitung aus?

§ 203 StGB regelt Verstöße gegen das Berufsgeheimnis. Durch eine Gesetzesänderung des § 203 Abs. 3 und 4 StGB wurde der Weg für eine straffreie Auslagerung bestimmter Tätigkeiten auf externe Anbieter auch für Berufsgeheimnisträger geebnet.
Der neue Absatz 3 stellt klar, dass bei Einbeziehung bestimmter Dienstleister keine unbefugte Offenbarung erfolgt. Notwendig ist dafür, dass die mitwirkende Person in die berufliche Tätigkeit der schweigepflichtigen Person einbezogen ist. Unter diesen Personenkreis fallen insbesondere Personen, die mit der Wartung und Pflege Ihres PV-Systems betraut sind. Die Einbeziehung sonstiger mitwirkender Personen muss außerdem im Einvernehmen mit der schweigepflichtigen Person erfolgen. Unter diesen Voraussetzungen liegt selbst ohne ausdrückliche Entbindung kein Verstoß gegen die Schweigepflicht vor. (Details siehe Gesetzesbegründung: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Neuregelung_Schutzes_von_Geheimnissen_bei_Mitwirkung_Dritter_an_der_Berufsausuebung_schweigepflichtiger_Personen.pdf?__blob=publicationFile&v=1).

Nach § 203 Abs. 4 Nr. 1 StGB ist es erforderlich, dass der Personenkreis der sonstigen mitwirkenden Personen ausdrücklich zur Geheimhaltung verpflichtet wird. Kommt der Berufsgeheimnisträger dieser Verpflichtung zur Geheimhaltung nicht nach, dann macht er sich strafbar. Eine Hilfestellung finden Sie hier: https://www.bitkom.org/Bitkom/Publikationen/Muster-zur-Umsetzung-des-Gesetzes-zur-Neuregelung-des-Schutzes-von-Geheimnissen-bei-der-Mitwirkung-Dritter-an-der-Berufsausuebung-schweigepflichtiger-Personen.html.

Patienteninformation zum Datenschutz

Wie müssen die Patienten über die Datenverarbeitung in der Arztpraxis informiert werden?

Ein Muster zur Patienteninformation (Art. 13 DSGVO) stellt die KBV zur Verfügung (http://www.kbv.de/html/datensicherheit.php), das unter Punkt 1 und 5 noch vom Praxisinhaber ausgefüllt werden muss. Bei Punkt 5 muss die für Arztpraxen zuständige Aufsichtsbehörde eingetragen werden:

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)
Hausanschrift:
Promenade 18
91522 Ansbach
Deutschland
Erreichbarkeit:
Telefon +49 (0) 981 180093–150
Telefax +49 (0) 981 180093–850
E-Mail: poststelle@lda.bayern.de
Internet: www.lda.bayern.de
Das BayLDA überwacht die Einhaltung des Datenschutzrechts im nicht-öffentlichen Bereich in Bayern, das heißt, u.a. bei den freiberuflich Tätigen.

Zur Erfüllung der Informationspflichten gegenüber den Patienten genügt für Patienten, die die Arztpraxis aufsuchen, der Aushang in der Praxis. Der Praxisinhaber sollte den Patienten die Informationen auf Wunsch auch schriftlich zur Verfügung stellen. Eine unterschriftliche Kenntnisnahme ist nicht erforderlich **(siehe dazu auch: https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_aerzte.pdf).**

Diese Informationspflichten bestehen auch gegenüber Patienten, die die Arztpraxis nicht aufsuchen (z. B. Pflegeheimbewohner, Patientenbehandlung im ärztlichen Bereitschaftsdienst oder Notarztdienst).

Wann ist eine Patienteninformation über die Datenverarbeitung in der Arztpraxis erforderlich?

Eine Information ist immer dann erforderlich, wenn personenbezogene Daten über den Patienten von der Arztpraxis beim Patienten selbst oder über den Patienten erhoben werden. Die Informationspflicht wird grundsätzlich durch den Aushang der Patientenin-

formation in der Arztpraxis erfüllt. Auf Wunsch ist die Information dem Patienten schriftlich auszuhändigen. Erfolgt die Datenerhebung im Rahmen des ärztlichen Bereitschaftsdienstes oder des Notarztdienstes, muss die Information am Einsatzort erfolgen.
Auslöser der Informationspflicht ist das Erheben von Daten. Soweit die Arztpraxis sich also nicht selbst Patientendaten beschafft (alle Fachgebiete, die Leistungen ohne Arzt-/Patientenkontakt erbringen, z. B. Laborärzte, Pathologen), liegt keine Datenerhebung vor. Damit besteht auch keine Verpflichtung zur Information der Patienten nach Art. 13, 14 DSGVO.
Zur Informationspflicht bei eingehenden Telefonaten und bei Ärzten: https://www.lda.bayern.de/media/FAQ_InformationspflichtenTelefon.pdf sowie https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkte 7.1.4 und 7.1.6.

Praxishomepage (s. a. Auftragsverarbeitung)

Welche Inhalte muss eine Datenschutzerklärung zur Praxishomepage haben?

In der Datenschutzerklärung zur Website muss umfassend darüber aufgeklärt werden, ob und welche Daten von Besuchern der Website verarbeitet werden. Darüber hinaus müssen auch für diese Datenverarbeitungen die Informationen nach Art. 13 DSGVO gegeben werden (Beispiel: Datenschutzerklärung unter www.lda.bayern.de). Welche Informationen dies im Einzelnen sind, lässt sich nicht in einem Musterformular, das für alle Arztpraxen gültig sein kann, darstellen. Möglicherweise können sich die Arztpraxen bei der Erstellung der Datenschutzerklärung von ihrem Homepagebetreiber unterstützen lassen.
Als Grundlage für Ihre Datenschutzerklärung kann auch folgendes Muster dienen:
https://www.kvbw-admin.de/api/download.php?id=2961

Hinweise zum Einsatz von Cookies: https://upload-magazin.de/blog/29945-cookies-dsgvo/?platform=hootsuite
Hinweise des Bayerischen Landesamtes für Datenschutzaufsicht:
https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkte 8.2 (Datenschutzbestimmungen auf Websites, 8.3 (Cookie-Banner), 8.4 (Kontaktformular), 8.5 Fotos auf Websites).

Google Fonts auf Websites

Google stellt für Webdesigner eine Infrastruktur bereit, mit der die benötigten Schriftdateien hochgeladen werden können. Das Landgericht München (Az.: 3 O 17493/20) sorgte für Aufsehen, weil es einem Kläger gegen einen Betreiber einer Website aufgrund des Einsatzes von Google Fonts Schadensersatz zusprach. Das löste eine Abmahnwelle aus.
Es versuchen derzeit etliche Trittbrettfahrer, Arztpraxen zur Zahlung eines pauschalierten Schadensersatzes (in der Regel 100,-- bis 250,-- €) zu bewegen.
Es ist daher empfehlenswert, zu prüfen, ob auf der Homepage einer Arztpraxis Schriftarten eingesetzt werden, die von Google Servern geladen und nicht lokal hinterlegt sind.

Elektronische Kommunikation mit Patienten

Ist eine E-Mail-Kommunikation mit Patienten zulässig?

Nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht ist eine unverschlüsselte E-Mail-Kommunikation mit Patienten nur unter bestimmten Voraussetzungen zulässig. Näheres hierzu finden Sie hier https://www.lda.bayern.de/media/baylda_report_07.pdf unter Punkt 9.6, unter: https://www.lda.bayern.de/media/FAQ_Zip.pdf und unter https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt16.7.
Eine Kommunikation per unverschlüsselter E-Mail mit dem Patienten sollte, unter Beachtung der Hinweise des BayLDA, erst dann erfolgen, wenn der Patient zuvor schriftlich in diese Kommunikationsform eingewilligt hat und der Arzt eine verschlüsselte Kommunikation anbieten kann.

Informationsquellen zur E-Mail-Verschlüsselung
https://www.heise.de/security/meldung/pEp-Erste-Anwendungen-von-Pretty-Easy-Privacy-fuer-Windows-und-Android-3254151.html
https://rufposten.de/blog/2018/07/17/pep/
https://www.mit-sicherheit-gut-behandelt.de/digitale-arztpraxis/email.html
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesseltkommunizieren/Einsatzbereiche/einsatzbereiche.html

Ist der Einsatz von Messenger-Diensten (z. B. WhatsApp) in Arztpraxen zulässig?

Zum Einsatz von Messenger-Diensten gibt es verschiedene Hinweise von Datenschutzaufsichtsbehörden.

https://www.lda.bayern.de/media/baylda_report_07.pdf, Punkt 22.1
https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 8.6
https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/23_DIB/DIB-2017.pdf, Punkt 12.6.
https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 8.6
Aufgrund der Tatsache, dass durch WhatsApp weiterhin Metadaten in den USA verarbeitet werden und Adressdaten aus dem telefoneigenen Adressbuch des Nutzers ohne Einwilligung der Betroffenen erhoben werden, ist ein datenschutzkonformer Einsatz des Messengers in der Regel nicht zu begründen. Das BayLDA empfiehlt daher datenschutzkonforme Alternativen zu WhatsApp.
Informationen zu div. Messenger-Diensten finden Sie hier:
https://www.ejwue.de/service/rechtsfragen/d/news/datenschutz-in-der-jugendarbeit-udn-messengerdienste/
https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-die-datenschutzregeln-im-ueberblick-13055
https://www.test.de/Messenger-Apps-Ein-Aussenseiter-schlaegt-WhatsApp-Co-4884453-4884458/

Ist der Einsatz externer Anrufbeantworter (Mailbox) zulässig?

Nach Auskunft des BayLDA ist die Nutzung einer Mailbox bei einem externen Dienstleister (Telekommunikationsunternehmen) zulässig, da auch die Inhalte der Mailbox beim Dienstleister dem Fernmeldegeheimnis unterliegen. Die Inanspruchnahme dieser Dienstleistung stellt keine Auftragsverarbeitung dar.

Manche Dienstleister bieten an eingehende Sprachnachrichten als E-Mail an den Empfänger weiterzuleiten. U. E. muss in diesem Fall sichergestellt werden, dass diese E-Mail nach dem Stand der Technik verschlüsselt ist und nur von der Arztpraxis gelesen werden kann.

Kann ein Arzt Kommentare auf Bewertungsportalen, wie jameda, löschen lassen?

Löschansprüche gegen Jameda stehen Ärzten zu, wenn eine Bewertung gegen interne Nutzungsrichtlinien von Jameda verstößt. Ein Verstoß gegen die internen Nutzungsrichtlinien liegt zum Beispiel vor, wenn

- die Bewertung nicht den behandelnden Arzt betrifft
- der Behandlungskontakt mehr als 4 Jahre zurückliegt
- die Bewertung eine beleidigende Äußerung ist

Liegt kein Verstoß gegen die Nutzungsrichtlinie von Jameda vor, kann sich ein Lösch- und Unterlassungsanspruch bei Meinungen ergeben, die beleidigend oder ehrverletzend sind. Zudem besteht ein Löschanspruch des bewerteten Arztes bei unwahren Tatsachenbehauptungen – unabhängig davon, ob sie beleidigend sind oder nicht.

(vgl. dazu den Tätigkeitsbericht des BayLDA 2009/10 4.1.4 und Tätigkeitsbericht 2013/14 Ziff. 6.6 und 7.5). Die Tätigkeitsberichte sind unter https://www.lda.bayern.de/de/taetigkeitsberichte.html abrufbar.

Hinweise im Tätigkeitsbericht 2017/2018: https://www.lda.bayern.de/media/baylda_report_08.pdf, Punkt 8.1

Was kann im Wege der Betriebsprüfung vom Finanzamt eingesehen werden? Gibt es Beschränkungen bei Rechnungen o.ä. Dokumenten auf denen patientenbezogene Daten stehen?

Antwort BayLDA:

Hierzu gab es 2009 eine Grundsatzentscheidung des Bundesfinanzhofes (BFH). Das Bayerische Landesamt für Steuern führt dazu u.A. folgendes aus.

1. Grundsatz

Der BFH hat in einem Grundsatzurteil Leitlinien zum Auskunftsverweigerungsrecht ausgeführt (BFH v. 28. 10. 2009 VIII R 78/05, BStBl. 2010 II S. 455): Nach § 102 Abs. 1 Nr. 3 AO können u. a. Rechtsanwälte, Notare, Steuerberater und Ärzte die Auskunft über das verweigern, was ihnen in dieser Eigenschaft anvertraut oder bekannt geworden ist. Nach § 104 Abs. 1 S. 1 AO können diejenigen Personen, die die Auskunft verweigern dürfen, auch die Vorlage von Urkunden verweigern. Dabei besteht allerdings kein umfassendes Verweigerungsrecht, sondern nur ein jeweils auf die einzelne Unterlage bezogenes.

Geschützt sind alle mandanten- bzw. patientenbezogenen Daten, insbesondere die Identität des Mandanten bzw. Patienten und die Tatsache seiner Beratung. Das Gesetz schützt das Vertrauensverhältnis zwischen dem Berufsgeheimnisträger und seinem Mandanten bzw. Patienten. Für den Schutz des Vertrauensverhältnisses oder seine Gefährdung macht es keinen Unterschied, in welchem Steuerrechtsverhältnis es zu einer Offenbarung der mandanten- bzw. patientenbezogenen Informationen gegenüber der Finanzverwaltung kommt. § 102 AO gilt deshalb für eigene Steuersachen des Berufsträgers sowie für gegen ihn gerichtete Auskunftsersuchen im Besteuerungsverfahren eines Dritten.

Allerdings darf eine Auskunftsverweigerung nicht soweit führen, dass die Finanzverwaltung an einer ordnungsgemäßen und einheitlichen Besteuerung (Art. 3 GG i. V. m. § 85 AO) gehindert ist. Das Gebot einer gleichmäßigen Besteuerung könnte nämlich beeinträchtigt sein, wenn sich Angehörige bestimmter Berufsgruppen unter Berufung auf eine bestehende Verschwiegenheitspflicht generell der Überprüfung ihrer im Besteuerungsverfahren gemachten Angaben entziehen könnten (BFH-Urteil vom 8. 4. 2008 VIII R 61/06, BStBl. 2009 II S. 579).

2. Ausnahmen vom Auskunftsverweigerungsrecht des Berufsgeheimnisträgers

Vorlage von Unterlagen, die keine Vorgänge betreffen, die im Zusammenhang mit der beruflichen Tätigkeit stehen (z. B. Einkünfte aus Kapitalvermögen und aus Vermietung und Verpachtung).

Vorlage von Unterlagen ohne Hinweis auf die Identität der Mandanten bzw. Patienten und deren Beratung bzw. Behandlung (z. B. Eingangsrechnungen, Gehaltsabrechnungen).

Erteilung von Auskünften und Vorlage von Unterlagen nach Entbindung von der Schweigepflicht (§ 102 Abs. 3 AO).

Rechtsanwälte dürfen die nach § 4 Abs. 5 S. 1 Nr. 2 EStG erforderlichen Angaben zu Teilnehmern und Anlass einer Bewirtung in der Regel nicht unter Berufung auf die anwaltliche Schweigepflicht verweigern (BFH-Urteil vom 26. 2. 2004 IV R 50/01, BStBl. 2004 II S. 502). Die Entscheidung ist auf andere Berufsträger im Sinne des § 102 Nr. 3 AO übertragbar.

Auch die in § 102 AO genannten Berufsgruppen müssen im eigenen Besteuerungsverfahren zur Klärung von Treuhandverhältnissen alles Zumutbare unternehmen, um den Nachweis zu erbringen, dass es sich bei den von ihnen verwahrten Rechten oder Sachen nicht um eigenes, sondern um fremdes Vermögen handelt (BFH-Beschluss vom 23. 2. 2011 VIII B 126/10, BFH/NV 2011 S. 1283; BFH-Urteil vom 27. 9. 2006 IV R 45/04, BStBl. 2007 II S. 39).

Vorlage von Nachweisen unter Wahrung der berufsrechtlichen Verschwiegenheitspflicht, das heißt in neutralisierter Form. Dies kann z. B. durch Schwärzung mandanten- bzw. patientenbezogener Daten erfolgen. Der Berufsträger kann jedoch auch andere Mittel wählen. Die Anonymisierung darf allerdings nicht dazu führen, dass der Finanzverwaltung eine Überprüfung der steuerlichen Verhältnisse des Berufsträgers auf Vollständigkeit und Richtigkeit unmöglich wird (vgl. hierzu Tz. 4).

3. Datenzugriff nach § 147 Abs. 6 AO

Enthalten Datenbestände – unabhängig ob in Papierform oder elektronisch – dem Auskünfte- und Vorlageverweigerungsrecht unterliegende Daten, obliegt es dem Berufsgeheimnisträger, durch entsprechende Maßnahmen eine geeignete Zugriffsbeschränkung sicherzustellen. Wie bzw. in welchem Umfang diese Einschränkung vorgenommen werden kann, ist im jeweiligen Einzelfall zu entscheiden. Es liegt ausschließlich in der Entscheidungssphäre des Berufsträgers, welches Datenverarbeitungssystem er einsetzt

und welche steuerlich relevanten Unterlagen er damit erstellt bzw. darin verarbeitet. Damit liegt es auch in seiner Verantwortung, das System so auszuwählen und einzusetzen, dass einerseits seine Geheimhaltungspflichten gewahrt sind und andererseits der Finanzverwaltung der gesetzlich eingeräumte Zugriff nach § 147 Abs. 6 AO, insbesondere auch der unmittelbare und mittelbare Zugriff, auf alle steuerlich relevanten Daten, die keinem Auskunftsverweigerungsrecht unterliegen, möglich ist und unter anderem auch die Zugriffsberechtigung („Prüferrolle") im Datenverarbeitungssystem entsprechend ausgestaltet werden kann.
Als Mittel der Anonymisierung kommen insoweit beispielhaft Zugriffsberechtigungskonzepte, die eine hinreichende Datentrennung gewährleisten und mit eindeutigen Ordnungs- bzw. Identifikationsmerkmalen arbeiten in Betracht, die keine Rückschlüsse auf die Identität des Mandanten zulassen.
Nimmt ein Berufsgeheimnisträger in seiner Datenverarbeitung die für die Erfüllung seiner Verpflichtungen erforderliche Trennung seiner Daten nicht vor, hindert das die Finanzbehörde nicht, den Zugriff auf die Daten im vorliegenden Bestand zu verlangen (FG Baden-Württemberg v. 16. 11. 2011 4 K 4819/08 und FG Rheinland-Pfalz v. 20. 1. 2005 4 K 2167/04, EFG S. 667).

4. Beweislast

Ist dem Finanzamt die Prüfung steuermindernder Tatsachen verwehrt, weil der Berufsgeheimnisträger die Einsicht in seine Unterlagen unter Hinweis auf seine Verschwiegenheitspflicht verweigert, so geht dies zu Lasten des Berufsträgers (BFH-Urteil vom 14. 5. 2002 IX R 31/00, BStBl. II S. 712 zur Vorlage eines Fahrtenbuchs).
Verweigert z. B. ein Arzt jedwede Auskunft über Diagnosen und Behandlungsmethoden, kann nach den Grundsätzen der objektiven Feststellungslast die Umsatzsteuerbefreiung nicht gewährt werden, soweit Anhaltspunkte für steuerpflichtige Leistungen an Patienten gegeben sind (BFH-Beschluss vom 18. 2. 2008 V B 35/06, BFH/NV S. 1001).

5. Kontrollmitteilungen

Wird beabsichtigt im Rahmen der Außenprüfung eines Berufsgeheimnisträgers Kontrollmitteilungen zu fertigen, ist der Steuerpflichtige hierüber rechtzeitig vorher zu informieren, um ihm die Möglichkeit eines gerichtlichen Rechtsschutzes zu eröffnen (BFH-Urteil vom 8. 4. 2008 VIII R 61/06, BStBl. 2009 II S. 579).

6. Kein Verwertungsverbot

§ 102 AO gibt bestimmten Berufsträgern das Recht, Auskünfte zu verweigern. Ob das Recht ausgeübt wird, steht dem Berufsträger frei. Erteilt der Berufsträger freiwillig Auskünfte, so besteht kein Verwertungsverbot. Ein Hinweis auf das Auskunftsverweigerungsrecht ist nicht erforderlich (BFH-Beschluss vom 1. 2. 2001 XI B 11/00, BFH/NV S. 811).
Diesen Ausführungen folgt auch die datenschutzrechtliche Wertung, alles was das Finanzamt verlangen darf, darf auch vorgelegt werden.

Zusammenfassend und vereinfacht lässt sich folgende Regel aufstellen:
Die ärztliche Schweigepflicht ermöglicht bis zu einem gewissen Grad die Einsicht in Unterlagen zu verweigern. Eine Prüfung als solche muss aber dennoch möglich sein, sodass eine Entbindung von der Schweigepflicht oder Schwärzung von patientenbezogenen Angaben in Betracht kommt.

Wie ist mit Kollaborationsplattformen (z. B. Videokonferenz, Tumorpanels (Dekom), gemeinsame Server eines Praxisnetzes) umzugehen?

Antwort BayLDA:
Der Betreiber der Kollaborationsplattform wird in der Regel auch Auftragsverarbeiter sein, wenn diese personenbezogene Daten für den Arzt verarbeitet. Mit ihm ist ein Vertrag nach Art. 28 DSGVO abzuschließen.
Die Einbeziehung von weiteren Behandlern im Wege der Kollaborationsplattform ist grds. möglich, sofern die berufsrechtlichen Regelungen dies erlauben oder der Patient eingewilligt hat.
Bei der technischen Umsetzung und Auswahl der Plattform sollte auf ausreichende Datensicherheitsmaßnahmen geachtet werden (z.B.: Ende-zu-Ende- Verschlüsselung, 2-Faktor-Authentifizierung bei der Anmeldung, nicht nur Username und Passwort).

Was muss ich bei Videoüberwachung beachten?

Umfassende Informationen zum Thema Videoüberwachung gibt es hier:
https://www.lda.bayern.de/de/thema_videoueberwachung.html

Für die Prüfung der Rechtmäßigkeit der (Daten-)Verarbeitung durch nicht öffentliche Stellen ist zunächst auf Art. 6 Abs. 1 S. 1 lit. f DSGVO als Rechtsgrundlage abzustellen. Danach ist die Verarbeitung im Rahmen der Videoüberwachung rechtmäßig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Sofern der Praxisinhaber ein berechtigtes überwiegendes Interesse nachweisen kann, kann die Verarbeitung erlaubt sein; es müssen allerdings dann auch Hinweisschilder angebracht und verhindert werden, dass neben Patienten und potentiellen Straftätern nicht auch Mitarbeiter über Gebühr überwacht werden. Die Videoüberwachung muss im Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden. Außerdem müssen die Informationspflichten nach Art. 13 DSGVO erfüllt werden.

Darf ich Bilder von Patienten in meine Patientenakte nehmen, um mich später etwa bei Telefonanrufen an den Patienten zu erinnern?

Rechtsgrundlage hierfür kann nur eine Einwilligung der Patienten sein, diese muss freiwillig und durch eine eindeutige Handlung erfolgen, reines Nichtstun/Über sich ergehen lassen, genügt nicht.

Vorstehendes gilt nicht, soweit die Bilder zur Behandlungsdokumentation erforderlich sind.

Telematikinfrastruktur

Ist eine Arztpraxis für die Sicherheit der Telematikinfrastruktur (TI) verantwortlich?

Entscheidend ist, wo sich ein möglicher Angriff auf die Daten ereignet. Sollte es auf Grund fehlender Datenschutzmaßnahmen innerhalb des Praxisnetzwerks, z.B. fehlende Absicherung der Hard- oder Software mittels Firewall, Zugriffsbeschränkung o.ä., zu einem Datenschutzvorfall kommen, ist der betreffende Arzt bzw. Psychotherapeut verantwortlich. Diese Verantwortlichkeit für die allgemeine IT-Sicherheit des zuständigen Arztes bzw. Psychotherapeuten in der Praxis bestand auch schon vor der Einführung der TI. Die gematik stellt in ihrem Informationsblatt "Datenschutz und Haftung in der Telematikinfrastruktur" klar, dass die Haftung des Arztes bzw. des Psychotherapeuten nach der Datenschutzgrundverordnung in jedem Fall ausscheidet, wenn die zugelassenen Komponenten (insbesondere der Konnektor) der TI bestimmungsgemäß verwendet werden und gemäß den im Betriebshandbuch der Komponenten beschriebenen Anforderungen aufgestellt und betrieben werden.

Eine Haftung scheidet nach Auffassung der gematik in diesem Fall aber auch nach jeder anderen vergleichbaren Norm (Vertrags- oder Deliktsrecht) aus, da nach allen haftungsrechtlichen Tatbeständen den Datenverarbeiter ein Verschulden treffen müsse. Ein solches Verschulden liegt bei sachgemäßem Anschluss jedoch nicht vor. Die gematik weist außerdem darauf hin, dass dies auch für jegliche strafrechtliche Haftung des Arztes bei der Nutzung eines Konnektors gelte.

Die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 12. September 2019 zum Thema TI beschlossen, dass die gematik für die zentrale Zone der TI („TI-Plattform Zone zentral“) allein verantwortlich ist.

Ferner vertritt die DSK die Auffassung, dass die gematik für die Konnektoren – also den dezentralen Bereich der TI – mitverantwortlich im Sinne des Art. 26 DSGVO ist.
Den Beschluss der DSK können Sie hier einsehen:
https://www.datenschutzkonferenz-online.de/media/dskb/20190912_beschluss_zur_gematik.pdf
Zu diesem Beschluss der DSK hat die KBV am 30. September 2019 eine Stellungnahme abgegeben. Hierin hat sie klargestellt, dass dieser sich mit ihrer Auffassung deckt, dass ab dem Konnektor die gematik für Datenschutz und Datensicherheit zuständig ist. Für die Sicherheit der eigenen Praxis ist und bleibt weiterhin der Arzt beziehungsweise Psychotherapeut verantwortlich (vgl. auch https://www.kbv.de/html/1150_57673.php).

Die KBV hat eine **„Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragspsychotherapeutischen Versorgung“** erstellt (§ 75b SGB V). Hierdurch sollen die IT-Systeme der Praxen und die sensiblen Daten in den Praxen noch besser geschützt werden.
Hier finden Sie weitere Informationen zur IT-Sicherheitsrichtlinie der KBV:
KBV - IT-Sicherheitsrichtlinie

Datenschutz-Folgenabschätzung

Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen?

Auch bei der Verarbeitung von Gesundheitsdaten muss nicht immer ein hohes Risiko bei der Verarbeitung im datenschutzrechtlichen Sinn bestehen, so dass ein Praxisinhaber nur in Ausnahmefällen eine Datenschutz-Folgeabschätzung vornehmen muss. Vor allem bei telemedizinischen Verfahren, bei denen ein Arzt eine hohe Anzahl von Gesundheitsdaten über neue Technologien verarbeitet, neue Geschäftsfelder eröffnet oder über das freie Internet kommuniziert werden, sollte der Verantwortliche prüfen, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Das Risiko definiert sich dabei nicht ausschließlich an der Anzahl oder an der Art der Daten, sondern besonders am Informationsgehalt über den einzelnen Betroffenen, der sich aus ihrer Verarbeitung und dem Kontext ergibt.

Ausführliche Informationen stellt das BayLDA zur Verfügung: https://www.lda.bayern.de/de/dsfa.html.
Das BayLDA hat zudem eine Liste mit Datenverarbeitungen erstellt, die immer eine DSFA erfordern: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf. Für Ärzte ist dort insbesondere der Punkt 16 von Bedeutung (Telemedizin erfordert unter bestimmten Voraussetzungen eine DSFA).