RECHT 01.05.2018

Keine Angst vor dem bösen „Wolf“

Die neue EU-Datenschutz-Grundverordnung in Klinik und ärztlicher Praxis

Die EU-Datenschutz-Grundverordnung (DS-GVO) wirft ihre Schatten voraus. Zahlreiche Verlautbarungen haben bereits vor dem Inkrafttreten zu großen Verunsicherungen, zum Teil aber auch zu völlig übertriebenem Aktionismus geführt. Richtig ist allein, dass die EU-Datenschutz-Grundverordnung am 25.05.2018 ohne Übergangsregelungen in Kraft treten wird. Die damit einhergehenden Bestimmungen werden zudem zu umfassenden Neuerungen beim Umgang mit personenbezogenen Daten – auch in der ärztlichen Praxis – führen. Angst oder übertriebenen Aktionismus müssen die Neuregelungen aber nicht auslösen. Die wichtigsten Fragen und Antworten erläutern wir im Überblick:

1. Worum geht es, was regelt die DS-GVO?

Die DS-GVO dient dem Schutz natürlicher Personen bei der Verarbeitung und Nutzung ihrer personenbezogenen Daten und sichert gleichzeitig den freien Verkehr dieser Daten. Dadurch wird eine EU-weite Harmonisierung des Datenschutzrechtes erreicht. Erfasst werden der manuelle und der automatisierte Umgang mit personenbezogenen Daten Einzelner. Dabei genügt es schon, wenn der Betroffene mittelbar (beispielsweise durch eine Kennziffer) bestimmbar ist. So ist nicht nur der einzelne Patient „Betroffener“ im Sinne der DS-GVO; erfasst werden insbesondere auch Daten von Probanden in Studien, die anhand der erhobenen Daten, einer Kennziffer o.ä. identifizierbar sind. Daher ist die DS-GVO in nahezu jedem ärztlichen Betätigungsfeld relevant. Die gesetzlichen Bestimmungen zum Umgang mit personenbezogenen Daten gelten aber auch nach innen, also z.B. für angestellte ärztliche und nicht ärztliche Mitarbeiter in Arztpraxen und Kliniken oder auch im Zusammenhang mit medizinischen Register- oder Zertifizierungsverfahren. Wirklich wesentliche Abweichungen zum Schutzzweck des bisher und auch zukünftig geltenden Bundesdatenschutzgesetztes (BDSG) bestehen aber nicht.

2. Was sind Daten, welche Daten sind betroffen?

Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“. Der Begriff der Informationen ist dabei umfassend und betrifft sämtliche Informationen zu einer Person. Die geschützte Person wird im Datenschutzrecht als „Betroffener“ bezeichnet. Gesundheitsbezogene Daten sind die in der Klinik oder ärztlichen Praxis notwendigerweise von Patienten erhobenen Daten, die – wie bisher – einen besonderen Schutz genießen. Gesundheitsdaten sind definitionsgemäß 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.

Zu den von der DS-GVO geschützten Daten gehören aber auch alle Daten von Personen, die im Klinikbetrieb oder einer Arztpraxis selbst beschäftigt sind. Ausgenommen von den datenschutzrechtlichen Regelungen sind – wie bisher – vollständig anonymisierte Daten, bei denen ein Personenbezug sicher ausgeschlossen werden kann. Studien und andere Forschungsvorhaben, die sich ausschließlich auf vollständig anonymisierte Patientendaten stützen, unterfallen daher nicht den datenschutzrechtlichen Regelungen der DS-GVO und des BDSG.

3. Wer unterfällt den Regelungen der DS-GVO?

Ärzte sind ständig mit personenbezogenen Daten Einzelner in Kontakt und verarbeiten diese. Sie erheben, speichern und verwenden Patientendaten und müssen diese nach Ablauf der gesetzlichen Aufbewahrungspflicht löschen. Die DS-GVO ist daher in ausnahmslos jeder Arztpraxis, in jeder klinischen Einrichtung und in jedem medizinischen Forschungslabor zu beachten, unabhängig von der Anzahl der Mitarbeiter, des Umsatzvolumens, der Anzahl der Patienten oder dem Zweck der Verwendung personenbezogener Daten.

4. Wann und unter welchen Voraussetzungen ist die Datenverarbeitung zulässig?

Voraussetzung für die Verarbeitung personenbezogener Daten ist stets, dass die betroffene Person hierin eingewilligt hat oder – wenn eine Einwilligung nicht vorliegt oder nicht eingeholt werden kann – dies zur Erfüllung vertraglicher Pflichten (Behandlungsvertrag) oder aufgrund einer Rechtspflicht (Hilfeleistung in Notfällen) geschieht. Auch die personenbezogenen Daten eines bewusstlos eingelieferten Patienten dürfen selbstverständlich – wie bisher – verarbeitet werden, da dies erforderlich ist, um lebenswichtige Interessen des Patienten zu schützen.

Natürlich ist auch die Erfassung und Verarbeitung personenbezogener Daten im gesamten Personalwesen nach den Neuregelungen der DS-GVO und des BDSG nach wie vor zulässig. Zur Auszahlung des Gehalts und zur Erstellung eines Arbeits- oder Weiterbildungszeugnisses müssen die personenbezogenen Daten vom jeweiligen Arbeitgeber genutzt werden können.

5. Welche Verpflichtungen ergeben sich aus der DS-GVO und dem BDSG?

Art. 5 der DS-GVO regelt die allgemeinen Grundsätze für die Verarbeitung von personenbezogenen Daten. Insbesondere gelten die Grundsätze der Rechtmäßigkeit der Erhebung, der Zweckbindung, der Datenminimierung, der Speicherbegrenzung, der Vertraulichkeit und der Rechenschaftspflicht. Personenbezogene Daten dürfen demnach nur auf rechtmäßige Weise und für einen bestimmten definierten Zweck erhoben und verarbeitet werden. Dabei ist stets nur das für die Zweckerreichung erforderliche Minimum an Daten über den kürzest-möglichen Zeitraum zu verarbeiten. Selbstverständlich sind die Daten vor dem unbefugten Zugriff Dritter zu schützen. Die betroffenen Personen sind über die Datenverarbeitung umfassend zu informieren.

Mit der Erhebung und Verarbeitung personenbezogener Daten gehen umfassende Auskunftsansprüche der Betroffenen einher. Daher hat der für die Datenverarbeitung Verantwortliche (Praxisinhaber, Klinikgeschäftsführung, Wissenschaftler) alle Maßnahmen zu treffen, welche die Einhaltung der gesetzlichen Bestimmungen erst ermöglichen. Zudem muss er im Falle eines Auskunftsersuchens des Betroffenen alle Informationen in präziser und leicht verständlicher Form zur Verfügung stellen zu können. Dazu zählt etwa auch eine umfangreiche Dokumentation über die Verarbeitungstätigkeiten mittels eines Verfahrensverzeichnisses. So soll erreicht werden, dass die betroffenen Personen überhaupt in die Lage versetzt werden, die ihnen zustehenden Rechte wahrzunehmen.

Im Übrigen treffen den Verantwortlichen verschiedene Melde- und Mitteilungspflichten gegenüber dem Betroffenen oder der Aufsichtsbehörden. So muss jeder, der personenbezogene Daten verarbeitet, die ihm bekannt werdenden Verletzungen des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde (Landesdatenschutzbeauftragter) und dem von der Verletzung Betroffenen melden.

In bestimmten Fällen ist die Benennung eines eigenen Datenschutzbeauftragten vorgeschrieben. Dies betrifft insbesondere Betriebe (Praxen), in denen sich mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Dabei werden alle Personen unabhängig von ihrer Arbeitszeit mitgezählt, die Zugriff auf die Daten haben, also neben den Praxisinhabern insbesondere auch medizinisches Fachpersonal, nicht aber z.B. Reinigungspersonal. Zum Datenschutzbeauftragten kann ein Beschäftigter des Praxisinhabers bestellt werden; ein Datenschutzbeauftragter kann aber auch extern auf der Grundlage eines entsprechenden Dienstleistungsvertrages bestellt werden. Der oder die Praxisinhaber selbst kommen für die Tätigkeit des Datenschutzbeauftragten nicht in Betracht. Wer letztlich zum Datenschutzbeauftragten bestellt worden ist, muss der zuständigen Aufsichtsbehörde (in NRW z.B. der Landesbeauftragte für Datenschutz und Informationsfreiheit) benannt werden. Hierzu werden derzeit automatisierte, internetbasierte Meldeverfahren entwickelt. Die Aufgaben des Datenschutzbeauftragten bestehen in erster Linie in einer Beratung des Verantwortlichen für die Datenverarbeitung (Praxisinhaber, Klinikgeschäftsführung), der Überwachung der Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und dem Kontakt zur zuständigen Aufsichtsbehörde.

Werden personenbezogene Daten an Dritte – z.B. externe Dienstleister (Privatärztliche Abrechnungsstellen, Softwarewartung, Labore, Cloudsyteme etc.) – weitergegeben, ist besondere Vorsicht geboten. Hierbei kann es sich um eine einfache Übermittlung, eine eigene oder gemeinsame Verantwortlichkeit oder um eine Datenverarbeitung im Auftrag handeln. Dritte können auf diese Weise grundsätzlich in die Datenverarbeitung wirksam und rechtmäßig einbezogen werden. Hier bestehen jedoch jeweils besondere Voraussetzungen und Überwachungspflichten, die gegebenenfalls eine Vertragsanpassung für die Zusammenarbeit mit solchen externen Dienstleistern erfordern. Die Weitergabe geschützter, der Geheimhaltung unterliegender personenbezogener Daten an solche externen Dienstleistungsunternehmen ist auch mit der gesetzlichen Ergänzung in § 203 StGB vereinfacht worden.

6. Welche Rechte haben die Betroffenen?

Wo die DS-GVO einerseits umfassende Pflichten auferlegt, werden den betroffenen Personen umgekehrt umfassende Rechte und Ansprüche zugeordnet. So können die Betroffenen die Datenverarbeitung einschränken, die Übertragung veranlassen, fehlerhafte Daten berichtigen und auch vollständig löschen lassen. Selbstverständlich muss aber insbesondere die Datenlöschung auch mit den gesetzlichen und standesrechtlichen Aufbewahrungspflichten in Einklang stehen, sodass sich hier an den im ärztlichen Bereich geltenden Aufbewahrungspflichten keine Änderungen ergeben. Und natürlich haben die Betroffenen das Recht auf Auskunft und Information (s.o.) binnen eines Monats ab Antragstellung.

7. Welche Sanktionen drohen bei Verstößen?

Verstöße gegen die Verpflichtungen aus der DS-GVO und dem BDSG können mit empfindlichen Sanktionen geahndet werden. Es steht den betroffenen Personen dabei auch frei, Verstöße an die Aufsichtsbehörden zu melden, es drohen dabei Geldbußen und ggf. die Verpflichtung zur Entrichtung von Schadensersatz. Ordnungsrechtliche Verstöße gegen die Bestimmungen der DS-GVO und des BDSG werden in der Regel mit Geldbußen geahndet; dabei bemisst sich die Höhe der festgesetzten Bußgelder danach, mit welcher Nachhaltigkeit gegen gesetzliche Bestimmungen oder Auflagen der Aufsichtsbehörde verstoßen wird oder auch danach, ob es sich um einen Erstfall oder um eine wiederholte Ordnungswidrigkeit handelt. In besonders schweren Fällen kann ein gesetzlicher Verstoß auch als Straftat gewertet werden, die Freiheitsstrafen oder Geldstrafen nach sich ziehen können. Allerdings werden die Aufsichts- bzw. Ordnungsbehörden angesichts der Vielzahl der nun zu beachtenden Neuregelungen anfangs sehr zurückhaltend mit der Höhe der festgesetzten Bußgelder sein. Die Ausrede, man habe von den Neuregelungen und den damit einhergehenden Verpflichtungen nichts gewusst, hilft aber auch hier nicht, da auch hier der Grundsatz gilt: „Nichtwissen schützt vor Strafe nicht“.

8. Was ist jetzt von Praxisinhabern und Klinikgeschäftsführungen zu tun?

a) Ermitteln Sie Ihren datenschutzrechtlichen Status-quo

Zunächst einmal sollten Sie Ihren datenschutzrechtlichen Status-quo ermitteln, dies erleichtert die Umsetzung des neuen Rechts. Klären Sie, um welche Daten es sich handelt (Patientendaten sind beispielsweise besonders schützenswerte Daten nach Art. 9 DS-GVO) und wie diese verarbeitet werden. In der Regel geschieht dies elektronisch unter Einsatz entsprechender Software. Auch wer Zugriff auf die Daten hat und an wen diese ggf. aufgrund von Verträgen weitergegeben werden, ist relevant. Die Sicherheit der Daten vor dem unbefugten Zugriff Dritter muss stets gewährleistet sein. Prüfen Sie zudem, ob Sie zu einer Datenschutzfolgenabschätzung (Art. 35 DS-GVO) verpflichtet sind.

b) Erstellen Sie ein Datenverarbeitungsverzeichnis

Sämtliche Datenverarbeitungen sind in einem entsprechenden Verzeichnis festzuhalten. Hierbei sind alle in Art. 30 DS-GVO aufgeführten anfallenden Verarbeitungsprozesse und Informationen zu dokumentieren. Das Führen eines solchen Verzeichnisses ist verpflichtend. Es ist schriftlich oder in elektronischer Form zu führen. Es empfiehlt sich daher, eine entsprechende Tabelle anzulegen oder geeignete Software zu verwenden.

In dem Verzeichnis sind folgende Informationen aufzulisten:

- Name und Kontaktdaten des/der Verantwortlichen (z.B. Praxisinhaber) und (sofern notwendig) des Datenschutzbeauftragten;
- Die Zwecke der Datenverarbeitung (z.B. Krankenbehandlung, Abrechnung erbrachter Leistungen, etc.):
- Angaben zu den Kategorien der betroffenen Personen (z.B. Patienten) und der Kategorie personenbezogener Daten (z.B. Stammdaten, Gesundheitsdaten wie Laborbefunde, Diagnosen etc.);
- Die Kategorien von Empfängern mit/ohne Auslandsbezug, die in Kontakt mit den Daten kommen (z.B. eine Verrechnungsstelle, Labore, Krankenversicherungen, weiterbehandelnde Ärzte/Krankenhäuser, IT-Dienstleister, etc.);
- Löschfristen der Daten (unter Beachtung der gesetzlichen Aufbewahrungsfristen);
- Beschreibung der technischen/organisatorischen Maßnahmen, die zur Sicherheit der Daten ergriffen wurden (z.B. Verschlüsselung).

c) Prüfen und ggf. aktualisieren Sie Ihre Dienstleitungsverträge mit Dritten

Wenn Sie Dritten Zugriff auf die Ihnen vorliegenden Daten gewähren bzw. diese weiterleiten, sind die entsprechenden Verträge mit den Dritten anzupassen. Hierbei kann es sich beispielsweise um private Abrechnungsdienstleister oder Ihren IT-Dienstleister handeln. Je nach Ausgestaltung des Rechtsverhältnisses ist der Dritte Ihnen gegenüber weisungsgebunden oder er selbst wird zum Verantwortlichen, wenn er die Daten in eigenem Interesse und zu eigenen Geschäftszwecken nutzt.

Auch als sogenannte Auftragsverarbeiter (Art. 28 DS-GVO) sind Dritte ebenfalls zur Einhaltung des Datenschutzes verpflichtet. Durch entsprechende vertragliche Vereinbarungen – und Kontrollen – haben Sie sicherzustellen, dass der Dritte diese Regelungen einhält.

Sprechen Sie also Ihre Vertragspartner auf den Datenschutz an und fordern Sie, entsprechende Datenschutzerklärungen in die Verträge aufzunehmen bzw. bestehende Vereinbarungen an die neue Rechtslage anzupassen. Kann Ihr Vertragspartner einen hinreichenden Datenschutz nicht gewährleisten bzw. haben Sie berechtige Zweifel an der ordnungsgemäßen Umsetzung, sollten Sie das Festhalten an dem Dienstleistungsvertrag grundsätzlich überdenken und ggf. zu einem anderen Anbieter wechseln.

Der schriftliche Vertrag zur Auftragsdatenverarbeitung sollte dabei mindestens folgende Punkte beinhalten:

- Eine Garantie des Dritten zur Einhaltung des gesetzlichen Datenschutzes inkl. Verschwiegenheitsverpflichtung aller Beteiligter (auch Mitarbeiter);
- Ihre allgemeine Genehmigung, dass der Dritte selbst weitere Auftragsverarbeiter beauftragen darf. Im Falle eines Wechsels des weiteren Auftragsverarbeitenden steht Ihnen ein Einspruch zu. Oder: Der Dritte holt immer vor Beauftragung eines weiteren Auftragsdatenverarbeitenden Ihre schriftliche Genehmigung hierzu ein. Der Vertrag zwischen dem Dritten und dem weiteren Auftragsdatenverarbeiter muss ebenfalls eine Verpflichtung nach den datenschutzrechtlichen Regelungen enthalten;
- Der Dritte verpflichtet sich, geeignete Maßnahmen zur Sicherheit der Daten gemäß Art. 32 DS-GVO zu treffen;
- Der Dritte verpflichtet sich, Sie bei der Einhaltung der datenschutzrechtlichen Pflichten zu unterstützen und erforderliche Informationen unverzüglich zur Verfügung zu stellen;
- Der Dritte verpflichtet sich, nach Abschluss seiner jeweiligen Leistungserbringung (unter Wahrung von gesetzlichen Aufbewahrungspflichten) die Daten zu löschen oder zurückzugeben;
- Der Dritte erbringt Nachweise Ihnen gegenüber, dass er die Regelungen des Datenschutzes einhält. Zudem ist er verpflichtet, Überprüfungen durch Sie oder einen von Ihnen beauftragten Prüfer zu ermöglichen und

hieran mitzuwirken. Der Dritte ist zudem verpflichtet, Sie unverzüglich zu informieren, sofern er eine erteilte Weisung für datenschutzrechtlich rechtswidrig hält.

Je nach vertraglicher Ausgestaltung kann es auch vorkommen, dass sowohl Sie als auch Ihr Vertragspartner „gemeinsam Verantwortliche“ im Sinne des Datenschutzrechts sind. In diesem Fall sollten Sie vertraglich regeln, wer datenschutzrechtlich im Einzelnen für welche Aspekte verantwortlich ist und welche Pflichten gegenüber der betroffenen Person (Patient) er jeweils übernimmt.

d) Bestellen Sie ggf. einen Datenschutzbeauftragten

Wenn sich bei Ihnen mindestens zehn Personen (Sie eingeschlossen) mit der Verarbeitung personenbezogener Daten beschäftigen, sind Sie verpflichtet, einen Datenschutzbeauftragten zu ernennen. Dies kann einer Ihrer Mitarbeiter sein oder ein externer Dienstleister. Ihnen – dem Verantwortlichen – ist es nicht erlaubt, selbst Datenschutzbeauftragter im eigenen Betrieb zu sein. Übernimmt ein Mitarbeiter diese Position, ist er natürlich entsprechend zu schulen.

e) Informieren Sie Ihre Patienten und Ihr Personal

Die betroffenen Personen (Patienten, eigenes Personal) haben umfassende Auskunftsrechte, denen bereits bei Erhebung der Daten Rechnung zu tragen ist. So können beispielsweise ein entsprechender Aushang in der Arztpraxis oder der jeweiligen Klinik mit den notwendigen Informationen und die Möglichkeit, hiervon Kopien auszuhändigen, ausreichen. Oder es erfolgt eine postalische Übersendung, z.B. im Falle der Aufnahme eines Mitglieds in einen Verein.

Folgende Informationen sind nach der DS-GVO insbesondere mitzuteilen (aus anderen Vorschriften können sich weitere Informationspflichten ergeben):

- Daten (Namen/Kontakt) des Verantwortlichen und (ggf.) des Datenschutzbeauftragten,
- Informationen zu den Daten,
- Kategorien (z.B. Stammdaten, Sozialversicherungsdaten, Gesundheitsdaten),
- Datenquellen (i.d.R. von dem Betroffenen selbst),
- Zweck der Datenverarbeitung (Krankenbehandlung, Abrechnung, etc.),
- Rechtsgrundlagen für die Verarbeitung (z.B. aufgrund Behandlungsvertrag),
- Dauer der Verarbeitung, Löschfristen,
- Berechtigte Interessen zur Verarbeitung, ggf. von Dritten,
- Mögliche Empfänger/Empfängerkategorien von Daten,
- Bestehen einer automatischen Entscheidungsfindung / Profiling,
- Rechte des Betroffenen
- Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruchsrecht und Widerruf einer Einwilligung (für die Zukunft), Beschwerdemöglichkeit bei der Aufsichtsbehörde

f) Holen Sie ggf. Einwilligungen Ihrer Patienten zur Datenverarbeitung ein

Die Datenverarbeitung durch Sie – und die von Ihnen eingesetzten Dritten – kann zunächst einmal aufgrund gesetzlicher Regelung (z.B. zur Erfüllung des mit dem Betroffenen geschlossenen Behandlungsvertrages) oder aufgrund ausdrücklicher Einwilligung des Betroffenen rechtmäßig erfolgen. Auch vor dem Hintergrund der berufs- und strafrechtlich relevanten ärztlichen Schweigepflicht ist besonderes Augenmerk auf die Einwilligung bei der Verarbeitung und Weitergabe von Patientendaten zu legen.

g) Schulen und Sensibilisieren Sie Ihre Mitarbeiter/innen für den Datenschutz

Ihre Mitarbeiter/innen kommen regelmäßig in Kontakt mit personenbezogenen Daten. Sie sollten sie daher nachhaltig und im eigenen Interesse für datenschutzrechtliche Themen und die Verschwiegenheitspflicht sensibilisieren. Ihre Mitarbeiter sollten auch eine entsprechende Verpflichtungserklärung abgeben. Möglicherweise ist es hilfreich, mithilfe des Datenschutzbeauftragten interne Richtlinien und Handlungsanweisungen zu Wahrung der datenschutzrechtlichen Belange zu entwickeln.

h) Sorgen Sie für Datensicherheit

Sichern Sie die Ihnen vorliegenden Daten vor dem Zugriff Unbefugter. Hierzu gehört in erster Linie ein entsprechend gesichertes EDV-System. Aber auch das Mithören von Gesprächen durch andere Patienten oder durch das Liegenlassen von Akten – beispielsweise am Empfangstresen – ist datenschutzrechtlich unzulässig. Die internen Abläufe sollten auch dahingehend überprüft und nötigenfalls geändert werden.

i) Halten sie sich bereit für Anfragen

Die betroffenen Personen (Patienten, eignes Personal) haben den für die Datenverarbeitung Verantwortlichen (Praxisinhaber, Klinikgeschäftsführungen) gegenüber umfangreiche Auskunftsrechte, denen der Verantwortliche nach Eingang des entsprechenden Antrags binnen eines Monats nachkommen muss. Geht ein solcher Antrag bei Ihnen ein, sollten Sie diesen also umgehend bearbeiten. Durch entsprechende Organisation der Datenverarbeitung im Vorfeld kann sichergestellt werden, dass die Informationen ohne größeren Aufwand zusammengestellt und dem Antragsteller übermittelt werden.

k) Informieren Sie sich über Arbeitshilfen und Informationen im Datenschutz

Die Kassenärztliche Bundesvereinigung und die Bundesärztekammer, aber auch einzelne Landesärztekammern, haben angekündigt, allgemeine Informationen und Arbeitshilfen zur Umsetzung der neuen Datenschutzbestimmungen der DS-GVO und des überarbeiteten BDSG herauszugeben. Im Deutschen Ärzteblatt, Heft 10/2018 vom 09. März 2018, sind die überarbeiteten „Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ veröffentlicht. Beide

Standesorganisationen haben zudem einen „Datenschutz-Check 2018 – Was müssen Arztpraxen angesichts der neuen Vorschriften zum Datenschutz tun?“ herausgegeben. Auch diese Hinweise finden Sie im Deutschen Ärzteblatt vom 09.03.2018, Heft 10/2018. Diese enthalten auch weiterführende Empfehlungen und Muster für das Verzeichnis der Datenverarbeitungstätigkeiten, für die Auftragsdatenverträge und für die Umsetzung von Informationspflichten.

Im Zuge der fortschreitenden Digitalisierung unserer Gesellschaft, gerade im Gesundheitswesen, werden die Anforderungen an den Schutz personenbezogener Daten immer wichtiger. Der richtige Umgang mit personenbezogenen Daten ist daher „Chefsache“. In diesem Sinne müssen sich alle Praxisinhaber und Klinikgeschäftsführungen zwangsläufig mit den Neuregelungen der DS-GVO und des BDSG befassen. Bei näherem Hinsehen und der Umsetzung der geforderten (vertraglichen) Strukturen sind die Hürden nicht so hoch, wie es auf den ersten Blick den Eindruck macht. Guter Datenschutz führt auch zu einer besseren Compliance gegenüber Patienten und eigenem Personal. Nutzen Sie diese Möglichkeiten.

Sailer R, Wienke A: Keine Angst vor dem bösen „Wolf“. Passion Chirurgie. 2018 Mai, 8(05): Artikel 04_7a.