Verschärfung des Datenschutzrechts in 2018 – dringender Handlungsbedarf für niedergelassene Ärzte

Ab Mai 2018 steigen die rechtlichen Ansprüche und damit der tatsächlich zu leistende Aufwand für den Datenschutz in Unternehmen, in Verbänden und auch in den niedergelassenen Praxen. Die Rechtslage wird zudem komplizierter.
Alle Arztpraxen müssen sich 2018 eingehend mit dem Thema Datenschutz auseinandersetzen und klären, ob und welche neuen Verpflichtungen auf sie zukommen. Hintergrund ist der Ersatz der seit 1995 geltenden EU-Datenschutz-Richtlinie und des „alten" noch bis 24. Mai 2018 geltenden Bundesdatenschutzgesetzes durch neue Vorschriften. Ziel ist die weitere Vereinheitlichung des Datenschutzrechts in den Mitgliedstaaten.

Dr. Michael Stehr

Die rechtlichen Grundlagen

In Deutschland gelten **ab 25. Mai 2018** die Datenschutzgrundverordnung der Europäischen Union (**EU-DSGVO**) in direkter Anwendung und das neue Bundesdatenschutzgesetz (**BDSG-neu**). Das BDSG-neu setzt einerseits die Vorgaben der EU-Richtlinie 2016-680 (RL(EU)2016/680) um, andererseits wird die EU-DSGVO in einigen Punkten konkretisiert. An anderen Stellen wurden vom Bundesgesetzgeber Öffnungsklauseln genutzt – hiervon sind auch die **§§ 22 und 38 BDSG-neu** betroffen, die zentrale Bedeutung haben für die nachfolgenden Ausführungen. Dies führt zu Unübersichtlichkeit und erwartbar nicht ganz leichter Handhabung der rechtlichen Grundlagen. Auf die Gerichte kommt sicher Arbeit zu.

Das BDSG-neu gilt ergänzend zur EU-DSGVO, es hat gegenüber dem bis 24. Mai 2018 geltenden BDSG-alt deshalb eine vollkommen neu geordnete Struktur.

Ab 25.05.2018 sind alle Unternehmer (auch Arztpraxen) gesetzlich verpflichtet, die EU-DSGVO und das BDSG-neu (Teile 1 und 2) umzusetzen.

Was sind Daten und wen betreffen die neuen Regeln?

Die EU-DSGVO und das BDSG enthalten Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten. Sie schützen die Grundrechte natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten. Sie schützen damit den Anspruch auf Privatsphäre, die Autonomie gegenüber Staat und anderen Personen sowie die Handlungsfreiheit der Person – und damit unverzichtbare Voraussetzungen jedes freiheitlich-demokratischen Gemeinwesens.

Die EU-DSGVO ist die vorrangige Rechtsquelle. Sie findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters innerhalb der EU erfolgt, unabhängig davon, ob die Datenverarbeitung selbst in der Union stattfindet.

Zur Einführung einige **zentrale Begriffsbestimmungen** des Artikels 4 EU-DSGVO, die verdeutlichen, weshalb stationäre Einrichtungen und niedergelassene Ärzte prüfen müssen, ob und wie sie sich zum Thema Datenschutz verhalten sollen:

- **„Personenbezogene Daten"**
  sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. **Hierzu gehören Patientendaten, also Name, Adresse, Geburtsdatum, Versichertenstatus usw.;**

- **„Gesundheitsdaten"**
  sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Dies sind **Anamnesedaten,**

Diagnosen, Indikationsstellungen, Ergebnisse aus Labor, bildgebenden Verfahren pp. und Behandlungsentscheidungen, Verordnungen usw.. Man kann also ohne weiteres feststellen, dass Ärzte mit den persönlichsten und sensibelsten Arten von Informationen über Personen umgehen.

- **„Verarbeitung von Daten“**
  meint jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. **Die Verarbeitung von Daten in der Arztpraxis beginnt schon beim Anlegen der Stammdaten des Patienten. Sie setzt sich fort über das Einpflegen aktueller Diagnosen, Behandlungsentscheidungen, Verordnungen usw.**

- **„Dateisystem“**
  bezeichnet jede **strukturierte Sammlung personenbezogener Daten**, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. In jeder Praxis-EDV werden Daten systematisch erfasst und gegliedert. Auch eine systematisch geführte Karteikartensammlung kann schon als System in diesem Sinne betrachtet werden.

- **„Unternehmen“**
  ist eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen. **Auch der freiberuflich in eigener Praxis tätige Arzt ist Unternehmen in diesem Sinne!**

- **„Verantwortlicher“**
  ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. In der Regel ist das „Unternehmen“ selbst – **also auch der in eigener Praxis tätige Arzt** – verantwortlich, weil er über die Datenverarbeitung in der Praxis entscheidet.

- **„Auftragsverarbeiter“**
  ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Hierzu gehören z.B. die **privatärztlichen Verrechnungsstellen**, die vom Arzt abrechnungsrelevante Daten erhalten.

- **„Verletzung des Schutzes personenbezogener Daten“**
  ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.
  Daten dürfen nur von berechtigten Stellen oder Personen im Unternehmen eingesehen werden. Es gibt viele Möglichkeiten der Verletzung des Anspruchs der Betroffenen auf Schutz ihrer Daten. Schutzverletzungen können sowohl durch Mitarbeiter des Verantwortlichen, des Auftragsverarbeiters als auch durch unbefugte Dritte geschehen. Verletzungen können durch Bußgelder oder im Wege der Strafverfolgung geahndet werden.

Wie sieht Datenschutz aus? Welche Vorkehrungen müssen getroffen werden?

Was muss also getan werden zum Datenschutz? Maßnahmen sind in kurzem abstraktem Überblick u.a.:

- Definition und Umsetzung von **unternehmensinternen Datenschutzrichtlinien**, von Datenschutzkonzept und Datenschutzmanagementsystem,
- Gestaltung der **technischen und organisatorischen Maßnahmen** zur Einhaltung der Datenschutzvorschriften,
- **Datenschutzkonforme Gestaltung von Datenflüssen** im Unternehmen und zu externen Partnern,
- **Erstellen und Aktualisieren eines Verfahrensverzeichnisse** bzw. eines Verzeichnisses über die Datenverarbeitungstätigkeiten,
- **Überwachung der Einhaltung der rechtlichen Vorgaben** durch Mitarbeiter und EDV,
- **Überwachung der externen Partner**, sofern diese Daten aus dem Unternehmen erhalten.

Diese Maßnahmen erfordern **Fachkenntnisse hinsichtlich der EDV und des Datenschutzrechts**. Diese Fachkenntnisse müssen aufgrund der Rechtsentwicklung und des technischen Fortschritt stetig aktualisiert werden.

Wer „macht“ Datenschutz? – Brauchen Ärzte einen Datenschutzbeauftragten?

Daten werden im Unternehmen durch interne Verfahrensvorgaben und Dienstvorschriften geschützt. Diese Vorkehrungen sind **schriftlich** festzuhalten. Die **Landesdatenschutzbeauftragten als Aufsichtsbehörde** können jederzeit Einblick in die Schutzvorkehrungen verlangen.

Aus den vorhergehenden Ausführungen folgt, dass der Unternehmer den Datenschutz verantwortet. Folglich ist der Inhaber eines Unternehmens verpflichtet, den Datenschutz selbst und in eigener Person zu organisieren. Radio Eriwan kennt dazu den passenden Kommentar: Im Prinzip ja, aber …

Denn die Vorschriften verlangen für viele Fallkonstellationen die **Benennung eines „vom Chef unabhängigen“ Datenschutzbeauftragten**. Dieser muss **spezifische Qualifikationen** nachweisen und soll die Maßnahmen des Datenschutzes im Unternehmen überwachen. Er ist dann auch erster Ansprechpartner der Aufsichtsbehörde, wenn es um Aspekte des Datenschutzes im Unternehmen geht. Eine Pflicht zur Benennung eines DSB kann erwachsen aus der Anzahl der Mitarbeiter des Unternehmens, die mit den Daten ständig arbeiten (5.1.) oder aus Art und Umfang der im Unternehmen verarbeiteten Daten (5.2.).

Ab zehn Mitarbeiter: Datenschutzbeauftragter (DSB) ist Pflicht

Nach **§ 38 Abs. 1 BDSG** führt die Handhabung von Daten zur Pflicht der Benennung eines Datenschutzbeauftragten, **wenn mindestens zehn Mitarbeiter** ständig mit der automatisierten Verarbeitung von Daten zu tun haben, also etwa Patientendaten in der Praxis-EDV lesen oder verändern – dies dürfte regelmäßig alle angestellten Ärzte und alle MFAs betreffen. Praxisinhaber werden nicht mitgerechnet und es kommt nur auf die Mitarbeiterzahl an, nicht auf Vollzeitäquivalente wie im Arbeitsrecht.

Kleinere Praxen – was tun?

EU-Recht: für Arztpraxen ist DSB fast immer Pflicht

Nach **Art. 37 Abs. 1 EU-DSGVO** ist durch den Verantwortlichen oder den Auftragsverarbeiter ein Datenschutzbeauftragter zu benennen,

- wenn … die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, … welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, … oder …
- in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 besteht.

Zwei Kriterien müssen erfüllt sein:

- Datenverarbeitung gehört zu den Kerntätigkeiten und
- Art und Umfang der Daten machen eine Überwachung der tätigen Personen notwendig.

Zunächst wird sicher jeder Arzt bestätigen, dass seine Kerntätigkeit in der Behandlung von Patienten besteht und die Datenverarbeitung lediglich ein notwendiges Beiwerk darstellt. Im Sinne des Rechts ist die Sache jedoch anders zu beurteilen.

Die Ende 2016 veröffentlichte Stellungnahme der Artikel 29 Gruppe enthält erste Klarstellungen zur „**Kerntätigkeit**" i.S.d. Art. 37 Abs. 1 b DSGVO. Im Zusammenhang mit Erwägungsgrund 97, ist hierunter **jede Tätigkeit** zu verstehen, **die essentiell für die Erreichung der Ziele des Unternehmens ist**. Als Beispiel wird ausdrücklich die Verarbeitung von Gesundheitsdaten genannt, deren Handhabung zur Erreichung des Zwecks einer Klinik unverzichtbar ist.

Dieser Gedankengang ist auch auf die niedergelassenen Ärzte in der ambulanten Versorgung anzuwenden.

Zweitens sind nach Art. 37 Abs. 1 c iVm. Art. 9 Abs. 1, Abs. 2 lit. h EU-DSGVO **Gesundheitsdaten besondere Arten von Daten**, die die Bestellung eines Datenschutzbeauftragten dann zur Pflicht machen, wenn eine „umfangreiche Verarbeitung" dieser Daten erfolgt (vgl. auch Erwägungsgrund Nr. 53 zu Art. 9 EU-DSGVO). Das ist leicht nachvollziehbar, denn Gesundheitsdaten stellen schon aufgrund ihrer aus Sicht der betroffenen Patienten gegebenen Sensibilität eine besondere Art von Daten dar, die dann eine Überwachung von mit den Daten befassten Personen rechtfertigt, wenn viele Patienten betroffen sind.

Aber was ist in diesem Sinne „umfangreich"? Hierzu äußert sich die EU-DSGVO nicht selbst, im Erwägungsgrund Nr. 91 heißt es aber: „Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten … betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes … erfolgt." Die Erwägungsgründe sind Auslegungshilfen.

Eine Praxis, die von einem Arzt mit einer MFA betrieben wird, ist als klein in diesem Sinne anzusehen. Die schwache Formulierung „sollte" lässt den Behörden die Option, auch kleinen Praxen die Benennung eines DSB aufzuerlegen. Was gilt für einen Arzt, der fünf MFA beschäftigt? Hier muss man aufgrund der besonderen Sensibilität von Gesundheitsdaten wohl von einer Pflicht zur Benennung eines DSB ausgehen.

Diese nur bedingt übersichtliche Rechtsanordnung wird vom deutschen Recht in ihrer Unklarheit noch übertroffen. Die Bundesrepublik macht Gebrauch von den Gestaltungsmöglichkeiten, die die EU-DSGVO den Nationalstaaten lässt. Das deutsche Recht findet solange Anwendung, wie es den von der EU gelassenen Gestaltungsspielräumen entspricht, das ist für die nachfolgenden Ausführungen gegeben.

Deutsches Recht: für Arztpraxen ist DSB Option

§ 22 Abs. 1 BDSG erlaubt die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 durch nichtöffentliche Stellen (= Unternehmen),

- wenn sie zum Zweck der **Gesundheitsvorsorge**,
- für die **Beurteilung der Arbeitsfähigkeit** des Beschäftigten,
- für die **medizinische Diagnostik**, die **Versorgung oder Behandlung im Gesundheits- oder Sozialbereich,**
- für die **Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich**,
- oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist,

und diese Daten von **ärztlichem Personal** oder durch **sonstige Personen**, die einer **entsprechenden Geheimhaltungspflicht unterliegen,** oder unter deren Verantwortung verarbeitet werden.

§ 22 Abs. 2 BDSG schreibt sodann vor, dass „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen" sind. Weiter heißt es:

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

- technisch organisatorische Maßnahmen um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
- Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
- Benennung einer oder eines Datenschutzbeauftragten,
- Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
- Pseudonymisierung personenbezogener Daten,
- Verschlüsselung personenbezogener Daten,

- Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen …"

Dass zum Datenschutz Maßnahmen ergriffen werden müssen, ist also Pflicht. In der Auflistung von Maßnahmen ist jedoch die Benennung eines DSB nur eine unter verschiedenen Optionen, die in Erwägung gezogen werden müssen. Leider bringt auch die Begründung zum Gesetzentwurf BDSG-neu (BT-Drs 18/11325) kein Licht ins Dunkel, unter welchen Umständen ein Datenschutzbeauftragter gebraucht wird, die Auslegung wird den Datenschutzbehörden und der Gerichtsbarkeit überlassen:

„Absatz 2 Satz 1 und 2 setzt das Erfordernis aus Artikel 9 Absatz 2 Buchstabe b, g und i der Verordnung (EU) 2016/679 um, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person" bzw. „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" vorzusehen. Die in Absatz 2 Satz 2 aufgeführten Maßnahmen treffen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet."

Kurz zusammengefasst: Die Benennung eines Datenschutzbeauftragten ist für Unternehmen mit weniger als 10 Mitarbeitern, die Gesundheitsdaten verarbeiten, in Deutschland nur eine „Wahlpflicht" auf Basis einer Pflicht zur Ergreifung von Maßnahmen aus einem Optionenkatalog. Man kann auch andere Maßnahmen ergreifen. Die Auswahl der Maßnahmen darf jedoch nicht willkürlich gehandhabt werden. Das Unternehmen muss vielmehr abwägen, welche Optionen angesichts der Qualität und der Mengen der Daten unter Berücksichtigung von Risiken, Aufwand und Kosten ergriffen werden müssen. Die zur Verfügung stehenden Optionen sind im § 22 lediglich beispielhaft und nicht abschließend abgebildet. Erst die Rechtsprechung wird hier zu einer Konkretisierung kommen und damit die für alle Anwender notwendige Rechtssicherheit erzeugen.

Ein praktischer Hinweis: Angesichts der Komplexität des Themas, der Notwendigkeit spezifischer Fachkenntnisse zur richtigen Anwendung des Datenschutzes und der Risiken hinsichtlich Bußgeld und Strafverfolgung **ist zu empfehlen, dass Arztpraxen einen Datenschutzbeauftragten benennen**.

Wo bekommt man den Datenschutzbeauftragten her?

Die Vorschriften erlauben die Benennung eines angestellten Mitarbeiters oder eines externen Sachkundigen. Zur **internen Besetzung des DSB** kann man **in kleinen und mittleren Unternehmen nicht raten**, denn der interne DSB investiert Arbeitsstunden, die ihm anderswo fehlen, und er muss regelmäßig auf Kosten des Praxisinhabers Schulungen absolvieren. Zudem genießt er **besonderen Kündigungsschutz** noch ein Jahr über seine Amtszeit hinaus. Außerdem wird sein Verhältnis zum Chef nach neuem Recht spannungsreicher: nach altem Recht hatte der DSB auf Einhaltung des Datenschutzes hinzuwirken, ab dem 25. Mai 2018 muss der DSB den Datenschutz überwachen.

Besser ist es also, einen DSB extern zu beauftragen, auch wenn dies Kosten verursacht. Ein externer DSB kann auch Nebennutzen erzeugen, z.B. durch Überarbeitung der Datenmanagement-Verfahren, hier seien vor allem die Stichworte Datensparsamkeit und Einbindung möglichst weniger Personen in einen Prozess angeführt.

Zusammenfassung

Müssen Arztpraxen einen DSB benennen? **Ab 10 Mitarbeitern in jedem Falle**. Bei weniger Mitarbeitern nur dann, wenn andere von den Vorschriften vorgesehene Maßnahmen nicht hinreichend sind. Zu empfehlen ist die Benennung eines DSB auch kleineren Praxen, denn die Organisation des Datenschutzes in der Praxis erfordert nicht unerhebliche EDV- und Rechtskenntnisse.

Am Markt agieren viele mittlere und größere Dienstleister, aber auch Rechtsanwaltskanzleien als Anbieter von Leistungen im Datenschutz. Die BVKJ-Service GmbH sondiert derzeit am Markt, ob bundesweit tätige Anbieter gefunden werden können, die in der Lage sind, einer Vielzahl von Praxen standardisierte Lösungen im Rahmen einer Benennung als Datenschutzbeauftragte anzubieten.

Korrespondenzanschrift:
Dr. jur. Michael Stehr
Geschäftsführer, 51069 Köln
E-Mail: michael.stehr@uminfo.de

Red.: WH