Ratgeber

DATENSCHUTZ

Alles neu mit der

Datenschutz-grundverordnung?

Am 25. Mai 2018 ist die neue Datenschutzgrundverordnung der EU (DSGVO) in Kraft getreten. Das bedeutet für Berufsgruppen, die mit sensiblen personenbezogenen Daten arbeiten, ein Umdenken sowie Anpassen der Workflows und Sicherheitsstandards. Die DSGVO legt außerdem Wert darauf, dass nur die minimal notwendigen Daten abgefragt und gespeichert werden. Auch müssen sie sachlich richtig und aktuell vorliegen, andernfalls gehören sie gelöscht. Besonderes Augenmerk legt die Verordnung auf die angemessene Sicherheit der Daten. Schließlich soll kein Dritter unbefugt Zugang erlangen.

Einerseits soll der Datenschutz jedes Bürgers gewährleistet werden, andererseits muss weiterhin die Datenverarbeitung durch Unternehmen möglich sein:

- Daten dürfen nur rechtmäßig erhoben worden sein.
- Kunden/Patienten haben ein Recht auf Transparenz, was den Ursprung der Daten und die Art ihrer Verarbeitung angeht.
- Schon vor der Datenerhebung muss deren Zweck feststehen, von dem auch später nicht abgewichen werden darf. Daten für Zweck A erheben und für Zweck B verwenden, schließt sich also aus.

Die Verantwortung für den Datenschutz liegt beim behandelnden Zahnarzt oder bei dem zuständigen Datenschutzbeauftragten (Art. 37 Abs. 1 DSGVO), denn gemäß Art. 9 Abs. 1 DSGVO sind Gesundheitsdaten als besonders schützenswert anzusehen.

Dabei ist ein Datenschutzbeauftragter verpflichtend einzustellen oder zu ernennen, wenn mehr als neun Personen mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind.

DATENSCHUTZ IN DEN PRAXISRÄUMEN

Datenschutz beginnt schon beim Gespräch mit dem Patienten am Telefon. Dort sollten die Daten zur Authentifizierung stets abgefragt und nicht einfach vorausgesetzt oder vorgelesen werden. So kann eine versehentliche Weitergabe von patientenbezogen Daten an Dritte schon am Empfang verhindert werden und die Integrität der ärztlichen Schweigepflicht gemäß § 203 StGB gewahrt werden. Alle Computer und mobilen Endgeräte, die sensible Daten von Patienten verarbeiten oder speichern, sollten vor dem Zugriff durch Patienten oder andere Dritte geschützt werden. Patientenakten dürfen nicht unbeaufsichtigt, für jedermann frei zugänglich in den Praxisräumen liegen. Alle patientenbezogenen Daten, die unter die Datenschutzgesetzgebung fallen, sind als sensibel einzustufen. Das bloße Vorhandensein von mehreren Datenteilen wie Name und Adresse führt zu Assoziationsmöglichkeiten, in welche die betroffene Person meist nicht eingewilligt hat, sodass hier schnell die Datenschutzgrundverordnung verletzt werden kann[1].

Qdent 2018 | 2 (2) | 42–44

DATENSICHERUNG UND ABRECHNUNGSPROGRAMME

Über Datenschutz nachdenken muss man auch bei der der täglich durchzuführenden Datensicherung des Abrechnungsprogramms und anderer EDV-Einrichtungen der Praxis. Eine Verschlüsselung ist angeraten. Die sicherste Möglichkeit, die auch von der Bundeszahnärztekammer empfohlen wird, stellt die absolute Trennung mobiler Endgeräte von sensiblen Patienteninformationen am Arbeitsplatz dar. Der Internetzugriff sollte dann von einem anderen Gerät vorgenommen werden[2]. Dies ist aber im Zeitalter der digital vernetzten Praxis, in der die Datenübertragung zwischen den einzelnen Behandlungsräumen zum Alltag gehört, schwierig umzusetzen. Da digitales Röntgen und die Verwaltung über ein praxiseigenes Netzwerk laufen, kann dieses Netzwerk natürlich auch von außen für Dritte auffindbar und hackbar sein.

Besonders heikel wird es, wenn die Abrechnung an einen externen Dienstleister abgegeben wird. Dann muss mit diesem eine vertragliche Datenschutzvereinbarung auf Grundlage der DSGVO getroffen werden, womit ab dem Zeitpunkt der Übermittlung der Daten der Behandler von der Überwachung der Einhaltung des Datenschutzes befreit ist (§ 10 Abs. 6 GOZ; gilt auch bei der Inanspruchnahme von Fremdlaboren). Nach der Rechtsprechung des Bundesgerichtshofs stellt die Weitergabe der Daten zum Zweck der Abrechnung ohne Zustimmung des Patienten einen Verstoß gegen das Verbotsgesetz des § 203 StGB dar, weil damit die ärztliche Schweigepflicht verletzt wird[3]. Auch das Bundesdatenschutzgesetz empfiehlt aus Beweisgründen die vorherige Einholung einer schriftlichen Einwilligung[3].

AUSNAHMEN

Bei der Veröffentlichung von Patientenfällen ist für intraorale Aufnahmen keine gesonderte Einwilligung des Patienten erforderlich. Allerdings ist, solange man den Patienten auf einem solchen Bild identifizieren könnte, die ausdrückliche und schriftliche Genehmigung bereits vor Betätigung des Auslösers einzuholen. Andernfalls kommt dies einem Verstoß gegen das Recht am eigenen Bild gleich (i. S. v. § 201a StGB) und kann mit einer erheblichen Geldstrafe geahndet werden.

Die DSGVO gilt nicht für die Verarbeitung personenbezogener Daten zum Zwecke der Prävention, Aufdeckung und Verfolgung von Straftaten der zuständigen Behörden. In diesem Fall greift letztlich die ärztliche Schweigepflicht, von der ärztliches Personal im Rahmen einer Verwicklung oder Bezeugung einer möglichen Straftat mittels eines richterlichen Urteils jedoch entbunden werden darf.

SANKTIONEN

Mit der neuen Datenschutzgrundverordnung gehen auch neue mögliche Sanktionen zu Verstößen einher. So sind Bußgelder bei Rechtsverstößen von bis zu 4 % des Jahresumsatzes eines Unternehmens oder 20 Mio. Euro gemäß Art. 83 Abs. 5 DSGVO zulässig[4].

WAS ÄNDERT SICH FÜR ZAHNÄRZTE UND ZAHNMEDIZINISCHES PERSONAL?

- Patienten dürfen nur noch mit ihrer schriftlichen Einwilligung zu Recallterminen angeschrieben werden.
- Patienten müssen schriftlich einwilligen, dass ihre Daten an externe Dienstleister wie Labore, Abrechnungsstellen etc. weitergegeben werden dürfen.

HAT EIN PATIENT UNEINGESCHRÄNKTES VETORECHT, WENN ES UM DIE WEITERGABE SEINER DATEN GEHT?

- Bei einigen strukturellen Vorgängen dürfen patientenbezogene Daten ohne die Genehmigung des Patienten an Dritte außerhalb der Praxis weitergegeben werden (z. B. Rechnungsdaten an das Finanzamt, die Krankenkasse, die Landeszahnärztekammer, einen Gutachter o. ä.).
- Ein Vetorecht besteht nur bei den sensiblen Daten bezüglich der gesundheitlichen Situation (Röntgenbilder, Intraoralaufnahmen, Dokumentation, Therapieverläufe).

WIRD DURCH DIE NEUE DATENSCHUTZGRUNDVERORDNUNG DIE PRAXISVERWALTUNG AUFWENDIGER UND KOMPLIZIERTER?

- Der Patient muss über die Weitergabe seiner Daten an Dritte aufgeklärt werden (nur zu medizinisch oder verwaltungstechnisch notwendigen Zwecken zulässig). Sicherheitsstandards der benutzten Hard- und Software sind zu prüfen und anzupassen.
- Weitere schriftliche Einwilligungen des Patienten sind nur in besonderen Fällen notwendig.

WAS DARF DER PATIENT OHNE EINWILLIGUNG ZUM DATENSCHUTZ PER POST ODER E-MAIL ZUGESTELLT BEKOMMEN?

- Rechnungen, Mahnungen und therapiebezogene Informationen bekommt der Patient nach wie vor regulär.
- Werbung zu Praxisveranstaltungen, Aktionen oder regelmäßige Recallanrufe dürfen nur nach vorheriger Einwilligung an den Patienten gesendet werden (gilt nicht für Terminerinnerungen).

MAXIMILIAN DOBBERTIN

8. Fachsemester
Johann Wolfgang Goethe-Universität Frankfurt am Main
E-Mail: maximiliandobbertin@hotmail.de

JOHANNES JÄGER

Dipl.-Jur. Univ., Rechtsreferendar
Julius-Maximilians-Universität Würzburg
E-Mail: johannesmjaeger@gmail.com

LITERATUR

1. LZK Thüringen (Hrsg.). Patientendokumentation, Schweigepflicht und Datenschutz in der Zahnarztpraxis. September 2013. https://www.lzkth.de/lzkth2/ressources.nsf/(UNID)/72AD206FE9ED87BDC125827F002D6917/$file/patientendokumentation_schweigepflicht_und_datenschutz_in_der_zahnarztpraxis.pdf. Letzter Zugriff: 30.04.2018.
2. BZÄK/KZBV (Hrsg.). Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV. April 2015. https://www.bzaek.de/fileadmin/PDFs/za/datenschutzleitfaden.pdf. Letzter Zugriff: 30.04.2018.
3. Lenhard TH, Kazemi R. Datenschutz in der Zahnarztpraxis. Köln: Deutscher Zahnärzte Verlag, 2016:17.
4. DSVGO. 2018. https://dsgvo-gesetz.de/art-83-dsgvo. Letzter Zugriff: 30.04.2018.