
Foto: privat


Foto: privat

Was Ärztinnen über die neue DSGVO wissen müssen

CHRISTIANE KLIESOW UND DOROTHEE QUICK

Die neue Datenschutzgrundverordnung (DSGVO) verunsichert seit ihrem Inkrafttreten im Mai 2018 auch Vereine wie den DÄB und verursacht bürokratischen Stress. Als Gastbeitrag haben wir bei der Ärztekammer Nordrhein angefragt, was Ärztinnen über die neue DSGVO wissen müssen. Zwei Juristinnen haben geantwortet.

Im Mai 2018 hat ein neues Kapitel zum Thema Datenschutz begonnen. Ursprünglich gedacht für große Internetfirmen wie Google oder Facebook, erfassen die neuen Regelungen jedoch alle, die personenbezogene Daten verarbeiten, auch die kleinste Arztpraxis, denn Gesundheitsdaten sind als besondere Kategorie von personenbezogenen Daten besonders geschützt. In jeder Praxis ist somit ein Bewusstsein für Datenschutz zu entwickeln: Neben der DSGVO finden sich Schutzregelungen für personenbezogene Daten auch im Bundesdatenschutzgesetz und in speziellen Fachgesetzen für den heilberuflichen Bereich.

Niedergelassene Ärztinnen und Ärzte haben beim Datenschutz folgende Punkte zu beachten: Internes Datenschutzmanagement, Schutz der Patientendaten (Arzt-Patienten-Verhältnis), Verhältnis zu externen Dienstleistern und Dritten (externe Stellen) und Verhältnis zu den Aufsichtsbehörden (Datenschutzstellen). Verstöße gegen den Datenschutz können mit beachtlichen Sanktionen geahndet werden.

Datenschutzmanagement in der ärztlichen Praxis

1. Für die Praxis benötigen Ärztinnen und Ärzte ein *Datenschutzkonzept*, um auf Nachfrage nachweisen zu können, dass sie die datenschutzrechtlichen Vorschriften kennen und wahren. Dazu kann beispielsweise eine interne Datenschutzrichtlinie erstellt werden, in welcher der gesamte Umgang mit den Daten festgelegt wird, zum Beispiel das Verhalten Patientinnen und Patienten gegenüber, Diskretion in den Praxisräumen, Auskünfte am Telefon, die Art der Datenspeicherung, Verwahrung der Patientenakten, klare Verantwortlichkeiten, Mitarbeiterinfo über die Einhaltung von Schweigepflicht und Datenschutz, Zugriffsbeschränkungen, Verhalten bei Datenpannen oder auch Nachweis der Rechtsgrundlagen für Datenverarbeitung.

2. Zur Organisation des Datenschutzes gehört auch, dass die internen Verarbeitungsvorgänge in der Praxis überprüft und gegebenenfalls angepasst werden müssen. Möglicherweise sind technisch-organisatorische Schutzmaßnahmen einzuführen. In seltenen Fällen wird eine sogenannte „Datenschutzfolgenabschätzung" durchzuführen sein. Diese dient dazu, mögliche Risiken bei der Verarbeitung von Patientendaten abzuschätzen und Abhilfemaßnahmen festzulegen. Vorsicht ist besonders bei Daten von Kindern und bei sogenannten genetischen Daten geboten.

3. Jede Ärztin hat zudem ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Darin werden die Tätigkeiten erfasst, bei denen personenbezogene Daten verarbeitet werden. Die Aufstellung ist auf Verlangen der Aufsichtsbehörde vorzulegen. Bei fehlendem Verzeichnis drohen Geldstrafen: Ein Beispiel ist unter https://www.aekno.de/downloads/aekno/Muster-Verzeichnis-von-Verarbeitungstaetigkeiten-Stand-23.04.2018.pdf verfügbar.

4. Einige Arztpraxen werden auch einen Datenschutzbeauftragten benennen müssen. Das hängt von der Größe der Praxis und vom Umfang der gespeicherten Daten ab. Ein Datenschutzbeauftragter ist zwingend immer dann zu benennen, wenn mehr als 10 Personen in der Praxis mit der Verarbeitung von Daten beschäftigt sind oder wenn eine Datenschutzfolgenabschätzung durchgeführt werden muss. Die zu benennende Person kann eine angestellte Ärztin oder ein angestellter Arzt, eine medizinische Fachangestellte oder eine externe Firma sein, nicht aber die Praxisinhaberin oder der Praxisinhaber. Die notwendigen Kenntnisse können in Schulungen erworben werden. Wurde eine Person als Datenschutzbeauftragte(r) benannt, ist sie der zuständigen Aufsichtsbehörde zu nennen und dort im Meldeportal für Kontaktdaten einzutragen.

5. Praxen, die eine Internet- oder eine Facebook-Seite anbieten, sollten ihre Datenschutzerklärungen und den technischen Standard ihrer Homepage überprüfen. Patientendaten dürfen niemals unverschlüsselt über das Internet versendet werden.

Datenschutz für Patientinnen und Patienten

1. Im Rahmen eines Behandlungsverhältnisses beruht die Datenverarbeitung auf einer vertraglichen Grundlage. Das Erfassen, Speichern und die Bearbeitung von Patientendaten ist damit gesetzlich gestattet. Hinsichtlich aller Verarbeitungsvorgänge, die sich nicht direkt aus dem Behandlungsvertrag ergeben (zum Beispiel Datenweitergabe an Dritte), ist eine Einwilligung der Patientin oder des Patienten erforderlich. Die Einwilligung muss nicht zwingend schriftlich erfolgen; sie muss aber nachweisbar sein. Es wird daher in einigen Fällen empfohlen, eine schriftliche Einwilligung einzuholen, unter anderem bei der Datenweitergabe an die private Krankenversicherung, privatärztliche Verrechnungsstellen, Seniorenheime, im Rahmen der Teilnahme an der hausarztzentrierten Versorgung, bei Selektivverträgen oder auch beim Recall. Fälle, in denen bereits vor Einführung der DSGVO aufgrund spezialgesetzlicher Regelung eine schriftliche Einwilligung erforderlich war, bleiben erhalten, wie zum Beispiel das Schriftformerfordernis gegenüber gesetzlich Versicherten bei Hausärzten § 73 I lit. b SGB V und bei Zahnärzten § 10 VI GOZ.

2. Die Rechte der Patientinnen und Patienten wurden erheblich gestärkt. Neu ist das umfassende Auskunftsrecht. Neben dem Recht auf Einsichtnahme in die Patientenakte erweitert die DSGVO das Auskunftsrecht erheblich. Die Patienten erhalten diese Auskünfte unentgeltlich und haben das Recht auf Berichtigung und Löschung ihrer Daten, die Einschränkung der Datenverarbeitung und auf Datenportabilität.

3. Die Datenschutzgrundverordnung sieht umfangreiche Informationspflichten für die Praxisinhaberin vor, die der Transparenz bei der Datenverarbeitung dienen sollen. Ärztinnen und Ärzte sind verpflichtet, ihre Patienten über diese Rechte zu informieren, am sichersten durch Übergabe eines Infoblattes und entsprechender Dokumentation der Übergabe in der Patientenakte. Ein Muster für die Praxis ist unter https://www.aekno.de/downloads/aekno/Muster-eines-Informationsblattes-fuer-Patienten-Stand-23.04.2018.pdf erhältlich.

Datenschutz und externe Dienstleister*innen

1. Soweit Verträge mit externen Dienstleistern bestehen oder abgeschlossen werden sollen, müssen diese auf ihre Vereinbarkeit mit den neuen datenschutzrechtlichen Vorschriften, den strafrechtlichen Regelungen zur ärztlichen Schweigepflicht und darauf geprüft werden, ob eine Auftragsverarbeitung vorliegt (so zum Beispiel bei Verträgen über die Wartung von Praxis-EDV-Anlagen, die Vernichtung von Patientenakten/Datenträgern, die Nutzung von Cloud-Diensten oder mit privatärztlichen Verrechnungsstellen). Sofern es sich um eine Auftragsdatenverarbeitung handelt, ist ein Vertrag zu schließen, der den Anforderungen der Art. 28. ff DSGVO entspricht. Der Auftragsverarbeiter muss von dem Auftraggeber unter Berücksichtigung seiner Eignung sorgfältig ausgewählt werden. Er darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Der Auftragsverarbeiter haftet gemeinsam mit dem Auftraggeber und hat zahlreiche datenschutzrechtliche Pflichten zu erfüllen. Die Gesamtverantwortung verbleibt aber beim Auftraggeber. Verträge über eine Auftragsdatenverarbeitung müssen auch eine Verpflichtung der mitwirkenden Dritten zur Geheimhaltung enthalten. Ärztinnen und Ärzte sollten sich gegebenenfalls juristisch beraten lassen.

2. Keine Auftragsverarbeitung sind rein technische Wartungen sowie in der Regel die Beauftragung von Steuerberatern, Rechtsanwälten und sonstigen Geheimnisträgern.

Aufsichtsbehörden für den Datenschutz

1. Zuständige Aufsichtsbehörde sind die Datenschutzbeauftragten des jeweiligen Bundeslandes. Sie überwachen als unabhängige Landesbehörde die Anwendung der datenschutzrechtlichen Vorschriften der DSGVO und des Bundesdatenschutzgesetzes und beraten Datenverarbeiter*innen und Bürger*innen.

2. Datenpannen und Datenschutzverstöße sind innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde zu melden und in der Praxis zu dokumentieren, zum Beispiel Hackerangriffe, der versehentliche Verlust von Datenträgern oder die Missachtung von Datenschutzvorgaben durch Mitarbeiter der Praxis. Kann die Meldung nicht zeitnah erfolgen, ist sie nachzuholen und eine entsprechende Begründung für die verzögerte Meldung beizufügen. Besteht das Risiko, dass durch die Datenpanne das Persönlichkeitsrecht der Betroffenen verletzt wird, müssen auch sie unverzüglich informiert werden.

3. Von einer Meldung kann abgesehen werden, wenn voraussichtlich kein Risiko für die Rechte und Freiheiten der betroffenen Patienten besteht, weil bereits Maßnahmen zum Datenschutz ergriffen wurden, zum Beispiel durch geeignete technische und organisatorische Maßnahmen (Verschlüsselung der Daten etc.).

Weitere hilfreiche Informationen

Informationsblätter und Mustervorlagen der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern, zum Beispiel auch zur Einwilligung, finden sich auf der Homepage der Ärztekammer Nordrhein unter https://www.aekno.de/page.asp?pageID=8917. Sie behandeln vertieft die einzelnen Themen wie Datenschutzbeauftragte(r), Datenschutzfolgenabschätzung, Einwilligung, Rechte der Patientinnen und Patienten etc. Die Blätter werden regelmäßig aktualisiert. ◄

Christiane Kliesow, Syndikusrechtsanwältin und Ass. iur. Dorothee Quick arbeiten in der Rechtsabteilung der Ärztekammer Nordrhein in Düsseldorf.

E-Mail: Dorothee.Quick@aekno.de
E-Mail: Christiane.Kliesow@aekno.de