Datenschutz-Folgenabschätzung

Die Kassenärztliche Vereinigung Westfalen-Lippe (KVWL) möchte Vertragsärzten und Vertragspsychotherapeuten eine Hilfestellung zur Umsetzung der seit dem 25. Mai 2018 anzuwendenden EU-Datenschutz-Grundverordnung (DS-GVO) geben. Hierzu veröffentlicht die KVWL die Serie „DS-GVO kompakt", die sukzessive wichtige Pflichten der DS-GVO behandelt.
Teil 5 widmet sich der Datenschutz-Folgenabschätzung (DSFA) und deren Voraussetzungen.

Einführung

Die Verarbeitung von Gesundheitsdaten beinhaltet aufgrund der Sensibilität dieser Daten immer ein gewisses Risiko. Realisieren kann sich ein solches Risiko insbesondere in Form von Datenpannen, die den Verlust der Vertraulichkeit der Daten mit sich bringen. Denkbar sind verschiedene Szenarien wie Hackerangriffe, Viren, Anwendungsfehler o. ä. Da sich als Konsequenz solcher Datenpannen durchaus empfindliche Schäden, wie z. B. Diskriminierung oder Rufschädigung ergeben können, sieht die DS-GVO unter bestimmten Voraussetzungen verpflichtend die Durchführung einer DSFA vor. Diese soll mit geeigneten – meist technisch-organisatorischen – Maßnahmen dabei helfen, die Risiken einzudämmen.

Erforderlichkeit einer DSFA

Der verantwortliche Praxisinhaber kann sich freiwillig für die Durchführung einer DSFA entscheiden. Unter den nachfolgenden Bedingungen ist er hierzu jedoch verpflichtet. Ob die DSFA in der Arztpraxis verpflichtend ist, ist von dem Ergebnis einer Vorprüfung abhängig. Ziel der Vorprüfung ist festzustellen, ob durch die Datenverarbeitung voraussichtlich ein hohes Risiko (für die Rechte der von der Datenverarbeitung betroffenen Personen) entsteht und wie diesem begegnet werden kann. Wird die „Risikoträchtigkeit" der Verarbeitung bejaht, ist eine DSFA durchzuführen. Wird hingegen festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, ist eine DSFA nicht zwingend erforderlich. Allerdings sind auch beim Absehen von der DSFA die hierfür maßgeblichen Gründe schriftlich zu dokumentieren; dies folgt aus der Verpflichtung zur Rechenschaftslegung.[1]

Die DS-GVO selbst benennt einen Katalog von Faktoren, die nach Wertung des Verordnungsgebers wahrscheinlich zu einem hohen Risiko führen. Daneben haben die unabhängigen Datenschutzbehörden des Bundes und der Länder eine sog. „Blacklist" oder „Muss-Liste" veröffentlicht, in der Verarbeitungsvorgänge genannt sind, die in jedem Fall eine DSFA auslösen.[2] Für Arztpraxen sind hier lediglich Telemedizin-Lösungen benannt. Von den aus der DS-GVO stammenden Faktoren sind im Rahmen der Vorprüfung für die Arztpraxis insbesondere die im Folgenden benannten von Bedeutung:

a) Umfang der Datenverarbeitung

Gesundheitsdaten nach Art. 9 Abs. 1 DS-GVO sind personenbezogene Daten besonderer Kategorie, bei denen eine DSFA immer schon dann durchzuführen ist, wenn eine umfangreiche Verarbeitung stattfindet.

Bei Einzelpraxen (auch in Praxisgemeinschaft) liegt nach Auffassung des Normgebers per se keine umfangreiche Datenverarbeitung vor, weshalb hier grundsätzlich keine DSFA durchzuführen ist.[3]

Daraus folgt jedoch im Umkehrschluss nicht, dass in Gemeinschaftspraxen oder MVZ immer eine DSFA vorzunehmen ist,

Teil 5

weil dort eine umfangreiche Datenverarbeitung unterstellt werden muss. Als Faustregel wird derzeit davon ausgegangen, dass eine solche die DSFA auslösende umfangreiche Datenverarbeitung erst bei Gemeinschaftspraxen und MVZ vorliegt, in denen mehr als vier Ärzte tätig sind.

Auf jeden Fall ist aber eine DSFA durchzuführen, wenn für die Praxis ein betrieblicher Datenschutzbeauftragter bestellt werden muss.[4] Da die Bestellung eines betrieblichen Datenschutzbeauftragten davon abhängig ist, ob zehn oder mehr Personen (unabhängig, ob Arzt oder sonstiges Praxispersonal) ständig mit der Datenverarbeitung beschäftigt sind, unterstellt der Gesetzgeber wohl, dass damit auch zwangsläufig eine umfangreiche Datenverarbeitung einhergeht.

b) **Sonstige Gründe**
Im Einzelfall kann die Pflicht zur Durchführung einer DSFA unabhängig vom Umfang der Datenverarbeitung schon allein aufgrund der Art der verarbeiteten Daten bestehen. Dies ist beispielsweise der Fall, wenn besonders sensible genetische Daten verarbeitet werden (z. B. im Bereich der Reproduktionsmedizin).

Eine Videoüberwachung kann auch Anlass für eine DSFA sein. Nach der Rechtslage ist dies allerdings nur dann der Fall, wenn das Kriterium der „weiträumigen Überwachung öffentlich zugänglicher Bereiche“ erfüllt ist.[5] Eine Videoüberwachung in einer Arztpraxis erfasst grundsätzlich nur den dortigen eingeschränkten Publikumsverkehr, so dass das für eine DSFA maßgebliche Kriterium in der Regel „quantitativ“ nicht erfüllt ist.

c) **Verarbeitungen durch andere Stellen**
Bei Verarbeitungen, die aus technisch-organisatorischer Sicht von einer anderen Stelle betrieben werden, endet die Verantwortlichkeit der Praxis in der Regel bei der Übergabe der personenbezogenen Daten in die „fremde“ Infrastruktur. Daher ist eine DSFA z. B. in Bezug auf den Einsatz der Telematikinfrastruktur nicht erforderlich; dies hat der Bundesbeauftragte für den Datenschutz ausdrücklich bestätigt.

Durchführung einer Datenschutz-Folgenabschätzung

Ausgangspunkt für die Durchführung einer DSFA ist die übergeordnete Zweckbestimmung, die mit der Datenverarbeitung verfolgt wird.[6] Ausgehend von dieser Zweckbestimmung ist im Rahmen der DSFA eine – zu dokumentierende – systematische Beschreibung der Verarbeitungsvorgänge in der Praxis. Diese Dokumentation kann beispielsweise anhand des „Lebenszyklusses“ eines personenbezogenen Datums (von der Datenerhebung bis zur Löschung) erfolgen. Dabei sind der definierte Zweck der Verarbeitung sowie

1 Vgl. Art. 5 Abs. 2 DSGVO
2 https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSFA-Muss-Liste-1_0.pdf
3 vgl. Erwägungsgrund 91 DSGVO
4 § 38 Abs. 1 BDSG in Ergänzung zu Art. 37 Abs. 1 lit. c) DSGVO, Art. 35 Abs. 1 und 3 DSGVO)
5 Vgl. Erwägungsgrund 91 DSGVO
6 Vgl. KVWL kompakt 6/2018, DSGVO kompakt Teil 3.

die bei der Verarbeitung beteiligten Stellen und Systeme anzugeben. Hierbei bieten sich grafische Darstellungen z. B. durch Datenflussdiagramme an. Ferner muss der Verantwortliche die Legitimität des mit der Verarbeitung verfolgten Zieles darlegen.

Im Anschluss an die Beschreibung der Verarbeitungsvorgänge erfolgt die Risikobewertung als eigentliches Kernstück der DSFA. Dabei werden die Eintrittswahrscheinlichkeit eines definierten Risikos und die möglichen Auswirkungen für Betroffene analysiert. Risiken, die schützenswerte Güter gefährden (wie z. B. Verlust der Vertraulichkeit oder Datenintegrität) sind bei der Bewertung besonders zu beachten. Auch sollten die möglichen Auswirkungen einer Datenpanne dargelegt werden.

Nach der Identifizierung des Risikos sind abschließend geeignete – in der Regel technisch-organisatorische – Abhilfemaßnahmen zu benennen. Die Beschreibung solcher Maßnahmen kann über ein Sicherheitskonzept erfolgen.[7] Nach der Darlegung der Abhilfemaßnahmen hat der Verantwortliche zu entscheiden, ob weiterhin ein hohes Risiko für Rechte und Freiheiten von Betroffenen besteht. Ist dies der Fall, muss eine Konsultation der zuständigen Datenschutz-Aufsichtsbehörde[8], vorgenommen werden.

Bestehende Datenverarbeitungen

Für Datenverarbeitungsverfahren, die bereits vor Inkrafttreten der DS-GVO eingesetzt wurden und aktuell fortgeführt werden, kann von einer DSFA unter folgenden Bedingungen abgesehen werden:

- es wurde die nach dem BDSG (alte Fassung) erforderliche Vorabkontrolle durchgeführt,
- das Verfahren wurde durch den Datenschutzbeauftragten geprüft,
- der Verarbeitungsvorgang wird noch immer auf dieselbe Art durchgeführt,
- das mit dem Verarbeitungsvorgang verbundene Risiko hat sich nicht geändert.[9]

Haben sich diese Bedingungen in einer Weise verändert, dass nunmehr ein hohes Risiko für die Patienten wahrscheinlich ist, muss die DSFA hingegen auch für schon eingeführte bzw. bestehende Verfahren durchgeführt werden. Dies kann auch für Risiken gelten, die sich beispielsweise aufgrund des Einsatzes neuer Technologien verändern. Davon unabhängig sind Verarbeitungen grundsätzlich in regelmäßigen Zeitabständen auf mögliche Veränderungen der damit einhergehenden Risiken zu überprüfen.

7 Vgl. KVWL kompakt 6/2018, DS-GVO KOMPAKT Teil 3 für ein Beispiel eines Sicherheitskonzepts.
8 Im Zuständigkeitsbereich der KVWL ist dies die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW).
9 Dabei werden unter der Art der Verarbeitung die Durchführungsbedingungen, wie z. B. Umfang, Zweck, erfasste personenbezogene Daten, Identität der für die Verarbeitung Verantwortlichen oder der Empfänger, Speicherfristen oder technische und organisatorische Maßnahmen etc. verstanden.