DATENSCHUTZ-GRUNDVERORDNUNG

Teil 2: Erstellung eines Verzeichnisses zu Datenverarbeitungsvorgängen und Aufstellen interner Maßnahmen zum Datenschutz

Der Datensicherheit kommt in Arztpraxen aufgrund der Verarbeitung besonders sensibler Gesundheitsdaten eine bedeutende Rolle zu. Der zweite Teil der Serie zum neuen Datenschutzrecht befasst sich daher mit dem seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) in Arztpraxen notwendigen Verzeichnis von Datenverarbeitungstätigkeiten und der Aufstellung praxisinterner Maßnahmen zum Schutz der Daten.

1. Materialien

Materialien und Muster zu den aufgeworfenen Fragestellungen finden Sie auf der Website der Landesärztekammer Brandenburg (www.laekb.de) und bei der KBV (www.kbv.de).

2. Verzeichnis über Datenverarbeitungsvorgänge

Art. 30 DSGVO verpflichtet die Arztpraxen ein Verzeichnis über die üblicherweise anfallenden Verarbeitungstätigkeiten anzulegen. Das Verzeichnis soll die Transparenz der Verarbeitung personenbezogener Daten und die rechtliche Absicherung gegen mögliche Bußgelder gewährleisten. Das Verzeichnis ist schriftlich zu führen, wobei dies auch in einem elektronischen Format (z.B. PDF-Dokument) erfolgen kann.

Für die Praxen bedeutet dies, dass zunächst zusammengetragen werden sollte, wo überall personenbezogene Daten verarbeitet, also etwa erhoben, gespeichert, bearbeitet oder weitergeleitet werden. In einem weiteren Schritt sollten zu jeder Tätigkeit die folgenden Angaben hinzugefügt werden:

- Zweck der Verarbeitung (z. B. ärztliche Dokumentation)
- Betroffene Personengruppen (z. B. Patienten, Beschäftigte)
- Datenkategorien (z. B. Gesundheitsdaten, Personaldaten)
- Empfängergruppen (z. B. andere Ärzte, Kassenärztliche Vereinigung)
- Fristen für die Löschung (z. B. zehn Jahre)

Schließlich sind der Name des Verantwortlichen, die Kontaktdaten der Praxis und ggf. die des Datenschutzbeauftragten zu nennen.

3. Aufstellung von Maßnahmen zum internen Datenschutz

Verantwortliche für die anfallenden personenbezogenen Daten haben geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen (Art. 32 DSGVO). Zwar macht die neue DSGVO keine genauen Angaben darüber, welche Vorkehrungen dazu zu treffen sind, allerdings gibt es einige Punkte, die regelmäßig beim Betrieb einer Arztpraxis zu beachten sind. Dazu gehören vor allem folgende Regeln:

- Patientendaten werden ausschließlich verschlüsselt über das Internet verschickt (z. B. nicht mit einfacher E-Mail)
- Zugriffsrechte auf Dateien und Ordner sind in der Praxis genau verteilt
- In der Praxis wird auf Diskretion geachtet und wenn möglich sind Anmeldung und Wartebereich räumlich getrennt
- Patientenakten werden sicher verwahrt, der Computer ist mit einem Passwort gesichert, die Bildschirmsperre aktiviert und Patientenunterlagen werden unter Verschluss gehalten, wenn der Arzt nicht im Raum ist
- Vertrauliche Patientengespräche finden stets in geschlossenen Räumen statt
- Bei Auskünften am Telefon wird die Identität des Anrufers gesichert (z. B. durch Zusatzfragen oder einen Rückruf)
- Es ist festgelegt, wann und durch wen personenbezogene Daten gelöscht bzw. vernichtet werden
- Patientendaten werden nach DIN-Normen vernichtet
- Es wird festgelegt, was bei Datenpannen und Datenschutzverstößen zu tun ist und wer die Meldung übernimmt (i.d.R. innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde)
- Mitarbeiter der Praxis wurden zur Wahrung des Datenschutzes und der ärztlichen Schweigepflicht verpflichtet

Die Aufzählung ist lediglich beispielhaft. Es sollte daher im Einzelfall für jede Praxis überprüft werden, welche weiteren datenschutzrelevanten Situationen regelmäßig auftreten und wie damit umzugehen ist.

Bei Fragen im Einzelfall können Sie sich an die Rechtsabteilung der Landesärztekammer Brandenburg wenden (Frau Menz, Tel. 0331 505605-560).

■ *Ass. jur. Roger Zesch,*
Dr. jur. Daniel Sobotta