

Datenschutz-Check-up 2018

Am 25.05.2018 ist die Übergangsphase zur Einrichtung der Maßnahmen der EU-Datenschutz-Grundverordnung abgeschlossen. Mit folgenden Maßnahmen will der Gesetzgeber das Bewusstsein für den Datenschutz in Arztpraxen stärken. Wir helfen bei der Umsetzung, um die erheblichen Sanktionen bei Nichtbeachtung zu vermeiden.

I. Interne Datenschutzorganisation/ Datenschutzmanagement der Praxis

Zum Nachweis der Wahrung des Datenschutzes gemäß der DS-GVO benötigen die Praxen ein Datenschutzmanagement, dass die getroffenen Maßnahmen dokumentiert und sicherstellt.

1. Dazu überprüfen wir alle internen Verarbeitungsvorgänge in der Arztpraxis. Dies umfasst auch die Erstellung der (TOM) technisch organisatorischen Maßnahmen. Da diese in den einzelnen Praxen recht ähnlich sind, vergleichen wir unsere bisherigen Erkenntnisse auf Abweichungen in Ihrer Praxis und machen keine tagelangen Analysen.
2. Erstellung eines Verzeichnisses für Verarbeitungsvorgänge in der Arztpraxis im Sinne einer Bestandsaufnahme auf welcher Grundlage welche Daten erhoben und verarbeitet werden.
3. Gegebenenfalls Erstellung einer Datenschutzfolgen-Abschätzung gem. Art. 35 DS-GVO. Dies ist eine umfassende Risikobewertung der Art, des Umfangs und der Zwecke der Verarbeitung persönlicher Daten.
4. Benennung eines Datenschutzbeauftragten bei dauerhafter Beschäftigung von mehr als 10 Mitarbeitern (ohne Ärzte/ Ärztinnen). Dies kann bei entsprechender Sachkunde ein Mitarbeiter oder ein externer Dienstleister sein.
5. Erstellung einer internen Datenschutzrichtlinie, die bereits als Teil des Qualitätsmanagements vorliegen sollte. Auch hier liefern wir die entsprechenden Vorlagen.
6. Überprüfung vorhandener Datenschutzformulare und Verträge mit Dienstleistern insbesondere der Einwilligungserklärung, die einen Hinweis auf ihre Widerruflichkeit enthalten muss.
7. Sicherheit des Systems, Zugangskontrolle zum Raum, in dem der Server steht, Prüfung des technischen Zugangs von außen, Installation einer Firewall oder der Konfiguration des Routers. Passwortsicherheit der Arbeitsplätze, Passwortwechselroutine.

II. Patientenverhältnis

1. Einwilligungserklärung für besondere Datenverarbeitungsvorgänge wie Weitergabe von Befunden an den Hausarzt, Forderungseinzug über Inkassounternehmen

2. Informationspflichten

Entsprechende Vordrucke werden gestellt. Die Einhaltung obliegt dem Praxisinhaber

3. Auskunftsrecht des Patienten

Neben dem Einsichtsrecht gemäß § 630g BGB (Behandlungsvertrag) existiert das datenschutzrechtliche Auskunftsrecht (Art. 15 EU-DSGVO), durch das Patienten vom Arzt Auskunft über die zu ihrer Person ggf. gespeicherten Daten verlangen können. Dafür sollte in einer internen Datenschutzrichtlinie ein bestimmtes Verfahren eingerichtet werden, um entsprechende Anfragen schnell beantworten zu können.

4. Recht auf Löschung

Gleiches gilt für den Anspruch des Patienten auf Datenlöschung. Dieser steht zwar im Widerspruch mit den Regeln zur Aufbewahrung von Patientendaten, ist aber im Zweifel den Regelungen der Ärztekammer vorrangig, weil höchstpersönlich. Es ist hier ein Verfahren zu beschreiben unter welchen Bedingungen der Patient die Löschung seiner Daten verlangen kann.

Im Rahmen der regelmäßigen Löschungsfristen (Art. 17 EU-DSGVO) sollte in einer internen Datenschutzrichtlinie ein bestimmtes Verfahren festgelegt werden, z. B. wann und durch wen die Daten z. B. nach Ablauf von Aufbewahrungsfristen gelöscht werden sollen.

III. Verhältnis zu externen Dienstleistern und Dritten

Soweit Verträge mit externen Dienstleistern, z. B. zur Ausführung von Wartungsaufgaben an der Praxis-EDV-Anlage oder mit privaten Verrechnungsstellen bestehen oder abgeschlossen werden sollen, müssen diese Verträge auf ihre Vereinbarkeit mit den neuen datenschutzrechtlichen Vorschriften sowie mit den strafrechtlichen Bestimmungen zur ärztlichen Schweigepflicht überprüft werden.

1. Anpassung vertraglicher Vereinbarung mit externen Dienstleistern nach den Vorschriften zur Auftragsverarbeitung. Sofern es sich um eine Auftragsverarbeitung handelt (z. B. Wartungsdienste für die Praxis-EDV oder Nutzung von Cloud-Diensten), sollten entsprechende Vereinbarungen getroffen werden, deren Anforderungen sich aus Art. 28 Abs. 3 EU-DSGVO ergeben.

2. In Verträgen mit externen Dienstleistern sind neben den datenschutzrechtlichen Vorgaben auch Verpflichtungen aufzunehmen, nach denen die mitwirkenden Dritten zur Geheimhaltung verpflichtet werden. Das Unterlassen kann zu einer Strafbarkeit führen.

3. Meldung von Datenpannen und -verstößen

Datenpannen (z. B. Hackerangriffe) und Datenschutzverstöße (z. B. durch Mitarbeiter) sind der zuständigen Aufsichtsbehörde in der Regel innerhalb von 72 Stunden zu melden. Dafür sollte in einer internen Datenschutzrichtlinie festgelegt werden, wer für die Meldung zuständig ist. Die Meldepflicht ist problematisch, sofern der Verantwortliche sich selbst belasten würde, einen Verstoß gegen die ärztliche Schweigepflicht begangen zu haben. Die Meldung ist dann zwar vorzunehmen. Es besteht aber ein prozessuales Verwertungsverbot und die Meldung kann in einem Strafverfahren oder im Ordnungswidrigkeitenverfahren nur mit Zustimmung des Arztes verwendet werden.

IV. Bußgeldvorschriften

Nach dem bisherigen BDSG konnten Bußgelder von bis zu 300.000 Euro verhängt werden, nunmehr beträgt die maximale Geldbuße im Rahmen von Art. 83 DSGVO 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist. Von Relevanz für eine Praxis sind insbesondere:

- a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43
- b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
- c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49