14 Pflicht zur Vornahme einer Datenschutzfolgenabschätzung

14.1 Einführung in die Datenschutzfolgenabschätzung

Zunehmend wird in den einschlägigen Medien, auf Veranstaltungen etc. die Frage aufgeworfen, ob ein Arzt zukünftig aufgrund der Vorgaben der DSGVO eine bzw. mehrere sog. Datenschutzfolgenabschätzungen (im Nachfolgenden DSFA) durchführen muss. Dabei fällt jedoch auch schnell auf, dass dieses Thema zwar immer angerissen wird, aber in den seltensten Fällen konkrete Ausführungen dazu gemacht werden, was dieser sperrige Begriff eigentlich meint, wann eine DSFA nötig ist und ganz besonders auch, wie eine DSFA durch wen durchgeführt werden sollte. Dass dieses Thema immer, wenn es um die DSGVO geht, zwar der Vollständigkeit halber genannt, aber nie eingehend thematisiert wird, ist auch nicht verwunderlich. Denn es handelt sich um einen nur schwer vollständig greifbaren, hochkomplexen, bisher noch wenig thematisierten Bereich des Datenschutzes. Im Prinzip weiß daher derzeit eigentlich noch keiner so wirklich, wie man mit einer DSFA umgehen muss. Um Ihnen, lieber Leser, jedoch eine kleine Vorstellung davon zu geben, was eine DSFA ist und was möglicherweise auf Sie zukommen könnte, wenn ein von Ihnen geplanter Verarbeitungsvorgang die Notwendigkeit zur Durchführung einer DSFA auslöst, sollen im Nachfolgenden die wichtigsten Aspekte zur DSFA dargestellt werden.

Ob ein Arzt/eine Praxis zur Durchführung einer DSFA verpflichtet ist, lässt sich nicht generell sagen und hängt wie immer vom jeweiligen Einzelfall ab.

Es gilt die Grundformel, dass, wenn **viele Personen** auf eine **Vielzahl von sensiblen Daten** mittels **neuester Technologie** zugreifen können und die Auswirkungen einer „falschen" bzw. unerlaubten Datenverarbeitung **hohe Risiken für die Betroffenen** bedeuten können, es nicht unwahrscheinlich ist, dass eine DSFA durchgeführt werden muss.

Die DSFA, im Englischen als „privacy impact assessment" bezeichnet, ist der Nachfolger der damaligen, in Deutschland mehr oder weniger bekannten und etablierten „Vorabkontrolle". Sowohl die Vorabkontrolle als auch die DSFA betreffen Datenverarbeitungen, die für Betroffene, aus welchen Gründen auch immer, mit einem hohen, wie auch immer gearteten Risiko verbunden sind. Aufgrund der Risikogeneigtheit dieser Verarbeitungen sieht es der EU-Gesetzgeber als zwingend notwendig an, dass Verantwortliche bei der DSFA die relevanten Verarbeitungen genau analysieren, bewerten und entsprechend des Risikos die notwendigen technischen und organisatorischen Schutzmaßnahmen treffen (*vgl. hierzu auch Kapitel 16*).

14.2 Pflicht zur Durchführung

Um sich eine grobe Vorstellung von einer DSFA zu verschaffen, empfiehlt sich zunächst der Blick in den Gesetzeswortlaut von Art. 35 Abs. 1. Hierin heißt es (wesentliche Anforderungen sind hervorgehoben):

*„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."*

Aus dieser Regelung lässt sich schon einiges zum Wesen der DSFA und zu der Frage, wann eine solche Abschätzung von wem vorzunehmen ist, ableiten.

14.3 Verpflichteter zur DSFA = Der Verantwortliche

Verpflichteter zur Durchführung einer DSFA ist nach Art. 35 Abs. 1 DSGVO der Verantwortliche. Dies ist je nach Organisationsstruktur der Einzelarzt, die Praxis, das MVZ, das Krankenhaus etc. (Hinweise dazu, wer in den jeweiligen Organisationen verantwortlich ist, finden sich in *Kapitel 4.2*.)

Hersteller von Medizinprodukten oder sonstiger Software, mit der Patientendaten verarbeitet werden sollen, sind deshalb, wenn sie nicht als (Mit-)Verantwortliche für diese Verarbeitung anzusehen sind, von sich aus auch nicht verpflichtet, eine solche Abschätzung vorzunehmen. Weil sie aber oftmals die einzigen sein dürften, die gewisse Fragen im Rahmen einer DSFA beantworten können, ist es essenziell, sie vertraglich zu verpflichten, bei einer DSFA, die eine Praxis/MVZ ggf. durchführen muss, ggf. als Auftragsverarbeiter mitzuwirken (*siehe hierzu Kapitel 17.3.6*).

Es ist daher dringend anzuraten, die bisher bestehenden vertraglichen Regelungen mit diesen Herstellern (Auftragsverarbeitern) danach zu überprüfen, ob und inwiefern die entsprechenden Hersteller als Auftragsverarbeiter den Verantwortlichen bei der Durchführung der DSFA zu unterstützen haben.

Nach Analyse der einzelnen Verträge dürfte sich ein sehr gemischtes Bild ergeben. So dürfte man schnell feststellen, dass in manchen Verträgen derartige Klauseln fehlen. Manche Verträge beinhalten explizit eine solche Regelung, in manchen ist sie verklausuliert enthalten. Es dürfte aber auch Verträge geben, die grundsätzlich solche Klauseln enthalten. Doch wird darin vielfach geregelt, dass der Auftragsverarbeiter den Verant-

wortlichen nur gegen eine entsprechende (entgeltliche) Aufwandsentschädigung bei der DSFA unterstützen wird. In der DSGVO ist von einer Entgeltlichkeit der Unterstützung durch den Auftragsverarbeiter jedoch keine Rede und es widerspricht eigentlich auch dem Wesen einer Auftragsverarbeitung, dass ein Auftragsverarbeiter diese essenziellen Informationen nur gegen Geld an den Verantwortlichen gibt. Aus diesem Grund ist zu empfehlen, derartige, für den Verantwortlichen (z. B. den Arzt) nachteilige Klauseln aus den Verträgen zu streichen bzw. nicht zu akzeptieren!

14.4 Verarbeitungsvorgang

Eine DSFA bezieht sich grundsätzlich auf einen bzw. mehrere Verarbeitungsvorgänge. Mit Verarbeitungsvorgang ist die Gesamtheit bestimmter Datenverarbeitungstätigkeiten gemeint, die notwendig sind, um einen oder mehrere bestimmte Zwecke zu erfüllen. Der Begriff „Verarbeitungsvorgang" erfasst damit automatisch die in Zusammenhang mit diesem Vorgang stehenden zu verarbeitenden Daten inkl. der an der Verarbeitung beteiligten IT-Systeme und Geschäftsprozesse (*siehe hierzu auch Kapitel 11.4*). Gerade weil für die DSFA eine genaue Kenntnis über die entsprechenden Verarbeitungsvorgänge essenziell ist, ist eine umfassende Transparenz über alle der relevanten, zu verarbeitenden Daten, der konkreten Datenflüsse, der an der Datenverarbeitung beteiligten Parteien und der eingesetzten IT-Systeme zwingend notwendig (*vgl. Kapitel 7.4*).

Nur wenn man weiß, wie die Datenverarbeitung genau stattfindet, ist es möglich, etwaige Gefahren/Risiken zu identifizieren und zu bewerten.

Es ist ferner auch durchaus möglich, mehrere Verarbeitungsvorgänge/Verarbeitungstätigkeiten, die mit einem ähnlichen/vergleichbaren Risiko einhergehen, in einer DSFA gemeinsam zu betrachten und zu bewerten. Ähnliche Risiken dürften insbesondere dort bestehen, in denen ähnliche bzw. miteinander

vernetzte Technologien zur Erfüllung eines Zwecks eingesetzt werden (bspw. vernetzte Software-Medizinprodukte, die alle gemeinsam an ein Patientenmanagementsystem angeschlossen sind.)

14.5 Erforderlichkeit der Durchführung

Wie u. a. in *Kapitel 12.1.4* dargestellt, muss theoretisch bei jeder in einer Praxis, MVZ oder im Krankenhaus durchgeführten Verarbeitungstätigkeit eine mehr oder weniger umfangreiche Risikoanalyse durchgeführt werden. Kommt man im Rahmen dieser Analyse zum Ergebnis, dass bei der Datenverarbeitung ein hohes Risiko für Betroffene besteht und somit ein gewisser „Risikoschwellenwert" überschritten ist, gilt es, eine DSFA durchzuführen. Um der in Art. 5 Abs. 2 enthaltenen Rechenschaftspflicht gerecht zu werden, gilt es in jedem Falle, die Entscheidung hinsichtlich der Durchführung einer DSFA inkl. der Angabe der diesbezüglichen Erwägungen ausreichend zu dokumentieren.

Wie aus Art. 35 Abs. 3 deutlich wird, sieht die DSGVO insbesondere bei Persönlichkeitsbewertungen („Profiling"), beim Scoring, bei einer Videoüberwachung (im öffentlichen Raum), bei umfangreichen Verarbeitungen besonderer Kategorien von Daten (wie Patienten-/Gesundheitsdaten) gemäß Art. 9, 10 oder beim Einsatz neuer Technologien, deren Funktions-/Wirkungsweise man bzw. der Verantwortliche/Auftragsverarbeiter noch nicht einschätzen kann, als erforderlich an. In all diesen Fällen dürfte entweder aufgrund der Menge der zu verarbeitenden Daten, der Sensibilität der Daten oder der nur schwer einzuschätzenden Konsequenzen, ein hohes Risiko für Betroffene mit der Datenverarbeitung verbunden sein. Der Datenschutzausschuss, als Vereinigung der europäischen Aufsichtsbehörden, wird bald auf seiner Webseite eine Liste veröffentlichen, in denen die Verarbeitungsvorgänge/-tätigkeiten aufgeführt sind, bei denen zwingend eine DSFA durchzuführen ist.