01.09.2018 Datenschutz

Der Datenschutzbeauftragte in Arztpraxen

J. Heberer

Nachdem am 25.05.2018 die EU-Datenschutzgrundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSGneu) in Kraft getreten sind, gehören Fragen zum Datenschutzbeauftragten zu den häufigsten der juristischen Beratungspraxis. Einige dieser Fragen werden im Nachfolgenden behandelt.

Wann muss eine Arztpraxis einen Datenschutzbeauftragten bestellen?

Zunächst seien die Rechtsgrundlagen genannt, da in der Praxis oftmals der Irrtum herrscht, dass es für die Benennungspflicht lediglich auf die Anzahl der Beschäftigten ankomme:

Art. 37 Abs. 1 lit. c) DSGVO legt fest, dass auf jeden Fall ein Datenschutzbeauftragter vom Verantwortlichen zu benennen ist, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO besteht. Zu diesen besonders sensiblen Daten zählen genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Ergänzend ist nach der deutschen Gesetzeslage gemäß § 38 Abs. 1 BDSGneu von einer Arztpraxis ein Datenschutzbeauftragter zu benennen, wenn

1. in der Arztpraxis in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, oder
2. in der Arztpraxis Datenverarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung i. S. d. Artikel 35 DSGVO unterliegen.

Folglich ist die Benennungspflicht eines Datenschutzbeauftragten entweder abhängig

1. von der Beschäftigtenzahl oder

2. von der Erforderlichkeit einer Datenschutz-Folgenabschätzung oder
3. von der Kerntätigkeit des Verantwortlichen, die in der umfangreichen Verarbeitung besonderer Kategorien von Daten, wie Gesundheitsdaten, bestehen muss.

Hinsichtlich der Anzahl der Beschäftigten ist zu sagen, dass hierzu angestellte und freie Mitarbeiter (also angestellte Ärzte, MFAs, Verwaltungskräfte), Leiharbeitnehmer, Auszubildende und Praktikanten, sofern diese ständig, also nicht nur gelegentlich, personenbezogene Daten automatisiert verarbeiten, zählen. Leider wurde durch den Gesetzgeber versäumt, eindeutig zu klären, ob der/die Praxisinhaber selbst auch dazu zählen. Denn dieser ist schließlich auch selbst mit der automatisierten Datenverarbeitung ständig beschäftigt. Die Bundesärztekammer sowie die Kassenärztliche Bundesvereinigung vertreten allerdings die Auffassung, dass der/die Praxisinhaber nicht mitzuzählen sind. Diese Auffassung dürfte nach Ansicht des Verfassers auch richtig sein, da der Wortlaut davon spricht, dass der „Verantwortliche (= Praxisinhaber) mindestens zehn Personen beschäftigt". Ebenso war nach der bisherigen datenschutzrechtlichen Regelung die verantwortliche Stelle nicht mitzuzählen. Hätte man hier eine Rechtsänderung gewollt, hätte dies nach Meinung des Verfassers klar geregelt werden müssen. Gleichwohl ist dies ein Umstand, der gegebenenfalls abschließend durch die zukünftige Rechtsprechung geklärt werden müsste.

Für die Zahl der beschäftigten Personen ist ansonsten ausschließlich die „Kopfzahl" maßgeblich, sodass der Umfang der Beschäftigung, also Teilzeit- oder Vollzeit, irrelevant ist. Unberücksichtigt bleiben können dabei Beschäftigte, die normalerweise nicht auf die Daten zugreifen können, wie dies beispielsweise beim Reinigungspersonal der Fall ist.

Sofern danach regelmäßig weniger als zehn Personen ständig mit der Datenverarbeitung zu tun haben, kann eine Benennung aber trotzdem erforderlich sein, wenn die Kerntätigkeit der Praxis in der umfangreichen Verarbeitung von Gesundheitsdaten besteht. Aus Erwägungsgrund 97 DSGVO ergibt sich, dass im privaten Sektor sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit bezieht. Hierbei wird nach derzeitiger Kenntnis des Verfassers allgemein davon ausgegangen, dass zur Kerntätigkeit auch alle Vorgänge zählen, die fester Bestandteil der Haupttätigkeit sind. Dies bedeutet nach Ansicht des Verfassers, dass die ärztliche Dokumentation und die Patientendatenverwaltung in Arztpraxen damit letztendlich dem Begriff der Kerntätigkeit unterliegen. Folglich wäre gemäß Art. 37 Abs. 1 lit. c) DSGVO allein hiernach von einer Benennungspflicht einer jeden Arztpraxis unabhängig von der Beschäftigtenzahl auszugehen.

Allerdings muss die Kerntätigkeit der Verarbeitung nach dem Verordnungswortlaut „umfangreich" sein. Hier stellt sich also die nächste Frage. Leider ist der Wortlaut der DSGVO nicht eindeutig. Dies muss also zukünftig durch die Rechtsprechung ausgelegt werden. Einen Hinweis bietet zumindest Erwägungsgrund 91, wonach eine umfangreiche Verarbeitung nicht vorliegen soll, wenn die Verarbeitung personenbezogene Daten von Patienten betrifft und durch einen einzelnen Arzt erfolgt. Wenn also die Arztpraxis aus einem Einzelarzt besteht (und weniger als zehn Beschäftigte im vorgenannten Sinne hat), dann wird aus Sicht des Verfassers in der Regel keine umfangreiche Verarbeitung von Gesundheitsdaten vorliegen, sodass grundsätzlich kein Datenschutzbeauftragter zu benennen ist.

Dies kann jedoch im Einzelfall anhand der konkreten Umstände und der sonstigen Anforderungen an eine umfangreiche Verarbeitung dann anders zu beurteilen sein, wenn die Gesundheitsdatenverarbeitung der Einzelpraxis weit über den Umfang einer üblichen Einzelarztpraxis hinausgeht, beispielsweise wenn diese derart viele Patienten hat, sodass der Betroffenenkreis erheblich den eines nach dem genannten Erwägungsgrund privilegierten, durchschnittlichen Einzelarztes überschreitet.

Was hier unter einem üblichen Umfang zu verstehen ist, ist rechtlich derzeit noch nicht abschließend geklärt. Die Bundesärztekammer und die KBV gehen in ihren Hinweisen und Empfehlungen vom 16.02.2018 davon aus, dass für einzelne Facharztbereiche Behandlungsfallzahlen von bis zu 1.500 Patienten pro Quartal durchschnittlich sind, sodass eine Orientierung am Wert von ca. 6.000 Datensätzen über einen Zeitraum von einem Jahr erfolgen könne, wobei die aufgrund von Aufbewahrungsfristen ohnehin schon dokumentierten Patientendatensätze hinzuzurechnen seien [1]. Dieses Tatbestandsmerkmal bedarf somit der Auslegung und Klarstellung durch die Verordnungsgeber oder die zukünftige Rechtsprechung.

Letztendlich kann ebenfalls unabhängig von der Beschäftigtenzahl die Bestellung eines Datenschutzbeauftragten nach der dritten Variante gemäß § 38 Abs. 1 Nr. 2 BDSGneu dann erforderlich werden, wenn die Datenverarbeitung in der Arztpraxis eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO erfordert. Eine solche ist immer dann erforderlich, wenn eine Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Eine Verwendung neuer Technologien liegt beispielsweise im Fall der Telemedizin vor. Ein solch hohes Risiko liegt nach dem Verordnungswortlaut insbesondere vor, bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten. Unter Bezugnahme auf die zuvor gemachten Ausführungen zur Annahme einer umfangreichen Verarbeitung wird man somit auch hier davon ausgehen können, dass dies bei einer durchschnittlichen Einzelarztpraxis nicht gegeben sein wird, sodass diese auch hiernach keinen Datenschutzbeauftragten benötigt.

Zusammenfassend kann man somit feststellen, dass in jeder ärztlichen Einrichtung zwingend ein Datenschutzbeauftragter zu benennen ist, wenn mindestens zehn Mitarbeiter mit der automatisierten Datenverarbeitung ständig befasst sind.

Bei weniger als zehn derart Beschäftigten ist nach dem Verordnungswortlaut lediglich eine durchschnittliche Einzelarztpraxis von den beiden anderen Tatbeständen einer Benennungspflicht ausgenommen.

Umstritten und noch nicht rechtssicher geklärt ist die Frage, ob dies bedeutet, dass alle sonstigen Arzteinrichtungen, also Praxen mit mehreren Berufsträgern, wie Berufsausübungsgemeinschaften, Mehrarzteinrichtungen wie ein MZV oder Organisationsgemeinschaften wie Praxisgemeinschaften, zwingend im Umkehrschluss einen Datenschutzbeauftragten benennen müssen, wenn diese weniger als zehn Beschäftigte haben. Hierfür spricht, dass der Wortlaut der Verordnung ausdrücklich die Verarbeitung lediglich durch einen einzelnen Arzt als nicht umfangreich privilegiert.

Dagegen lassen sich jedoch folgende Argumente anführen: Die Bundesärztekammer und die Kassenärztliche Bundesvereinigung vertreten diesbezüglich in ihren Hinweisen vom Februar 2018 in Bezug auf Berufsausübungsgemeinschafen eine andere Auffassung, wenn dort die Behandlung durch einen „einzelnen Arzt“ erfolgt und dieser die Dokumentation verantwortet. Wenn in einer Berufsausübungsgemeinschaft mit mehreren Ärzten im Vergleich zum durchschnittlichen Einzelarzt keine umfangreiche Verarbeitung stattfindet, wenn also keine signifikant höhere Anzahl an Patientendatensätzen verarbeitet wird, dann könne man auch hiernach nicht von einer umfangreichen Verarbeitung ausgehen (vgl. BÄK/KBV, a. a. O). Folglich werde dann auch kein Datenschutzbeauftragter benötigt. Dieses Argument lässt sich aus Sicht des Verfassers zumindest dann gut vertreten, wenn es sich um eine übliche BAG handelt, die weder fach- noch ortsübergreifend tätig ist und auch aufgrund der weiteren Umstände des Einzelfalls, insbesondere Praxisgröße, Patientenanzahl sowie geplanten Verarbeitungen, sich hiervon keine abweichende Beurteilung ergibt.

Die gleiche Rechtsunsicherheit gilt für Organisationsgemeinschaften wie einer Praxisgemeinschaft. Denn hier arbeiten zwar mehrere Ärzte unter gemeinsamer Nutzung der Infrastruktur zusammen, es liegen aber eigentlich getrennte Praxen vor, d. h. es findet eine getrennte Behandlung, Dokumentation, Abrechnung und damit eine getrennte Datenverarbeitung statt. Bundesärztekammer und KBV vertreten auch hier die Auffassung, dass für diese nichts anderes gelten kann als für eine Einzelarztpraxis, da die Voraussetzungen des Erwägungsgrundes 91 aufgrund der getrennten Behandlung durch nur einen Arzt in diesen Fällen regelmäßig erfüllt werden, sodass keine Benennungspflicht vorliegt. Auch der Verfasser ist der Meinung, dass für Praxisgemeinschaften, wenn aufgrund der übrigen Umstände keine abweichende Beurteilung einer umfangreichen Verarbeitung gerechtfertigt ist, diese Privilegierung gelten muss.

Eine rechtssichere Auskunft für BAGs, MVZs und Praxisgemeinschaften verbietet sich bedauerlicherweise mangels abschließend geklärter Rechtslage. Folglich muss aus juristischer Sicht diesen Einrichtungen aus Gründen der Rechtssicherheit, gerade im Hinblick auf die Bußgelder, geraten werden, einen Datenschutzbeauftragten zu benennen, wenn sie weniger als 10 Beschäftigte unterhalten.

Zur Rechtssicherheit wird auch empfohlen, dies mit der jeweils zuständigen Landesdatenschutzbehörde zu klären, da diese die Einhaltung der DSGVO überwacht.

Somit ist dies leider abermals eine Frage, die rechtlich nicht abschließend geklärt ist und abgewartet werden muss, wie die Landesdatenschutzbehörden oder auch die künftige Rechtsprechung sich hierzu positionieren werden.

Wer kann Datenschutzbeauftragter sein?

Die DSGVO sieht ausdrücklich vor, dass sowohl ein Mitarbeiter der Arztpraxis (interner Datenschutzbeauftragter) als auch ein Dritter außerhalb der Arztpraxis (externer Datenschutzbeauftragter) zum Datenschutzbeauftragten benannt werden kann.

Mit dem externen Datenschutzbeauftragten muss ein Dienstleistungsvertrag abgeschlossen werden, auf dessen Grundlage er tätig wird. Dieser muss auch zudem zur Geheimhaltung verpflichtet werden, da ansonsten eine Strafbarkeit nach § 203 Abs. 4 S. 2 Nr. 1 StGB droht.

Bei der Benennung eines internen Datenschutzbeauftragten ist zu beachten, dass der Praxisinhaber nach herrschender Meinung selbst nicht Datenschutzbeauftragter sein kann, da sich aus der gleichzeitigen Stellung als Verantwortlicher und Datenschutzbeauftragter Interessenkonflikte ergeben können, die nach der DSGVO ausgeschlossen sein müssen. Dem internen Datenschutzbeauftragten muss zur Erfüllung seiner Aufgaben und zur Erhaltung seiner Fachkunde die erforderliche Arbeitszeit gewährt werden. Der konkrete Umfang muss im Einzelfall bestimmt werden. Des Weiteren muss der Praxisinhaber die für die Erfüllung dieser Aufgaben sowie die zur Erhaltung des Fachwissens erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen stellen. Dies bedeutet, dass hierunter unter anderem auch die Stellung ausreichender finanzieller Mittel, aus Sicht des Verfassers beispielsweise für Aus-, Fort- und Weiterbildungsveranstaltungen, fällt.

Anzumerken ist noch zum einen, dass der Datenschutzbeauftragte bei der Ausübung seiner Tätigkeit weisungsfrei ist. Zum anderen besteht ein gesetzlicher Abberufungs- und Sonderkündigungsschutz, wenn ein Datenschutzbeauftragter verpflichtend ist, dessen Benennung also nicht auf rein freiwilliger Basis erfolgt. Sowohl eine

Abberufung als auch eine Kündigung sind dann nämlich nur aus wichtigem Grund wie im Falle einer fristlosten Kündigung nach § 626 BGB möglich. Sofern die Tätigkeit als Datenschutzbeauftragter regulär beendet wird, ist zudem nach § 6 Abs. 4 Satz 3 i. V. m. § 38 Abs. 2 BDSGneu eine ordentliche Kündigung des Arbeitsverhältnisses für ein Jahr ausgeschlossen, sofern nicht eine fristlose Kündigung aus wichtigem Grund gerechtfertigt ist.

Welche Qualifikation muss ein Datenschutzbeauftragter besitzen?

Nach Art. 37 Abs. 5 DSGVO wird dieser auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben benannt. Der Umfang der Datenverarbeitung und der Schutzbedarf der personenbezogenen Daten sind nach der DSGVO der Maßstab für die erforderliche Fachkunde. Der Datenschutzbeauftragte benötigt damit, wie nach bisheriger Rechtslage auch, entsprechende rechtliche, technische und organisatorische Kenntnisse.

Gemäß dem Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich vom 24./25.11.2010 über die Mindestanforderungen an Fachkunde und Unabhängigkeit des Datenschutzbeauftragten nach dem alten BDSG, der aus Sicht des Verfassers aber nach wie vor als maßgebliche Orientierungshilfe herangezogen werden kann, muss dieser zum einen über allgemeine datenschutzrechtliche und technisch-organisatorische Kenntnisse sowie zum anderen über solch branchenspezifische Kenntnisse verfügen.

Zum allgemeinen Datenschutzrecht zählen:

- Grundkenntnisse zu verfassungsrechtlich garantierten Persönlichkeitsrechten der Betroffenen und Mitarbeiter des Verantwortlichen und
- umfassende Kenntnisse zum Inhalt und zur rechtlichen Anwendung der für den Verantwortlichen einschlägigen Regelungen der DSGVO und des BDSGneu, auch technischer und organisatorischer Art, sowie
- Kenntnisse des Anwendungsbereiches datenschutzrechtlicher und einschlägiger technischer Vorschriften, der Datenschutzprinzipien und der Datensicherheitsanforderungen insbesondere nach Art. 32 DSGVO.

Die branchenspezifischen Kenntnisse umfassen [2]:

- umfassende Kenntnisse der spezialgesetzlichen datenschutzrelevanten Vorschriften, die für das eigene Unternehmen relevant sind,
- Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit (physische Sicherheit, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen, etc.),
- betriebswirtschaftliche Grundkompetenz (Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management, Marketing etc.),
- Kenntnisse der technischen und organisatorischen Struktur sowie deren Wechselwirkung bei dem zu betreuenden Verantwortlichen (Aufbau- und Ablaufstruktur bzw. Organisation der

verantwortlichen Stelle) und
- Kenntnisse im praktischen Datenschutzmanagement eines Verantwortlichen (z. B. Durchführung von Kontrollen, Beratung, Strategieentwicklung, Dokumentation, Verzeichnisse, Logfile-Auswertung, Risikomanagement, Analyse von Sicherheitskonzepten, Betriebsvereinbarungen, Videoüberwachungen, Zusammenarbeit mit dem Betriebsrat etc.).

Wie der aufmerksame Leser erkennt, sind dies lediglich die zu gewährleistenden Mindestanforderungen. Es wird somit deutlich, dass an die Fachkunde des Datenschutzbeauftragten hohe Anforderungen gestellt werden. Aus diesen Gründen wird man um eine Empfehlung, dass nur eine Person zum Datenschutzbeauftragten benannt werden sollte, die entsprechend geeignete Aus-, Fort- und Weiterbildungsveranstaltungen absolviert hat, nicht herumkommen.

Form und Befristung der Benennung

Weder die DSGVO noch das BDSGneu schreiben eine einzuhaltende Form vor. Aus Nachweisgründen empfiehlt sich jedoch die Schriftform oder zumindest die Textform. Auch über eine Dauer der Benennung wird nicht festgelegt, sodass grundsätzlich eine befristete Benennung zulässig ist. Allerdings muss darauf geachtet werden, dass die Befristung nicht zu kurz gewählt wird, da hierdurch die zu gewährleistende Unabhängigkeit des Datenschutzbeauftragten gefährdet werden kann. Hier wird man wohl davon ausgehen müssen, dass eine lediglich sechsmonatige Befristung zur Probezeit für neu eingestellte Datenschutzbeauftragte unwirksam sein dürfte (vgl. Arbeitsgericht Dortmund, Urteil vom 20.02.2013 – 10 Ca 4800/12). Allgemein wird von einer wirksamen Befristung ausgegangen, wenn diese mindestens zwei Jahre beträgt, da nur dann der Datenschutzbeauftragte seine Aufgaben sinnvoll wahrnehmen kann.

Fazit

Der Datenschutz und dessen praktische bzw. technisch-organisatorische Umsetzung sind keine einfachen Themen. Es muss in jedem Einzelfall genauestens geprüft werden, ob ein Datenschutzbeauftragter benötigt wird, wer damit beauftragt wird und ob diese Person auch die notwendigen Anforderungen, die einem Datenschutzbeauftragten abverlangt werden, erfüllen kann. Aufgrund der zum Teil noch ungeklärten Rechtslage ist es allerdings leider auch für Juristen oftmals schwer und beruflich unbefriedigend, wenn in einigen Fällen keine eindeutigen und abschließend gesicherten Rechtsauskünfte erteilt werden können.

Literatur

[1] vgl. BÄK/KBV, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, Dt. Ärzteblatt 2018; 115 (10): A-453/B-395/C-395; DOI: 10.3238/arztebl.2018.ds01

[2] s. hierzu insgesamt: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Mindestanforderungen an Fachkunde und Unabhängigkeit des Beauftragten für den Datenschutz nach § 4f Abs. 2 und 3 BDSG, S. 1-2, unter:
https://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.html

PRAXISTIPP

Am 25.05.2018 traten die neue EU-Datenschutzgrundverordnung (DSGVO) und das hiermit korrespondierende neue Bundesdatenschutzgesetz (BDSGneu) in Kraft. Die darin enthaltenen Regelungen gelten unmittelbar und sind somit ab diesem Zeitpunkt für Ärzte verbindlich, d. h. sowohl die DSGVO als auch das BDSGneu sind zu beachten.

Die für Arztpraxen einschlägigsten Neuerungen hat der BDC-Justitiar Herr Dr. J. Heberer für Sie in enem Artikel „Das neue Datenschutzrecht“ zusammengestellt. Sie finden ihn HIER auf BDC|Online.

Der BDC ermöglicht seinen Mitgliedern im Rahmen von individuellen Einzelvertragsvereinbarung gemeinsam mit dem BDC-Datenschutzbeauftragten Herrn Menge (bei Bedarf Kontakt via BDC) die neue Datenschutzgrundverordnung in der eigenen Praxis zu organisieren und einzuhalten.

Heberer J: Der Datenschutzbeauftragte in Arztpraxen. Passion Chirurgie. 2018 September, 8(09): Artikel 04_09.

Autor des Artikels

Dr. jur. Jörg Heberer

Justitiar des BDC, Rechtsanwalt und Fachanwalt für Medizinrecht

Rechtsanwaltskanzlei Dr. Heberer & Kollegen

> kontaktieren