Umsetzung der EU-DSGVO in der kieferorthopädischen Praxis

Von Simone Uecker, Praxisberaterin bei 4MED Consult, München.

„Die Sicherheit von Patientendaten und der Schutz der Praxis-IT gehörten bereits von Beginn an zu den Grundsätzen der Praxis“, bestätigt der niedergelassene Kieferorthopäde, den Simone Uecker bereits seit 2017 in den Vorbereitungen auf die EU-DSGVO betreut. Somit waren eine Firewall, Systemtrennung zwischen Praxisnetz und freiem Internetzugang, differenzierte Zugriffsrechte oder Schlösser an Karteikartenschränken bereits eine Selbstverständlichkeit und die parallele Nutzung von physischer Karteikarte und digitaler Patientenakte Teil des Sicherheitskonzepts, um auch bei Komplettausfall der Praxis-IT die Versorgung der Patienten jederzeit sicherstellen zu können. Auch unter den modernen, technikaffinen Kieferorthopäden gibt es Freunde der Karteikarte – schnellere Übersicht, „Sicherheitsnetz“ gegen die Abhängigkeit von der IT-Verfügbarkeit und nur minimale Effizienzverluste aus der zusätzlichen PC-Eingabe sprechen auch im Jahr 2018 noch dafür. Der Datenschutz muss dann die physische und die digitale Kartei abdecken.

Abb. 1: Datenschutzrad – Schritte und Elemente zur Vorbereitung und Einhaltung von EU-DSGVO und BDSG (neu). *(Quelle: 4MED Consult)*

Erst die Abläufe kennen und überprüfen …

Die Umsetzung der Datenschutzrechte sollte nicht zu „wilder Dokumentitis“ führen. An erster Stelle steht die eingehende und ehrliche Prüfung der eigenen Arbeitsweisen. Der erste Anlaufpunkt für den Kieferorthopäden und die Beraterin war das bestehende QM-System der Praxis, in dem bereits die praxiskritischen Prozesse dokumentiert waren. Hier fanden sich schon einige Vorgehensweisen, die zum Datenschutz und zur Sicherheit der Daten beigetragen haben und somit schnell als Teil der „technischen und organisatorischen Maßnahmen“ (TOM) identifiziert werden konnten.

Mit einem Rundgang durch die Praxis mit Fokus auf die Patientendaten lassen sich die verarbeiteten Daten zunächst als Überblick sammeln. Hier zeigte sich, dass der Grundsatz der Datenminimierung, also nur die für die Behandlung wirklich erforderlichen Daten zu erfassen, bereits Grundprinzip der Praxis war. Natürlich merken sich Behandler und das Praxisteam persönliche Details der Patienten (z. B. den geplanten Urlaub oder das passionierte Hobby), um beim nächsten Termin auch wieder ein paar persönliche Worte zu sprechen – in der Patientenakte hatte diese Information aber noch nie etwas zu suchen, und das wird sich auch nicht ändern.

Der kritische Blick auf die Praxis hat aber auch einige Verbesserungspotenziale offenbart, die zunächst zum Wohle des Datenschutzes und der Patienten umgesetzt wurden. Mit jedem Schritt der Verbesserung und Umsetzung ging die Schulung des Praxisteams und die Dokumentation des verbesserten Prozesses einher. Das bedeutet zwar kontinuierliche Arbeit am QM, aber mit diesem Zugang war es möglich, parallel zum laufenden Praxisbetrieb schrittweise die Vorbereitung auf die EU-DSGVO und den eigenen Anspruch an den Datenschutz umzusetzen.

Die eine oder andere „Verschlimmbesserung" hat die Praxis natürlich auch erlebt. So musste das Team beispielsweise feststellen, dass das permanente Sperren und Entsperren der Bildschirme, um einen Zugriff z. B. durch wartende Patienten zu verhindern, den Arbeitsablauf erheblich stören. Um hier Sicherheit zu schaffen, sollte eine technische Lösung zur Sperre gefunden werden, und der Bildschirmschoner genügte den Ansprüchen der Praxis nicht. Nach einigen Fehlversuchen mit ungeeigneten Lösungen konnte schließlich ein System gefunden werden, das einfach zu administrieren ist und zugleich nur eine verhältnismäßig kleine Investition erfordert. So entsperren sich die Bildschirme wie von Geisterhand, sobald ein Mitarbeiter anwesend ist. Ist kein Mitarbeiter in der Nähe, wird der Bildschirm innerhalb weniger Sekunden wieder gesperrt. So wird der Ablauf nicht gestört, die Arbeit der Behandlungsassistenz vereinfacht und keine komplizierten Passwörter können vergessen werden.

Viele der in den letzten Jahren mit Kunden erarbeiteten und praktisch bewährten Lösungen lassen sich schnell und meist mit geringem Aufwand in der Praxis umsetzen – seien es transpondergesteuerte PC-Sperren, Passwortsicherheit oder eine echte Systemtrennung des Internets vom Praxisnetz. Die genaue Art der Umsetzung ist auch immer von der Praxis, ihrer Größe, der technischen Ausstattung und Komplexität abhängig, sodass z. B. in Kleinpraxen nicht immer in komplexe und teure Lösungen investiert werden muss, um Sicherheit zu schaffen.

… dann dokumentieren

In der Dokumentation hat der Praxis das „Datenschutzrad" von 4MED Consult als Grundgerüst geholfen (Abb. 1). Viele Praxen stellen sich die Frage, wie sie denn nun wirklich vorgehen sollen, um der EU-DSGVO und dem BDSG (neu) gerecht zu werden. Das Datenschutzrad zeigt nicht nur die erforderlichen Elemente eines Datenschutzmanagementsystems, sondern auch die aufeinander aufbauenden Schritte zur GDPR Readiness.[1] „Ein logisches Vorgehen, bei dem jeder Schritt auf die vorangegangenen Schritte aufbaut, macht die Vorbereitungen viel einfacher und effizienter. Habe ich den grundsätzlichen Ansatz der Praxis zum Datenschutz (Datenschutzrichtlinie) und die Abläufe (Verfahren und TOMs) in der Praxis verstanden, kann ich die Rechtsgrundlagen der Datenverarbeitung zusammenfassen und durch Einwilligungen und Verarbeitungsverträge ergänzen, wo diese erforderlich sind. Danach bleibt noch die Information und Kommunikation mit den Patienten und Mitarbeitern, um die Vorbereitungen abzuschließen", erklärt Simone Uecker. Mithilfe einer so strukturierten Vorgehensweise konnte mit dem Kieferorthopäden auch geklärt werden, in welchem Bereich das Praxisteam selbst tätig wurde und wo die Praxisberaterin agieren sollte. Die Datenschutzrichtlinie, das Einholen der Auftragsverarbeitungsverträge, die Prozesse zu den Betroffenenrechten und die Dokumentation ergänzender Arbeitsanweisungen im Rahmen der TOMs konnte die Praxis nach kurzer Einschulung selbst durchführen.

„Für mich sind die Verarbeitungstätigkeiten der spannendste Schritt."

„Bei dem Verzeichnis der Verarbeitungstätigkeiten waren wir über Hilfe von außen sehr dankbar. Diese Arbeit ist wahrscheinlich der Schritt der meisten Bürokratie in der EU-DSGVO-Vorbereitung", verrät der Kieferorthopäde. Simone Uecker sieht das naturgemäß gegenteilig – wo der Kieferorthopäde Bürokratie wittert, sieht die Beraterin Potenziale: „Während ich die Verarbeitungstätigkeiten einer Praxis erfasse, bekomme ich eine detaillierte Idee, welche technischen und organisatorischen Maßnahmen vorliegen müssen, um diese Daten und ihre Verarbeitungsschritte zu schützen. So kann ich der Praxis genaue Hinweise geben, wo möglicherweise noch zusätzliche Maßnahmen ergriffen oder zumindest im QM dokumentiert werden sollten."

Nur die Dokumentation der technischen Maßnahmen bereitet Simone Uecker manchmal Kopfschmerzen: „Nach fast 15 Jahren in der IT spreche ich auch als Betriebswirt die Sprache der IT-Techniker. Ein IT-Sicherheitskonzept zu prüfen und zu durchleuchten – und manchmal auch zu dokumentieren – ist eine Aufgabe, der ich mich mit meiner Technikaffinität gerne stelle." Trotzdem wünscht sich die Praxisberaterin, dass die IT-Dienstleister proaktiv den betreuten

Praxen eine umfassendere Dokumentation zur Verfügung stellen, und das in einem Format, das der Praxisinhaber zumindest in Grundzügen verstehen kann. Damit wird es dem Inhaber erleichtert, eine qualifizierte Entscheidung zu seinen IT-Sicherheitsmaßnahmen und zu möglichen Investitionen in diesem Bereich zu treffen.

Die Website in Zeiten der EU-DSGVO

Die Vielzahl an Plug-ins, Tools und Funktionalitäten, die sich in Websites einbinden lassen, ist verführerisch: Onlinekarten für die Wegbeschreibung, Analysetools zur Prüfung der Besucherzahlen und der Werbeanzeigen, Newsletter, Kontaktformulare, Like-Buttons und vieles mehr. Doch welche Daten im Hintergrund erfasst und an die Anbieter weitergegeben werden, ist vielfach nicht bekannt. Auch wenn diese Funktionen meist auch in Zeiten der EU-DSGVO legitimiert werden können (oder dem Besucher schlicht die Möglichkeit zur individuellen Deaktivierung bieten) … Sind wirklich alle Funktionen nötig? Die etablierte kieferorthopädische Praxis konnte dies schnell beantworten: „Bestmöglicher Service ist mir für meine Patienten und Interessenten wichtig. Aber die Websitebesucher zu durchleuchten, bringt Patienten und Praxis keinen Nutzen. Wir kennen unsere Patienten persönlich und wissen aus vielen Gesprächen, was unsere Patienten an uns schätzen. Diese Vorzüge präsentieren wir authentisch und ehrlich auch auf unserer Website – dafür brauchen wir keine Analysetools, die Nutzerdaten im Hintergrund sammeln." Die Datenschutzerklärung für die Website ist mit diesem Vorgehen weniger komplex – auch wenn der Anwalt trotzdem zu etwas mehr Details rät, um allen Informationspflichten gerecht zu werden.

Auch zukünftig am Ball bleiben!

Die Vorbereitungen zur EU-Datenschutz-Grundverordnung konnten in der kieferorthopädischen Praxis größtenteils bis zum 25. Mai abgeschlossen werden, und auch erste Auskunftsanfragen von Patienten über ihre verarbeiteten Daten sind bereits beantwortet. Der Datenschutz-Selbstcheck im nächsten Jahr ist bereits geplant, um das Datenschutzmanagementsystem, z. B. an neue Abläufe, anzupassen. Heute beschäftigt sich die kieferorthopädische Praxis vorwiegend damit, das Praxisteam regelmäßig zu schulen. Hier steht der Fokus nicht auf den rechtlichen Maßgaben der EU-DSGVO, sondern auf den praktischen Schritten im Arbeitsablauf. Schnell können Praxis- und Patientendaten durch Angriffe Cyberkrimineller diskreditiert werden oder einfach dadurch, dass eine neue Mitarbeiterin die Antivirussoftware aus Unwissenheit täglich deaktiviert und so den Schutz der Praxis gefährdet.

Ausblick

Wie kann sich das Praxisteam gegen Cyberkriminelle schützen und auf welche Elemente sollte im IT-Sicherheitskonzept der Praxis besonderer Wert gelegt werden? Im nächsten Artikel verrät Simone Uecker ihre praktischen Tipps zum Schutz der Praxis und ihrer Daten im Rahmen der technischen und organisatorischen Maßnahmen.

1 GDPR Readiness ist der internationale Fachbegriff zur Vorbereitung und Erfüllung der Europäischen Datenschutz-Grundverordnung (EU General Data Protection Regulation = GDPR).

kontakt

Mag. (FH) Simone Uecker
4MED Consult
Landsberger Straße 302
80687 München
Tel.: 089 57847487
info@4med-consult.de
www.4med-consult.de

Infos zur Autorin