Sicher durch den Datenschutz-Dschungel

Beitragsserie „DS-GVO kompakt", Teil 1: Verantwortlichkeiten und organisatorische Aufgaben

Die KVWL möchte Vertragsärzten und Vertragspsychotherapeuten eine Hilfestellung hinsichtlich der Umsetzung der seit dem 25. Mai 2018 anzuwendenden EU-Datenschutz-Grundverordnung (DS-GVO) geben. Hierzu veröffentlichen wir die Beitragsserie „DS-GVO kompakt", die sukzessive wichtige Pflichten der DS-GVO behandelt. Teil 1 widmet sich zum Auftakt den Verantwortlichkeiten in der DS-GVO und den hierbei bestehenden organisatorischen Aufgaben.

Verantwortlichkeiten

Die Vorgaben der DS-GVO richten sich primär an den „Verantwortlichen". Der Verantwortliche wird gesetzlich definiert als „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet".[1] Er ist auch Adressat für mögliche Bußgelder nach der DS-GVO.

Bezogen auf die Vertragsärzte und Vertragspsychotherapeuten ergibt sich hinsichtlich der Verantwortlichkeit in der Regel Folgendes:

a) Einzelpraxis

Im Falle einer Einzelpraxis ist der Praxisinhaber „Verantwortlicher".

b) Praxisgemeinschaft

Bei einer Praxisgemeinschaft werden Räume, Geräte und Personal gemeinsam genutzt. Ansonsten arbeiten die in einer Praxisgemeinschaft verbundenen Ärzte getrennt voneinander. Sie behandeln ihre eigenen Patienten und führen insoweit auch jeweils eine eigene Patientenkartei.

Jeder einzelne Arzt ist *„Verantwortlicher"* im Sinne der DS-GVO, soweit es um die Verarbeitung der Daten „seines" Patientenstammes geht. Wenn die beteiligten Ärzte – als Arbeitgeber – die personenbezogenen Daten der gemeinsamen Mitarbeiter verarbeiten, ist hingegen die Praxisgemeinschaft als solche verantwortliche Stelle.

c) Gemeinschaftspraxis

Bei der Gemeinschaftspraxis schließen sich mehrere Ärzte mit dem Ziel zusammen, gemeinsam Patienten zu behandeln. Dies erfolgt überwiegend in der Rechtsform einer BGB-Gesellschaft (GbR).

Personenbezogene Daten von Patienten werden in einer gemeinsamen Patientenkartei verarbeitet. In diesem Fall ist die Gemeinschaftspraxis als GbR *„Verantwortlicher"* im Sinne der DS-GVO sowohl hinsichtlich der Patientenkartei als auch hinsichtlich des gemeinschaftlich genutzten Personals und der hierbei anfallenden Daten.

d) Medizinisches Versorgungszentrum

Medizinische Versorgungszentren (MVZ) sind ärztlich geleitete Einrichtungen, in denen Ärzte als freiberufliche Vertragsärzte und/oder als angestellte Ärzte (fachübergreifend) tätig sind. Sie sind in unterschiedlichen Rechtsformen organisiert, so beispielsweise als GbR, Partnerschaftsgesellschaft (PartG) oder als Gesellschaft mit beschränkter Haftung.

Wie bei der Gemeinschaftspraxis, existiert ein gemeinsamer Patientenstamm und das vorhandene Personal wird gemeinschaftlich genutzt. Auch hier ist das MVZ in Gestalt der gewählten Rechtsform *„Verantwortlicher"* hinsichtlich der Umsetzung der Vorgaben der DS-GVO.

Organisatorische Aufgaben

Die Leitung eines Verantwortlichen (z.B. der Praxisinhaber oder Geschäftsführer eines MVZ) sorgt für die Einhaltung und Umsetzung der DS-GVO.

a) Systematisierter Datenschutz

Der Verantwortliche hat in Abhängigkeit der Risiken, die mit den Datenverarbeitungsprozessen in der Praxis für die Rechte und Freiheiten der betroffenen Personen einhergehen, technisch-organisatorische Maßnahmen zu ergreifen, die eine DS-GVO konforme Datenverarbeitung sicherstellen. Hierbei verlangt die DS-GVO vom Verantwortlichen ein systematisiertes Vorgehen, das die Planung, Implementierung, Durchführung, Überprüfung und Weiterentwicklung des Datenschutzes einschließlich Dokumentation in der von ihm zu verantwortenden organisatorischen Einheit umfasst. Dabei sind folgende Einzelgesichtspunkte zu berücksichtigen:

- Einrichtung einer Datenschutz-Organisation
- Risikobewertungen
- Sensibilisierung und Schulung der Mitarbeiter
- Durchführung von Kontrollen
- Einsatz „datenschutzfreundlicher" Technologien
- IT-Sicherheit nach dem „Stand der Technik"
- Datenschutz-Folgenabschätzung
- Nachweise und Dokumentationen
- Umsetzung der Betroffenenrechte

Die KVWL wird zu einzelnen dieser Themen gesonderte Hinweise veröffentlichen.

b) Einrichtung einer Datenschutz-Organisation

Wichtiger Bestandteil eines systematisierten Datenschutzes stellt die Einrichtung einer Datenschutz-Organisation dar. Dies kann der Verantwortliche durch die Benennung eines Datenschutzbeauftragten sicherstellen.

Die Aufgabe des Datenschutzbeauftragten kann ein fachlich qualifizierter Mitarbeiter (nicht der Praxisinhaber oder Geschäftsführer) oder ein externer Datenschützer übernehmen.[2] Ist ein Verantwortlicher gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten zu benennen (zur Verpflichtung siehe nachfolgend Buchst. c)), kann er dies gleichwohl freiwillig tun, um auf diese Weise für die Einrichtung einer Datenschutz-Organisation zu sorgen.

Andernfalls müssen die Verantwortlichkeiten für die Umsetzung der gesetzlichen Vorgaben, so auch hinsichtlich eines systematisierten Datenschutzes, auf andere Weise organisiert werden; hierbei kommt dem Praxisinhaber bzw. Geschäftsführer eine wesentliche Rolle zu.

c) Pflicht zur Benennung eines Datenschutzbeauftragten

Die DS-GVO[3] bzw. das BDSG[3] n.F. verpflichten den Verantwortlichen einen Datenschutzbeauftragten zu benennen, wenn eine der nachfolgenden Voraussetzungen erfüllt ist:

aa) Anzahl der Beschäftigten

Sind bei einem Verantwortlichen (z. B. die Praxis oder ein MVZ) in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener

Daten beschäftigt, muss ein Datenschutzbeauftragter benannt werden.[4] Hierzu genügt, wenn diese Personen regelmäßig Verarbeitungsaufgaben wahrnehmen, wenn auch die Datenverarbeitung nicht deren Haupttätigkeit ist; so beispielsweise die elektronische Erfassung von Terminen am Empfang. Ob der oder die ärztlichen Praxisinhaber – als Verantwortliche – bei der Berechnung des Schwellwertes von > 10 mitzählen, ist umstritten. Der Landesdatenschutzbeauftragte in NRW legt das Gesetz wohl so aus, dass alle mit der Datenverarbeitung beschäftigten Personen zu berücksichtigen sind, unabhängig davon, welchen Status sie haben. Wenn Sie dieser Auffassung folgen, minimieren Sie das Risiko von Beanstandungen durch den Landesdatenschutzbeauftragten.

bb) Datenschutz-Folgenabschätzung
Unabhängig von der Anzahl der Beschäftigten, ist ein Datenschutzbeauftragter auch dann zu benennen, wenn der Verantwortliche für zumindest einen Datenverarbeitungsvorgang eine Datenschutz-Folgenabschätzung (DSFA) durchführen muss.[5] Eine DSFA wird gesetzlich gefordert, wenn eine Datenverarbeitung nach Art, Form und Umfang „wahrscheinlich ein **hohes Risiko** für die Rechte und Freiheiten von natürlichen Personen mit sich bringt".[6]

Von einem solchen, die Pflicht zur Durchführung einer DSFA auslösenden **„hohen Risiko"**, geht die DS-GVO als Regelbeispiel bei einer **„umfangreichen Verarbeitung von Gesundheitsdaten"** aus.[7]

Bei Einzelpraxen ist regelmäßig eine Pflicht zur Durchführung einer DSFA zu verneinen, da hier die Komponente der **„umfangreichen Verarbeitung"** nicht erfüllt ist. Dies gilt in der Regel auch für eine Praxisgemeinschaft mit getrennten Patientenkarteien und damit unterschiedlichen Verantwortlichkeiten für die verarbeiteten Gesundheitsdaten.

Bei Gemeinschaftspraxen oder MVZ wird die Schwelle **„zur umfangreichen Verarbeitung von Gesundheitsdaten"** ab einer bestimmten Anzahl von dort tätigen Ärzten und betreuten Patienten überschritten sein. Als Faustregel ist davon auszugehen, dass in Gemeinschaftspraxen/MVZ, in denen **bis zu vier Ärzte** in Vollzeit tätig sind, noch **keine umfangreiche** Datenverarbeitung erfolgt. Größere Praxiseinheiten unterliegen – wegen des damit einhergehenden Umfangs der Datenverarbeitung – einer Verpflichtung zur Durchführung der DFSA, an die wiederum die Pflicht zur Ernennung eines Datenschutzbeauftragten geknüpft ist.

Der Verantwortliche ist – sofern ein Datenschutzbeauftragter zu bestellen war – verpflichtet, die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen und auch diese Daten dem Landesdatenschutzbeauftragten als Aufsichtsbehörde mitzuteilen.[8]

---

[1] Art. 4 Ziff. 7 DS-GVO
[2] Art. 37 Abs. 6 DS-GVO
[3] Art. 37 DS-GVO/§ 38 BDSG n.F.
[4] Vgl. § 38 Abs. 1 Satz 1 BDSG n.F.
[5] § 38 Abs. 1 Satz 2 BDSG n.F.
[6] Art. 35 DS-GVO
[7] Art. 35 Abs. 3b DS-GVO
[8] Art. 37 Abs. 7 DS-GVO