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 Tätigkeit aber hauptsächlich nur Kriterium 4 (Vertrauliche Daten), Kriterium 5 (umfangreiche Datenverarbei-

[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

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

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

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 Maßnahmen 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 Ange-

hörigen 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									