Europäisches Datenschutzrecht in der Zahnarztpraxis

gespeichert · dokumentiert · geschützt

Die Europäische Datenschutz-Grundverordnung (DSGVO) ist ab Ende Mai 2018 in allen Mitgliedsländern der EU anzuwenden. Der deutsche Gesetzgeber hat seine in einigen Artikeln erlaubten Gestaltungsräume mit der Verabschiedung des neuen Bundesdatenschutzgesetzes (BDSG) genutzt. Beide Gesetze sind ab den 25. Mai 2018 für die Verarbeitung personenbezogener Daten in Ihrer Praxis bindend.

Patienten, Personal, Lieferanten …

Das Ziel des Datenschutzrechts ist die Umsetzung des in der Charta der Grundrechte der EU verbürgten Rechts auf Schutz der persönlichen Daten. Hierzu ist ein umfassendes Regelwerk geschaffen worden, das kaum vereinfachende Regelungen für kleinere Praxen kennt.
Personenbezogene Daten sind in Ihrer Zahnarztpraxis alle Daten, die sich einer Person zuordnen lassen, also nicht nur die Patientendaten, sondern ebenso Personaldaten, Lieferantendaten sowie technische Daten, die einen Personenbezug haben können, beispielsweise Telekommunikationsdaten.

Mathias Richter

Datenschutzbeauftragter Gerd-Jürgen Golze, zertifizierter Datenschutzauditor und IT-Sicherheitsbeauftragter

Das Datenschutzrecht lässt die Verarbeitung personenbezogener Daten nur unter bestimmten Bedingungen zu. Die Daten dürfen nur für einen eindeutigen Zweck und wenn eine Einwilligungserklärung oder ein Vertrag mit der betroffenen Person besteht oder ein Gesetz es erlaubt, verarbeitet werden. Sie als Praxisinhaber sind für die Verarbeitung und die Einhaltung der DSGVO verantwortlich (sowohl gegenüber dem Betroffenen als auch den Aufsichtsbehörden) und rechenschaftspflichtig. Die Rechenschaftspflicht ist in der DSGVO sehr weit gefasst. Hieraus ergibt sich in der Praxis eine umfangreiche Verpflichtung zur Dokumentation, damit Sie die Einhaltung der DSGVO beweisen können.
Ein zentrales Dokument für die Erfüllung der Rechenschaftspflicht ist das Verzeichnis der Verarbeitungstätigkeiten. Zur Führung dieses Dokuments sind Sie verpflichtet. Die Aufsichtsbehörden können sich damit bei einer Überprüfung schnell einen Überblick über die Verarbeitung personenbezogener Daten machen. Allerdings ist es ebenso ein Instrument, um den Datenschutz in Ihrer Praxis gut zu organisieren.

Das Verzeichnis der Verarbeitungstätigkeiten umfasst zwingend folgende Angaben:
- Name und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Beschreibung der Kategorien betroffener Personen und der personenbezogenen Daten
- Kategorien von Empfängern
- ggf. Übermittlung in Drittstaaten
- Fristen für die Löschung der verschiedenen Datenkategorien
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Diese Angaben müssen sich auf die jeweiligen Verfahren beziehen, diese können u. a. sein:
- Personalwesen
- Lohnbuchhaltung
- Buchhaltung
- Arbeitszeiterfassung
- Patientenakte

Bereits mit den Pflichtangaben kann dieses Verzeichnis also einen erheblichen Umfang annehmen und zu einer beträchtlichen Fleißaufgabe werden.

Sie sollten sich bei der Erstellung des Verzeichnisses für jedes Verfahren folgende Fragen stellen und die Antworten dokumentieren:
- Was ist der Zweck dieser Verarbeitung und erhebe ich nur die für diesen Zweck erforderlichen Daten?
- Auf welcher Rechtsgrundlage darf ich die Daten verarbeiten?
- Ist die Rechtsgrundlage ggf. für besondere Daten nach Art. 9 DSGVO (z. B.: Gesundheitsdaten) ausreichend?
- Wie kann ich gewährleisten, dass die Daten richtig und vollständig sind?
- An wen gebe ich Daten weiter und auf welcher Rechtsgrundlage erfolgt dies?
- Habe ich eine Regelung, wann die Daten gelöscht werden?
- Haben Mitarbeiter nur Zugriff auf Daten, die sie zur Erfüllung ihrer Aufgaben brauchen?

Bei diesen Fragen könnten schon einige Maßnahmen anfallen, die Sie in Ihrer Praxis durchführen sollten. Vielleicht sind weitere Einwilligungserklärungen notwendig oder der Zugriff auf die Daten ist anders zu regeln.

Mit der Überlegung, wie ich die mir anvertrauten Daten vor Missbrauch schützen kann, eröffnet sich ein weiterer Fragenkatalog:
- Wie sind Akten, PCs und Server räumlich geschützt? Sind meine Akten und der Server in verschlossenen Schränken oder Räumen vor fremdem Zugriff sicher?

kras99 - fotolia.com

- Sind die Bildschirme so aufgestellt, dass Patienten Daten nicht mitlesen können?
- Sind die PCs mit Benutzernamen und Passwort geschützt?
- Haben Sie Ihr Personal im Datenschutz geschult und es auf die Einhaltung der zahnärztlichen Schweigepflicht sowie des Datengeheimnisses verpflichtet?
- Sind Ihre Mitarbeiter sensibilisiert, dass sie in der Kommunikation mit Patienten die Vertraulichkeit wahren? Können beispielweise Patienten im Wartebereich die Gespräche an der Rezeption mithören?

Und es gilt, Fragen zur IT-Sicherheit zu klären:

- Weist Ihre IT entsprechend dem Risiko der Verarbeitung für die betroffenen Personen ein angemessenes Schutzniveau auf?
- Erfolgt die Weitergabe von sensiblen Patienteninformationen per Mail oder andere digitalisierte Übertragungen abgesichert (VPN-Verbindung, Verschlüsselung o. ä.)?

Besonders kritisch sind hier Kostenvoranschläge und Rechnungen mit dem Namen des Patienten sowie Übertragungen von Patientenbildern zu sehen. Ein Patientenname darf niemals im Betreff einer Mail stehen, in welcher Rechnungen, Kostenvoranschläge oder andere sensible Daten verschickt werden.

Die gängige SSL- oder TLS-Mail-Verschlüsselung ist nach Aussage der Datenschutzbehörden nur bei pseudonymisierten Daten ausreichend, also wenn nur eine Auftragsnummer oder sog. XML-Nummer als Kennung vorhanden ist.

Ist eine Datenschutz-Folgenabschätzung erforderlich?

Die technischen und organisatorischen Schutzmaßnahmen sind im Hinblick auf die Meldepflicht von Datenschutzverstößen wichtig. In Zukunft muss jeder Datenschutzverstoß, der ein Risiko für die betroffene Person sein kann, der Aufsichtsbehörde innerhalb von 72 Stunden gemeldet werden. Im Zuge dieses Verfahrens wird bestimmt die Angemessenheit Ihrer IT-Sicherheit überprüft werden. Selbstverständlich ist es besser, dass keine Datenpanne passiert, aber hundertprozentige Sicherheit gibt es leider nicht.
Sie sehen, anhand der zu stellenden Fragen werden Sie Ihre gesamte Datenverarbeitung auf den Prüfstand stellen und dort, wo Sie Abweichungen vom geforderten Standard ermitteln, Maßnahmen ergreifen müssen, um die Sicherheit der Verarbeitungen zu verbessern (siehe Seite 13).

Sie sollten bei der Erstellung des Verzeichnisses eine Risikobewertung dieses jeweiligen Verfahrens aus Sicht der betroffenen Personen vornehmen und bewerten, ob Sie für bestimmte Verfahren zu einer Datenschutz-Folgenabschätzung verpflichtet sind.
Die Datenschutz-Folgenabschätzung ist eine detaillierte Analyse eines oder mehrerer Verfahren, bei der die Risiken für die Betroffenen Personen abgeschätzt und die ergriffenen Sicherheitsmaßnahmen bewertet werden.
Die Datenschutz-Folgenabschätzung hat bei der Frage, ob ein Datenschutzbeauftragter bestellt werden muss, eine besondere Bedeutung. Ein Datenschutzbeauftragter nach DSGVO und BDSG muss bestellt werden, wenn mindestens zehn Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind oder eine Datenschutz-Folgenabschätzung erforderlich ist.
In der DSGVO ist eine Datenschutz-Folgenabschätzung gefordert, wenn besondere Daten, wie Gesundheitsdaten in erheblichem Umfang verarbeitet werden. Allerdings soll nach Erwägungsgrund 91 DSGVO die Verarbeitung von Gesundheitsdaten durch einen einzelnen Arzt nicht als Verarbeitung in einem erheblichen Umfang gelten. Daher fällt die einzelne Zahnarztpraxis wohl nicht unter den Zwang der Datenschutz-Folgenabschätzung.

Interner oder externer Datenschutzbeauftragter?

Sollten Sie mit Ihrer Praxis der Pflicht unterliegen, einen betrieblichen Datenschutzbeauftragten zu bestellen, haben sie verschiedene Möglichkeiten. Sie können einen internen Datenschutzbeauftragten bestellen. Der interne Datenschutzbeauftragte dürfen nicht Sie selbst sein und der Mitarbeiter, den Sie dazu bestellen, darf nicht in einen Interessenkonflikt geraten. Deshalb werden die IT-Verantwortlichen oder in größeren Unternehmen die Personalchefs als ungeeignet angesehen. Wenn Sie einen geeigneten Kandidaten haben, müssen Sie ihn ausbilden lassen und ihm entsprechende Arbeitszeit und Freiraum zur Aufgabenerfüllung einräumen. Ihr interner Datenschutzbeauftragter unterliegt einem besonderen Kündigungsschutz und hat das Recht in alle Belange Ihres Unternehmens Einblick zu erhalten, in denen personenbezogene Daten verarbeitet werden. Die andere Möglichkeit besteht darin, einen externen Datenschutzbeauftragten zu bestellen. Dieser besitzt die nötige Fachkompetenz und kann unter Umständen die bessere Lösung sein.

Umfassende Information über Verarbeitung personenbezogener Daten

Weiterhin müssen Sie als Praxisinhaber im Blick haben, dass die Rechte der betroffenen Personen auf Auskunft und Berichtigung sowie Löschung gewahrt werden. Jede betroffene Person hat das Recht, über die Verarbeitung ihrer personenbezogenen Daten umfassend informiert zu werden. Sie sollten transparent machen, wie

und welche Daten Sie speichern und wann Sie sie löschen, aber auch, an wen Daten weitergeben werden. Denken Sie dabei auch an Ihr Dentallabor (siehe Seite 14).
Eine Weitergabe von personenbezogenen Daten nach Art. 9 DSGVO (besondere Arten von personenbezogenen Daten unter anderem Gesundheitsdaten) an Dritte erfordert datenschutzrechtlich eine entsprechende Rechtsgrundlage, zum Beispiel die eindeutige Einwilligung des Patienten zur Weitergabe seiner Daten an das bestimmte Dentallabor. Daneben sind die Rechtsvorschriften nach § 203 StGB und das Berufsrecht zu beachten.

Regelmäßige Überprüfungen protokollieren

Die Datenschutz-Compliance in Ihrer Praxis zu sichern, ist eine anspruchsvolle Aufgabe, die Sie in Zukunft begleiten wird. Sie sind verpflichtet, regelmäßig zu überprüfen, ob Ihre ergriffenen Maßnahmen zum Schutz der Ihnen anvertrauten Daten noch angemessen sind und dem Stand der Technik entsprechen. Diese regelmäßigen Überprüfungen sollten Sie unbedingt protokollieren und die sich daraus ergebenen Maßnahmen mit zeitlichen Vorgaben für die Umsetzung versehen. Nur so können Sie nachweisen, dass Sie ihre Rechtskonformität überprüfen und regelmäßig verbessern.

Bußgelder in Millionenhöhe möglich

Eine wesentliche Veränderung, die das neue Datenschutzrecht mit sich bringt, liegt bis auf die erhöhte Dokumentationspflicht nicht so stark in den Inhalten der Anforderungen, sondern in dem neu geschaffenen Sanktions-Regime. Die Höhe der Sanktionen ist auf maximal 20 Millionen Euro oder vier Prozent des weltweiten Unternehmensumsatzes festgelegt worden. Wobei sich die Tatbestände, die bußgeldwehrt sind, erheblich erweitert haben.
Auch wenn wir heute noch nicht abschätzen können, wie umfangreich und in welchen Höhen tatsächlich Bußgelder bei Verstößen festgesetzt werden, ist es ratsam, sich intensiv mit dem Thema Datenschutz in der Zahnarztpraxis zu beschäftigen.

Gerd-Jürgen Golze
www. datenschutzbeauftragter-berlin.com