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, die Rechtmäßigkeit von Datenverarbeitungsvorgängen zu überprüfen und die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen.

In heilberuflichen Einrichtungen wird in seltenen Fällen eine DSFA erforderlich sein. Im Vorfeld zu geplanten Datenverarbeitungsvorgängen muss jedoch 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 und auch nur ein 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. Nach Art. 35 Abs. 5 DSGVO kann eine entsprechende Liste auch für solche Datenverarbeitungsvorgänge veröffentlicht werden, bei denen explizit keine DSFA durchgeführt werden muss. (Beides ist bisher aber noch nicht geschehen!)

II. Grundsatz

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. Aber auch aus der Art der Daten, des Umfangs, der Umstände und der Zwecke der Verarbeitung können sich solche Risiken ergeben, deren Folgen abgeschätzt werden müssen.

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 gilt. Dies gilt insbesondere dann, wenn eine neue Datenverarbeitungstechnologie eingeführt wird.

III. Kriterien zur Beurteilung des Risikos und damit zur Frage der Erforderlichkeit der DSFA

Da Grundfrage für die Erforderlichkeit der Durchführung der DFSA, das Vorliegen eines „hohes Risikos“ ist, wird im Folgenden dargestellt, wie die Höhe des Risikos ermittelt werden kann:

1. Personenschädigung durch Datenverarbeitung

Hohe Risiken für die Rechte und Freiheiten natürlicher Personen können aus der Verarbeitung personenbezogener Daten hervorgehen, dies insbesondere dann, wenn es zu einem physischen, materiellen oder immateriellen Schaden, einer Rufschädigung, einem Identitätsdiebstahl oder –betrug, etc. (vgl. Erwägungsgrund (EW) 75 der DSGVO) kommen kann.

2. Einzelne Beurteilungskriterien

Bei der Beurteilung, ob aufgrund des hohen Risikos im Zusammenhang mit der Datenverarbeitung eine DSFA erforderlich ist, müssen folgende neun Kriterien[1] berücksichtigt werden:

1. Bewerten oder Einstufen, darunter das Erstellen von Profilen und Prognosen […]
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung […]
3. Systematische Überwachung […]
4. Vertrauliche Daten oder höchst persönliche Daten […]
5. Datenverarbeitung in großem Umfang […]
6. Abgleichen oder Zusammenführen von Datensätzen […]
7. Daten zu schutzbedürftigen Betroffenen […]
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen […]

[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 und gibt den Stand der Meinungsbildung vom 15.05.2018 wieder.

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

9. Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“ […]

Für Verarbeitungsvorgänge im Kontext der heilberuflichen Einrichtung (*) dürften als Kriterien für die Beurteilung, ob wahrscheinlich ein hohes Risiko vorliegt, hauptsächlich die **Kriterien Nr. 5, Nr. 7 und Nr. 8** einschlägig sein. Es bietet sich daher an, vor geplanten Datenverarbeitungen immer eine Vorprüfung auf Notwendigkeit einer Datenschutzfolgeabschätzung durchzuführen, die sogenannte „Schwellwertanalyse“. Ist das Ergebnis dieser Vorprüfung, dass durch die Datenverarbeitung aufgrund des Vorliegens der o. g. Kriterien wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen vorliegt, ist eine DSFA durchzuführen. Dies kann angenommen werden, wenn mindestens zwei dieser Kriterien erfüllt sind. Ist nach der Schwellwertanalyse eine DFSA nicht erforderlich, sollte dieses Ergebnis unbedingt dokumentiert werden, um diese Dokumentation erforderlichenfalls der Landesdatenschutzbeauftragen vorlegen zu können.

a) Daten zu schutzbedürftigen Betroffenen (Kriterium 7)

Daten zu schutzbedürftigen Betroffenen (Patientinnen/Patienten) werden als Risikokriterium angesehen, wenn zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt, d. h. den Personen ist es unter Umständen nicht ohne weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben. Als schutzbedürftige Betroffene gelten unter anderem Kinder, Senioren, Asylbewerber sowie insbesondere auch Patienten.

b) Anwendung neuer technologischer Lösungen (Kriterium 8)

aa) DFSA bei der Einführung eines neuen PVS oder neuer Funktionalitäten

Der Anwendung neuer technologischer Lösungen könnte in der heilberuflichen Einrichtung im Zusammenhang mit der Praxisverwaltungssoftware (PVS) Bedeutung zukommen. Die Anwendung neuer Technologien wird als Risikokriterium gesehen, da der Einsatz neuartiger Formen der Datenerfassung und -nutzung möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringen kann. Hier stellt sich die bis dato noch ungeklärte Frage, inwieweit PVS-Systeme als neue Technologie anzusehen sind. Denkbar wäre dies – jedenfalls nach hiesiger Auffassung – nur dann, wenn das PVS um neue Auswertungsfunktionalitäten für Patientendaten erweitert wird oder ein neues PVS mit erweiterten Funktionalitäten eingeführt wird. Im Regelfall wird man aber eher davon ausgehen dürfen, dass PVS-Systeme nicht als neue Technologien anzusehen sind.

Würde man jedoch im Einzelfall davon ausgehen, dass aufgrund einer neuen Funktionalität auch eine neue Technologie verwendet wird, dann dürfte eine DFSA regelhaft vorab durchzuführen sein, da PVS-Systeme immer auch Daten schutzbedürftiger Betroffener (s.o.) verarbeiten und damit automatisch zwei Kriterien erfüllt werden. Werden zwei Kriterien erfüllt, ist in den meisten Fällen eine DFSA obligatorisch durchzuführen (vgl. oben).

Generell ist daher zu empfehlen, vor der Einführung einer neuen PVS-Funktionalität oder eines neuen PVS, immer im Rahmen einer Schwellwertanalyse die Erforderlichkeit der DSFA zu prüfen. Ist danach keine DFSA durchzuführen, ist das Ergebnis dieser Analyse unbedingt zu dokumentieren (s.o.).

bb) DFSA bei geplanter Videoüberwachung (Kriterium 3)

Neue Technologien spielen häufig auch im Praxisumfeld eine Rolle. Insbesondere im Hinblick auf eine geplante oder ggf. bestehende **Videoüberwachung** ist eine DSFA zu erwägen (vgl. EW 91: optoelektronische Vorrichtungen). Hierfür gilt im Übrigen auch das Regelbeispiel des Art. 35 Abs. 3 c) DSGVO, wonach bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche zwingend eine DFSA durchzuführen ist. Danach ist bei einer weiträumigen und systematischen Überwachung die DFSA immer obligat durchzuführen. Allerdings dürfte es, soweit z.B. nur der Eingangsbereich der heilberuflichen Einrichtung überwacht wird, an der geforderten Weiträumigkeit und Systematik der Überwachung öffentlich zugängliche Bereiche fehlen. Daher dürfte eine DSFA bei der Videoüberwachung von heilberuflichen Einrichtung in den seltensten Fällen erforderlich sein. Davon unabhängig sind aber zu der generellen Zulässigkeit der Videoüberwachung von Arztpraxen insbesondere die Bestimmungen des § 4 BDSG zu beachten (vgl. hierzu das Informationsblatt Videoüberwachung in heilberuflichen Einrichtungen).

c) Umfangreiche Datenverarbeitung (Kriterium 5)

Nach dem Regelbeispiel des Art. 35 Abs. 3 DSGVO ist bei der umfangreichen Verarbeitung von Daten besonderer Kategorien eine DSFA vor einer geplanten Datenverarbeitung zwingend erforderlich. Im Fall der heilberuflichen Einrichtung betreffen geplante umfangreiche Verarbeitungsvorgänge hauptsächlich Gesundheitsdaten.[2]

[2] In heilberuflichen Einrichtungen werden auch Daten des dort angestellten Personals gespeichert. Hier dürfte der Umfang der

Gesundheitsdaten sind personenbezogene Daten besonderer Kategorie nach Art. 9 Abs. 1 DSGVO. Daher hat die Frage, wann eine umfangreiche Datenverarbeitung in der heilberuflichen Einrichtung vorliegt, eine große praktische Relevanz.

Der Begriff „umfangreiche Verarbeitung“ nach Art. 35 Abs. 3 b) ist in der DSGVO nicht definiert. Aus dem EW 91 der DSGVO ergeben sich jedoch Anhaltspunkte dazu, was der europäische Normgeber unter einer umfangreichen Datenverarbeitung versteht.

Danach sind für umfangreiche Verarbeitungsvorgänge solche, „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. […]“

Aus diesem Eingangssatz zum EW 91 lässt sich schließen, dass die DSFA vor allem für die Datenverarbeitung großer Konzerne gedacht ist. Daher ist hier die Rede von „großen Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene“ und bei denen in „großem Umfang eine neue Technologie eingesetzt wird“. (vgl. zu der Frage der umfangreichen Datenverarbeitung zudem die Ausführungen unter aa) und bb))

a. Einzelpraxen

Heilberufler in Einzelpraxen sind grundsätzlich aufgrund ihrer Größe und der damit verbundenen Menge der Daten, die dort verarbeitet werden, von der Pflicht zur Durchführung einer DSFA ausgenommen.

Im letzten Satz des EW 91 werden u.a. „einzelne Ärzte“ aufgrund ihres per se vermutlich geringen Datenverarbeitungsumfangs - sozusagen als Untergrenze - von der Pflicht zur Durchführung einer DSFA grundsätzlich befreit („negatives Regelbeispiel“): „[…] 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.“

Der EW 91 schließt allerdings mit seiner Formulierung „…Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten…“, nicht aus, dass in ganz besonderen Fällen (z.B. bei der Verarbeitung genetischer Daten, vgl. EW 75) auch bei einem Einzelarzt eine DSFA notwendig sein könnte.
In diesem Zusammenhang wird teilweise auch die Auffassung vertreten, dass niedergelassene Heilberufler generell, auch wenn sie in der Kooperationsform der Gemeinschaftspraxis oder in einem MVZ tätig sind, von der Pflicht zur DSFA ausgenommen sei, da sie im Verhältnis zu ihren Patienten immer einzelne Ärzte bleiben würden .Aus dem EW 91 geht jedoch das Gegenteil hervor: Die explizite Herausnahme von der Pflicht zur DSFA für Einzelpraxen indiziert, dass Heilberufler generell nicht von der DSFA ausgenommen sind. Hätte der Normgeber Heilberufler generell von dieser Pflicht befreien wollen, hätte er dies genau an dieser Stelle getan. Vielmehr hat sich der Normgeber dafür entschieden, bei „Einzelheilberuflern“ sozusagen pauschal die Untergrenze zu ziehen, bei der eine DSFA wohl nicht erforderlich ist.
Eine DSFA kann für eine Einzelpraxis allerdings durchzuführen sein, wenn die Voraussetzung unter III. d) vorliegen, z. B. bei der Verarbeitung genetischer Daten.

bb) Gemeinschaftspraxen / MVZ

Die ausdrückliche Herausnahme der Einzelpraxen von der Pflicht zur Durchführung der DSFA in EW 91 (s.o.) lässt indes nicht den Umkehrschluss zu, dass nunmehr alle **Gemeinschaftspraxen oder MVZ** vor geplanten Verarbeitungsvorgängen immer eine DSFA durchführen müssten. Hier kommt es wiederum auf den Umfang der geplanten Datenverarbeitung (Art. 35 Abs. 1 i.V.m. EW 91 sowie EW 89 der DSGVO) an.

Bei der Beurteilung, ob eine umfangreiche Datenverarbeitung vorliegt, sind insbesondere folgende Faktoren[3] zu berücksichtigen[4]:

- die Anzahl der von der Datenverarbeitung betroffenen Subjekte, entweder absolut oder prozentual im Verhältnis zur relevanten Bevölkerung;
- der Umfang der Daten und/oder der Umfang der in die Datenverarbeitung einbezogenen verschiedenen Datenarten

Datenmenge selbst in Berufsausübungsgemeinschaften mit mehr als 10 Beschäftigten nicht die Schwelle einer umfangreichen Datenverarbeitung erreichen. Daher wird diese Frage vorliegend ausgeklammert.

[3] Die Übersetzung aus dem Englischen ist durch den Autor selbst erfolgt – daher wird keine Gewähr für deren Richtigkeit übernommen.
[4] Die Art. 29 Arbeitsgruppe der EU hat sich damit bereits in ihrem Working Paper 29 (WP 29) auseinandergesetzt.und später in WP 248.

- die Zeitdauer oder Dauerhaftigkeit/Beständigkeit der Datenverarbeitungsaktivität;
- die geografische Reichweite der Datenverarbeitungsaktivität.

Unter Berücksichtigung dieser Kriterien nach der Leitlinie der Arbeitsgruppe 29 zur umfangreichen Datenverarbeitung dürfte bei der Verarbeitung von Patientendaten in Gemeinschaftspraxen/MVZ in der Mehrzahl der Fälle keine umfangreiche Datenverarbeitung vorliegen.

Dabei kommt es insbesondere auf die Größe der heilberuflichen Einrichtung, die Anzahl der Patienten und die konkret geplante Datenverarbeitung an. Bei durchschnittlichen Gemeinschaftspraxen mit 2 - 4 Heilberuflern dürfte es im Regelfall an einer umfangreichen Datenverarbeitung fehlen. Dies ergibt sich aus der Tatsache, dass die Anzahl der von der Datenverarbeitung betroffenen Personen (Patienten) auch bei einer Gemeinschaftspraxis von bspw. vier in Vollzeit arbeitenden Heilberuflern noch vergleichsweise gering ist. Bei einer hausärztlichen Gemeinschaftspraxis z.B. wären das max. 4000 Patienten pro Quartal. Verglichen mit der Datenverarbeitung bei Versicherungskonzernen oder Internet-Unternehmen sind dies nur wenige betroffene Personen.

Das gleiche gilt für die geografische Reichweite der Datenverarbeitungsaktivität. Diese ist nur sehr begrenzt, da der Einzugsbereich auch bei Gemeinschaftspraxen/MVZ selten mehr als 30 bis 40 Kilometer betragen dürfte. Etwas anderes könnte sich bei standortübergreifenden Berufsausübungsgemeinschaften ergeben. Aber auch hier sind die verschiedenen Standorte regelhaft unweit entfernt, so dass auch bei standortübergreifenden BAG in den meisten Fällen nur eine lokale Datenverarbeitungsaktivität anzunehmen sein dürfte.

Auch ist die Datenverarbeitung nur dann permanent (i.S.v. zeitlich beständig), wenn der Patient seinen Arzt jedes Quartal aufs Neue aufsucht. Dabei ist der Umfang der Daten überschaubar. Eine Kombination von Datenarten im engeren Sinne liegt nicht vor, da in den Praxisverwaltungssystemen in der Regel nur Gesundheitsdaten gespeichert werden.

In Bezug auf den Umfang der Zusammenführung/Kombination von Daten ist indes zwischen Gemeinschaftspraxen gleicher und unterschiedlicher Fachrichtung zu unterscheiden. Bei fachungleichen Gemeinschaftspraxen ist die Datentiefe – aufgrund der verschiedenen Fachrichtungen – deutlich größer und das potentielle Risiko dementsprechend höher.

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 Team zusammen zu stellen, das die Zwecke der einzelnen Verarbeitungsvorgänge prüft und die Risikobewertung und Abwägung zum Zweck und der Notwendigkeit der Datenverarbeitung durchführt. 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. Bestellung eines Datenschutzbeauftragten (DSB) als Konsequenz der Pflicht zur Durchführung der DSFA

Die Pflicht zur Durchführung eines DFSA löst nach § 38 Abs. 1 Satz 2 BDSG wiederum die Pflicht zur Benennung eines DSB aus. Die Bestellpflicht aufgrund der DFSA entsteht unabhängig von der Anzahl der mit der Datenverarbeitung beschäftigten Personen in der heilberuflichen Einrichtung. Auch wenn in der Praxis weniger als 10 Mitarbeiter mit der Datenverarbeitung beschäftigt sind, muss in diesen Fällen ein Datenschutzbeauftragter benannt werden (s. Infoblatt Betrieblicher Datenschutzbeauftragter).

VI. Fazit

Inhaber von Einzelpraxen müssen sich mit dem Thema Datenschutz-Folgenabschätzung im Grunde nicht beschäftigen, da diese hier nach den EW 91 der DSGVO nur in absoluten Ausnahmefällen erforderlich sein dürfte.

Auch für Datenverarbeitungsvorgänge von Gemeinschaftspraxen wird die Datenschutz-Folgenabschätzung regelhaft nicht erforderlich sein, da der Umfang der Datenverarbeitung hier immer noch als vergleichsweise gering einzuschätzen ist. Etwas anderes kann sich eventuell für große überörtliche und fachungleiche Gemeinschaftspraxen oder MVZ ergeben. Gleichwohl dürfte auch hier – außer bei sehr großen Praxiskonstellationen - eine DSFA im Regelfall nicht erforderlich sein. Allen grö-

ßeren Praxen, insbesondere Inhabern von Berufsausübungsgemeinschaften, ist zu empfehlen – obwohl eine DSFA nur in wenigen Fällen verpflichtend sein dürfte – vor jeder geplanten Datenverarbeitung eine Schwellwertanalyse durchzuführen.

Hinweis: Die Entscheidung, die DSFA nicht durchzuführen, sollte unter Angabe der maßgeblichen Erwägungen dokumentiert werden, um sie bei Bedarf der Aufsichtsbehörde vorlegen zu können. Der Verantwortliche hat insofern eine Nachweispflicht.

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.