Müssen Arztpraxen eine Datenschutz-Folgenabschätzung für geplante Datenverarbeitungsvorgänge durchführen?

Stand: 06.02.2018

Mit der Datenschutzgrundverordnung (DSGVO) wird das Konzept der Datenschutz-Folgenabschätzung in das europäische Datenschutzrecht integriert. Die Datenschutz-Folgenabschätzung (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.

Im Vorfeld zu geplanten umfangreichen Datenverarbeitungsvorgängen muss 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 und auch nur ein geringes Risiko besteht, muss die DSFA nicht durchgeführt werden. Andernfalls muss eine DSFA erfolgen.

Anmerkung:
Die Aufsichtsbehörden erstellen nach Art. 35 Abs. 4 DSGVO eine Liste der Verarbeitungsvorgänge für die (immer) eine DSFA durchzuführen ist. Nach Absatz 5 DSGVO kann eine entsprechende Liste auch für solche Datenverarbeitungsvorgänge veröffentlicht werden, bei denen explizit keine DFSA durchgeführt werden muss. (Beides ist bisher aber noch nicht geschehen!)

Im Fall der Arztpraxis betreffen geplante umfangreiche Verarbeitungsvorgänge im Grunde ausschließlich Gesundheitsdaten.[1] Gesundheitsdaten sind personenbezogene Daten gemäß Art. 9 Abs. 1 DSGVO, für die nach dem Regelbeispiel Art. 35 Abs. 3 b) bei ihrer Verarbeitung immer dann ein hohes Risiko angenommen wird, wenn sie umfangreich ist.

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

> ***EW 91 S. 1:*** *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 be-troffenen 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“.

a) Einzelpraxen

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 DFSA 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.*

Ärzte in Einzelpraxen sind daher grundsätzlich von der Pflicht zur Durchführung einer DSFA ausgenommen.

Der EW 91 legt allerdings mit seiner Formulierung „…Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten…“, nahe, dass in ganz besonderen Fällen auch bei einem Einzelarzt eine DFSA notwendig sein könnte. Dies dürfte aber rein hypothetischer Natur sein, so dass die Datenschutz-Folgenabschätzung für Ärzte in Einzelpraxis grundsätzlich nicht erforderlich ist.

[1] In Arztpraxen werden auch Daten des dort angestellten Personals gespeichert. Hier dürfte der Umfang der Datenmenge selbst in BAG mit mehr als 10 Angestellten nicht die Schwelle einer umfangreichen Datenverarbeitung erreichen. Daher wird diese Frage vorliegend ausgeklammert.

Anmerkung:
In diesem Zusammenhang wird teilweise auch die Auffassung vertreten, dass niedergelassene Ärzte, auch wenn sie in der Kooperationsform der Gemeinschaftspraxis oder in einem MVZ tätig sind, generell von der Pflicht zur DFSA 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 DFSA für Einzelpraxen indiziert, dass Ärzte generell nicht von der DFSA ausgenommen sind. Hätte der Normgeber Ärzte generell von dieser Pflicht befreien wollen, hätte er dies genau an dieser Stelle getan. Vielmehr hat sich der Normgeber dafür entschieden, bei Einzelärzten sozusagen pauschal die Untergrenze zu ziehen, bei der eine DFSA wohl nicht erforderlich ist.

b) Berufsausübungsgemeinschaften

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

Die Art. 29 Arbeitsgruppe[2] hat sich damit bereits in ihrem Working Paper (WP) 29 auseinandergesetzt und darauf in dem aktuellen WO 248 zur DFSA wieder zurückgegriffen. Danach seien bei der Beurteilung, ob eine umfangreiche Datenverarbeitung vorliegt, insbesondere folgende Faktoren[3] zu berücksichtigen:

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

Unter Berücksichtigung dieser Faktoren nach den Leitlinien des WP 248 der Arbeitsgruppe 29 zur umfangreichen Datenverarbeitung, dürfte bei der Verarbeitung von Patientendaten in Gemeinschaftspraxen/MVZ in der überwiegenden Zahl der Fälle keine umfangreiche Datenverarbeitung vorliegen.

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

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 BAG ergeben. Aber auch hier sind die Standorte in der vertragsärztlichen Versorgung regelhaft unweit entfernt. Es handelt sich daher im Grunde um eine lokale Datenverarbeitungsaktivität.

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 bzw. eine Kombination von Datenarten im engeren Sinne liegt nicht vor, da in den PVS 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.

[2] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[3] Die Übersetzung aus dem Englischen ist durch den Autor selbst erfolgt – daher wird keine Gewähr für deren Richtigkeit übernommen.

Fazit

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

Auch für Gemeinschaftspraxen und MVZ 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/MVZ ergeben. Gleichwohl dürfte auch hier – außer bei sehr großen Praxiskonstellationen - eine DSFA im Regelfall nicht erforderlich sein.

Den BAG ist zu empfehlen – obwohl eine DSFA nur in wenigen Fällen verpflichtend sein dürfte – in jedem Fall vor jeder geplanten Datenverarbeitung eine Prüfung auf Erforderlichkeit der DSFA 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.

Erwägungsgrund 91 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.