Kassenärztliche Vereinigung Nordrhein

Informationsblätter zum neuen Datenschutzrecht in der ambulanten Versorgung

2. Auflage – Stand 23.11.2018

Erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern unter Mitwirkung der Landesbeauftragten für den Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein, Zahnärztekammer Westfalen-Lippe sowie der Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe

Auftragsverarbeitung

I. Auftragsverarbeitung

Mit dem Geltungsbeginn der Datenschutzgrundverordnung (DSGVO) und dem Inkrafttreten des neuen Bundesdatenschutzgesetzes (BDSG) am 25.05.2018 gelten neue Regelungen auch für die Auftragsverarbeitung (AV). AV ist die Verarbeitung personenbezogener Daten durch einen Dienstleister ausschließlich auf Weisung eines Auftraggebers im Rahmen der diesbezüglichen Zweck- und grundsätzlichen Mittelbestimmung der Datenverarbeitung. Sie findet üblicherweise - aber nicht ausschließlich! - im Zusammenhang mit ausgelagerten unterstützenden, praxisorganisatorischen Tätigkeiten statt, für die der Praxisinhaber nicht nur in Bezug auf die datenschutzrechtlichen Aspekte die grundsätzliche Verantwortung behalten will oder auch aufgrund gesetzlicher Vorgaben behalten muss. Die AV ist daher von einer anderweitigen Übermittlung von Daten an Dritte bzw. einer eigenverantwortlichen Datenverarbeitung durch Dritte - etwa beim Inkasso - abzugrenzen. Relevanz für die Praxis hat die AV besonders bei der Einschaltung externer Dienstleister etwa in den Bereichen Honorarabrechnung, Terminvergabe, Marketing, EDV (z.B. Systembetreuung/-wartung, Vernichtung von Datenträgern, "Cloud-Computing"), Lohnabrechnung etc.

Die Annahme eines datenschutzrechtlichen Auftragsverarbeitungsverhältnisses stellt kein Urteil über die fachliche Wertigkeit der Tätigkeit des Auftragnehmers in ihrer Gesamtheit dar, sondern regelt ausschließlich den Aspekt der Verarbeitung personenbezogener Daten aufgrund der gesetzlich definierten datenschutzrechtlichen Verantwortlichkeit.

Ob eine Auftragsverarbeitung vorliegt, entscheidet sich zukünftig anhand der Frage, wer über die Zwecke und grundsätzlichen Mittel der Datenverarbeitung entscheidet und damit Verantwortlicher für die Daten im Sinne des Art. 4 Nr. 7 DSGVO ist. Der Anwendungsbereich der Auftragsverarbeitung ist damit künftig ausgeweitet, weil der Auftragnehmer auch über technisch-organisatorische Maßnahmen selbst entscheiden kann, ohne dass deshalb die Auftragsverarbeitung ausgeschlossen wäre (siehe hierzu Kurzpapier 13 der unabhängigen Datenschutzbehörden des Bundes und der Länder[1]). Für Auftraggeber einer AV führt dies nicht zu grundlegenden Änderungen, weil ihre Obliegen-heiten als datenschutzrechtlich Verantwortliche weitestgehend dem bisherigen § 11 BDSG entsprechen. Die Auftragnehmer werden dagegen deutlich stärker in die Pflicht genommen.

In Einzelfällen kann allerdings die strukturelle Änderung der Auftragsverarbeitung dazu führen, dass Datenübermittlungsvorgänge, die bisher als „Funktionsübertragung“ gewertet wurden, jetzt als Auftragsverarbeitung eingeordnet werden müssen. Dies betrifft beispielsweise die Beauftragung von einigen Laborleistungen, weil es nur noch darauf ankommt, wer alleinverantwortlich bestimmt, in welcher Weise die Daten verarbeitet werden und welche Untersuchungen zu erbringen sind (Zweckbestimmung).

Ob eine AV - mit den entsprechenden Rechtsfolgen - vorliegt, richtet sich ausschließlich nach den gesetzlichen Vorgaben, kann also nicht vertraglich festgelegt bzw. ausgeschlossen werden. Im Falle einer AV ist die Übermittlung der Daten an den Dienstleister insofern "privilegiert", als sie nicht den üblichen Anforderungen unterliegt und hierfür keine gesetzliche Erlaubnis oder gesonderte Einwilligung des Betroffenen erforderlich ist. Dafür müssen andererseits bestimmte rechtliche Anforderungen beachtet und Pflichten erfüllt werden.

Liegt eine AV vor, muss zwischen dem Verantwortlichen und dem Auftragsverarbeiter zwingend ein Vertrag in schriftlicher oder elektronischer Form geschlossen werden, der die Vorgaben des Art. 28 Abs. 3 DSGVO erfüllt. Ein ausführlich kommentiertes Muster, das auf die besonderen Belange des Gesundheitswesens eingeht, ist unter www.daebl.de/CS39 erhältlich.

Der Auftraggeber hat den Dienstleister ("Auftragsverarbeiter") sorgfältig und unter Berücksichtigung der Gewährleistung geeigneter technischer und organisatorischer
Maßnahmen für einen ausreichenden Datenschutz auszuwählen. So treffen ihn vor Vertragsschluss und auch während der Laufzeit (Art. 32 Abs. 1 lit. d) DSGVO) ge-

[1] https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Kurzpapiere-der-Datenschutzkonferenz-zur-DS-GVO.html

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

wisse Kontroll- und Dokumentationspflichten. In der Regel ist hierfür die Vorlage aktueller Dokumente ausreichend, aus denen sich ergibt, dass der Auftragsverarbeiter geeignet ist und die gesetzlichen Anforderungen erfüllt (z.B. durch Zertifizierungen). Ohne Genehmigung darf der Dienstleister keinen weiteren Auftragsverarbeiter einschalten.

II. Verantwortlichkeiten

Bei der AV bleibt die Verantwortung für die Einhaltung datenschutzrechtlicher Vorgaben grundsätzlich bei dem Auftraggeber ("Verantwortlicher"). Er ist daher auch Ansprechpartner für die von der Datenverarbeitung betroffenen Personen und verantwortlich bezüglich der den Betroffenen nach Art. 12 bis 23 DSGVO und §§ 32 ff. BDSG zustehenden Rechte wie Information, Auskunft, Berichtigung, Löschung etc. Der Auftragsverarbeiter hat den Verantwortlichen hierbei aber ggf. ebenso zu unterstützen wie bei Erfüllung der Pflichten nach Art. 32 bis 36 DSGVO; beides ist auch zwingend vertraglich zu regeln.

Soweit der Auftragsverarbeiter allerdings gegen die vertraglich festgelegte Datenverarbeitung bzw. gegen Weisungen des Verantwortlichen verstößt, indem er die Zwecke und Mittel der Verarbeitung selber bestimmt, gilt er selber als Verantwortlicher (Art. 28 Abs. 10 DSGVO).

Verantwortlicher und Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Datenschutzniveau zu gewährleisten. Dies beinhaltet vor allem die in Art. 32 DSGVO und (bei Verarbeitung "besonderer Kategorien" von Daten wie Gesundheitsdaten) in § 22 Abs. 2 BDSG genannten Maßnahmen. Im Rahmen einer AV gilt dies sowohl hinsichtlich der Erbringung der AV an sich (z.B. externe Honorar- oder Lohnabrechnung) als auch für den dafür erforderlichen Datentransfer an den Auftragsverarbeiter.
Der bzw. die jeweiligen Datenschutzbeauftragten sind in alle Fragen frühzeitig einzubinden. Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, hat er diese dem Verantwortlichen unverzüglich zu melden (Art. 33 Abs. 2 DSGVO).

III. Haftung, Bußgelder

Für materielle oder immaterielle Schäden infolge eines Verstoßes gegen die DSGVO haften im Außenverhältnis jeder Verantwortliche und jeder beteiligte Auftragsverarbeiter zunächst gemeinsam für den gesamten Schaden (Art. 82 Abs. 1, Abs. 4 DSGVO).

Wer nachweist, dass er "in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist" (Art. 82 Abs. 3 DSGVO), ist von der Haftung befreit. Wer Schadenersatz gezahlt hat, kann im Innenverhältnis von den übrigen beteiligten Verantwortlichen oder Auftragsverarbeitern den Teil zurückzufordern, der dem jeweiligen Verantwortungsanteil entspricht. Die Haftung des Auftragsverarbeiters beschränkt sich dabei allerdings auf Verstöße gegen speziell ihm gesetzlich auferlegte Pflichten oder für Schäden infolge der Nichtbeachtung oder des Zuwiderhandelns gegen Anweisungen des Verantwortlichen.

Verschärft wurden die Bußgeldandrohungen. Bei Verstößen gegen die gesetzlichen Pflichten drohen Verantwortlichen und Auftragsverarbeitern nach Art. 83 Abs. 3 DSGVO empfindliche Geldbußen.. Aufsichtsbehördliche Sanktionen können, soweit erforderlich, in angemessener Höhe erfolgen.

IV. Beachtung der Schweigepflicht

Im Zusammenhang mit der AV ist darauf hinzuweisen, dass auch der Straftatbestand der Verletzung der ärztlichen Schweigepflicht (§ 203 StGB) im Oktober 2017 geändert bzw. ergänzt wurde. Das Heranziehen externer Dienstleister war nach der bisherigen Gesetzesregelung nicht ohne strafrechtliches Risiko, sofern der Dienstleister dadurch von geschützten Geheimnissen erfahren konnte.

Nach der Neufassung des § 203 StGB ist es nun nicht mehr strafbar, ein geschütztes Geheimnis gegenüber Personen zu offenbaren, "die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit [...] erforderlich ist". Dafür werden andererseits die "mitwirkenden Personen" in die Strafbarkeit mit einbezogen, sofern sie selber geschützte Geheimnisse unbefugt offenbaren. Den "Berufsgeheimnisträgern"(Arzt, Zahnarzt etc.) sind wiederum Sorgfaltspflichten auferlegt, welche die Verschwiegenheit der mitwirkenden Personen sicherstellen sollen; insbesondere müssen diese zur Geheimhaltung verpflichtet werden. Es ist unbedingt zu empfehlen, dies zu dokumentieren.

Selbstverständlich sind daneben die berufsrechtlichen Regelungen zur Schweigepflicht zu beachten, die unter Umständen, allerdings eher in Ausnahmefällen, strenger sein können.

V. Praxishinweis

Es besteht keine grundsätzliche Pflicht, bisher bereits abgeschlossene Vereinbarungen zur AV zu ersetzen, sofern diese bereits alle inhaltlichen und formalen Anforderungen der DSGVO erfüllen. Geboten ist jedoch, diese dementsprechend

und unter Hinzuziehung der Auftragsverarbeiter zu prüfen. Diese dürften hieran schon angesichts der sie neu treffenden Haftung ein verstärktes Interesse haben.

Anlage:

DSGVO ab dem 25.05.2018

Erwägungsgrund 81

Damit die Anforderungen dieser Verordnung in Bezug auf die vom Auftragsverarbeiter im Namen des Verantwortlichen vorzunehmende Verarbeitung eingehalten werden, sollte ein Verantwortlicher, der einen Auftragsverarbeiter mit Verarbeitungstätigkeiten betrauen will, nur Auftragsverarbeiter heranziehen, die – insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen – hinreichende Garantien dafür bieten, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, die den Anforderungen dieser Verordnung genügen. Die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen. Die Durchführung einer Verarbeitung durch einen Auftragsverarbeiter sollte auf Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Recht der Union oder der Mitgliedstaaten erfolgen, der bzw. das den Auftragsverarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zwecke der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien von betroffenen Personen festgelegt sind, wobei die besonderen Aufgaben und Pflichten des Auftragsverarbeiters bei der geplanten Verarbeitung und das Risiko für die Rechte und Freiheiten der betroffenen Person zu berücksichtigen sind. Der Verantwortliche und der Auftragsverarbeiter können entscheiden, ob sie einen individuellen Vertrag oder Standardvertragsklauseln verwenden, die entweder unmittelbar von der Kommission erlassen oder aber nach dem Kohärenzverfahren von einer Aufsichtsbehörde angenommen und dann von der Kommission erlassen wurden. Nach Beendigung der Verarbeitung im Namen des Verantwortlichen sollte der Auftragsverarbeiter die personenbezogenen Daten nach Wahl des Verantwortlichen entweder zurückgeben oder löschen, sofern nicht nach dem Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Art. 4 Nr. 8 DSGVO - Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck [...] Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Art. 28 DSGVO – Auftragsverarbeiter

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

(2) Der Auftragsverarbeiter nimmt keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen in Anspruch. Im Fall einer allgemeinen schriftlichen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben.

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter

a) die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen – auch in Bezug auf die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation – verarbeitet, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet;

b) gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

c) alle gemäß Artikel 32 erforderlichen Maßnahmen ergreift;

d) die in den Absätzen 2 und 4 genannten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

e) angesichts der Art der Verarbeitung den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III genannten Rechte der betroffenen Person nachzukommen;

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt;

g) nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht,
h) dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und Überprüfungen – einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt.

Mit Blick auf Unterabsatz 1 Buchstabe h informiert der Auftragsverarbeiter den Verantwortlichen unverzüglich, falls er der Auffassung ist, dass eine Weisung gegen diese Verordnung oder gegen andere Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

(4) Nimmt der Auftragsverarbeiter die Dienste eines weiteren Auftragsverarbeiters in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Verantwortlichen auszuführen, so werden diesem weiteren Auftragsverarbeiter im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in dem Vertrag oder anderen Rechtsinstrument zwischen dem Verantwortlichen und dem Auftragsverarbeiter gemäß Absatz 3 festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden muss, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen dieser Verordnung erfolgt. Kommt der weitere Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten jenes anderen Auftragsverarbeiters.

(5) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 1 und 4 des vorliegenden Artikels nachzuweisen.

(6) Unbeschadet eines individuellen Vertrags zwischen dem Verantwortlichen und dem Auftragsverarbeiter kann der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 des vorliegenden Artikels ganz oder teilweise auf den in den Absätzen 7 und 8 des vorliegenden Artikels genannten Standardvertragsklauseln beruhen, auch wenn diese Bestandteil einer dem Verantwortlichen oder dem Auftragsverarbeiter gemäß den Artikeln 42 und 43 erteilten Zertifizierung sind.

(7) Die Kommission kann im Einklang mit dem Prüfverfahren gemäß Artikel 93 Absatz 2 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(8) Eine Aufsichtsbehörde kann im Einklang mit dem Kohärenzverfahren gemäß Artikel 63 Standardvertragsklauseln zur Regelung der in den Absätzen 3 und 4 des vorliegenden Artikels genannten Fragen festlegen.

(9) Der Vertrag oder das andere Rechtsinstrument im Sinne der Absätze 3 und 4 ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(10) Unbeschadet der Artikel 82, 83 und 84 gilt ein Auftragsverarbeiter, der unter Verstoß gegen diese Verordnung die Zwecke und Mittel der Verarbeitung bestimmt, in Bezug auf diese Verarbeitung als Verantwortlicher.

Art. 29 DSGVO - Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 DSGVO - Sicherheit der Verarbeitung

(1) 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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 82 DSGVO - Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen,die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Anlage:

DSGVO ab dem 25.05.2018

Erwägungsgrund 81 pp.

….

Rechte von Patientinnen und Patienten

I. Recht auf Auskunft und Akteneinsicht

Anstelle des Auskunftsrechts der Patientinnen und Patienten gemäß Art.15 DS-GVO kommt im Bereich der Gesundheitsberufe grundsätzlich die speziellere und bereits bestehende Regelung des § 630g Abs. 1 S. 1 Bürgerliches Gesetzbuch (BGB) zur Anwendung. Dies ist möglich, weil die Öffnungsklausel des Art. 9 Abs. 4 DS-DVO es den Mitgliedstaaten, u. a. für Gesundheitsdaten erlaubt, zusätzlich zu den Regelungen der DS-GVO weitere Bedingungen und Einschränkungen aufrechtzuerhalten oder einzuführen. Auf diese Weise sind die Mitgliedstaaten berechtigt, eigene Anforderungen an den Umgang mit den entsprechenden Patientendaten als besondere Kategorie von personenbezogenen Daten vorzusehen. In der Praxis sind also die Vorschriften über den Behandlungsvertrag (§§ 630a-g BGB) sowie die diesbezüglichen Regeln in den Berufsordnungen als Vorschriften vorrangig gegenüber den Regelungen der DS-GVO zur Auskunft, Berichtigung und Einschränkung der Verarbeitung anzuwenden. Die Rechtsvorschriften zum Behandlungsvertrag wurden durch das sog. Patientenrechtegesetz bereits 2013 (s. BGBl. 2013 Teil I 2013, S. 277 ff.) in das BGB eingefügt. Anliegen des Gesetzgebers war die Vereinheitlichung des Arztrechts, das bis dahin in verstreuten Einzelvorschriften geregelt und durch die Rechtsprechung geprägt war.

Die Akteneinsicht ist gemäß § 630g Abs. 1 S. 1 BGB zu gewähren, soweit nicht der Einsichtnahme erhebliche therapeutische Gründe oder sonstige erhebliche Rechte Dritter entgegenstehen. Die Ablehnung ist zu begründen (§ 630g Abs. 1 Satz 3 BGB).

§ 630 g BGB verpflichtet zur unverzüglichen Einsichtsgewährung. Hierzu sieht Lafontaine[1] vor: *„Die Einsicht muss unverzüglich, also ohne schuldhaftes Zögern (§ 121 Abs. 1 Satz 1 BGB) gewährt werden. Unverzüglich bedeutet nicht sofort und (…) auch nicht jederzeit, sondern mit der bei Einhaltung der gebotenen Sorgfalt und gebotenen Beschleunigung. Eine allgemeine Zeitangabe verbietet sich. Zu berücksichtigen sind auch hier die Umstände des Einzelfalles*."

II. Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung

Die Patientenakte muss der Dokumentationspflicht des jeweils behandelnden Arztes genügen. Diese Pflicht ist in § 630f BGB geregelt. Nach dieser Vorschrift ist der Behandelnde verpflichtet, zum Zwecke der Dokumentation in unmittelbarem zeitlichem Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen.

Inhaltlich fordert § 630f Abs. 2 BGB eine Aufnahme der folgenden Informationen in die Patientenakte: Aufzeichnungen zu sämtlichen aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärungen sowie Arztbriefe.

Wenn ein Patient die „umgehende Löschung" fordert, steht diesem Begehren die in § 630f Abs. 3 vorgesehene grundsätzliche Aufbewahrungsfrist von 10 Jahren oder längere Aufbewahrungsfristen (z. B. § 28 Röntgenverordnung = 30 Jahre) entgegen.

Sofern inhaltliche Berichtigungen von erwiesenermaßen falschen Eintragungen vorgenommen werden sollen, sind diese gemäß § 630f Abs. 1 Satz 2 und 3 BGB nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Dieser Gesichtspunkt der Revisionsfähigkeit gilt sowohl für Papierakten als auch für Praxisverwaltungssysteme (s. hierzu den Datenschutzbericht 2017, Gliederungspunkt 10.4, S. 76).

Soweit sich Patienten im Einzelnen auf „ihr Recht auf Löschung oder ihr Recht auf Vergessenwerden" berufen, kommt die Anwendung des Art. 18 DSGVO in Betracht, also das Recht auf Einschränkung der Verarbeitung. Einschränkung der Verarbeitung meint das Vorgehen,

[1] in: Herberger/Martinek/Rüßmann u. a. , jurisPK-BGB, 8. Aufl. 2017, § 630g BGB, Rn. 125

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

welches nach der alten Rechtslage unter den Begriff der Sperrung gefasst wurde. Ist die Verarbeitung eingeschränkt, so dürfen diese personenbezogenen Daten nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden. Sie sind entsprechend zu markieren.

III. Antragsbearbeitung

1) **Anweisung zur Antragsbearbeitung für Mitarbeiter**
Für jede heilberufliche Einrichtung ist zu empfehlen, eine kurze schriftliche Anweisung für die Mitarbeiter zu erstellen, wie zu verfahren ist, wenn ein Patient seine o. g. Rechte geltend macht, z. B. Regelung von Zuständigkeit, Ablauf und der Dokumentation/Ablage. Es sind gerade solche (eher einfachen) organisatorischen Maßnahmen, die angesichts der einzuhaltenden Bearbeitungsfrist sinnvoll sind. Die entsprechenden Anträge sind grundsätzlich "unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags" (Art. 12 Abs. 3 DSGVO) zu bearbeiten

2) **Antragstellung sowie -bearbeitung**
Antragstellung sowie -bearbeitung (z.B. Übermitteln von Informationen oder Mitteilungen über getroffene Maßnahmen) können grundsätzlich schriftlich "oder in anderer Form" erfolgen (z.B. also auch mündlich oder elektronisch), siehe Art. 12 Abs. 1 DSGVO. Ein elektronischer Antrag ist "nach Möglichkeit" auch elektronisch zu beantworten, sofern der Betroffene nichts andere angibt.

3) **Identitätsüberprüfung**
Wichtig ist, dass der Verantwortliche stets "alle vertretbaren Mittel" zu nutzen hat, um die Identität des Anfragenden zu überprüfen (siehe Art. 11 und 12 Abs. 6 DSGVO; Erwägungsgründe 63 und 64 der DSGVO). Problematisch ist insofern z.B. eine einfache E -Mail – Anfrage / Beschwerde (E-Mail ohne Signatur) oder eine telefonische Eingabe. Es wird empfohlen, postalisch bei der betroffenen Person nachzufragen, ob die vorliegende Anfrage / Beschwerde von ihr verfasst wurde. Anschließend könnte die weitere Kommunikation mit ihr wunschgemäß per verschlüsselter E-Mail abgewickelt werden.

d) (**keine) Unentgeltlichkeit?**
Die LDI sieht hier – abweichend und in Ausnahme von I. – keinen Vorrang des BGB, sondern der DSGVO. Dieser Meinung schließt sich die Arbeitsgemeinschaft ausdrücklich nicht an. Dieser Rechtsstreit ist bisher nicht durch ein Urteil entschieden, es bleibt abzuwarten.

Arbeitsgemeinschaft: Wie oben ausgeführt, stellt §630g Abs. 2 BGB jedoch eine zulässige nationale Sonderregelung auf, die bedingt, dass für die Abschrift auch weiterhin die übliche Gebühr (50 Cent pro Seite für die Seiten 1 – 50, ab der 51. Seite 15 Cent, analog Nr. 7000 VV RVG, 1,50€ pro CD/DVD, ansonsten Selbstkostenpreise) verlangt werden kann. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

LDI: Im Falle der Fertigung von Abschriften ist entsprechend des europarechtlichen Gedankens des Anwendungsvorrangs eine Unentgeltlichkeit in den Fällen anzunehmen, in denen erstmalig eine Abschrift verlangt wird. Das Verhältnis der der nationalen zur europäischen Rechtsordnung wird von dem Grundsatz geprägt, dass das Recht der EU in allen Mitgliedstaaten einen Anwendungsvorrang gegenüber dem jeweiligen nationalen Recht beansprucht. Dies ergibt sich daraus, dass das Unionsrecht in allen Staaten der EU kohärent, effektiv und autonom gelten muss, um wirksam zu sein. Dieser Vorrang des Unionsrechts wurde vom EuGH bereits früh (s. Urt. v. 15.07.1964, Az. C-6/64) erklärt und von den obersten Gerichten der Mitgliedstaaten grundsätzlich akzeptiert (vgl. z. B. BVerfG v. 09.06.1971, Az. 2 BvR 225/69). Während § 630 g Abs. 2 BGB vorsieht, dass der Patient (auch elektronisch) Abschriften von der Patientenakte verlangen kann, in Bezug auf welche er dem Behandelnden die entstandenen Kosten zu erstatten hat, enthält Art. 15 Abs. 3 DS-GVO die Regelung, dass der Verantwortliche eine erste Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, unentgeltlich zur Verfügung stellt. Für alle weiteren Kopien, die die betroffene Person verlangt, kann der Arzt als Verantwortlicher ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

Ausnahmen für die Unentgeltlichkeit können gemacht werden für offenkundig unbegründete oder exzessive oder häufig wiederholte Anträge einer betroffenen Person (siehe Art. 12 Abs. 5 DSGVO); hier kann ein angemessenes Entgelt verlangt oder eine weitere Mitteilung abgelehnt werden.

Wird ein Antrag bzw. dessen Bearbeitung abgelehnt, ist der Antragsteller spätestens innerhalb eines Monats

über die Gründe sowie über die Möglichkeit, einer Beschwerde bei der Aufsichtsbehörde oder einer Klage zu unterrichten.

V. Gesetzliche Regelungen

Artikel 15 DSGVO

Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;
b) die Kategorien personenbezogener Daten, die verarbeitet werden;
c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Erwägungsgründe der DSGVO (ab dem 25.05.2018)

EW 63 der DSGVO

(63) *Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffener Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen*

Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

EW 64 der DSGVO

***(64)** Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von Online-Diensten und im Fall von Online-Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.*

§ 34 BDSG ab dem 25.5.2018

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in § 27 Absatz 2, § 28 Absatz 2 und § 29 Absatz 1 Satz 2 genannten Ausnahmen nicht, wenn

1. *die betroffene Person nach § 33 Absatz 1 und 3 nicht zu informieren ist oder*
2. *die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsgemäßer oder vertraglicher*

Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Artikels 18 der Verordnung (EU) 2016/679 einzuschränken.

(3) Wird der betroffenen Person durch eine öffentliche Stelle des Bundes keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

Betrieblicher Datenschutzbeauftragter

I. Benennung eines Datenschutzbeauftragten

Das neue Datenschutzrecht verschärft die Datenschutzbestimmungen.Heilberufler (*) haben als Verantwortliche im Sinne von Art. 4 Nr. 7 der europäischen Datenschutzgrundverordnung (DSGVO) in Zukunft grundsätzlich in drei Fällen einen Datenschutzbeauftragten zu benennen
1) wenn der Verantwortliche und der Auftragsverarbeiter „in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen" (§ 38 Abs. 1 Satz 1 BDSG in Ergänzung zu Art. 37 Abs. 1 lit. c) DSGVO) oder2) wenn eine sogenannte Datenschutz-Folgenabschätzung vorzunehmen ist (§ 38 Abs. 1 BDSG in Ergänzung zu Art. 37 Abs. 1 lit. c) DSGVO, Art. 35 Abs. 1 und 3 DSGVO) oder
3) wenn „die Kerntätigkeit des Verantwortlichen [...] in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 [...] besteht" (Art. 37 Abs. 1 lit. c) DSGVO).

1) Fall 1: Beschäftigung von mindestens 10 Personen (sog. „10 -Personen -Regel")

Sind in einer heilberuflichen Einrichtung „in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten" beschäftigt,muss in jedem Fall ein Datenschutzbeauftragter benannt werden (§ 38 Abs. 1 Satz 1 BDSG in Ergänzung zu Art. 37 Abs. 1 lit. c) DSGVO). Die 10-Personen-Regel gilt nur für Beschäftigte, die regelmäßig mit der Datenverarbeitung beschäftigt sind. Das sind zum Beispiel angestellte Heilberufler, Sprechstundenhilfen, Auszubildende, Volontäre und freie Mitarbeiter, jedoch kein Reinigungspersonal.
Laut Beschluss der Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 26.4.2018 soll auch der Verantwortliche, z.B. der Praxisinhaber, von der 10-Personen - Regel erfasst sein. „In der Regel" ist eine Person ständig mit Datenverarbeitung beschäftigt, wenn sie dafür zumindest auf längere Zeit mit einer gewissen Regelmäßigkeit vorgesehen ist. Es muss nicht ihre Hauptaufgabe sein. Die Verarbeitung erfolgt nur dann automatisiert, wenn sie unter Einsatz von Datenverarbeitungsanlagen (Computer/Tablets etc.) oder in strukturierten Verzeichnissen (Patientenkartei) erfolgt.

Dokumentieren Beschäftigte des Heilberuflers zum Beispiel die Diagnose oder nehmen sie am Empfang Daten auf, sind sie „in der Regel" mit Datenverarbeitung beschäftigt.

2) Fall 2: Datenschutz-Folgenabschätzung

Der Verantwortliche ist verpflichtet, einen Datenschutzbeauftragten zu benennen, wenn bei ihm in der heilberuflichen Einrichtung eine Datenverarbeitung vorgenommen wird, die einer sogenannten „Datenschutz-Folgenabschätzung" unterliegt (§ 38 Abs. 1 BDSG in Ergänzung zu Art. 37 Abs. 1 lit. c) DSGVO, Art. 35 Abs. 1 und 3 DSGVO).

Nach Art. 35 Abs. 1 DSGVO ist eine Datenschutz-Folgenabschätzung erforderlich, wenn „die Form der Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat". Dies ist etwa anzunehmen bei der Verarbeitung von genetischen Daten (EW 75, 34 der DSGVO) sowie bei Verwendung von Cloud-Diensten.

Bei „umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO", mithin bei Gesundheitsdaten, Art. 35 Abs. 1. 3 lit. b DSGVO muss diese Verarbeitung ein hohes Risiko darstellen, damit die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht.

Nicht umfangreich sind grundsätzlich Verarbeitungen durch einen einzelnen Heilberufler (Arzt, Apotheker, etc.;EG 91 der DSGVO) und in Fällen, in denen weniger als 10 Personen mit der Datenverarbeitung betraut sind.

Eine Einzelpraxis wird danach grundsätzlich keinen Datenschutzbeauftragten benötigen, es sei denn, es werden z.B. genetische Daten verarbeitet oder das Patientenaufkommen übersteigt die durchschnittlichen Zahlen erheblich. Bei Praxisgemeinschaften, in denen jeder Heilberufler seine Daten getrennt speichert und verwaltet, gelten die Regelungen für die Einzelpraxis entsprechend. Das gilt auch für Berufsausübungsgemeinschaften. Größere Praxen und MVZ werden aufgrund ihrer Größe und Mitarbeiterzahl (10 -Personen-Regel) einen Datenschutzbeauftragten benennen müssen. Die „umfangreiche Verarbeitung" ist nur ein Kriterium, um einzu-

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

schätzen, ob ein „hohes Risiko für die Rechte und Freiheiten natürlicher Personen" bestehen könnte. Das ist auch der Fall, wenn die Datenverarbeitung das Risiko birgt, dass dadurch zum Beispiel die betroffene Person diskriminiert oder ihr Ruf geschädigt werden kann oder die Person einen finanziellen Verlust erleidet.

Zur Bestimmung des Risikos beachten Sie bitte auch das Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) zum Thema „Risiko für die Freiheiten und Rechte natürlicher Personen, bitte beachten Sie ferner das Informationsblatt „Datenschutz-Folgenabschätzung" mit detaillierten Beispielen.

3) Fall 3: Kerntätigkeit des Verantwortlichen besteht in der umfangreichen Verarbeitung von Gesundheitsdaten

Heilberufler sind nach der europäischen Datenschutzgrundverordnung verpflichtet, einen Datenschutzbeauftragten zu benennen, wenn die „Kerntätigkeit des Verantwortlichen [...] in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 Abs. 1 DSGVO besteht".

Beim Patienten erhobene Gesundheitsdaten (EG 35 der DSGVO) gehören als personenbezogene Daten zur besonderen Kategorie von Daten (Art. 9 Abs. 2 lit. h , Art. 4 Nr. 15 DSGVO).

„Kerntätigkeit“ ist die Haupttätigkeit eines Unternehmens. Dazu zählen alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Angehörige eines Gesundheitsberufs müssen im Regelfall personenbezogene Daten ihrer Patienten verarbeiten, um die Diagnosen und ggf. Medikationen etc. nachhalten und die Behandlungsleistungen abrechnen zu können. Folglich gehört dies zu den Kerntätigkeiten von Heilberufen. Um eine Benennungspflicht auszulösen bedarf es neben der Kerntätigkeit zudem aber auch einer **umfangreichen** Verarbeitung (siehe oben).

Über die Vorschrift des § 38 Abs. 1 S. 1 BDSG, die als deutsches Recht die europäischen Regelungen ergänzt, hat der Verantwortliche dann, wenn in seiner Einrichtung eine Datenschutz-Folgenabschätzung durchgeführt werden muss, immer zwingend einen Datenschutzbeauftragten zu benennen, also immer, wenn die Datenverarbeitung im heilberuflichen Betrieb umfangreich ist.

Fazit: Jeder Heilberufler muss prüfen, ob er einen Datenschutzbeauftragten in seinem Betrieb benennen muss. Bei Einzelpraxen oder Praxisgemeinschaften wird dies in der Regel nicht der Fall sein, es sei denn, dass ein außergewöhnlicher Datenumfang oder besonders sensible Daten im Einzelfall eine andere Beurteilung erfordern.

In jedem Fall ist ein Heilberufler verpflichtet, einen Datenschutzbeauftragten zu benennen, wenn mindestens 10 Personen in der Regel und ständig mit Datenverarbeitung beschäftigt sind und/oder wenn eine Datenschutz-Folgenabschätzung zwingend durchgeführt werden muss.

Grundsätzlich gilt: Die Benennung eines Datenschutzbeauftragten ist gem. Art. 37 Abs. 4 S. 1 DS-GVO auch auf freiwilliger Basis möglich. Dies ist zu empfehlen, um die Einhaltung der datenschutzrechtlichen Bestimmungen zu erleichtern und damit ggf. aufsichtsbehördliche Maßnahmen zu vermeiden. Wer kein Risiko eingehen möchte, sollte sich entsprechend vorbereiten und sich beraten lassen oder Erkundigungen bei der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW) einholen.

II. Berufliche Qualifikation und Fachwissen eines Datenschutzbeauftragten

Der Datenschutzbeauftragte wird benannt „auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens [...], das er auf dem Gebiet des Datenschutzrechts und der Datenschutzrechtspraxis besitzt, sowie auf der Grundlage seiner Fähigkeiten zur Erfüllung der in Artikel 39 genannten Aufgaben" (Art. 37 Abs. 5 i.V.m. Art. 39 Abs. 1 DSGVO).

Was das konkret für die Auswahl der Person heißt, ist im Gesetz unbestimmt geblieben und richtet sich nach Umfang der Datenverarbeitung und dem erforderlichen Schutz (EW 97 der DSGVO).

Es kann sowohl ein interner als auch ein externer Datenschutzbeauftragter benannt werden (Art. 37 Abs. 6 DSGVO).

1. Interner Datenschutzbeauftragter

Abhängig von Umfang und Art der Datenverarbeitung kann bei entsprechender Schulung ein Mitarbeiter der heilberuflichen Einrichtung zum Datenschutzbeauftragten benannt werden.

Voraussetzung für die Benennung eines Mitarbeiters, zum internen Datenschutzbeauftragten, zum Beispiel einer Medizinischen Fachangestellten, ist, dass der Mitarbeiter rechtlich und technisch auf dem Gebiet des Datenschutzes entsprechend geschult ist und sich ein intensives Fachwissen in diesem Bereich angeeignet hat. Bundesweit gibt es eine Vielzahl! unterschiedlicher

Schulungsmöglichkeiten. Welche Schulungen erforderlich sein werden, um die gesetzlichen Anforderungen an einen Datenschutzbeauftragten zu erfüllen, ist noch offen.

Zu bedenken ist bei der Bestellung eines internen Datenschutzbeauftragten auch, dass es sich um eine umfangreiche Aufgabe handelt, für die der Mitarbeiter entsprechende Zeit benötigt.

Der Verantwortliche selbst, also zum Beispiel der Praxisinhaber, kann nicht Datenschutzbeauftragter sein!

Ein interner Datenschutzbeauftragter unterliegt einem besonderen Kündigungsschutz; er ist während seiner Tätigkeit als Datenschutzbeauftragter nicht ordentlich kündbar, ähnlich einem Betriebsratsmitglied. Auch nach Beendigung der Aufgabe als Datenschutzbeauftragter genießt der Mitarbeiter noch ein weiteres Jahr Kündigungsschutz (§ 38 Abs. 2 i.V.m. § 6 Abs. 4 BDSG). Fristlose Kündigungen aus wichtigem Grund bleiben weiterhin möglich.

2. Externer Datenschutzbeauftragter

Die Wahrnehmung der datenschutzrechtlichen Aufgaben kann auch ein externer Datenschutzbeauftragter übernehmen. Das können ein Unternehmen oder eine externe natürliche Person sein, z.B. ein Rechtsanwalt oder eine von einem ärztlichen Qualitätsnetz bestimmte MFA einer Praxis, die für die anderen Mitglieder externe Datenschutzbeauftragte ist. Diese/r muss zur Geheimhaltung verpflichtet werden, da Angehörige von Heilberufen sich ansonsten strafbar machen können (§ 203 Abs. 4 S.2 Nr. 1 StGB n.F.). Die berufsrechtlichen Vorschriften sind insoweit ebenfalls einzuhalten.

Zusätzlich zur Benennung eines externen Datenschutzbeauftragten kann es durchaus sinnvoll sein, dass im heilberuflichen Betrieb ebenfalls jemand benannt wird, der für den Datenschutz zuständig ist, zumindest als Ansprechpartner für den externen Datenschutzbeauftragten. Es ist auch denkbar, einen internen Datenschutzbeauftragten zu benennen, der von einem externen unterstützt wird, z.B. bei der Durchführung einer Datenschutz-Folgenabschätzung.

III. Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist verantwortlich für die interne Kontrolle zur Einhaltung des Datenschutzes (Art. 39 DSGVO). Er erfüllt seine Pflichten in vollständiger Unabhängigkeit. Er berät den Verantwortlichen und klärt ihn und die übrigen Mitarbeiter darüber auf, wie die datenschutzrechtlichen Verpflichtungen umzusetzen sind. Er schafft Zuständigkeiten und überwacht die Einhaltung der rechtlichen Vorgaben. Dabei arbeitet er mit dem jeweiligen Landesdatenschutzbeauftragten zusammen.

Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet. Ihm steht ebenso wie einem Heilberufler ein Zeugnisverweigerungsrecht zu (§§ 38 Abs. 2, 6 Abs. 5 S. 2, Abs. 6 BDSG). Verstößt er gegen seine Schweigepflicht, macht er sich strafbar (§ 203 Abs. 4 S. 1 StGB n.F.). Die berufsrechtlichen Vorschriften sind insoweit ebenfalls einzuhalten.

IV. Veröffentlichung der Kontaktdaten

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen, z.B. auch auf der Homepage, und der zuständigen Aufsichtsbehörde mitzuteilen (Art. 37 Abs. 7 DSGVO). Zuständige Aufsichtsbehörde in Nordrhein-Westfalen ist die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW, Postfach 20 04 44, 40102 Düsseldorf, www.ldi.nrw.de/metanavi_Kontakt).
Die LDI NRW bietet die Möglichkeit, die Meldung der Kontaktdaten der Datenschutzbeauftragten nach Art. 37 Abs. 7 DS-GVO über das Online-Meldeportal (kostenfrei) vorzunehmen.

Auf diese Weise erhalten die meldenden Stellen eine sofortige Bestätigung und Dokumentation über ihre Meldung, haben die Möglichkeit einer zukünftigen Pflege „ihrer“ Daten und einer jederzeitigen Selbstauskunft über die im Meldeportal über das Unternehmen gespeicherten Daten. Die Daten können seit dem **25. Mai 2018** der LDI NRW mitgeteilt werden.

V. Sanktionen bei Verstößen

Verstößt der Verantwortliche gegen die Vorschriften über die Benennung eines Datenschutzbeauftragten, seine Stellung oder Aufgaben nach den Artikeln 8, 11, 25-39, 42 und 43 DSGVO, drohen hohe Bußgelder von bis zu 10 Mio. EUR oder von bis zu 2 % des Jahresumsatzes, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 4 lit. a DSGVO). Die Mitteilung der Kontaktdaten des Datenschutzbeauftragten gegenüber der LDI NRW kann sanktionslos bis zum 31.12.2018 erfolgen.

Vl. Zusammenfassung

Seit dem 25. Mai 2018 sind datenschutzrechtliche Neuerungen in Kraft getreten. Sie verschärfen das bisher geltende Datenschutzrecht.

Ob Angehörige von Heilberufen ab dem 25. Mai 2018 einen Datenschutzbeauftragten benötigen, ist je nach

Größe der heilberuflichen Einrichtung unterschiedlich zu beurteilen. Alle Heilberufler haben jedoch die Pflicht zu prüfen, ob sie einen Datenschutzbeauftragten benennen müssen. Obligatorisch muss ein Datenschutzbeauftragter benannt werden
- bei einer Praxis, in der mindestens 10 Personen in der Regel ständig mit der Verarbeitung von Daten beschäftigt sind,
- wenn in der Praxis zwingend eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

Einzelpraxen und Praxisgemeinschaften benötigen in der Regel keinen Datenschutzbeauftragten, es sei denn, das Patientenaufkommen des einzelnen Heilberuflers weicht erheblich vom Durchschnitt ab oder es werden besonders schützenswerte Daten (z.B. genetische Daten) verarbeitet. Das gilt auch bei mit weniger als zehn Personen.
Datenschutzbeauftragter kann auch ein Mitarbeiter des Verantwortlichen sein (interner Datenschutzbeauftragter). Voraussetzung dafür ist, dass der Mitarbeiter rechtlich und technisch auf dem Gebiet des Datenschutzes entsprechend versiert ist und sich ein intensives Fachwissen in diesem Bereich angeeignet hat. Ein interner Datenschutzbeauftragter genießt während seiner Tätigkeit und noch ein Jahr danach Kündigungsschutz. Möglich ist ebenfalls, eine externe Person mit dem Datenschutz zu beauftragen (externer Datenschutzbeauftragter). Der Verantwortliche hat diese zur Verschwiegenheit zu verpflichten.

Der Verantwortliche selbst, z.B. ein Praxisinhaber, kann nicht Datenschutzbeauftragter sein, eignet sich aber als Ansprechpartner für datenschutzrechtliche Fragestellungen.

Unter Berücksichtigung der Wichtigkeit des Datenschutzes, der derzeitigen rechtlichen Unsicherheit bei der Beurteilung des einzelnen Falles und der hohen Bußgelder bei Verstoß gegen die neuen Datenschutzregelungen wird aus Gründen der Vorsicht dringend empfohlen, sich mit den neuen Regelungen zu befassen und gegebenenfalls anwaltlichen Rat einzuholen oder sich bei der LDI NRW auf der Homepage (www.ldi.nrw.de) zu erkundigen.

Dort finden Sie umfangreiche Unterlagen und FAQs zum Thema Datenschutzbeauftragter

VII. Gesetzliche Regelungen

Artikel 37 Datenschutzgrundverordnung (DSGVO)
Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b) 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

***c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9** oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 **besteht**.*

(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.

(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche oder der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauftragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vorgeschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, handeln.

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Artikel 38 DSGVO
Stellung des Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.

(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Artikel 39 DSGVO
Aufgaben des Datenschutzbeauftragten

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.
…

(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

Erwägungsgründe der DSGVO

(61) *Dass sie betreffende personenbezogene Daten verarbeitet werden, sollte der betroffenen Person zum Zeitpunkt der Erhebung mitgeteilt werden oder, falls die Daten nicht von ihr, sondern aus einer anderen Quelle erlangt werden, innerhalb einer angemessenen Frist, die sich nach dem konkreten Einzelfall richtet. Wenn die personenbezogenen Daten rechtmäßig einem anderen Empfänger offengelegt werden dürfen, sollte die betroffene Person bei der erstmaligen Offenlegung der personenbezogenen Daten für diesen Empfänger darüber aufgeklärt werden. Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck zu verarbeiten als den, für den die Daten erhoben wurden, so sollte er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und andere erforderliche Informationen zur Verfügung stellen. Konnte der betroffenen Person nicht mitgeteilt werden, woher die personenbezogenen Daten stammen, weil verschiedene Quellen benutzt wurden, so sollte die Unterrichtung allgemein gehalten werden.*

(91) *Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entspre-*

chend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

***(97)** In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, dessen Kerntätigkeit in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfordern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.*

§ 38 Bundesdatenschutzgesetz (BDSG)

(ab dem 25.05.2018)
Datenschutzbeauftragte nichtöffentlicher Stellen

(1) Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen,** *oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt oder Meinungsforschung,* ***haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

(2) § 6 Absatz 4, 5 Satz 2 und Absatz 6 finden Anwendung, § 6 Absatz 4 jedoch nur, wenn die Benennung einer oder eines Datenschutzbeauftragten verpflichtend ist.

§ 203 StGB n.F.
Verletzung von Privatgeheimnissen

Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,

3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4.

Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

5.

Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

6.

staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7.

Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1.

Amtsträger,

2.

für den öffentlichen Dienst besonders Verpflichteten,

3.

Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4.

Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5.

öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6.

Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfasst worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.
(2a) (weggefallen)
(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,

2.

als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder

3.

nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.
(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Datenschutzbehörde

I. Aufsichtsbehörde

In Nordrhein-Westfalen ist die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW) die zuständige Aufsichtsbehörde für die Heilberufler (*). Als unabhängige Landesbehörde ist sie für die Überwachung der Anwendung der Vorschriften der Datenschutzgrundverordnung (DSGVO), einschlägiger Regelungen des Bundesdatenschutzgesetzes (BDSG) sowie landesgesetzlicher Datenschutzbestimmungen zuständig, damit die Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung geschützt werden und der freie Verkehr personenbezogener Daten in der Europäischen Union erleichtert wird. Die Kontaktdaten der LDI NRW lauten:

Die Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

II. Aufgaben

Die DSGVO enthält in Artikel 57 einen umfangreichen Aufgabenkatalog von 22 unterschiedlichen Einzelaufgaben für die Aufsichtsbehörde. Nach den bisher geltenden datenschutzrechtlichen Bestimmungen war die Aufsichtsbehörde als Fach- und Rechtsaufsicht eingesetzt.

Herauszustellen sind hinsichtlich des Aufgabenkatalogs insbesondere folgende maßgeblichen Aufgaben im Bereich der Verarbeitung von Daten in einer Einrichtung eines Heilberuflers (Praxis, Medizinisches Versorgungszentrum, Apotheke etc.):

- Überwachung und Durchsetzung der Anwendung der DSGVO;
- Beratung von Datenverarbeitern;
- Belehrung von Betroffenen;
- Bearbeitung von Beschwerden;
- Festlegung von Standardvertragsklauseln bei Auftragsverarbeitungen;
- Erfassung von Datenverarbeitungsarten;
- Beratung im Rahmen der Datenschutz-Folgenabschätzung;
- Aufzeichnung von Datenschutzverstößen;
- Erfüllung jeder sonstiger Aufgabe im Zusammenhang mit dem Schutz
- personenbezogener Daten.

III. Befugnisse

1.
In Artikel 58 DSGVO sind der LDI zahlreiche Befugnisse eingeräumt worden, die der Einhaltung und Durchsetzung der datenschutzrechtlichen Bestimmungen sowie der Betroffenenrechte dienen. Vier Befugnisarten sind dabei zu unterscheiden:

a) Untersuchungsbefugnisse, Art. 58 Abs. 1 DSGVO

Grundsätzlich darf die Aufsichtsbehörde den für die Datenverarbeitung Verantwortlichen, den Auftragsverarbeiter und auch deren Vertreter anweisen, alle Informationen bereitzustellen, die für die Aufgabenerfüllung erforderlich sind. Insbesondere Artikel 31 DSGVO statuiert eine Pflicht zur Zusammenarbeit
mit den Aufsichtsbehörden.

Als weiterer Grundsatz gilt, dass der Aufsichtsbehörde zwar auf alle personenbezogenen Daten Zugriff gewährt werden muss und die Aufsichtsbehörde auch die Möglichkeit hat, Geschäftsräume des Verantwortlichen zu betreten. Gleichwohl ist hier eine Ausnahme im Bereich von Berufsgeheimnisträgern zu nennen. Die Aufsichtsbehörde hat keine Untersuchungsbefugnisse gegenüber den in § 203 Abs. 1, 2a und 3 Strafgesetzbuch genannten Personen oder deren Auftragsverarbeitern, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde (§ 29 Abs. 3 S. 1 BDSG). Dies wäre bei dem ausdrücklichen Begehren eines Patienten, die Verarbeitung der eigenen Patientendaten durch die Aufsichtsbehörde überprüfen zu lassen, nicht der Fall. Ansonsten ist der Aufsichtsbehörde die Einsichtnahme in Patientenunterlagen verwehrt. Sie kann allenfalls ihre Untersuchungsbefugnisse im Hinblick auf die Einhaltung sonstiger datenschutzrechtlicher Bestimmungen (z.B. Führung

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

des Verfahrensverzeichnisses) wahrnehmen. Bei Feststellung von Verstößen gegen Datenschutzbestimmungen kann die Aufsichtsbehörde datenschutzrechtliche Hinweise erteilen und entsprechende Datenschutzprüfungen durchführen.

b) Abhilfebefugnisse, Art. 58 Abs. 2 DSGVO

Die Aufsichtsbehörde kann bei möglichen Verstößen nach Artikel 58 Absatz 2 DSGVO vor Verstößen gegen datenschutzrechtlichen Bestimmungen warnen, oder, wenn sie Verstöße festgestellt hat, Maßnahmen ergreifen, um diese abzustellen und/oder zu ahnden. Diese Maßnahmen reichen von einer Warnung über Anweisungen an den Verantwortlichen bis hin zu einem Verbot der Datenverarbeitung sowie der Verhängung von Geldbußen. Auch obliegt der Aufsichtsbehörde die Anordnung der Berichtigung, Löschung oder beschränkten Verarbeitung von personenbezogenen Daten. Eine entsprechende Anordnung kann allerdings nur unter Berücksichtigung von gesetzlichen Aufbewahrungsfristen erfolgen, so dass z.B. eine dokumentierte Diagnosestellung grundsätzlich nicht vor Ablauf der Aufbewahrungsfristen aus der Behandlungsdokumentation gelöscht werden darf.

c) Beratende Befugnisse, Art. 58 Abs. 3 lit. a) bis b) DSGVO

Die Aufsichtsbehörde berät Verantwortliche, wenn diese sich im Rahmen einer Datenschutz-Folgenabschätzung nach Artikel 36 DSGVO an sie wenden. Außerdem gibt sie Stellungnahmen gegenüber politischen Institutionen und der Öffentlichkeit ab.

d) Genehmigungsbefugnisse, Art 58 Abs. 3 lit. d) bis j) DSGVO

Unter die Genehmigungsbefugnisse fallen die Genehmigung der Datenverarbeitung, die Beurteilung von Verhaltensregeln, die Akkreditierung von Zertifizierungsstellen, die Beurteilung von Zertifizierungen und die Billigung von Zertifizierungskriterien..

2.
Die DSGVO bietet zudem den Mitgliedsstaaten die Möglichkeit, den Aufsichtsbehörden weitere Befugnisse einzuräumen. Davon hat die Bundesrepublik Deutschland Gebrauch gemacht: Gemäß 38 Abs. 6 DSGVO stellt der Verantwortliche sicher, dass der Datenschutzbeauftragte bei Erfüllung seiner Aufgaben und Pflichten nicht in einen Interessenkonflikt gerät. Eine Verletzung dieser Pflicht kann mit einem Bußgeld geahndet werden (Art. 83 Abs. 4 lit. a DSGVO).

3.
Abschließend sei darauf hingewiesen, dass in der DSGVO weitere bzw. konkretisierende Befugnisse der Aufsichtsbehörde sowie in diesem Zusammenhang stehenden Pflichten des Verantwortlichen verankert sind. Hier seien insbesondere genannt:

- Datenschutzverletzungen („Datenpannen") sind vom Verantwortlichen zu dokumentieren. Die Dokumentation ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung der datenschutzrechtlichen Bestimmungen (Art. 33 Abs. 5 DSGVO);
- Der Verantwortliche kann verpflichtet sein, die betroffene Person bei „Datenpannen" zu benachrichtigen. Die Aufsichtsbehörde kann insoweit von dem Verantwortlichen verlangen, dies nachzuholen (Art. 34 Abs. 4 DSGVO).

Datenschutzerklärung auf der Homepage

I. Einführung

Zur Sicherung der Transparenz für die von der Datenverarbeitung Betroffenen sieht die europäische Datenschutzgrundverordnung (DSGVO) umfangreiche Informationspflichten für die Verantwortlichen (z.B. Inhaber einer heilberuflichen Einrichtung(*)) vor. Grundsätzlich sind solche Informationen dann zugänglich zu machen, wenn Daten erhoben werden.

In der heilberuflichen Einrichtung werden Daten immer dann direkt oder bei Dritten erhoben, wenn sich die Patientin/der Patient vorstellt oder der Heilberufler Kontakt z.B. mit weiteren Leistungserbringern hat. Hier verweisen wir auf das Informationsblatt „Informationspflichten nach der Datenschutzgrundverordnung".

Allerdings werden auch bei einem Besuch der Homepage des Heilberuflers Daten erhoben, entweder durch den Seitenbetreiber selbst oder durch weitere an der Seitenübermittlung beteiligten Akteure, z.B. Hosts oder Provider. Hierbei handelt es sich u. a. um Informationen zur Zugriffszeit, übertragener Datenmenge, Ausgangsort der Navigation zur Seite (z.B. von Google), Daten über Browser und Betriebssystem sowie die IP-Adresse.

Bereits aufgrund der Übermittlung ihrer IP-Adresse werden die Websitebesucher individualisierbar. Hieraus ergibt sich auch bei einer bloß informativen „Einfach–Webseite“ (ohne z.B. Formulare oder Analysesoftware) die Notwendigkeit, den Vorgaben des Datenschutzrechts auch auf der Homepage zu entsprechen.

Grundsätzlich ändert sich hinsichtlich der Informationen, deren Zurverfügungstellung notwendig sein kann, wenig gegenüber den Anforderungen, denen Sie auch im persönlichen Kontakt zu Patienten unterliegen. Die hiesige Information lehnt sich daher eng an die „Patienteninformation zum Datenschutz — Muster für Ihre Praxis" der Kassenärztlichen Bundesvereinigung (abrufbar unter: http://www.kbv.de/media/sp/Praxisinformation_Datenschutz_Patienteninformation_Muster.docx) an.

Aufgrund der Vielfältigkeit der Homepages, die von o.g. „Einfach-Homepages" mit Bild vom Heilberufler, Adresse und Telefonnummer bis zu Online-Verwaltungssystemen mit automatischer Terminvergabe und Zugriff auf die Patientenakte reichen, ist es unmöglich, eine für alle gleichermaßen verwendbare Datenschutzerklärung zu erstellen.

Dennoch soll die nachfolgende Datenschutzerklärung als Richtschnur gelten, mit der die wichtigsten Informationen vermittelt werden können. Sie erhebt keinen Anspruch auf Vollständigkeit, und es wird für die Richtigkeit keine Haftung übernommen.

II. Grundgerüst einer (Muster-)Datenschutzerklärung

Hinweis: Es handelt sich nachstehend um eine unverbindliche Anregung für eine Datenschutzerklärung, für dessen Richtigkeit oder Vollständigkeit angesichts der Komplexität der Materie und der Verschiedenheit der jeweiligen Datenverarbeitungsvorgänge in den unterschiedlichen heilberuflichen Einrichtungen keine Gewähr übernommen werden kann und die nicht ungeprüft übernommen werden sollte.

Sehr geehrte Damen und Herren, sehr geehrte Patientinnen und Patienten,

der Schutz Ihrer personenbezogenen Daten ist uns wichtig. Nach der EU-Datenschutzgrundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck auf unserer Homepage personenbezogene Daten erhoben und verwendet werden, auf welche Art dies geschieht und welchen Umfang dies hat. Dieser Information können Sie auch entnehmen, welche Rechte Sie hinsichtlich des Datenschutzes haben. Diese Datenschutzerklärung bezieht sich auf unser Internetangebot. Sie bezieht sich ausdrücklich nicht auf das Behandlungsverhältnis. Insoweit werden Sie bei Besuch der Praxis gesondert informiert.

1. Verantwortlich für die Datenverarbeitung ist:

Dr. Heinz Mustermann

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

oder: Gemeinschaftspraxis Dr. Heinz und Ulrike Mustermann
oder: MVZ Musterstadt GmbH, vertreten durch den Geschäftsführer...

Adresse (Straße, Nummer, PLZ, Stadt)
Kontaktdaten (Telefon, E-Mail...)

Sie erreichen den zuständigen Datenschutzbeauftragten **(sofern überhaupt benötigt)** unter:

Name
Anschrift
Kontaktdaten

2. Bereitstellung der Website und Erstellung von Protokoll- oder Log-Dateien

Die Seite www.drmustermann.de ist besuchbar, ohne Angaben zu Ihrer Person zu machen. Gleichwohl werden schon bei dem einfachen Seitenaufruf Informationen zum Zugriff (Datum, Uhrzeit, übertragene Datenmenge, Navigationsherkunft, Browser, Betriebssystem, IP-Adresse) gespeichert.
Das Internetangebot wird bei (Name, Kontaktdaten des Hosters) gehostet. Der Hoster empfängt zu diesem Zweck folgende, bei jedem Zugriff auf Inhalte des Internetangebotes in sogenannten Protokoll- oder Log-Dateien vorübergehend gespeicherte Daten, die möglicherweise eine Identifizierung zulassen. Folgende Daten werden hierbei erhoben:

- Datum und Uhrzeit des Abrufs
- Name des aufgerufenen Internetdienstes, der aufgerufenen Ressource und der verwendeten Aktion
- Abfrage, die die Person (Client) gestellt hat
- übertragene Datenmenge
- Meldung, ob der Abruf erfolgreich war
- IP-Adresse des aufrufenden Rechners
- Clientinformationen (u.a. Browser, Betriebssystem)

Rechtsgrundlage für die vorübergehende Speicherung dieser Daten ist Art. 6 Abs. 1 lit. f DS-GVO.

Die Daten aus den Protokoll- bzw. Logdateien dienen zur Sicherstellung der Funktionsfähigkeit der Website. Zudem dienen sie zur Abwehr und Analyse von Angriffen.

In diesen Zwecken liegt auch unser berechtigtes Interesse an der Datenverarbeitung.

Die Daten werden bis zu (Zeitraum der Speicherung) Stunden direkt und ausschließlich für Administratoren zugänglich aufbewahrt. Danach sind sie nur noch indirekt über die Rekonstruktion von Sicherungsbändern verfügbar und werden nach (Zeitpunkt Löschung) endgültig gelöscht.

3 . Cookies/ Analyse-Software

Führen Sie hier bitte aus, was genau geschieht, wenn Sie solche Datenverarbeitungsdienste nutzen, insbesondere, welche Art von Cookies für welchen Zweck auf der Website verwendet wird. Benennen Sie die Rechtsgrundlagen für die Verwendung der jeweiligen Cookies. In diesem Zusammenhang wird auf das Positionspapier der Datenschutzkonferenz vom 26.04.2018 zur weiteren Anwendbarkeit des Telemediengesetzes (abrufbar unter https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf) verwiesen. Daraus ergibt sich, dass Einwilligungen für den Einsatz von Cookies erforderlich sein können, sofern unter Zuhilfenahme von Drittanbietern und unter Verwendung von detaillierten Nutzerprofilen das Nutzungsverhalten im Internet (also webseitenübergreifend) protokolliert und ausgewertet, also getrackt, wird.

4. Kommunikation mit uns

- **Newsletter**:

Auf unserer Webseite können Sie sich in unseren Newsletter-Verteiler eintragen lassen. Dazu wird Ihre E-Mail-Adresse erhoben. Weitere Kontaktdaten – etwa Name oder Pressemedium – sind nicht erforderlich und sollten nicht angegeben werden.
Für die Verarbeitung der Daten wird im Rahmen des Aufnahmevorgangs Ihre Einwilligung eingeholt und auf diese Datenschutzerklärung verwiesen.

Rechtsgrundlage für die Verarbeitung dieser Daten nach der Aufnahme ist Art. 6 Abs. 1 lit. a DSGVO.

Die Erhebung Ihrer E-Mail-Adresse dient dazu, Newsletter zuzustellen.

Ihre Daten werden gelöscht, sobald sie für die Erreichung des Zweckes ihrer Erhebung nicht mehr erforderlich sind. Ihre E-Mail-Adresse wird demnach solange gespeichert, wie das Abonnement des Newsletters aktiv ist.

Sie haben das Recht, Ihre datenschutzrechtliche Einwilligungserklärung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der

aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Das Abonnement des Newsletters können Sie jederzeit kündigen. Schicken Sie uns dazu einfach eine E-Mail an (E-Mail-Adresse) mit dem Betreff „Kündigung“.

- **E-Mails/Formulare**

Führen Sie hier bitte aus, welche Daten für welchen Zweck erhoben werden, wenn man eine E-Mail sendet oder ein Webseitenformular ausfüllt. Benennen Sie die Rechtsgrundlagen (dies kann z. B. Art. 6 Abs. 1 f) DS-GVO sein) und informieren Sie darüber, wie lange und für welchen Zweck die Daten gespeichert werden.

5. Ihre Rechte

Sie haben das Recht, über die Sie betreffenden personenbezogenen Daten einschließlich eventueller Empfänger und der geplanten Speicherdauer Auskunft zu erhalten sowie erteilte Einwilligungen mit Wirkung für die Zukunft zu widerrufen. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen gemäß Art. 16 DS-GVO ein Recht auf Berichtigung zu. Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Art. 17, 18 und 21 DS-GVO). Darüber hinaus steht Ihnen unter bestimmten Voraussetzungen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu.

Die Verarbeitung Ihrer Daten erfolgt auf Basis von gesetzlichen Regelungen. Nur in Ausnahmefällen benötigen wir Ihr Einverständnis. In diesen Fällen haben Sie das Recht, die Einwilligung für die zukünftige Verarbeitung zu widerrufen.

Sie haben ferner das Recht, sich bei einer Datenschutzaufsichtsbehörde Ihrer Wahl zu beschweren, wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt. Hierzu gehört auch die für mich/uns zuständige Aufsichtsbehörde in Nordrhein-Westfalen, die Sie unter folgenden Kontaktdaten erreichen können:
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
(LDI NRW), Kavalleriestraße 2-4, 40213 Düsseldorf,
Telefon: 0211/384240, Fax: 0211-3842410, E-Mail: poststelle@ldi.nrw.de.

III. Telemediengesetz

Die Verpflichtungen nach § 5 Telemediengesetz (TMG) haben sich nicht geändert, sie sind weiterhin im Impressum anzugeben. Dazu gehören:

1. Name und Anschrift, bei juristischen Personen die Rechtsform (z.B. GmbH) und der Vertretungsberechtigte (z.B. Geschäftsführer), Angaben zum Gesellschaftskapital

2. Kontaktdaten inkl. E-Mail

3. Name und Anschrift der Aufsichtsbehörde (d.h. der jeweiligen Kammer, bei Kassen(zahn)ärzten auch die der KV)

4. bei Partnerschaftsgesellschaften: Registername und Registernummer (z.B. HRB 12345, AG Bochum)

5. gesetzliche Berufsbezeichnung (z.B. „Arzt", „Apotheker"), Verleihungsstaat der Berufsbezeichnung, Bezeichnung der berufsrechtlichen Regelungen (Heilberufsgesetz und jeweilige Berufsordnung) und wie diese zugänglich sind (z.B. „Berufsordnung für die nordrheinischen Ärztinnen und Ärzte, herunterladbar hier: (Link))

6. ggf. USt-ID-Nr.

7. bei Gesellschaften, die sich in Liquidation befinden, Angaben hierüber.

Im Übrigen wird auf die Pflichten aus § 13 TMG hingewiesen.

IV. Haftungsausschluss für externe Links

Wie bisher sollte die Haftung für externe Links auf der Homepage ausgeschlossen werden.

V. Transparenz und Zugänglichkeit

Die Texte müssen in einfacher, lesbarer Sprache und Schrift abgesetzt sein, die Angaben müssen von jedem Punkt der Homepage in maximal zwei Klicks erreichbar sein.

Datenschutz-Folgenabschätzung

I. Einführung

Mit der europäischen Datenschutzgrundverordnung (DSGVO) wird das Konzept der Datenschutz-Folgenabschätzung (DSFA) in das europäische Datenschutzrecht
integriert. Die DSFA ist eine vertiefte datenschutzrechtliche Prüfung, die gemäß Art. 35 DSGVO in bestimmten Fällen durchgeführt werden muss. Sie soll helfen, Risiken für Rechte und Freiheiten von Betroffenen bei der Verarbeitung ihrer personenbezogenen Daten zu beschreiben und zu bewerten.

Im Vorfeld zu geplanten Datenverarbeitungsvorgängen müssen daher die Intensität der Beeinträchtigung für Betroffene und die Risiken für die Ausübung von Grundrechten abgeschätzt werden. Wird festgestellt, dass durch den geplanten Verarbeitungsvorgang eine solche Beeinträchtigung nicht hoch ist, mithin „nur“ ein mittleres oder geringes Risiko besteht, muss die DSFA nicht durchgeführt werden. Andernfalls muss eine DSFA erfolgen.

Die Landesdatenschutzbeauftragten erstellen nach Art. 35 Abs. 4 DSGVO eine Liste der Verarbeitungsvorgänge für die (immer) eine DSFA durchzuführen ist (Positivliste). Es kann von den Aufsichtsbehörden auch eine Liste mit Verarbeitungsvorgängen erstellt werden, bei denen keine DFSA durchgeführt werden muss.

Die Positivliste ist auf den Webseiten der LDI NRW unter folgender Adresse zu finden:https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Datenschutz-Folgenabschaetzung.html

II. Grundsatz

Eine DSFA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Risiken für die Rechte und Freiheiten natürlicher Personen können sich nach Art. 35 DSGVO aus der Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien ergeben.

Entsprechende Risiken können sich auch aus der Art der Daten, des Umfangs, der Umstände und den Zwecken der Verarbeitung ergeben. Ziel der DSFA ist es, solche Risiken abzuschätzen, um ggf. geeignete Schutzmaßnahmen ergreifen zu können.

Eine DSFA ist also immer dann durchzuführen, wenn ein Verarbeitungsvorgang „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat" und für den fraglichen Verarbeitungsvorgang keine Ausnahme greift (s.o.). Dies gilt insbesondere dann, wenn eine neue Datenverarbeitungstechnologie eingeführt wird. Inhalt der DSFA sind insbesondere Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Vorgaben der DSGVO nachgewiesen werden kann.

Dreh- und Angelpunkt der DSFA sind immer konkrete Datenverarbeitungsvorgänge.
Gibt es aber ähnliche Verarbeitungsvorgänge bei demselben Verantwortlichen, die ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden.

III. Schwellwertanalyse (Vorprüfung der Erforderlichkeit einer DSFA)

1. Grundsätze

Die Pflicht zur Durchführung der DFSA ergibt sich immer aus einer Risikobewertung. Hierzu wird im Vorfeld eine sog. **Schwellwertanalyse** durchgeführt. Ergibt diese ein voraussichtlich hohes Risiko, dann ist eine DFSA durchzuführen. Ist dies nicht der Fall, dann ist eine DFSA nicht erforderlich. In jedem Fall ist aber die Schwellwertanalyse mit ihren wesentlichen entscheidungserheblichen Erwägungen zu dokumentieren und aufzubewahren, damit diese im Zweifel der Aufsichtsbehörde vorgelegt werden kann.

Einige Faktoren, die regelhaft ein hohes Risiko der Datenverarbeitung mit sich bringen, sind in Art. 35 Abs. 3 DSGVO selbst aufgeführt. Zusätzlich hat die sog. Artikel-29-Datenschutzgruppe der Europäischen Union in ihre Leitlinie weitere Risikofaktoren aufgenommen.

Als Beurteilungskriterien für das Vorliegen eines hohen Risikos hat die Artikel 29-Arbeitsgruppe neun Kriterien benannt[1]. Relevant sind im Kontext der heilberuflichen

[1] Siehe hierzu die systematische Zusammenstellung der Working Party 29 (Artikel 29 Arbeitsgruppe) in ihrem Working Paper 248.

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

Tätigkeit aber hauptsächlich nur Kriterium 4 (Vertrauliche Daten), Kriterium 5 (umfangreiche Datenverarbeitung) und Kriterium 7 (Daten zu schutzbedürftigen Betroffenen). Das heißt jedoch noch nicht, dass schon bei der Erfüllung eines Kriteriums schon in jedem Fall eine DFSA durchzuführen wäre.

a) Vertrauliche Daten oder höchstpersönliche Daten - (Kriterium 4)

Dieses Kriterium wird im Zusammenhang der heilberuflichen Tätigkeit regelmäßig erfüllt, da Gesundheitsdaten besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 DSGVO darstellen und daher sozusagen per legem als vertraulich und höchstpersönlich zu qualifizieren sind. Ferner sind genetische Daten äußerst risikobehaftet, da diese besonders viele Rückschlüsse über die betroffene Person zulassen.

b) Umfangreiche Datenverarbeitung (Kriterium 5 sowie Art. 35 Abs. 3 DSGVO)

Das wohl wichtigste Kriterium im Rahmen der Schwellwertanalyse in heilberuflichen Einrichtungen wird wohl die Frage des Vorliegens eines Risikos wegen umfangreicher Datenverarbeitung sein, denn nach dem Regelbeispiel des Art. 35 Abs. 3 DSGVO ist bei der umfangreichen Verarbeitung von Daten besonderer Kategorien (also auch Gesundheitsdaten) eine DSFA vor einer geplanten Datenverarbeitung zwingend erforderlich.

Der Begriff „umfangreiche Verarbeitung" nach Art. 35 Abs. 3 b) ist in der DSGVO jedoch nicht definiert. Daher ist die Frage, wann eine umfangreiche Datenverarbeitung vorliegt, hier von besonderer Relevanz.

Aus dem EW 91 der DSGVO ergeben sich - jedoch im Sinn eine Negativabgrenzung - Anhaltspunkte dazu, was der europäische Normgeber unter einer umfangreichen Datenverarbeitung versteht. Für Einzelpraxen wird durch das negative Regelbeispiel des EW 91 eine Ausnahme konstituiert. Danach sind „einzelne Ärzte“ von der Pflicht zur Durchführung einer DSFA grundsätzlich befreit:

> *EW 91:*
> *„[…] Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Ange-hörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.“*

Ausgeschlossen ist dadurch die Pflicht zu einer DFSA jedoch nicht. In besonderen Fällen (z.B. bei der Verarbeitung genetischer Daten, vgl. EW 75) ist vielmehr aufgrund der hohen Datentiefe auch der Einzelarzt zur DFSA verpflichtet.

Die Ausnahme in EW 91 heißt aber im Umkehrschluss nicht, dass damit jede Praxis, in der mehr als ein Berufsträger tätig ist, obligat eine DFSA durchführen muss.

Es stellt sich daher die Frage, wann in Berufsausübungsgemeinschaften und MVZ konkret von einer umfangreichen Datenverarbeitung ausgegangen werden muss.

Zur Feststellung des Umfangs der Datenverarbeitung ist insbesondere die Zahl der betroffenen Subjekte zu berücksichtigen.

Bei der Beurteilung, ob eine umfangreiche Datenverarbeitung vorliegt, sind neben der Anzahl der betroffenen Subjekte der Datenverarbeitung aber auch noch folgende Faktoren zu berücksichtigen[2]:

- der Umfang der Daten und/oder der Umfang der in die Datenverarbeitung einbezogenen verschiedenen Datenarten
- die Zeitdauer oder Dauerhaftigkeit/ Beständigkeit der Datenverarbeitungsaktivität;
- die geografische Reichweite der Datenverarbeitungsaktivität.

Daher ist beispielsweise bei der Bewertung des Umfangs der Datenverarbeitung auch zu berücksichtigen, welche zusätzlichen Daten verarbeitet werden. Hier kommen in der Arztpraxis sog. Annexdaten, wie Laborberichte, Arztbriefe, Entlassbriefe nach stationärer Behandlung in Krankenhäusern oder nach Kuren in Betracht.

Die Zeitdauer oder Beständigkeit der Datenverarbeitungsaktivität ist in Arztpraxen bereits aufgrund der nach Berufsordnung und Vertragsarztrecht geltenden Aufbewahrungspflichten von mindestens 10 Jahren recht hoch.

Die o.g. Kriterien sollten im Rahmen einer Gesamtschau in die Prüfung einzubeziehen, ob insgesamt durch die Datenverarbeitung ein hohes Risiko für die Betroffenen vorliegt. Da die Bewertung aufgrund der Individualität des konkreten Falles nur im Rahmen einer Zusammenschau zu bewerten sind, kann eine Schwellwertprüfung

[2] Vgl. Working Paper 248 der Artikel 29 Arbeitsgruppe.

nicht durch eine pauschale Formel o.ä. abgebildet werden.

Für die Schwellwertanalyse kann es aber hilfreich sein mit einer Matrix der Risikokriterien zu arbeiten, die zum Beispiel folgendermaßen aussehen könnte:

Siehe Ende des Informationsblattes

Umso stärker die in der Matrix genannten Parameter betroffen sind, umso eher ist im Ergebnis der Schwellwertanalyse eine DSFA obligat durchzuführen

Da es sich um eine recht komplexe und einzelfallbezogene Prüfung handelt, ist wäre es natürlich wünschenswert, wenn man die Prüfung auf eine Faustformel reduzieren könnte. Dies ist leider so nicht möglich. Gleichwohl geht die Konferenz der Datenschutzbeauftragten von Bund und Ländern – zwar im Kontext der Frage um die Bestellpflicht eines Datenschutzbeauftragten - davon aus, dass eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten in der Regel nicht angenommen werden kann, wenn in einer Gemeinschaftspraxis weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind (Beschluss der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder - DSK - vom 26.04.2018). In diesem Sinne kann daher übertragen auf die DFSA sozusagen als „Faustregel" davon ausgegangen werden, dass in der Regel keine Pflicht zur Durchführung einer DFSA besteht, wenn in Gemeinschaftspraxen/MVZ weniger als 10 Mitarbeiter tätig sind, die sich regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigen.

Beachte: Werden dagegen besonders sensible Daten verarbeitet, kann die DSFSA sogar schon bei einem Einzelarzt erforderlich sein (siehe Beispiel unter Punkt 2 c)).

c) Daten zu schutzbedürftigen Betroffenen – (Kriterium 7)

In heilberuflichen Einrichtungen etwa werden in der Regel auch Daten von schutzbedürftigen Betroffenen, wie z.B. Kindern oder Senioren verarbeitet. Zwischen diesen Betroffenen und dem Verantwortlichen (Arzt oder Apotheker) besteht regelmäßig ein größeres Machtungleichgewicht, da es für diese Personen - aufgrund ihrer entweder noch nicht genügenden geistigen Reife oder aber altersbedingten Einschränkungen - nicht ohne weiteres möglich ist, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben. Auch besteht hier oft eine stärkere Abhängigkeit im Verhältnis Arzt und Patient, die es gerade für diesen Personenkreis schwierig macht, eigene freie Entscheidungen zur Verarbeitung ihrer Daten zu treffen.

2. Beispiele:

a) MVZ GmbH mit angestellten Ärzten verschiedener Fachdisziplinen

Insgesamt zehn Berufsträger aus fünf verschiedenen Facharztgruppen. Das MVZ verfügt über drei Betriebsstätten in verschiedenen Orten und behandelt pro Quartal ca. 12.000 Patienten bei einem Patientenstamm von ca. 100.000 Patienten insgesamt. Von den 12.000 Patienten (GKV und PKV) werden ca. 5.000 Patienten von mehreren Ärzten bzw. Fachgruppen behandelt. Das PVS ist einheitlich für alle Patienten eingerichtet und die Abrechnung bei der KVWL erfolgt für alle Ärzte über die Hauptbetriebsstätte des MVZ.

Beurteilung:

Entsprechend der obigen Matrix verfügt das MVZ über einen großen Patientenstamm mit einer entsprechend hohen Anzahl an Behandlungs- und Arztfällen pro Quartal und Fachrichtung. Ferner ist auch die Ausdehnung mit drei Betriebsstätten groß. Da die Patientenverwaltung sowie die Abrechnung zentral erfolgt, ist auch der Grad der IT-Nutzung hoch. Es liegt neben einer hohen Datentiefe/ Komplexität und Kumulation insbesondere eine Verarbeitung von Daten besonderer Kategorien in großem Umfang vor.

Da im vorliegenden Fall alle Spalten der Matrix stark betroffen wären, müsste hier zur Abschätzung des sich aus dem Risiko der Datenverarbeitung ergebenden Risikos zwingend eine DFSA durchgeführt werden.

b) Gemeinschaftspraxen mit zwei in eigener Zulassung tätigen Orthopäden in einer Betriebsstätte.

Die Ärzte behandeln ca. 2.200 Patienten (GKV und PKV) pro Quartal. Aufgrund von Patienten die im Quartal mehrfach behandelt werden müssen, sowie gegenseitigen Abwesenheiten entstehen jedes Quartal ca. 4000 Arzt-Patienten-Kontakte (Arztfälle). Die Gemeinschaftspraxis hat ein gemeinsames PVS und reicht die Abrechnung einheitlich ein.

Beurteilung:
Die vorliegende Praxis erfüllt die in der Matrix aufgeführten Punkte nur teilweise. Die Patientenzahl der Gemeinschaftspraxis ist mit 2.200 Behandlungsfällen recht gering und entspricht der Fallzahl großer Einzelpraxen. Die verarbeiteten Daten sind im Wesentlichen rein orthopädisch, da hier keine andere Fachrichtung mitarbeitet (inkl. ggf. Annexunterlagen, wie Laborberichte, Arztbriefe, etc.).

In diesem Fall ist nicht von einem hohen Risiko durch die Datenverarbeitung in der Praxis auszugehen, so dass eine DSFA hier nicht erforderlich ist.

Hinweis: Gleichwohl ist die Datenverarbeitung der Praxis derart auszugestalten, dass die ergriffenen technisch-organisatorischen Maßnahmen eine datenschutzkonforme Verarbeitung dieser Daten sicherstellen.

c) Gynäkologische Einzelpraxis mit dem Schwerpunkt Reproduktionsmedizin.

Die Praxis behandelt an ihrem einzigen Standort pro Quartal ca. 600 Patientinnen mit ca. 1500 Arzt-Patienten-Kontakten). Im Vorfeld der Behandlung werden aufwändige Laboruntersuchungen sowie teilweise auch humangenetische Untersuchungen durchgeführt. Es fallen viele Annexunterlagen (Laborberichte, Arztbriefe, etc.) an.

Beurteilung:
Es handelt sich hier um eine Einzelpraxis, für welche die Privilegierung nach EW 91 gilt, wonach eine DSFA bei Einzelpraxen grundsätzlich nicht erforderlich ist. Auch ist die Zahl der Behandlungsfälle mit nur 600 Patienten pro Quartal sehr niedrig, die Frequenz der Arztkontakte im Vergleich aber eher hoch. Allerdings werden in dieser Einzelpraxis besonders vertrauliche medizinische Daten, inkl. genetischer Daten, verarbeitet. Dabei werden in der Regel nicht nur Daten der Patientinnen sondern auch deren Partner gespeichert.

Obwohl hier eine Einzelpraxis vorliegt, wird hier aufgrund der besonders vertraulichen Daten und der Verarbeitungstiefe der Daten (genetische Daten), eine DSFA obligat durchzuführen sein.

IV. Durchführung einer DSFA

Die formellen Anforderungen zur Durchführung einer DSFA ergeben sich aus Art. 35 DSGVO in Verbindung mit den Erwägungsgründen 84, 90, 91, 92 und 93 der DSGVO. Es bedarf einer sorgfältigen Planung der DFSA. Es bietet sich an, hierzu ein DSFSA-Team zusammen zu stellen. Dieses muss zunächst die Verarbeitungsvorgänge, ggf. von anderen Geschäftsprozessen isoliert, detailliert beschreiben (inkl. aller Datenflüsse) und ihre Zwecke festgehalten. Auch müssen die betroffenen Personen und die Akteure identifiziert werden.

Im entscheidenden Schritt muss das von dem Verarbeitungsvorgang ausgehende Risiko bewertet werden, indem die mit dem Verarbeitungsvorgang verfolgten Zwecke mit dem Eingriff in die Rechte und Freiheiten der Betroffenen abgewogen werden. Dabei ist auch zu prüfen, ob nicht eine weniger belastende Alternative zur Verfügung steht.

Die ermittelten Risiken müssen durch technische und organisatorische Abhilfemaßnahmen in der heilberuflichen Einrichtung minimiert werden. Verbleibende Restrisiken werden dokumentiert.

Eine DSFA ist kein abgeschlossener einmaliger Vorgang. Eine kontinuierliche Überprüfung der Risiken gehört zum allgemeinen in der Praxis zu etablierenden Datenschutzmanagement.

Aufgrund der Komplexität der Prüfung ist zu empfehlen, zumindest bei der erstmaligen Vorprüfung (Schwellwertanalyse) externe Hilfe in Anspruch zu nehmen.

V. Pflicht zur Benennung eines Datenschutzbeauftragten (DSB) als Konsequenz der Pflicht zur Durchführung der DSFA

Ist in der heilberuflichen Einrichtung eine DFSA durchzuführen, löst dies nach § 38 Abs. 1 Satz 2 BDSG wiederum die Pflicht zur Benennung eines DSB aus. Diese Pflicht aufgrund der DFSA entsteht damit unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen in der heilberuflichen Einrichtung. Auch wenn in der Praxis weniger als zehn Mitarbeiter mit der Datenverarbeitung beschäftigt sind, muss in diesem Fall ein Datenschutzbeauftragter benannt werden (s. Infoblatt Betrieblicher Datenschutzbeauftragter).

VI. Fazit

Inhaber von Einzelpraxen und kleineren Praxisgemeinschaften von unter 10 Personen müssen sich wegen der Ausnahmeregelung in EW 91 und im Hinblick auf den DSK – Beschluss vom 26.04.2018 mit dem Thema Datenschutz-Folgenabschätzung nur dann auseinandersetzen, wenn bei ihnen eine große Verarbeitungstiefe der Daten vorliegt, wie dies z.B. bei Humangenetikern, Reproduktionsmedizinern oder Pathologen (Molekularpathologie) der Fall sein kann.

Berufsausübungsgemeinschaften und MVZ müssen dagegen vor einer geplanten Datenverarbeitung eingehend prüfen, ob eine DSFA erforderlich ist. Dies gilt insbesondere für große überörtliche und fachungleiche Gemeinschaftspraxen oder MVZ.

Zu beachten ist, dass selbst wenn für den geplanten Datenverarbeitungsvorgang keine DSFA durchzuführen ist, die heilberufliche Einrichtung nicht von den weiteren sich aus der DSGVO ergebenden sachlichen Verpflichtungen entbunden ist. Vielmehr ist die Verarbeitung von Gesundheitsdaten in allen Fällen derart auszugestalten, dass die ergriffenen technisch-organisatorischen Maß-

nahmen eine datenschutzkonforme Verarbeitung dieser Daten sicherstellen.

Hinweis: Die Entscheidung, die DSFA nicht durchzuführen, sollte unter Angabe der maßgeblichen Erwägungen dokumentiert werden, um bei Bedarf seinen Nachweispflichten gegenüber der Aufsichtsbehörde nachkommen zu können.

VII. Gesetzliche Regelungen

Art. 35 DSGVO
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke

einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Erwägungsgrund 75 der DSGVO

Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

Erwägungsgrund 91 der DSGVO

Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht

als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

	Anzahl Patienten (absolut)	Anzahl der Behandlungsfälle[3] pro Quartal	Anzahl der Arztfälle[4] pro Quartal	Anzahl der Fachrichtungen	Angestellte Ärzte	Mehr als eine Betriebsstätte	Hohe Intensität und Verarbeitungstiefe bei der IT-Nutzung	Anzahl Behandlung besonders schutzbedürftiger Betroffener	Besonders schutzwürdige und vertrauliche Gesundheitsdaten
Praxis / BAG									

Legitimationsgrundlagen für die Datenverarbeitung

I. Gesetzliche Grundlagen

Die grundsätzlichen Datenverarbeitungsvorgänge im Rahmen eines Behandlungsverhältnisses beruhen auf gesetzlichen Grundlagen. Art. 9 Abs. 2 lit. h DSGVO erlaubt die Verarbeitung von Daten auf der Grundlage eines Behandlungsvertrags. Wird ein Behandlungsvertrag mit einem Patienten geschlossen, ist keine zusätzliche Einwilligung in die Verarbeitung der dafür erforderlichen personenbezogenen Daten durch den Arzt bzw. die Ärztin und seine bzw. ihre Mitarbeiterinnen und Mitarbeiter notwendig, sofern die weiteren Voraussetzungen beachtet werden (Verarbeitung nur durch den Berufsgeheimnisträger bzw. sein Personal, Art. 9 Abs. 3 DSGVO, und die Erforderlichkeit der Datenverarbeitung für die Erfüllung des Behandlungsvertrags).

Zur Erfüllung des Behandlungsvertrags gehört nicht nur die Behandlung, sondern auch die Erstellung der Abrechnung durch die Ärztin bzw. den Arzt selber. Wird die Durchführung der Abrechnung an eine externe Abrechnungsstelle durch Abtretung der Honorarforderung bzw. zur selbständigen Erstellung der Rechnungen abgegeben, ist eine Einwilligung des Patienten in die dafür notwendige Datenübermittlung zwingend einzuholen. Auch wenn es aus praxisorganisatorischen Gründen sinnvoll und effizient erscheinen mag, die Abrechnung auszulagern, ist die externe Abrechnungsstelle weder Vertragspartner des Behandlungsvertrages, noch ist deren Einschaltung für die Erfüllung des Vertrages im datenschutzrechtlichen Sinne erforderlich. Nur für den Fall, dass lediglich die „Schreibarbeit“ ohne eigene inhaltliche Entscheidungsspielräume an Dritte ausgelagert wird, die Art und Weise der Abrechnung vom Heilberufler vorgegeben und Rechnung auch in seinem Namen gestellt wird, kommt ggf. eine Auftragsverarbeitung in Betracht. Diese verlangt keine Einwilligung der betroffenen Person, aber den Abschluss eines AV-Vertrages mit dem Dienstleister.

Ebenfalls von einer gesetzlichen Grundlage gedeckt sind

- alle Datenverarbeitungen zum Zwecke der Abrechnung an die KV in dem Umfang, der im SGB V vorgesehen ist, sowie auch
- sämtliche bisher existierende, im SGB V oder in anderen Gesetzen vorgesehene Datenverarbeitungsvorgänge einschließlich beispielsweise gesetzlich festgelegter Meldepflichten wie gegenüber dem Krebsregister.

II. Einwilligung

Nur wenn derjenige, der die Daten verarbeiten will, sich weder auf eine gesetzliche Regelung, noch einen Behandlungsvertrag mit dem Betroffenen berufen kann, muss eine Einwilligung eingeholt werden.

Eine datenschutzrechtliche Einwilligung ist laut Art. 4 Nr. 11 DSGVO „jede freiwillig für den bestimmten Fall, in informierter Weise unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Art 9 Abs. 2 lit. a) DSGVO ergänzt dies dahingehend, dass eine Einwilligung in die Verarbeitung von Gesundheitsdaten ausdrücklich zu erfolgen hat. Ein Schweigen des Patienten ist nicht ausreichend. Eine konkludente Einwilligung ist nur dann ausreichend, wenn sie durch eine eindeutige, unmissverständlichem bestätigende Handlung mit ausdrücklichem Erklärungsgehalt bezogen sowohl auf die betroffenen Daten, als auch den konkreten Verwendungszweck, vorgenommen wird. Konkludente Einwilligungen sind daher in nahezu keinem Fall ausreichend.

Anders als bisher ist diese Einwilligung nunmehr nicht mehr ausschließlich schriftlich möglich. Der Verantwortliche muss jedoch nachweisen können, dass der Betroffene in die Datenverarbeitung – im Falle von Gesundheitsdaten ausdrücklich – eingewilligt hat und diese Einwilligung den Voraussetzungen der DSGVO entspricht. Es empfiehlt sich daher, eine genaue Dokumentation der eingeholten Einwilligungen vorzunehmen. Im Zweifel ist die Schriftform nicht zuletzt aus Beweisgründen auch weiterhin empfehlenswert.

-

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

Zudem ist in bestimmten Fällen die Schriftform auch weiterhin gesetzlich zwingend vorgeschrieben, z. B.

- beim Entlassmanagement nach § 39 Abs. 1a SGB V,
- im Rahmen der Teilnahme an strukturierten Behandlungsprogrammen beispielsweise bei Mitbehandlung (hausarztzentrierte Versorgung; § 73 Abs. 1b Satz 1 SGB V) sowie bei
- genetischen Untersuchungen oder Analysen (§ 8 Abs. 1 GenDG).

Die Einwilligung sollte sich auf alle zu demselben Zweck oder denselben Zwecken vorgenommenen Verarbeitungsvorgänge beziehen. Eine pauschale Einwilligung im Sinne einer generellen Einwilligung in alle in Betracht kommenden zukünftigen Datenverarbeitungskonstellationen ist nicht ausreichend, erst Recht nicht in dem Sinne, dass durch den Abschluss eines Behandlungsvertrags ohne Weiteres konkludent auf die Erteilung einer solchen Generaleinwilligung geschlossen werden könnte. Die betroffene Person kann nur wirksam im Sinne der DSGVO einwilligen, wenn sie zumindest grundsätzlich weiß, wer der Verantwortliche ist und zu welchem Zweck die Daten verarbeitet werden sollen (Erwägungsgrund 42 Satz 4). Zudem muss sich die Einwilligung auf einen bestimmten Fall beziehen (Art. 4 Nr. 11 DSGVO).

Trotz all dieser Anforderungen muss gewährleistet sein, dass die betroffene Person ihre Einwilligung frei von Zwang gibt. Es kann nur dann davon ausgegangen werden, dass eine betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat, also in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (siehe Erwägungsgrund 42 der DSGVO). Dies ist beispielsweise dann nicht der Fall, wenn die Erfüllung des Behandlungsvertrages von einer Einwilligung in eine Datenweitergabe abhängig gemacht wird, obwohl die Einwilligung für die Behandlung an sich nicht erforderlich ist, sondern nur diese Datenweitergabe dann nicht erfolgen kann und die Durchführung des Behandlungsvertrages noch sinnvoll erfolgen kann (Art. 7 Abs. 4 i.V.m. Erwägungsgrund 43 DSGVO, sogenanntes Koppelungsverbot).

III. Unwirksamkeit der Einwilligung

Eine Einwilligung, die nicht den dargestellten Anforderungen genügt, ist unwirksam und kann nicht als Rechtsgrundlage für eine Datenverarbeitung herangezogen werden.

Grundsätzlich lässt sich jedoch eine unwirksame oder widerrufene Einwilligung für einen Datenverarbeitungsvorgang, der auch auf eine andere Legitimationsgrundlage hätte gestützt werden können, nicht ohne Weiteres durch diese andere Grundlage ersetzen, denn der für die Datenverarbeitung Verantwortliche muss die Grundsätze der Fairness und Transparenz (Art. 5 Absatz 1 Buchstabe a DSGVO) beachten.

IV. Widerruf

Die Einwilligung in die Verarbeitung seiner personenbezogenen Daten kann die Patientin/der Patient jederzeit mit Wirkung für die Zukunft widerrufen (Art. 7 Abs. 3 DSGVO). Einwilligungsgestützte Verarbeitungsvorgänge in der Vergangenheit bleiben also rechtmäßig. Auf die Widerruflichkeit der Einwilligung muss der verantwortliche vor Abgabe der Einwilligung hinweisen.

Bezüglich der Rechtsfolgen einer entfallenen Einwilligung mit Blick auf die weitere Speicherung der auf der Grundlage der Einwilligung verarbeiteten Daten und zu den Löschpflichten beachten Sie bitte unsere weiteren Informationsblätter.

Informationspflichten nach der Datenschutz -Grundverordnung

I. Inhalt der Informationspflicht

Zur Sicherung der Transparenz für die von der Datenverarbeitung Betroffenen sieht die Datenschutzgrundverordnung (DSGVO) umfangreiche Informationspflichten für die Verantwortlichen vor, die Gesundheitsdaten verarbeiten.

In Artikel 13 DSGVO und ergänzend in § 32 BDSG (Bundesdatenschutzgesetz) werden die Anforderungen für Verantwortliche, also hier für Heilberufler (*) geregelt, wenn die Daten unmittelbar bei der betroffenen Person, in der Regel also hier bei der Patientin/bei dem Patienten erhoben werden (Direkterhebung). Artikel 14 DSGVO und ergänzend § 33 BDSG regeln die Anforderungen bei Erhebung von Daten bei einem Dritten (Dritterhebung).

Sowohl bei der Direkterhebung als auch bei der Dritterhebung bestehen grundsätzlich Informationspflichten des Heilberuflers gegenüber Patientinnen und Patienten zur Angabe von:

• Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters in der heilberuflichen Einrichtung,
• Kontaktdaten des ggf. vorhandenen, vom Heilberufler bestellten Datenschutzbeauftragten,
• Zweck und Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten
• Empfänger/Kategorien von Empfängern der Patientendaten (z.B. Krankenkassen und Verrechnungsstellen),
• einer ggf. beabsichtigten Übermittlung von Patientendaten an einen Empfänger in einem Drittland/ eine Internationale Organisation (z. B. Nutzung von Cloud-Diensten); in diesem Falle ist über die Erfüllung der weiteren in Art. 13 Abs. 1 lit. f) DSGVO genannten Voraussetzungen zu informieren.

Zur Verfügung zu stellen sind weiterhin Informationen

• zur Dauer, für die die Patientendaten gespeichert werden sollen, (z. B. Aufbewahrungsfristen nach den ärztlichen Berufsordnungen (10 Jahre), § 630 lit. f Abs. 3 Bürgerliches Gesetzbuch - 10 Jahre -, § 28 Abs. 3 Röntgenverordnung und § 85 Abs. 3 Strahlenschutzverordnung -30 Jahre-),
• über datenschutzrechtliche Ansprüche der Patientin/des Patienten (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung („Sperrung"), Widerspruchsrecht, Datenübertragbarkeit; siehe hierzu die näheren Hinweise im Informationsblatt „Auskunftsrechte von Patientinnen und Patienten"),
• das Recht auf Widerruf einer Einwilligung im Hinblick auf die weitere Verarbeitung,
• das Recht der Patientin/des Patienten auf Beschwerde bei einer Datenschutzbehörde,
• zur Quelle, aus der die personenbezogenen Daten stammen,
• zur gesetzlichen oder vertraglichen Verpflichtung des Heilberuflers, Patientendaten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung.

II. Form der Informationspflicht

Gemäß Artikel 12 Abs. 1 DSGVO sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zu übermitteln. Die Informationen sind schriftlich oder in anderer Form, ggf. elektronisch zu übermitteln. Auf Verlangen ist die Information auch mündlich möglich. Wenn die Information Aussagen enthält, die nichts allgemeiner Art sind (also alle Patienten und Patientinnen gleichermaßen betreffen), sondern sich speziell auf die Verarbeitung der Daten der betroffenen Person beziehen, muss die Auskunft begehrende Person (Patientin/ Patient) ihre Identität nachweisen können. Die Informationen müssen grundsätzlich unentgeltlich zur Verfügung gestellt werden.
Es wird empfohlen, für Patientinnen und Patienten ein Schriftstück vorzubereiten, in denen die geforderten Informationen vermittelt werden. Die Überreichung dieses Schriftstückes an Patientinnen und Patienten sollte aus Beweisgründen in der Patientenakte dokumentiert werden (siehe „Informationsblatt für Patientinnen/Patienten").

Die Informationen sind seit dem 25.05.2018 nicht nur neuen Patientinnen und Patienten zu erteilen, sondern auch Patientinnen und Patienten, die in einem Behandlungsverhältnis mit dem Verantwortlichen standen und

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

bei denen neue Daten erhoben werden, z.B. weil sie erneut in der heilberuflichen Einrichtung erscheinen. Auch für die übrigen Altpatienten und -patientinnen empfiehlt es sich aus Gründen der Transparenz, die Informationen zur Datenverarbeitung in geeigneter Weise (z.B. zum Nachlesen auf der Homepage) bekannt zu machen.

Für Patientinnen und Patienten wurde ein Informationsblatt zum Datenschutz entwickelt. Verwiesen wird auch auf die Homepage der LDI NRW und die dort abrufbaren Informationen (siehe Kurzpapier Nr. 10 der unabhängigen Datenschutzbehörden des Bundes und der Länder: „Informationspflichten bei Dritt-und Direkterhebung").

III. Ausnahmen von der Informationspflicht

Die DSGVO und das BDSG sehen Ausnahmen für die Informationspflichten vor.

1) Die Informationspflicht entfällt bei der Direkterhebung, wenn die Patientin oder der Patient bereits über die Informationen verfügt (Art. 13 Abs. 4 DSGVO). Bei Weiterverarbeitung direkt erhobener Daten zu anderen Zwecken entfällt die nach Art. 13 Abs. 3 DSGVO bestehende Informationspflicht, wenn die Patientin oder der Patient bereits über die Informationen verfügt (Art. 13 Abs. 4 DS GVO), sowie in den in § 32 Abs. 1 Nr. 1 bis 5 BDSG genannten, eng auszulegenden Fallkonstellationen der Verarbeitung von Patientendaten (jeweils unter Abwägung gegenüber dem Recht der Patientin/des Patienten).

2) Die Informationspflicht entfällt bei der Erhebung bei Dritten,

- insbesondere, wenn die Patientin oder der Patient bereits über die Information verfügt (Art. 14 Abs. 5 lit. a) DSGVO; siehe die weiteren Ausnahmen unter lit. b) bis d) dieser Vorschrift)
- wenn durch die Erfüllung Informationen offenbart werden, die ihrem Wesen nach insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen (§ 29 Abs. 1 Satz 1 BDSG),
- wenn die Erteilung der Information die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, soweit nicht das sorgfältig zu prüfende berechtigte Interesse der Patientin/des Patienten an der Informationserteilung überwiegt (§ 33 Abs. 1 Nr. 2 lit. a) BDSG),
- wenn die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedsstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht (Schweigepflicht), unterliegen und daher vertraulich behandelt werden müssen (Art. 14 Abs. 5 lit. d) DSGVO).

IV. Gesetzliche Regelungen

Auszug aus dem BDSG neu ab dem 25.05.2018

§ 29 Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäß Artikel 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäß Artikel 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 34 Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist

die betroffene Person nach Artikel 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(3) Gegenüber den in § 203 Absatz 1, 2a und 3 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 1 Buchstabe e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoß gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt eine Aufsichtsbehörde im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

§ 32 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäß der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,

2. im Fall einer öffentlichen Stelle die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,

3. die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen,

4. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder

5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Die Sätze 1 und 2 finden in den Fällen des Absatzes 1 Nummer 4 und 5 keine Anwendung.

(3) Unterbleibt die Benachrichtigung in den Fällen des Absatzes 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 33 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 14 Absatz 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 und der in § 29 Absatz 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Fall einer öffentlichen Stelle

a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Artikels 23 Absatz 1 Buchstabe a bis e der Verordnung (EU) 2016/679 gefährden würde oder

b) die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss,

2. im Fall einer nicht öffentlichen Stelle

a) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder

b) die zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde; im Fall der Datenverarbeitung für Zwecke der Strafverfolgung bedarf es keiner Feststellung nach dem ersten Halbsatz.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

Auszug aus der DSGVO ab dem 25.05.2018

Artikel 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

Artikel 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) zusätzlich die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) die Kategorien personenbezogener Daten, die verarbeitet werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person die folgenden Informationen zur Verfügung, die erforderlich sind, um der betroffenen Person gegenüber eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

c) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

e) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

f) aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;

g) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(4) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erlangt wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; dies gilt insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Artikel 89 Absatz 1 genannten Bedingungen und Garantien oder soweit die in Absatz 1 des vorliegenden Artikels genannte Pflicht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist oder

d) die personenbezogenen Daten gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten dem Berufsgeheimnis, einschließlich einer satzungsmäßigen Geheimhaltungspflicht, unterliegen und daher vertraulich behandelt werden müssen.

Informationsblatt für Patientinnen/Patienten

Hinweis: Es handelt sich nachstehend um eine unverbindliche Anregung für ein Informationsblatt, für dessen Richtigkeit oder Vollständigkeit angesichts der Komplexität der Materie und der Verschiedenheit der jeweiligen Datenverarbeitungsvorgänge in den unterschiedlichen heilberuflichen Einrichtungen (*) **keine Gewähr** übernommen werden kann und das nicht ungeprüft übernommen werden sollte.

Informationsblatt für Patientinnen und Patienten zum Datenschutz

Sehr geehrte Patientin, sehr geehrter Patient,

gemäß der Datenschutz-Grundverordnung (DSGVO) sind wir seit dem 25.05.2018 verpflichtet, Ihnen bestimmte Informationen bei der Erhebung Ihrer personenbezogenen Daten zu erteilen. Dieser Verpflichtung kommen wir gerne mit Überreichung dieses Informationsblattes nach.

Namen und Kontaktdaten des Verantwortlichen:

[Erläuterung: Bitte geben Sie hier Namen und Kontaktdaten des oder der Praxisinhaber, also des „Verantwortlichen", an.]

Kontaktdaten des Datenschutzbeauftragten:

[Erläuterung: Sollten Sie einen internen oder externen Datenschutzbeauftragten benannt haben, geben Sie hier bitte dessen Kontaktdaten ein. Sollten Sie keinen Datenschutzbeauftragten benannt haben, so streichen Sie dieses Feld bitte komplett.
Anhaltspunkte dazu, ob Sie einen Datenschutzbeauftragten benannt müssen, können Sie unserem Informationsblatt „Betrieblicher Datenschutzbeauftragter" entnehmen]

Zwecke sowie Rechtsgrundlagen der Datenverarbeitung:

Grundlage einer Behandlung ist der Behandlungsvertrag, der auch formlos geschlossen werden kann. Diesen Behandlungsvertrag können wir nur ordnungsgemäß erfüllen, wenn wir Ihre Daten verarbeiten, beispielsweise Ihre Versichertendaten aufnehmen. Der Zweck der Datenverarbeitung besteht damit in erster Linie in der Durchführung des Behandlungsvertrages. In diesem Zusammenhang besteht eine gesetzliche Verpflichtung zur Verarbeitung Ihrer Daten. Ärzte, Psychotherapeuten und Zahnärzte müssen gemäß § 630f des Bürgerlichen Gesetzbuches (BGB) zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch führen. Hierin sind sämtliche aus fachlicher Sicht für die derzeitige und zukünftige Behandlung der Patienten wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen. Die Datenverarbeitung dient damit auch dem Zweck, diesen Dokumentationspflichten nachzukommen.

Bei den in Folge Ihrer ärztlichen/ zahnärztlichen/ psychotherapeutischen …. Behandlung durch uns verarbeiteten Daten handelt es sich um Patientendaten. Rechtsgrundlage für die Verarbeitung dieser Gesundheitsdaten ist Art. 9 Absatz 2 Buchstabe h) in Verbindung mit Absatz 3 DSGVO sowie § 22 Bundesdatenschutzgesetz (BDSG). Gesundheitsdaten werden ausschließlich bzw. unter Verantwortung von Personen verarbeitet, die einer strafrechtlich sanktionierten Schweigepflicht unterliegen.

Ihre Patientendaten werden auch zu dem Zweck der gesetzlich geregelten Übermittlung an festgelegte Empfänger verarbeitet (beispielsweise an den überweisenden Hausarzt, an Kassenärztliche Vereinigungen, an den Medizinischen

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

Dienst der Krankenversicherung). Auch erhalten wir von Dritten, beispielsweise von Ihrer Krankenkasse oder anderen Behandlern aufgrund gesetzlicher Regelungen oder Ihrer Einwilligung Informationen, die wir zur Durchführung des Behandlungsvertrages sowie zur Erfüllung unserer gesetzlichen Dokumentationspflicht (§ 630f BGB, s.o.) in der Behandlungsdokumentation speichern. Auch hierfür ist Rechtsgrundlage Artikel 9 Absatz 2 Buchstabe h) in Verbindung mit Absatz 3 DSGVO, § 22 BDSG.

In den Fällen, in denen eine Datenverarbeitung nicht zur Durchführung des Behandlungsvertrages erforderlich ist oder nicht auf gesetzlicher Verpflichtung beruht, wird eine Datenverarbeitung üblicherweise auf Ihrer ausdrücklichen Einwilligung beruhen. Rechtsgrundlage ist in diesen Fällen Artikel 9 Absatz 2 Buchstabe a) DSGVO.

Empfänger oder Kategorien von Empfängern der personenbezogenen Daten:

Aufgrund gesetzlicher Vorschriften ist es möglich, dass wir Daten an folgende Empfänger / Kategorien von Empfängern übermitteln:

[Erläuterung: Hier alle Empfänger von Daten Ihrer Patienten eintragen, an die Sie Patienten aufgrund gesetzlicher Vorschriften melden, z. B. Kassen(-zahn-)ärztliche Vereinigung (Nordrhein oder Westfalen-Lippe), Medizinischer Dienst der Krankenkassen usw.; die Empfänger können als Kategorie angegeben werden, beispielsweise Gesundheitsämter]

Darüber hinaus können wir Daten mit der ausdrücklichen Einwilligung von Patientinnen und Patienten übermitteln. Vor Erteilung einer solchen werden wir Sie darüber informieren, um welche Empfänger es sich im Einzelnen handelt.

Beabsichtigte Datenübermittlung an ein Drittland oder eine internationale Organisation:

[Erläuterung: Sollten Sie derartige Übermittlungen beabsichtigen, wäre dies hier darzustellen. Auch wäre über das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission zu informieren oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 DSGVO auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind, zu verweisen.
Beabsichtigen Sie keine derartigen Übermittlungen, entfällt die Überschrift.]

Dauer bzw. Kriterien für die Festlegung der Dauer der Datenspeicherung:

Personenbezogene Daten von Patienten sind grundsätzlich gemäß § 630f Absatz 3 BGB sowie den Vorschriften der jeweils einschlägigen Berufsordnung für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren.

[Erläuterung: Soweit in Ihrer Praxis weitere Aufbewahrungsfristen zu berücksichtigen sind, diese hier aufführen (Beispiel: Aufzeichnungen über Röntgenbehandlungen gemäß § 28 Absatz 3 Satz 1 Röntgenverordnung sind 30 Jahre lang nach der letzten Behandlung aufzubewahren.)]

In besonderen Fällen erfolgen eine längere Aufbewahrung als gesetzlich angeordnet, beispielsweise bei der Durchsetzung von Schadensersatz-, Versicherungs- und Rentenansprüchen des Patienten, soweit wir hiervon Kenntnis haben. Ebenso kann auch der gesundheitliche Zustand des Patienten eine über die Fristen hinausgehende Aufbewahrung erforderlich machen. Da auch zivilrechtliche Schadensersatzansprüche des Patienten gegen seinen Behandler gemäß § 199 Absatz 2 BGB erst nach 30 Jahren verjähren, behalten wir uns vor, die Patientenakte, soweit erforderlich, für die Dauer von 30 Jahren aufzubewahren.

Rechte der Betroffenen:

Im Rahmen der Vorschriften der Datenschutz-Grundverordnung haben Sie verschiedene Rechte im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten. Dazu gehören das Recht auf Auskunft, auf Berichtigung, auf Löschung, auf

Einschränkung der Verarbeitung, auf Widerspruch gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit. Soweit die Datenverarbeitung auf Ihrer Einwilligung beruht, können Sie diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Sie können hinsichtlich der Datenverarbeitung bei der zuständigen Aufsichtsbehörde Beschwerde einlegen. Aufsichtsbehörde ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Kavalleriestr. 2-4, 40213 Düsseldorf.

Automatisierte Entscheidungsfindung:

[Erläuterung: Wird in Ihrer Praxis eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 DSGVO durchgeführt, so ist dies anzugeben. Es sind aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person aufzuführen. Führen Sie derartige Entscheidungsfindungen nicht durch, entfällt die Überschrift.]

Meldung von Verletzungen des Schutzes personenbezogener Daten („Datenpanne“)

Für die Verarbeitung personenbezogener Daten müssen Verantwortliche wissen, dass den Auf- und Anforderungen der Aufsichtsbehörde (z.B. zur Erteilung von Auskünften bzw. Vorlage von Unterlagen oder zur Zusammenarbeit) nachzukommen ist, die diese im Rahmen ihrer Aufgabenerfüllung und ihrer Befugnisse an sie richten (Art. 31 der europäischen Datenschutzgrundverordnung - DSGVO -).

Unabhängig hiervon besteht eine umfassende Pflicht für Verantwortliche, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden.

Eine Verletzung des Schutzes personenbezogener Daten liegt nicht nur dann vor, wenn diese Dritten offen gelegt wurden bzw. sie unbefugt Zugang erlangt haben, sondern auch dann, wenn personenbezogene Daten unbeabsichtigt oder unberechtigt vernichtet, verloren oder verändert wurden (Art. 4 Abs. 12 DSGVO).

Wird dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten bekannt, muss er dies unverzüglich, d.h. ohne schuldhaftes Zögern, und möglichst binnen 72 Stunden der Aufsichtsbehörde melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko, z.B. der Persönlichkeitsrechte von Betroffenen, führt (Art. 33 Abs. 1 und 2 DSGVO). Erfolgt die Meldung nicht binnen 72 Stunden, muss die Verzögerung begründet werden.

Die Meldung muss enthalten:

• Art der Verletzung; soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen / Datensätze;
• Name, Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle;
• Beschreibung der wahrscheinlichen Folgen;
• Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung bzw. Abmilderung

Grundsätzlich nicht erforderlich ist es jedoch, eine Kopie der betroffenen Datensätze an die Aufsichtsbehörde zu übermitteln. Die Aufsichtsbehörden weisen zudem im Kurzpapier Nr. 18 darauf hin, dass „die Formulierung ‚nicht zu einem Risiko‘ von ihrem Sinn und Zweck ausgehend als ‚nur zu einem geringen Risiko‘ führend verstanden“ wird.

Zur Erleichterung einer den Anforderungen entsprechenden Meldung und um notwendige Rückfragen zu minimieren, hat die LDI NRW ein Meldeformular entwickelt, das unter ldi.nrw.de zur Verfügung steht.

Hat eine "Datenpanne" voraussichtlich ein hohes Risiko z.B. für das Persönlichkeitsrecht zur Folge, muss der Verantwortliche zusätzlich zur Meldung an die Aufsichtsbehörde auch die betroffenen Personen unverzüglich informieren (Art. 34 DSGVO). Die klar und einfach zu formulierende Benachrichtigung entspricht inhaltlich im Wesentlichen der o.g. Meldung an die Aufsichtsbehörde (mit Ausnahme der Zahl der Betroffenen/Datensätze). Eine Pflicht zur Benachrichtigung besteht nur dann nicht, wenn eine der folgenden Bedingungen erfüllt ist (siehe Art. 34 Abs. 3 DSGVO):

• Es wurden geeignete technische und organisatorische Vorkehrungen in Bezug auf die von der Datenschutzverletzung betroffenen Daten getroffen, ausdrücklich insbesondere z.B. Verschlüsselung, durch die die personenbezogenen Daten für Unbefugte unzugänglich gemacht wurden.
• Durch Maßnahmen nach der Datenschutzverletzung ist sichergestellt, dass ein hohes Risiko für Rechte und Freiheiten der Betroffenen "aller Wahrscheinlichkeit nach nicht mehr besteht".
• Die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden, in diesem Fall muss stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.

Unabhängig von oben Gesagtem ist jede Datenschutzverletzung stets einschließlich aller damit im Zusammenhang stehenden Fakten, der Auswirkungen und ergriffenen Abhilfemaßnahmen zumindest zu dokumentieren. Dies soll der Aufsichtsbehörde z.B. die Überprüfung der Einhaltung der Melde- oder Benachrichtigungspflicht ermöglichen (Art. 33 Abs. 5 DSGVO).

Kontaktdaten der Aufsichtsbehörde

Die Landesbeauftragte für Datenschutz und Informationsfreiheit

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

Nordrhein-Westfalen (LDI NRW)
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Nach Art. 30 DSGVO muss jeder Verantwortliche ein Verzeichnis aller (Daten -) Verarbeitungstätigkeiten führen. Nach Erwägungsgrund 82 der DSGVO soll der Verantwortliche „zum Nachweis der Einhaltung dieser Verordnung" das Verzeichnis von Verarbeitungstätigkeiten führen. Weiterhin kann die zuständige Aufsichtsbehörde
die Vorlage verlangen, um die betreffenden Stellen hoheitlich zu kontrollieren.

Sind solche Verzeichnisse auch für heilberufliche Einrichtungen (*) verpflichtend?

Zwar ist nach Artikel 30 Abs. 5 DSGVO in Betrieben unter 250 Mitarbeitern eine Ausnahme von der Pflicht zur Führung eines Verfahrensverzeichnisses vorgesehen, die Ausnahme betrifft aber nicht den Bereich der Verarbeitung von Gesundheitsdaten i. S. d. Artikel 9 Abs. 1 DSGVO. In heilberuflichen Einrichtungen ist daher stets ein Verfahrensverzeichnis zu erstellen. Ein entsprechendes (unter allen deutschen Aufsichtsbehörden abgestimmtes) Muster für ein Verzeichnis von Verarbeitungstätigkeiten finden Sie auf der Homepage der LDI. Neben dem Muster gibt es auch Hinweise zum Ausfüllen des Verzeichnisses.

Eine Kompromisslösung auf europäischer Ebene besteht jedoch dahingehend, dass der Umfang der Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, auf die Verarbeitungstätigkeiten beschränkt wird, die unter die jeweilige Ausnahme von Art. 30 Abs. 5 DSGVO fallen. Konkret bedeutet das: In Betrieben unter 250 Mitarbeitern müssen nur die Datenverarbeitungsprozesse aufgeführt werden, die besondere Datenkategorien nach Art. 9 Abs. 1 DSGVO (wie zum Beispiel Gesundheitsdaten) betreffen oder ein Risiko für die Rechte und Freiheiten der betroffenen Personen in sich bergen oder nicht nur gelegentlich erfolgen.

Für die Form des Verarbeitungsverzeichnisses ist es ausreichend, wenn es in einem elektronischen Format (z.B. Excel-Liste) geführt wird (die „elektronische Form" iSd. § 126a BGB ist dagegen nicht erforderlich!).

Verweise auf die Verarbeitungsprozesse sind im Verzeichnis erlaubt. Inhaltlich nicht ausreichend ist aber z. B. eine einfache Zusammenstellung von internen Hyperlinks.

Ein Dokument, das auf beigefügte Anlagen verweist, genügt indes den Anforderungen.

Das Verarbeitungsverzeichnis ist nicht obligatorisch (wie früher das Verfahrensverzeichnis nach altem BDSG) zu veröffentlichen, sondern muss nur auf Anfrage der zuständigen Aufsichtsbehörde vorgelegt werden.

Im Gegensatz zum alten Verfahrensverzeichnis ist das Verarbeitungsverzeichnis auch nicht mehr zwingend an den Datenschutzbeauftragten zu übergeben, sondern ist nach der DSGVO unmittelbar vom Verantwortlichen zu führen. Es ist aber zulässig, den Datenschutzbeauftragten mit der Erstellung, der Führung und der Pflege des Verzeichnisses um Unterstützung zu bitten.

Die Inhalte des Verarbeitungsverzeichnisses sind vollumfänglich dem Art. 30 Abs. 1 DSGVO zu entnehmen. Danach muss das Verzeichnis folgende Angaben umfassen:

a) Name und Kontaktdaten des Heilberuflers bzw. der verantwortlichen Heilberufler, ggf. eines mitverantwortlichen Auftragnehmers sowie des etwaigen Datenschutzbeauftragten
b) Zwecke der Verarbeitung
c) Kategorien betroffener Personen und der zugehörigen personenbezogenen Daten
d) Kategorien von Empfängern personenbezogener Daten
e) ggf. Übermittlung von personenbezogenen Daten außerhalb der EU
f) vorgesehene Löschfristen für personenbezogene Daten eine allgemeine Beschreibung der technisch-organisatorischen Maßnahmen, die die Datensicherheit der personenbezogenen Daten sicherstellt gemäß Art. 32 Abs. 1 DSGVO.

Ein **Musterverzeichnis** der Verarbeitungstätigkeiten für Ihre Einrichtung finden Sie ebenfalls bei uns.

Anmerkung:

Werden Leistungen, die personenbezogene Daten berühren, durch einen vom Heilberufler beauftragten Dienstleister erbracht (Auftragsdatenverarbeitung), so

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

muss dieser gemäß Art. 30 Abs. 2 DSGVO ebenfalls ein Verfahrensverzeichnis führen. Die Inhalte sind der vorbenannten Vorschrift zu entnehmen.

PATIENTENEINWILLIGUNG ZUM DATENAUSTAUSCH MIT LEISTUNGSERBRINGERN

Hinweis: Es handelt sich nachstehend um ein **unverbindliches Muster** für eine Patienteneinwilligung, für dessen Richtigkeit oder Vollständigkeit angesichts der Verschiedenheit der Datenverarbeitungsvorgänge in der jeweiligen Behandlungseinrichtung **keine Gewähr** übernommen werden kann. Das Muster ist dem jeweiligen Einzelfall entsprechend anzupassen. Datenempfänger müssen namentlich genannt werden, eine Pauschalisierung ist nicht zulässig.

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer Daten ist uns wichtig. Aufgrund des Behandlungsverhältnisses mit Ihnen dürfen wir Ihre Daten erheben und verarbeiten. Um Ihre Daten im Zusammenhang mit Ihrer Behandlung an weitere Leistungserbringer (z.B. andere Ärzte, Krankenhäuser, Labore) übermitteln (z.B. mittels Arztbrief) oder von weiteren Leistungserbringern einholen zu dürfen, bedarf es Ihrer Einwilligung. Ohne diese ist uns eine adäquate Behandlung und Information der Mitbehandler und Dienstleistungserbringer nicht möglich. Anderenfalls müssen wir Sie bitten, die Daten selbst an die Leistungserbringer zu übermitteln oder von diesen einzuholen. Wir weisen Sie darauf hin, dass auf Basis der genannten Dokumente einen Rückschluss auf Ihr Krankheitsbild zulässt. Ihre Einwilligung können Sie uns im Folgenden erteilen:

Hiermit willige ich,

Name: _____ Geb.Datum: _____

Adresse: _____

ein, dass meine personenbezogenen Daten (z. B. Name, Krankenkasse, Anamnese, Diagnose) über die Behandlung bei _____(*Name, Adresse der Ärztin/des Arztes, kann von Arztpraxis vorausgefüllt werden)*

zum Zwecke der weiteren Behandlung, sonstigen ärztlichen Versorgung, lückenlosen Dokumentation **in dem erforderlichen Umfang** an

□ die/den weiterbehandelnde(n) Ärztin/Arzt (Name/Anschrift) _____

□ das Krankenhaus / das MVZ _____

□ das Labor _____

□ _____

□ **weitergegeben** werden dürfen.

□ von diesen über meine Behandlung dort **im erforderlichen Umfang eingeholt** werden dürfen.

Mir ist bekannt, dass ich diese Einwilligung gegenüber der Ärztin/dem Arzt jederzeit formlos widerrufen kann. Der Widerruf gilt nur mit Wirkung für die Zukunft; bisherige Datenweitergaben bleiben rechtmäßig.

_____ den _____ _____

Ort Datum Unterschrift Patient/in

Patienteneinwilligung zur Übermittlung und Einholung von Daten

Hinweis: Es handelt sich nachstehend um ein **unverbindliches Muster** für eine Patienteneinwilligung, für dessen Richtigkeit oder Vollständigkeit angesichts der Verschiedenheit der jeweiligen Datenverarbeitungsvorgänge in den unterschiedlichen heilberuflichen (*) Einrichtungen **keine Gewähr** übernommen werden kann und das dem jeweiligen Einzelfall entsprechend anzupassen ist. Datenempfänger müssen namentlich genannt werden, eine Pauschalisierung ist nicht zulässig.

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer Daten ist uns wichtig. Aufgrund des Behandlungsverhältnisses mit Ihnen dürfen wir Ihre Daten erheben und verarbeiten. Um Ihre Daten im Zusammenhang mit Ihrer Behandlung an weitere Leistungserbringer (z.B. andere Ärzte, Krankenhäuser, Labore) übermitteln (z.B. mittels Arztbrief) oder von weiteren Leistungserbringern einholen zu dürfen, bedarf es Ihrer Einwilligung. Ohne diese ist uns eine adäquate Behandlung und Information der Mitbehandler und Dienstleistungserbringer nicht möglich. Ansonsten müssen Sie ggf. selbst die notwendigen Informationen zur Verfügung stellen. Rezepte, Verordnungen und ähnliche Daten dürfen nur an Sie unmittelbar herausgegeben werden. Es bedarf Ihrer Einwilligung, wenn diese an Dritte, z. B. Angehörige oder Pflegeeinrichtungen, herausgegeben werden sollen. Der Abholer muss sich dabei entsprechend ausweisen. Wir weisen Sie darauf hin, dass die Herausgabe von Dokumenten einen Rückschluss auf Ihr Krankheitsbild zulässt.

Mit freundlichen Grüßen

(Arzt)

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

PATIENTENEINWILLIGUNG

ZUR ÜBERMITTLUNG UND EINHOLUNG VON DATEN

I. DATENAUSTAUSCH MIT LEISTUNGSERBRINGERN

Hiermit willige ich,

Name: _____ Geb.-Datum: _____

Adresse: _____

ein, dass meine personenbezogenen Daten (z. B. Name, Krankenkasse, Anamnese, Diagnose) über die Behandlung zum Zwecke der weiteren Behandlung, sonstigen ärztlichen Versorgung, lückenlosen Dokumentation

bei _____(*Name, Adresse der Ärztin/des Arztes*, k*ann vom Arzt/von der Ärztin vorausgefüllt werden)*

in dem erforderlichen Umfang an

□ die/den weiterbehandelnde(n) Ärztin/Arzt (Name/Anschrift) _____

□ das Krankenhaus / das MVZ _____

□ das Labor _____

□ _____

□ **weitergegeben** werden dürfen.

□ von diesen über meine Behandlung dort **im erforderlichen Umfang eingeholt** werden dürfen.

II. REZEPTE UND VERORDNUNGEN

□ Ich willige ein, dass

□ Rezepte

□ Überweisungen

□ Verordnungen

□ Medikationspläne

□ _____

an

□ Angehörige / Personen (bitte Namen einsetzen) _____

□ Mitarbeiter des Pflegedienstes / Seniorenheims_____

□ Apotheke _____

□ _____

□ _____

□ übermittelt/übersendet werden dürfen.

□ von diesen abgeholt werden dürfen.

Mir ist bekannt, dass ich diese Einwilligung gegenüber der Ärztin/dem Arzt jederzeit formlos widerrufen kann. Der Widerruf gilt nur mit Wirkung für die Zukunft; bisherige Datenweitergaben bleiben rechtmäßig.

_____ den _____ _____

Ort Datum Unterschrift

Patienteneinwilligung zur Übermittlung von Rezepten und Verordnungen

Hinweis: Es handelt sich nachstehend um ein **unverbindliches Muster** für eine Patienteneinwilligung, für dessen Richtigkeit oder Vollständigkeit angesichts der Verschiedenheit der jeweiligen Datenverarbeitungsvorgänge in den unterschiedlichen heilberuflichen (*) Einrichtungen **keine Gewähr** übernommen werden kann und das dem jeweiligen Einzelfall entsprechend anzupassen ist. Datenempfänger müssen namentlich genannt werden, eine Pauschalisierung ist nicht zulässig.

Sehr geehrte Patientin, sehr geehrter Patient,

der Schutz Ihrer Daten ist uns wichtig. Aufgrund des Behandlungsverhältnisses mit Ihnen dürfen wir Ihre Daten erheben und verarbeiten. Wir dürfen Rezepte, Verordnungen und ähnliche Daten nur an Sie unmittelbar herausgeben. Es bedarf Ihrer Einwilligung, wenn diese an Dritte, z. B. Angehörige oder Pflegeeinrichtungen, herausgegeben werden sollen. Der Abholer muss sich dabei entsprechend ausweisen. Wir weisen Sie darauf hin, dass auf Basis der genannten Dokumente einen Rückschluss auf Ihr Krankheitsbild zulässt.

Mit freundlichen Grüßen

(Arzt)

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

PATIENTENEINWILLIGUNG ZUR ÜBERMITTLUNG VON REZEPTEN UND VERORDNUNGEN

Hiermit willige ich,

Name: _____ Geb.Datum: _____

Adresse: _____

_____

ein, dass

□ Rezepte

□ Überweisungen

□ Verordnungen

□ Medikationspläne

□ _____

□ _____

□ _____

an

□ Angehörige / Personen (bitte Namen einsetzen) _____

_____

_____

_____

□ Mitarbeiter des Pflegedienstes / Seniorenheims _____

_____

_____

_____

□ Apotheke _____

_____

_____

□_____

□_____

□ übermittelt/übersendet werden dürfen

□ von diesen abgeholt werden dürfen.

Mir ist bekannt, dass ich diese Einwilligung gegenüber der Ärztin/dem Arzt jederzeit formlos widerrufen kann. Der Widerruf gilt nur mit Wirkung für die Zukunft; bisherige Datenweitergaben bleiben rechtmäßig.

_____ den _____ _____

Ort Datum Unterschrift

Musterverzeichnis von Verarbeitungstätigkeiten

Rechtliche Grundlage: Artikel 30 Absatz 1 Datenschutz -Grundverordnung (DSGVO)
Bitte berücksichtigen Sie, dass für jede identifizierte Verarbeitungstätigkeit je ein Verzeichnis zu führen ist! Das Muster beinhaltet mögliche Tätigkeiten, die individuell einzufügen sind.

Angaben zum Verantwortlichen

Name:
Anschrift:
Telefon:
E-Mail:
Internet -Adresse:

Angaben zur Person des Datenschutzbeauftragten (sofern gem. Art. 37 DSGVO benannt)

Vorname und Name:
Anschrift:
Telefon:
E-Mail:

Verarbeitungstätigkeit

Datum der Anlegung:
Datum der letzten Änderung:

Bezeichnung der Verarbeitungstätigkeit:	**Allgemeine Bezeichnung der dokumentierten Verarbeitungstätigkeit, z. B.:** * "Dokumentation der Behandlung" * "E -Mail -Verarbeitung" * "Lohn- und Gehaltsabrechnung"
Zweckbestimmung:	**z.B.:** * Verarbeitungstätigkeit: "Dokumentation der Behandlung" -> Zweckbestimmung: sachgerechte therapeutische Behandlung und Weiterbehandlung; Erfüllung gesetzlicher Pflichten * Verarbeitungstätigkeit: "E-Mailverarbeitung" -> Zweckbestimmung: Durchführung der elektronischen Kommunikation * Verarbeitungstätigkeit: "Lohn- und Gehaltsabrechnung" -> Zweckbestimmung: Erstellung der Lohnabrechnung; Erfüllung gesetzlicher Pflichten Es können auch mehrere Zweckbestimmungen für eine Verarbeitung angegeben werden.
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO **z.B.**:	* Verarbeitung besonderer Kategorien personenbezogener Daten, Gesundheitsdaten auf der Grundlage eines Behandlungsvertrages (Art. 9 Abs. 2 lit. h DSGVO) * Einwilligung (Art. 6 Abs. 1 lit. A, Art. 7 DSGVO) * Wahrung berechtigter Interessen des Verantwortlichen oder des Dritten (Art. 6 Abs. 1 lit. f DSGVO)

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern

Erhebung der Daten

Betroffene Personengruppen	**z.B.:** Patienten, Mitarbeiter, Bewerber
Beschreibung der Datenkategorien / Art der gespeicherten Daten	**z.B.:** * Name / Vorname / Anrede / Titel, Geburtsdatum, Adressdaten * Gesundheitsdaten (besondere Kategorien personenbezogener Daten) * Lohn- und Gehaltsdaten * Zeiterfassungsdaten * Sozialversicherungsdaten * Vertragsdaten

Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können

Interne Empfänger (innerhalb der Einrichtung des Verantwortlichen)	**z.B.:** Praxispersonal, Personalabteilung, Buchhaltung, Auftragsverarbeiter
Externe Empfänger und Dritte, soweit nicht Auftragsverarbeiter	**z.B.:** externe andere Arzte / Psychotherapeuten, Kassenärztliche Vereinigungen, Krankenkassen, der Medizinische Dienst der Krankenversicherung, Ärztekammern, privatärztliche Verrechnungsstellen

Datenübermittlung in Drittstaaten / internationale Organisationen (z. B. Cloud-Dienste)

Datenübermittlung in Drittstaaten	Sofern eine Datenübermittlung in Drittstaaten erfolgt, ist vorab zu klären, ob Datenüermittlungen in ein Drittland oder an eine internationale Organisation stattfinden. Die Übermittlung von personenbezogenen Daten in Drittländer ist ausschließlich zulässig, wenn neben der Rechtmäßigkeit der Datenverarbeitung weiterführend das durch die DSGVO gewährleistete Schutzniveau in dem jeweiligen Drittland nicht untergraben wird. (ggf. Auskunft von der Aufsichtsbehörde einholen)

Fristen für die Löschung der verschiedenen Datenkategorien

Daten sind zu löschen, wenn sie nicht mehr benötigt werden; dabei sind ggf. Aufbewahrungsfristen zu beachten	**z. B.:** §630 lit. f Abs. 3 BGB (Behandlungsdokumentation) § 28 Abs. 3 RöV

Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen (TOM)

Allgemeine Beschreibung der technischen	Maßnahmen müssen unter anderem Folgendes einschließen: * die Pseudonymisierung und Verschlüsselung personenbezogener

und organisatorischen Maßnahmen (Art. 32 Abs. 1 DSGVO) Und des etwaigen verbleibenden Risikos unter Berücksichtigung der eingesetzten technisch organisatorischen Maßnahmen	Daten; * die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen; * die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; * ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zweck der Datenverarbeitungen sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche geeignete TOM, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DSGVO).

Prüfung durch den Verantwortlichen

Prüfung	erfolgt / nicht erfolgt
Datum, Unterschrift (Verantwortlicher)	