INTERVIEW Ein von Herzen kommendes „Hurra“ als Reaktion auf das Inkrafttreten der neuen Datenschutz-Grundverordnung, kurz DSGVO, war am 25. Mai weder von Praxisinhabern noch Unternehmern zu hören, doch der sich daraus ergebene Zugzwang schweißt alle zusammen. Im Doppelinterview beleuchten Datenschutzbeauftragter Holger Zürn sowie Rechtsanwalt Björn Papendorf sowohl die technischen als auch rechtlichen Komponenten bei der Umsetzung in der Zahnarztpraxis anhand von konkreten Fallbeispielen.

Kerstin Oesterreich

Damoklesschwert DSGVO: Hochkonjunktur für Abmahnungen

Holger Zürn, Datenschutzbeauftragter für das Unternehmen audius mit Stammsitz in Weinstadt, berät unter anderem dental bauer in allen datenschutzrechtlichen Belangen.

Herr Zürn, seit 2017 sind Sie für das Dentaldepot dental bauer als externer Datenschutzbeauftragter tätig. Wie genau verläuft die Zusammenarbeit?
Holger Zürn: Die DSGVO sieht als Aufgaben des DSB die Unterrichtung und Beratung des Verantwortlichen sowie die Überwachung der geltenden Datenschutzvorschriften vor. Wir bei audius haben dafür in den letzten Jahren ein Modell entwickelt, das wir auch bei dental bauer anwenden: Begonnen wurde mit einem eintägigen Grundlagen-Workshop mit Geschäftsführer Jörg Linneweh und IT-Leiter Hans-Joachim Schneider über die DSGVO, bei dem das weitere Vorgehen besprochen wurde. Anschließend ging es direkt mit der Basisprüfung weiter: Ziel war es, bis zum Inkrafttreten am 25. Mai die wichtigsten Punkte erledigt oder zumindest auf den Weg gebracht zu haben. Rückblickend wurde das gut gemeistert. Aktuell befinden wir uns in einem fortgeschrittenen Stadium der Basisprüfung, in dem ich durch alle für den Datenschutz relevanten Bereiche gehe, mit den Verantwortlichen spreche und Prozesse prüfe und dokumentiere – ähnlich wie ein Audit. Falls Anpassungen notwendig sind, werden diese je nach Dringlichkeit direkt umgesetzt oder für später eingeplant. Daran schließt sich die sogenannte Folgeprüfung an. Hier werden die für später eingeplanten Maßnahmen priorisiert und umgesetzt sowie aktuelle Themen bearbeitet. Auch Schulungen der Mitarbeiter gehören dazu.

Interner oder externer DSB – Wo liegen die Vor- und Nachteile?
Aus meiner Sicht macht ein interner Datenschutzbeauftragter erst ab einer gewissen Unternehmensgröße Sinn, nämlich dann, wenn dieser in Vollzeit beschäftigt werden kann. Ist dies nicht der Fall, wird immer ein Interessenskonflikt zwischen seiner täglichen Arbeit und dem Datenschutz bestehen. Auch das Thema Weiterbildung spricht für einen externen Datenschutzbeauftragten. Ich bilde mich sieben bis zehn Tage im Jahr zum Thema Datenschutz weiter. Dazu käme bei einem internen Datenschutzbeauftragten die Erstausbildung. Je nach Anbieter muss man mit fünf bis 15 Tagen rechnen. Dazu bringe ich als Externer die Erfahrung aus vielen anderen Unternehmen mit, verfüge über die notwendigen Dokumente und Vorlagen und muss diese nicht zeitintensiv erstellen.

Unter welchen Voraussetzungen müssen Praxisinhaber einen Datenschutzbeauftragten verpflichten?
Das ist in der DSGVO und dem Bundesdatenschutzgesetz (BDSG) leider etwas schwammig formuliert. Sind in der Regel zehn oder mehr Personen in der Praxis ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, ist laut BDSG ein Datenschutzbeauftragter zu bestellen. Gezählt werden müssen hierbei wirklich die Köpfe, also auch jede

„Ein interner Datenschutzbeauftragter macht erst ab einer gewissen Unternehmensgröße Sinn, nämlich wenn dieser in Vollzeit beschäftigt werden kann."

Holger Zürn

Teilzeitkraft. Prinzipiell müssen alle Mitarbeiter berücksichtigt werden, die über einen PC-Arbeitsplatz oder einen Zugang zu einem PC verfügen.
Was aber, wenn die Praxis weniger als zehn Mitarbeiter hat? Die DSGVO sagt, die Benennung eines Datenschutzbeauftragen ist notwendig, wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten besteht. Gesundheitsdaten zählen zu diesen besonderen Kategorien von Daten. Also wäre auch jetzt die Benennung eines Datenschutzbeauftragten verpflichtend. Allerdings gibt es noch den Erwägungsgrund 91 (auf Basis der Erwägungsgründe wurde die DSGVO erlassen). In diesem steht, dass die Verarbeitung personenbezogener Daten nicht als umfangreich gelten soll, wenn sie die Verarbeitung personenbezogener Daten von Patienten betrifft und durch einen einzelnen Arzt oder sonstige Angehörige eines Gesundheitsberufs erfolgt.
Zusammengefasst kann man sagen, dass ab zehn Personen im Praxisteam ein Datenschutzbeauftragter benannt werden muss, darunter nicht. So zumindest die heutige Interpretation.

Was verbirgt sich hinter der Anforderung „datenschutzkonform"?
Datenschutzkonform heißt erst einmal nichts anderes, als in der Praxis gesetzeskonform zu handeln. Neu ist aber, dass der Verantwortliche – der Praxisinhaber – die Einhaltung der Datenschutzgesetze nachweisen können muss, Stichwort Rechenschaftspflicht.

In welchen klassischen „Offlinebereichen" kommt es in Zahnarztpraxen regelmäßig zu Datenschutzverstößen und wie können diese vermieden werden?
Ein großes Thema ist der Empfangs- und Wartebereich. Am Empfang wird einfach viel telefoniert und teilweise werden auch personenbezogene Daten durchgegeben. Oder es wird mit dem Patienten direkt über vertrauliche Inhalte gesprochen. Wenn dann noch das Wartezimmer in Hörweite ist oder die Zimmer sehr hellhörig sind, ist der Datenschutzverstoß komplett. Um dies zu vermeiden, sind bauliche Maßnahmen

„Häufig ist es für den Laien schwierig, eine berechtigte von einer unberechtigten Abmahnung zu unterscheiden."

Björn Papendorf

oder zumindest Abstandshalter am Empfang notwendig. Weiter gilt es, die Mitarbeiter zu sensibilisieren, dass diese die Patienten erstens darauf hinweisen, Abstand zu halten, und zweitens selber darauf achten, welche Informationen sie in welchem Zusammenhang herausgeben und wer noch alles mithört.

Welche Grundsätze beim Gebrauch der Praxis-EDV gilt es, zu beachten?
Grundsätzlich ist darauf zu achten, dass die EDV gegen unbefugten Zugang abgesichert ist und die Monitore nicht einsehbar sind. Monitore können relativ einfach umgestellt werden, aber auch für die Authentifizierung am System gibt es heute praktikable Lösungen. Diese verhindern einerseits, dass Unbefugte Zugriff auf das System erhalten und ermöglichen andererseits den Nutzern einen schnellen Zugang, z.B. über ein Token, ohne ständig ein langes Passwort eingeben zu müssen. Auch Patientendaten unverschlüsselt, z.B. per E-Mail, zu versenden, verstößt gegen den Datenschutz. Es sollten also schleunigst alternative, sichere Übertragungswege gesucht werden.

Björn Papendorf ist Rechtsanwalt und Fachanwalt für Medizinrecht, LL.M. sowie geschäftsführender Partner der Kanzlei für Wirtschaft und Medizin kwm in Münster.

Wie können sich Praxisinhaber beim Thema Datenschutz rechtssicher aufstellen?
Björn Papendorf: Das Wichtigste ist, dass der Umgang mit den nötigen Pflichtdokumenten nach außen zeigt: Wir nehmen den Datenschutz ernst. Für diese Pflichtdokumente gibt es viele Muster im Internet. Davon können wir nur abraten, denn diese sind stets gleichsam zusammengeklaubt und nie aus einem Guss. Als Fachkanzlei für das Gesundheitswesen bieten wir ein Datenschutzpaket an, das alle Pflichtdokumente aus fachanwaltlicher Hand gefertigt, zusammenfasst. Damit können Praxisinhaber sicher sein, dass sie in puncto Verarbeitungsverzeichnis, Auftragsdatenverarbeitungsverträge, Datenschutzverpflichtung der Mitarbeiter und hinsichtlich der weiteren rechtlichen Anforderungen sicher aufgestellt sind.
Eine Alternative ist der Beitritt zu einem Datenschutzverband, in dem die Interessen der mit dem Datenschutz konfrontierten Praxen gebündelt werden. Gegen eine monatliche Gebühr erhalten Mitgliedspraxen das oben genannte Dokumentenpaket und können zugleich die Dienste eines externen Datenschutzbeauftragten mit in Anspruch nehmen.

Welche Verstöße werden oft gerügt?
Am häufigsten beschäftigen sich Abmahnungen mit allem, was der „Außendarstellung" der Praxis entspringt. Zuallererst meint dies die Datenschutzerklärung auf der Homepage, denn nichts ist so einfach, wie beispielsweise „Zahnarzt Münster" bei Google einzugeben und dann die Liste durchzuklicken, bis sich die erste Praxis ohne Datenschutzerklärung findet.
In den Fällen, in denen sich Praxisinhaber den vielen Fallstricken des Datenschutzrechts stellen und die Anforderungen umsetzen, steckt der Teufel im Detail, sodass bereits Kleinigkeiten abmahnfähig sein können. Beispielhaft seien hier nur die berühmt-berüchtigten Tracking-Tools in der Datenschutzerklärung genannt. Teilweise wissen Praxisinhaber gar nicht, dass ihre Homepage diese aktiviert hat und somit die Daten der Besucher mitschneidet. Wird darüber in der Datenschutzerklärung nicht aufgeklärt, kann eine berechtigte Abmahnung mit entsprechend negativen Folgen vorliegen.

Was gilt es, im Falle einer Abmahnung zu beachten?
Zunächst lässt sich sagen, dass die ganz große Abmahnwelle ausgeblieben ist. Dies liegt nicht zuletzt an der enormen Komplexität des Stoffs, die auch für viele Abmahn-Kanzleien, die schwarzen Schafe unseres Berufsstands, eine Herausforderung darstellt. Wir empfehlen jedem Praxisinhaber, eine Abmahnung im Zweifel einem Rechtsanwalt vorzulegen. Denn häufig ist es für den Laien schwierig, eine berechtigte von einer unberechtigten Abmahnung zu unterscheiden. Als grobe Faustformel kann man sich anhand der Sprache des Briefs orientieren: Große Abmahn-Kanzleien nutzen automatisierte Textgeneratoren, die selbstständig im Zuge eines Algorithmus das Internet durchforsten und nach Verstößen suchen. Die dazu generierten Texte wirken entsprechend hölzern. Handelt es sich hingegen um eine Kanzlei aus der Nähe des Praxisinhabers, die sich noch dazu mit der konkreten Situation vor Ort beim Praxisinhaber befasst zu haben scheint, so wird es sich wohl um einen konkurrierenden Zahnarzt aus der Region handeln, der nicht so einfach locker lassen wird. Dann ist Vorsicht geboten.

Was gilt es, als Betreiber einer „Praxis-Fanpage" auf Facebook zu beachten?
Das Grundproblem liegt nach dem viel zitierten Urteil des EuGH darin, dass den privaten Betreibern dieser Fanpages die gleichen Pflichten auferlegt werden wie beim Betrieb ihrer ureigenen Internetseiten – und das, obwohl eigentlich Facebook diese Seiten bereitstellt. Wer eine absolute Sicherheit haben möchte, der nimmt seine Facebook-Fanpage vom Netz. Für viele Praxisinhaber ist dies aber nicht praktikabel, weshalb wir einen Mittelweg empfehlen: Solange die konkreten Konsequenzen noch unklar sind, wird man die Fanpage online lassen können, man sollte jedoch auf jeden Fall einen Link zum Impressum und zur eigenen Datenschutzerklärung setzen. Damit setzt man immerhin die wesentlichen Informationspflichten nach Artikel 12 und 13 DSGVO auf der eigenen Fanpage um.

Was ist ein Verarbeitungsvertrag und inwieweit schützt er dental bauer Kunden?
Auftragsverarbeitungsverträge fluten momentan die Schreibtische deutscher Unternehmen. Ich persönlich halte dieses Rechtsinstrument für unglücklich. Die Praxis zeigt bereits jetzt, dass dieser Pflichtvertrag von allen mehr oder weniger ungelesen in der Schublade verschwindet. Dennoch verlangt der Gesetzgeber, dass immer dort, wo sich ein Datenschutzverantwortlicher den Diensten eines Dritten bei der Bearbeitung von Daten bedient, ein solcher Vertrag abzuschließen ist. Beispiele hierfür sind Auftragsverarbeitungsverträge zwischen dem Praxisinhaber und dem Labor, dem IT-Dienstleister oder mit der externen Abrechnungskraft. Anders als häufig angenommen wird, ist solch ein Vertrag mit dem eigenen Steuerberater nicht notwendig. Dies gilt auch dann, wenn der Steuerberater weniger beratend, sondern ausschließlich im Wege der Personalbuchhaltung und Gehaltsabrechnung tätig ist. Dies war bis vor einiger Zeit umstritten.
Der beste Schutz des Vertrags ist schon einmal darin zu sehen, dass man der neuen datenschutzrechtlichen Forderung nachkommt. Inhaltlich dient der Vertrag der Absicherung für Praxisinhaber im Falle von Verstößen, die ihre Auftragnehmer zulasten der Patienten begehen könnten. Aufgrund der klaren Verantwortungszuordnung ist es unter Umständen möglich, für die Schäden der Patienten im Innenverhältnis den eigenen Auftragnehmer in Regress zu nehmen.

Vielen Dank für das Interview.

dental bauer
Infos zum Unternehmen

Björn Papendorf
Infos zur Person

INFORMATION

dental bauer GmbH & Co. KG
Ernst-Simon-Straße 12, 72072 Tübingen
Tel.: 07071 9777-0
info@dentalbauer.de
www.dentalbauer.de

Holger Zürn
audius AG
Mercedesstraße 31
71384 Weinstadt
Tel.: 07151 36900284
info@audius.de
www.audius.de

RA Björn Papendorf, LL.M.
kwm – Kanzlei für Wirtschaft und Medizin
Partnerschaftsgesellschaft mbB
Albersloher Weg 10c
48155 Münster
Tel.: 0251 53599-23
papendorf@kwm-rechtsanwaelte.de
www.kwm-rechtsanwaelte.de