KVB
Kassenärztliche Vereinigung Bayerns

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

Stand: 17.03.2020

Inhalt

FAQs zum Datenschutz in der Arztpraxis

Wo finde ich Informationen und Hilfestellungen zur DSGVO?

Basisinformationen zur DSGVO, Muster zur Patienteninformation 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.

Auf unserer Homepage finden Sie Muster für Einwilligungserklärungen nach § 73 Abs. 1b SGB V, zur Bestellung eines Datenschutzbeauftragten, zur Verpflichtung der Mitarbeiter auf Einhalten 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/).

Eine weitere FAQ-Liste finden Sie auf der Homepage der Bayer. Landesärztekammer, http://www.blaek.de/, unter dem Punkt Datenschutz 2018 (EU-DSGVO) in der Rubrik Arzt und Recht.

Darüber hinaus hat sich die Bundesregierung am 03.07.2018 aufgrund einer kleinen Anfrage zu den Auswirkungen der DSGVO im Gesundheits- und Pflegebereich geäußert - http://dip21.bundestag.de/dip21/btd/19/031/1903194.pdf

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 (Muster s. o.)
- Datenschutzverpflichtung von Beschäftigten (Muster s. o.)

- Verfahren für Datenpannenmeldungen (Muster 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 - aufgrund gesetzlicher Bestimmungen

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

Liegt keine Überweisung vor, gilt § 73 Abs. 1b SGB V, d. h. die Datenübermittlung ist nur mit Zustimmung des Patienten möglich. Aus Gründen der Nachweisbarkeit ist jedoch weiterhin die Schriftform zu empfehlen.
Die Ausstellung einer Verordnung auf Krankenhauspflege steht einem Überweisungsschein in datenschutzrechtlicher Hinsicht gleich.

Dürfen Ärzte Krankenkassen oder Gesundheitsämtern Auskunft geben, wenn diese eine Anfrage stellen?

Personenbezogene Daten dürfen nur übermittelt werden, wenn eine Rechtsgrundlage die Datenübermittlung erlaubt. Dies kann eine Einwilligung des Patienten sein, mit der er einer Schweigepflichtentbindung zustimmt, oder eine Rechtsnorm, zum Beispiel eine gesetzliche Bestimmung im SGB V oder eine Regelung im Bundesmantelvertrag-Ärzte.

Anfragen von Krankenkassen auf einem vertragsärztlichen Formular beruhen auf einer Rechtsnorm, deshalb müssen Praxen solche Anfragen beantworten. Anders bei formlosen Anfragen: Bei diesen muss die Krankenkasse angeben, aufgrund welcher Rechtsgrundlage sie Auskunft haben will. Ansonsten sind Praxen nicht verpflichtet zu antworten.

Auch Anfragen anderer Stellen, etwa von Berufsgenossenschaften, Sozialgerichten oder Gesundheitsämtern, müssen eine Rechtsgrundlage haben. Es kann zum Beispiel sein, dass personenbezogene Daten an Gesundheitsämter übermittelt werden müssen, weil für bestimmte Krankheiten eine Meldepflicht aufgrund des Infektionsschutzgesetzes besteht.

Unterstützung bietet das 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 Bayer. Landesamt für Datenschutzaufsicht (am 30.01.19) wie folgt:

<u>Versorgungsamt (Zentrum Bayern Familie und Soziales)</u>
„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 sich dem ZBFS gegenüber einverstanden erklärt, dass es bei den von ihm benannten Ärzten Befundberichte einholen darf, und das ZBFS dem Arzt das Vorliegen dieser Einverständniserklärung bestätigt. Auf Anforderung stellt das ZBFS dem Arzt die Einverständniserklärung 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 Einverständniserklärung (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.

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).

Ergänzend verweisen wir auf eine Veröffentlichung des Ärztlichen Kreisverbandes Ebersberg, die vor dem Wirksamwerden der DSGVO veröffentlicht wurde: https://www.aekv-ebersberg.de/aktuelles/162-versorgung-von-heimpatienten-rechtliche-fallstricke-und-empfehlungen.html.

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

Wann dürfen Patientendaten per Fax übermittelt werden?

Bei dieser Fragestellung sind verschiedene Sachverhalte zu unterscheiden. Grundsätzlich wird der Versand von Patientendaten per Fax vom Bayer. Landesamt für Datenschutzaufsicht noch für zulässig erachtet.

- **Fax an andere Ärzte und öffentliche Stellen** (Ausnahme Beihilfestelle)
  Die Übermittlung von Patientendaten per Fax ist erlaubt. Der absendende Arzt darf davon ausgehen, dass diese Empfänger die notwendigen Maßnahmen getroffen haben, dass nur befugte Personen Zugang zu eingehenden Faxen haben. Wie uns das Bayer. Landesamt für Datenschutzaufsicht bestätigt hat, muss sich der absendende Arzt nicht mehr davon überzeugen (sich bestätigen lassen) dass auf Seiten des Faxempfängers nur Berechtigte Zugang zum Faxgerät haben.

- **Fax an Beihilfestellen**
  Es muss sichergestellt sein, dass sich das Zielfax in der Beihilfestelle befindet. Ein Fax an das allgemeine Faxgerät der Behörde ist nicht zulässig.

- **Fax an Patienten (an dessen Arbeitsplatz, in dessen Wohnung) oder andere Dritte**
  Nachdem nicht sichergestellt ist, dass in diesen Fällen nur der Patient oder ein anderer Berechtigter das Fax zur Kenntnis nehmen kann (beim Fax an den Arbeitsplatz erfolgt ggf. sogar eine Datenspeicherung im EDV-System des Arbeitgebers), ist hierfür eine entsprechende und nachweisbare Einwilligung des Patienten erforderlich. Beim Versand an andere Dritte muss sich der Versender zudem davon überzeugen, dass beim Dritten nur Berechtigte Zugang zu eingehenden Faxen haben.

Dürfen Patienten noch mit Namen aufgerufen werden?

Das Bayer. Landesamt für Datenschutzaufsicht hat uns am 06.08.2018 auf Nachfrage 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.

Wann müssen Patientendaten gelöscht werden?

Grundsätzlich sind personenbezogene Daten dann zu löschen, wenn diese zur Erfüllung des Behandlungsvertrages nicht mehr erforderlich sind und andere Rechtsvorschriften einer Löschung nicht entgegenstehen. Eine andere Rechtsvorschrift in diesem Sinne ist zunächst die ärztliche Berufsordnung, nach der die Patientenakte 10 Jahre (nach dem

Tag der letzten Behandlung) aufzubewahren ist. Andere Rechtsvorschriften wären z. B. auch das Gentechnikgesetz bzw. die Röntgenverordnung. 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 neu) oder die Unterlagen zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Stichwort: Vorwurf Behandlungsfehler) erforderlich sind (Art. 17 Abs. 3 Buchstabe e DSGVO).
Die Daten müssen - auch ohne dass der Patient dies verlangt - nach Ablauf dieser Fristen gelöscht werden.
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

Über ihre Rechte nach der DSGVO werden die Patienten abschließend mit der Patienteninformation zur DSGVO, die die KBV als Muster bereitgestellt hat (http://www.kbv.de/html/datensicherheit.php) informiert.

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 Arztwechsel ist die Weitergabe an den neuen Arzt jedoch möglich.
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 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.

Hinweis:
Der Bundestag hat am 27. Juni 2019 das sog. **Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz EU** beschlossen.
Dies betrifft unter anderem die Regelung zur Benennungspflicht eines Datenschutzbeauftragten. Hierbei werden kleine Praxen künftig entlastet. Der Gesetzgeber hat die Pflicht, einen betrieblichen Datenschutzbeauftragten zu benennen, von zehn Mitarbeiter, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, auf 20 erhöht (§ 38 Abs. 1 Satz 1 BDSG).

Der Bundesrat hat am 20. September 2019 diesem Gesetz zugestimmt und dieses wurde auch im Bundesgesetzblatt veröffentlicht.

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. Darüber hinaus ist zu prüfen, ob ein Fall des Art. 26 DSGVO vorliegt (Gemeinsam für die Verarbeitung Verantwortliche).

Auch überörtliche Berufsausübungsgemeinschaften sind rechtlich selbständige Praxen, d. h. auch diese müssen bei Erfüllung der o. g. Voraussetzungen 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.

Eine Mitarbeiterin unserer Praxis soll die Aufgabe des Datenschutzbeauftragten übernehmen. Benötigt sie eine besondere Aus- oder Fortbildung?

Antwort KBV

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 Ihre Mitarbeiterin das nötige Wissen aneignet, gibt es nicht.

Das BayLDA fordert seit Ende Juni 2018 für neue Datenschutzbeauftragte **nicht mehr** den Besuch eines mindestens 2tägigen Intensivseminars zum Erwerb der erforderlichen Kenntnisse.

Was unterscheidet interne und externe Datenschutzbeauftragte?

Antwort KBV

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

Praxisinhaber können aber auch einen externen Dienstleister beauftragen. Es besteht jedoch keine gesetzliche Verpflichtung zur Bestellung eines externen Datenschutzbeauftragten.

Bei dieser Variante fallen zusätzliche Kosten an, jedoch wird das Haftungsrisiko minimiert, denn bei Fehlern im Umgang mit dem Datenschutz haftet der externe Dienstleister. Welche Variante gewählt wird, muss der Praxisinhaber entscheiden.

Benötigen Gemeinschaftspraxen wie Einzelpraxen ab 20 Personen einen Datenschutzbeauftragten?

Antwort KBV

Ja, denn aus datenschutzrechtlicher Perspektive ist es nicht entscheidend, ob es sich um eine Einzelpraxis oder um eine andere Praxisform handelt. Die Vorgaben sind dieselben.

Ab 20 Personen muss ein Datenschutzbeauftragter bestellt werden: Müssen es Vollzeitstellen sein oder geht es um die Anzahl der Personen?

Antwort KBV
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 DSGVO die zuständige (Datenschutz-) Aufsichtsbehörde?

Die zuständige Aufsichtsbehörde für den nicht-öffentlichen Bereich, das heißt u.a. bei den freiberuflich Tätigen ist das Bayerischen 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 DSGV 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 Ransomeware (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 Verarbeitungsverzeichnis 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.

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 (Schweigepflichtsentbindungserklärung) erforderlich?“).

Hierzu vertritt eine außerbayerische Datenschutzaufsichtsbehörde eine andere Rechtsauffassung. Diese haben wir dem Bayer. Landesamt für Datenschutzaufsicht (BayLDA) mitgeteilt.
Das BayLDA teilt die Rechtsauffassung der außerbayerischen Datenschutzaufsichtsbehörde nicht, d.h. Laborpraxen sind gegenüber den einsendenden Ärzten in Bayern nach derzeitiger Rechtsauffassung keine Auftragsverarbeiter.
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 in der Regel 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 (alle?) 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-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.

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

Antwort LDA:
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 (Verletzung von Privatgeheimnissen) stellt u. a. den unbefugten Bruch der ärztlichen Schweigepflicht unter Strafe und wurde im Herbst 2017 insbesondere in den Abs. 2 und 3 geändert. Es wurde der Personenkreis der „sonstigen Personen, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken“ geschaffen (Details siehe Geset-

zesbegründung: 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). Unter diesen Personenkreis fallen insbesondere Personen, die mit der Wartung und Pflege Ihres PV-Systems betraut sind.

Die wesentlichen Änderungen des § 203 StGB sind im nachstehenden Text hervorgehoben:

„(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. **Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.**

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. **Ebenso wird bestraft, wer**

1. **als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,“**

Nach Abs. 4 Nr. 1 der vorstehenden Vorschrift ist es deshalb erforderlich dass der Personenkreis der sonstigen mitwirkenden Personen ausdrücklich zur Geheimhaltung verpflichtet wird. Eine Hilfestellung hierzu 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.

Damit die, durch die Änderung des § 203 StGB, geschaffenen Möglichkeiten zur Einbindung „sonstiger mitwirkender Personen“ tatsächlich genutzt werden können, bedurfte es jedoch noch einer Anpassung des Berufsrechts. Hierzu verweisen wir auf die Ausführungen des Berliner Datenschutzbeauftragten im Jahresbericht 2017 unter Punkt 7.6 (https://www.datenschutz-

berlin.de/fileadmin/user_upload/pdf/publikationen/jahresbericht/BlnBDI-Jahresbericht-2017-Web.pdf).

Die PTK Bayern hat zwischenzeitlich eine Anpassung der BO in § 8 Abs. 2 vorgenommen. Dort wurden - im Hinblick auf die Neufassung des § 203 StGB - die Worte „eine gesetzliche Vorschrift dazu berechtigt“ eingefügt.

Die entsprechende Anpassung der Musterberufsordnung Ärzte wurde auf dem 121. Deutschen Ärztetag im Dezember 2018 in Erfurt beschlossen. Diese Änderung wurde im Deutschen Ärzteblatt am 01. Februar 2019 veröffentlicht. Die Anpassung der Berufsordnung Ärzte Bayern stand auf der Tagesordnung des Bayerischen Ärztetages, welcher vom 11.10.-13.10.2019 stattfand.

Patienteninformation zum Datenschutz

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

Ein Muster zur Patienteninformation stellt die KBV zur Verfügung (http://www.kbv.de/html/datensicherheit.php). In dieses Muster tragen Sie unter Punkt 1 bitte noch die Daten zur Praxis sowie die Daten Ihres Datenschutzbeauftragten ein, soweit Sie einen Datenschutzbeauftragten bestellen müssen. Unter Punkt 5 ist noch die zuständige Aufsichtsbehörde einzutragen. In Bayern ist dies das Bayerische Landesamt für Datenschutzaufsicht, Promenade 18, 91522 Ansbach.

Zur Erfüllung der Informationspflichten gegenüber den Patienten genügt für Patienten, die die Arztpraxis aufsuchen der Aushang in der Praxis. Sie sollten den Patienten die Information auf Wunsch auch schriftlich zur Verfügung stellen. Außerdem können Sie die Information ggf. auch auf Ihre Homepage 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 Daten über den Patienten von der Arztpraxis beim Patienten selbst oder über den Patienten erhoben werden. Die Informationspflicht wird grundsätzlich durch den Aushang der Patienteninformation 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. Was unter Erheben zu verstehen ist, ist derzeit nicht abschließend rechtlich geklärt. Es ist deshalb - auch nach Abstimmung mit dem Bayer. Landesamt für Datenschutzaufsicht - vertretbar, den Begriff des Erhebens als das Beschaffen von Daten zu interpretieren. 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 verarbeitet werden. Darüber hinaus müssen jetzt 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 Ihnen gleichwohl dieses Muster dienen: https://www.kvbw-admin.de/api/download.php?id=2961
(s. dazu auch LG Würzburg, Beschluss v. 13.09.2018 – 11 O 1741/18 UWG unter:

http://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-22735?hl=true).
Hinweise zum Einsatz von Cookies: https://upload-magazin.de/blog/29945-cookies-dsgvo/?platform=hootsuite
Hinweise des Bayer. 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).

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.

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. Leider lässt sich diesen Veröffentlichungen nicht entnehmen, welche Messenger-Dienste für den Einsatz in Arztpraxen vorbehaltlos geeignet sind.
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.

Das BayLDA hält derzeit den Einsatz von WhatsApp nur dann für zulässig, wenn für WhatsApp ein Kommunikationsmittel eingesetzt wird, auf dem sich nur die Kontaktdaten von WhatsApp-Nutzern befinden (z. B. ein eigenes Smartphone nur für die Nutzung von WhatsApp, auf dem bei der ersten Nutzung nur die Telefonnr. der Arztpraxis gespeichert ist).

Nach einer Veröffentlichung in einer Fachzeitschrift gibt es auch die Möglichkeit WhatsApp in einem Container zu betreiben, der verhindert, dass WhatsApp auf gespeicherte Kontaktdaten zugreift. Sofern Sie diese Variante nutzen möchten, empfehlen wir eine Kontaktaufnahme mit dem BayLDA.

Nachdem WhatsApp aber auch erfasst, wer wann mit wem per WhatsApp (Metadaten der Kommunikation) bedarf die WhatsApp Nutzung einer nachweisbaren und freiwilligen Einwilligung des Patienten. Die Freiwilligkeit der Einwilligung setzt voraus, dass die Arztpraxis eine sichere Alternative (einen anderen sicheren Messenger Dienst) anbieten kann (siehe dazu: Ist eine E-Mail Kommunikation mit Patienten zulässig?).

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.

Wie ist mit Bewertungen auf Bewertungsportalen, wie jameda umzugehen?

Antwort BayLDA:

Die Rechtsprechung räumt hier dem Recht auf freie Meinungsäußerung großes Gewicht ein. Es wird nur in Ausnahmefällen die Möglichkeit geben, eine Löschung zu verlangen (vgl. dazu auch unseren Tätigkeitsbericht 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. Mit ihm ist ein Vertrag nach Art. 28 DS-GVO 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, Passwort).

Was muss ich bei Videoüberwachung beachten?

Antwort BayLDA:
Umfassende Informationen gibt es hier:
https://www.lda.bayern.de/de/thema_videoueberwachung.html

Einige Eckpunkte in Kürze:
Auch Videoüberwachung ist zunächst einmal verboten. Sofern Sie ein berechtigtes überwiegendes Interesse nachweisen können, kann sie 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 Verarbeitungstätigkeit aufgenommen werden.

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

Antwort BayLDA:
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?

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.

Datenschutz-Folgenabschätzung

Wann ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen?

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).