Verzeichnis von Verarbeitungstätigkeiten

Anhand einer Bestandsaufnahme wird ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 EU-DSGVO) mit entsprechenden Formular(en) für jede Gruppe erarbeitet.

Die Führung dieses Verzeichnisses ist Teil der neuen **Rechenschafts- und Nachweispflicht** des Verantwortlichen (immer Arzt) – bei Facharzt.QM wird der QM-Verantwortliche zukünftig auch der Datenschutz-Verantwortliche sein.

Das schriftlich oder elektronisch zu führende Verzeichnis hat sämtliche in Art 30 Abs. 1 S. 2 DSGVO aufgeführten Aufgaben zu enthalten und muss der Aufsichtsbehörde (in der Regel die Landesbeauftragten für den Datenschutz – Information auch über die Ärztekammer) jederzeit auf Anfrage zur Verfügung gestellt werden.

Auch ist zu bedenken, dass Ärzte infolge ihrer täglichen Verarbeitung höchst sensibler Gesundheitsdaten in ihren Einrichtungen eine besondere Verantwortung zur Wahrung von Datenschutz- und Berufsrecht tragen (vgl. Art. 24 Abs. 1 DS-GVO sowie die Vorgaben der Berufsordnung).

Verstöße gegen die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten können mit einer Geldbuße von bis zu 10.000.000 EUR oder von bis zu 2% des gesamten erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden (Art 83 Abs. 4 Buchst. A. DSGVO).

Bei Facharzt.QM wird das VVT der neu entwickelte Bereich DSGVO sein, in dem - spezifisch auf die medizinische Einrichtung – in das QM-Handbuch die wichtigen Vorlagen (nach einer Schwellenanalyse) zur Verfügung gestellt wird.

Der Gemeinsame Bundesausschuss (G-BA) ist das oberste Beschlussgremium der gemeinsamen Selbstverwaltung der Ärztinnen und Ärzte, Zahnärztinnen und Zahnärzte, Psychotherapeutinnen und Psychotherapeuten, Krankenhäuser und Krankenkassen in Deutschland. Rechtsgrundlage für die Arbeit des G-BA ist das Fünfte Sozialgesetzbuch (SGB V).

Die von ihm beschlossenen Richtlinien haben den Charakter untergesetzlicher Normen. Zudem hat der G-BA weitere wichtige Aufgaben im Bereich des Qualitätsmanagement und der Qualitätssicherung in der ambulanten und stationären Versorgung.

Datenschutz-Folgenabschätzung

Ergibt sich aus dem Verzeichnis von Verarbeitungstätigkeiten ein „**High Risk Faktor**“ muss eine **Datenschutz-Folgenabschätzung** (Art. 35 Abs. 7 DSGVO) erarbeitet werden.

Dabei werden

- die Verwendung **neuer Technologien** wie z.B. Cloud-Dienste (Art. 35 Abs. 1 DSGVO)
- drei **gesetzlich aufgeführte Fälle** wie z.B. Videoüberwachung in der Arztpraxis (Art. 35 Abs. 3 Buchst. c DSGVO)
- sowie die **umfangreiche Verarbeitung** von personenbezogenen Daten (Art. 35 Abs. 3 Buchst. b DSGVO)

analysiert.

Nach Erwägungsgrund 91 der DSGVO ist eine Verarbeitung **nicht** als **umfangreich** einzuordnen, wenn die Verarbeitung **personenbezogene Patientendaten** betrifft und durch einen **einzelnen Arzt** erfolgt.

Cave: **Umfangreich** bedeutet nicht unbedingt die Menge der Patientendaten, sondern die **Qualität der Daten** =

Wenn in einem **Informationssystem** (allen voran KIS) **genetische** oder **medizinische Daten** verarbeitet, **gendiagnostische Verfahre**n angewandt oder besonders **schutzbedürftige Patientengruppen** (z.B. Kinder oder psychisch Erkrankte) behandelt werden, ist immer eine Datenschutz-Folgenabschätzung durchzuführen.

Die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung kann bei der zuständigen Aufsichtsbehörde erfragt werden oder die medizinische Einrichtung führt eine **Schwellwertanalyse** durch und weist hiermit nach, dass durch technisch-organisatorische Vorkehrungen hinreichende Abwehrmaßnahmen ergriffen wurden, welche das **Risiko minimieren**.

Das Ergebnis der Datenschutz-Folgenabschätzung ist zu dokumentieren – ggfls. ist eine externe Datenschutzprüfung zu empfehlen.

strafrechtliche Schweigepflicht

Im § 203 Abs. 3 Satz 2 StGB ist die **strafrechtliche Schweigepflicht** für **externe Personen** oder **Unternehmen** formuliert.

Zu prüfen ist im einzeln z.B.:

- die Bereiche **Telekommunikation**, **Praxisverwaltungssystem**, **Steuerberatung** oder **Buchhaltung**
- alle Mitarbeiter von **Dienstleistungsunternehmen** oder **selbstständig tätige Personen**
- „**Qualitätsbestimmung**“ der Notwendigkeit der Weitergabe von Informationen

---

Hier ist v.a. noch einmal die elektronisch geführte Patientenkartei und damit die Weitergabe von medizinischen Daten zu benennen und die Schnittstelle zu „sonstige mitwirkenden Personen“

= die medizinische Einrichtung muss sicherstellen, dass jedes Unternehmen und deren Mitarbeiter nur Kenntnisse von Informationen hat, die für die Vertragserfüllung notwendig ist!

Mit jedem dieser „**sonstigen mitwirkenden Personen**“ muss zum einen ein Auftragsverarbeitungs-Vertrag abgeschlossen werden (Bestandteil VV), zum anderen muss mit jedem Mitarbeiter eine Geheimhaltungsverpflichtung unterschrieben werden.

Cave: Insbesondere Fernwartung IT-Systeme = verrät der Mitarbeiter Patientengeheimnisse macht sich auch der Arzt strafbar (§ 203 Abs. 4 Nr. 1 StGB)!