Haftungsfalle Datenschutz - Bestandsaufnahme und Handlungsempfehlungen*

Unter dem 30.03.2011 haben KZBV und BZÄK in einem gemeinsamen Leitfaden Vorgaben zu „Datenschutz- und Datensicherheit für die Zahnarztpraxis-EDV“ veröffentlicht. Nicht nur der Verfasser, sondern zahlreiche weitere, mit der Beratung der Zahnärzteschaft befasste Kollegen und Kolleginnen haben daraufhin Anrufe von besorgten Zahnärzten erhalten. Grund genug, die Problematik des Datenschutzes in der Zahnarztpraxis in nachfolgendem Beitrag näher zu beleuchten. Neben den im gemeinsamen Papier der Bundesverbände aus hiesiger Sicht zu kurz gekommenen datenschutzrechtlichen Grundlagen, sind dabei vor allem ergänzende und z.T. klarstellendende Aussagen zu den Themenkomplexen der elektronischen Behandlungsdokumentation, des Outsourcings sowie der Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten geboten. Neben den theoretischen Grundlagen werden dabei auch Handlungsoptionen des Zahnarztes konkret aufgezeigt und bewertet.

I. Was ist Datenschutz*recht*?

Pionier der Datenschutzgesetzgebung in Deutschland war nicht – wie man vielleicht vermuten könnte – der Bund, sondern das Land Hessen, welches die Problematik des Datenschutzes als erstes Land zum Gegenstand der Gesetzgebung machte. Bereits 1969 hatte das Land Hessen den Auftrag gegeben, "das Modell einer besonderen, neutralen und unabhängigen Instanz zu entwerfen", um den Risiken von "Herrschaftsbegünstigung und einseitiger Informationsmacht" durch die elektronische Datenverarbeitung zu begegnen. Ende 1970 wurde dann in Hessen das sogar weltweit erste Datenschutzgesetz verabschiedet. Auch auf Bundesebene nahmen die Beratungen zur Schaffung eines Datenschutzgesetzes erst Anfang der *1970er* Jahre an Fahrt auf. Der Bund hat seine Datenschutzgesetzgebung lange und intensiv vorbereitet. Nach einer fast sechs Jahre dauernden Diskussion über die Notwendigkeit und den Inhalt einer gesetzlichen Regelung des Umgangs mit personenbezogenen Daten wurde dann am 12. November 1976 das Bundesdatenschutzgesetzt (BDSG) im Bundestag beschlossen. Zum 1. Januar 1979 ist es vollumfänglich in Kraft getreten. Zu dieser Zeit hatten bereits die meisten Bundesländer Datenschutzgesetze erlassen. Zu Sinn und Zweck des Gesetzes führt der Gesetzesentwurf der Bundesregierung vom 25. Mai 1973 aus:

---

* Von *Dr. Robert Kazemi,* Rechtsanwalt und Partner der Kazemi & Lennartz Rechtsanwälte PartG.

"Die Information erlangt in unserer technisierten Welt immer größere Bedeutung. Die technischen Hilfsmittel für die schnelle und umfassende Bereitstellung sind vorhanden und werden ständig fortentwickelt. Das Informationsbedürfnis in allen Bereichen macht indessen auch vor der Privatsphäre des Menschen nicht Halt, in jeder denkbarer Eigenschaft werden Informationen von ihm und über ihn benötigt. Der dem Bürger vom Grundgesetz gewährte Freiheitsraum, die unantastbare Sphäre privater Lebensgestaltung drohen enger zu werden. Diese sich anbahnende Entwicklung gilt es durch ein umfassendes Datenschutzgesetz zu steuern. Das geltende Recht, das von einer Zersplitterung in viele, aufeinander nicht abgestimmte einschlägige Einzelvorschriften gekennzeichnet ist, geht den Anforderungen eines modernen Datenschutzes nicht gerecht."

Das Bundesdatenschutzgesetz strebt vor diesem Hintergrund einen grundlegenden Schutz der Privatsphäre vor Missbräuchen bei der Datenverarbeitung an. Dies geschieht im Prinzip in der Weise, dass der Umgang mit Daten in den besonders schutzbedürftigen Phasen der Datenverarbeitung, nämlich dem Speichern, Weitergeben, Verändern und Löschen, geregelt wird. Außerdem werden dem Betroffenen Abwehrechte gewährt, im Wesentlichen das Recht auf Auskunft über die zu seiner Person gespeicherten Daten, ein Anspruch auf Berichtigung unzutreffend gespeicherter Daten und unter bestimmten Voraussetzungen ein Anspruch auf Sperrung bzw. Löschung ihn betreffender Daten.

Im Kern geht es also nicht um einen absoluten (Geheimnis-)Schutz der persönlichen Daten, sondern darum, den Umgang mit Daten und der hieraus zu gewinnenden Erkenntnisse in einem Sinne auszugestalten, der es nicht gestattet, Daten ohne Wissen und Wollen des Betroffenen zu speichern und/oder zu verwenden. Datenschutz ist damit – um es auf eine einfache Formel zu bringen – der Schutz der Persönlichkeitssphäre beim Umgang mit Daten.

2. Wen verpflichtet und wen schützt das Datenschutzrecht – Zentrale Begriffe

Normadressat des Datenschutzrechts ist die "verantwortliche Stelle", denn sie ist es, die die sich aus dem Datenschutzrecht ergebenden Verpflichtungen zu beachten hat. Nach der in § 3 Abs. 7 BDSG enthaltenen Definition ist "verantwortliche Stelle" jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Derjenige, um dessen Belange es im Datenschutzrecht vorrangig geht, ist der Betroffene. Der Begriff des Betroffenen ist in § 3 Abs. 1 BDSG ebenfalls legal definiert als bestimmte oder bestimmbare natürliche Person, woraus zugleich folgt, dass juristische Personen (GmbH, Aktiengesellschaft etc.) durch das Datenschutzrecht grundsätzlich nicht geschützt werden.

Zweck des Datenschutzrechts ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Abs. 1 BDSG). Der Begriff des personenbezogenen Datums ist damit in der datenschutzrechtlichen Diskussion von entscheidender Bedeutung. § 3 Abs. 1 BDSG definiert diesen als "Einzelangabe über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Damit sind grundsätzlich alle Informationen, die mit einer natürlichen Person in Verbindung gebracht werden können, als schutzwürdige Daten anzusehen. Hierunter fallen beispielsweise: Name, Geburtsdatum, Geschlecht, Anschrift (auch Telefonnummer und E-Mail-Adresse), Familienstand, Staatsangehörigkeit, äußeres Erscheinungsbild, Ausbildungsstand, Beruf, Gesundheitszustand, biometrische Daten (DNA) wie auch Ton- und Bildaufnahmen einschließlich Röntgenbildern.

Aufgrund der Vorgaben in § 3 Abs. 9 BDSG unterliegen sensitive Daten als "besondere Arten personenbezogener Daten" einer besonderen Handhabung. Als besondere Arten personenbezogener Daten definiert das Gesetz Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Die Sensibilität derartiger Einzelangaben über eine natürliche Person rechtfertigt grundsätzlich den besonderen Schutz dieser Daten vor unbefugtem Umgang unabhängig davon, wie sensitiv das betreffende Datum in seiner konkreten Ausprägung tatsächlich oder nach allgemeiner Auffassung in der Gesellschaft ist. Der Zahnarzt kommt im Rahmen seiner Behandlungstätigkeit insbesondere mit derartigen besonderen personenbezogenen Daten in Kontakt.

3. Rechtsquellen des Datenschutzrechts

Neben dem BDSG als zentrales Gesetz betreffend die Erhebung, Verarbeitung und Nutzung personenbezogener Daten existieren eine Vielzahl sektorspezifischer Spezialregelungen, die in ihrem Anwendungsbereich dem BDSG vorgehen. Hier ist neben dem Telemediengesetz (TMG), welches – vereinfacht gesagt – die Datenerhebung über elektronische Medien,

vornehmlich das Internet, regelt, vor allem an die Bestimmungen zum Sozialdatenschutz in den besonderen Teilen des Sozialgesetzbuches SGB (vor im SGB V) zu denken.

Die Entstehungs- und Entwicklungsgeschichte der hier verankerten bereichsspezifischen Normen belegt, dass der Gesetzgeber dem Sozialdatenschutz in der gesetzlichen Krankenversicherung hohe Bedeutung beimisst. Er sah sich verpflichtet, spezialgesetzliche Grundlagen für die Verarbeitung personenbezogener Daten im Zusammenhang mit Leistungsabrechnungen im System der GKV zu schaffen (vgl. §§ 284 ff SGB V), um dem Recht der Versicherten auf informationelle Selbstbestimmung im Rahmen der krankenversicherungsrechtlichen Datenverwendung und -verarbeitung Rechnung zu tragen. Dies vor allem deshalb, weil die Verarbeitung personenbezogener Gesundheitsdaten, die zu einem guten Teil der ärztlichen Schweigepflicht unterliegen, von besonderer Sensibilität ist.

Auch das Bundessozialgericht (BSG) hat in seiner Rechtsprechung wiederholt die Bedeutung der ärztlichen Schweigepflicht wie auch des Sozialdatenschutzes hervorgehoben. In den entschiedenen Fällen ging es um die - aus Sicht des Leistungserbringers - umgekehrte Fallkonstellation, nämlich um die Frage, ob eine Offenbarung von Patientendaten gegenüber den Institutionen des Vertragsarztrechts unter Berufung auf die ärztliche Schweigepflicht verweigert werden darf. So wurde erst durch eine Entscheidung des BSG im Jahre 1983 geklärt, dass eine Offenbarung von Patientengeheimnissen durch Leistungserbringer (dort zur Durchführung des Gutachterverfahrens nach dem Bundesmantelvertrag-Zahnärzte) zulässig ist, wenn dies zur Sicherstellung der Funktionsfähigkeit der vertragsärztlichen Versorgung erforderlich ist und eine gesetzliche Offenbarungspflicht besteht. In einer grundlegenden Entscheidung aus dem Jahr 1985 hat das BSG klargestellt, dass der gesetzlichen Regelung über die vertragsärztliche Versorgung der Versicherten die Befugnis zugrunde liegt, Patientendaten innerhalb des vertragsärztlichen Versorgungssystems insoweit zu offenbaren, als ärztliche Behandlung in Anspruch genommen wird und die an der Leistungserbringung Beteiligten für ihren Leistungsbeitrag auf die Information angewiesen sind. Es hat zugleich aber darauf hingewiesen, dass die daraus herzuleitende Offenbarungsbefugnis des Arztes beschränkt ist, und betont, dass das besondere Vertrauensverhältnis zwischen Patient und Arzt eine wesentliche Bedingung für eine erfolgreiche Behandlung darstellt. Dem Vertragsarztrecht kann daher die Beschränkung entnommen werden, Patientendaten innerhalb der Zuständigkeiten des vertragsärztlichen Versorgungssystems und auch in diesem engen Bereich lediglich insoweit mitzuteilen, als dies die Leistungserbringung erforderlich macht.

Auch der Bundesgerichtshof (BGH) hat im Zusammenhang mit der Abtretung von Honoraransprüchen an privatärztliche Verrechnungsstellen hervorgehoben, dass die häufig über intimste Dinge Auskunft gebenden Abrechnungsunterlagen einen besonders wirksamen Schutz verdienen. Dieser ist grundsätzlich nur gewährleistet, wenn die Honorarabrechnung in einem von vornherein und sicher für den Patienten überschaubaren Bereich erfolgt; dies sei aber in der Regel allein die Praxis des Arztes einschließlich der für die Abrechnung zuständigen Mitarbeiter.

Aus alledem wird die besondere Bedeutung des Sozialdatenschutzrechtes und die Notwendigkeit vertiefter Kenntnisse auch dieses Bereiches deutlich. Der Vertragszahnarzt sollte sich daher auch mit dieser Materie befassen.

4. Anwendbarkeit des Datenschutzrechts im Rahmen des zahnärztlichen Wirkens

Im Rahmen der privatzahnärztlichen Behandlung verbleibt es hingegen bei der Anwendung des BDSG. Die hier normierten Pflichten werden jedoch durch die speziellen Anforderungen des zahnärztlichen Berufsrechts und ihrer (strafgesetzlichen und –prozessualen) Absicherung verschärf, ggf. sogar aufgehoben.

Der Zahnarzt übt gemäß §§ 1, 2 der Musterberufsordnung für Zahnärzte (MBOZ) einen freien und unabhängigen Beruf aus. Dabei unterliegt er strafbewehrten berufsrechtlichen Geheimhaltungspflichten. § 7 MBOZ verpflichtet den Zahnarzt, über alles, was ihm in seiner Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren. Diese berufsrechtliche Verschwiegenheitsverpflichtung wird strafrechtlich durch die Norm des § 203 StGB flankiert, der die unbefugte Offenbarung fremder Geheimnisse durch besonders benannte Geheimnisträger unter Strafandrohung stellt. In § 203 Abs. 1 Nr. 1 BDSG wird der Zahnarzt als Adressat und möglicher Täter der vorbenannten Strafnorm bezeichnet. Dem in § 203 Abs. 1 Satz 1 Genannten stehen gemäß § 203 Abs. 3 StGB ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.

Korrespondierend mit der Verpflichtung des Zahnarztes, ihm anvertraute Geheimnisse keinem Dritten zu offenbaren, finden sich die in der Strafprozessordnung normierten Zeugnisverweigerungsrechte der § 53 Abs. 1 Nr. 3 StPO (für den Zahnarzt) und des § 53a Abs. 1 StPO (für seine Gehilfen und die Personen, die zur Vorbereitung auf den Beruf an seiner berufsmäßigen Tätigkeit teilnehmen). Die strafrechtlichen Bestimmungen schützen –

wie das Berufsrecht - vornehmlich das Vertrauensverhältnis zwischen Arzt und Patient. Es geht hier also nicht primär um den Datenschutz, d.h. den Schutz vor der Verwendung personenbezogener Daten im Lichte des Grundrechts auf informationelle Selbstbestimmung, sondern vorwiegend um den Schutz des zwischen Arzt und Patient bestehenden und von Verfassungs wegen garantierten Vertrauensverhältnisses.

Festzuhalten bleibt damit, dass weder das Strafrecht noch das zahnärztliche Berufsrecht originäres Datenschutzrecht darstellen. Die hier normierten Verpflichtungen an den Zahnarzt strahlen allenfalls auf das Datenschutzrecht aus.

Wegen dieser Ausstrahlwirkung der zahnärztlichen Berufspflichten auf das Datenschutzrecht und mit Blick auf die Vorschrift des § 1 Abs. 3 BDSG, wird vertreten, dass die Bestimmungen des BDSG gegenüber der in § 7 MBOZ enthaltenen Verschwiegenheitsverpflichtungen subsidiär seien. Alle Daten, die unter das Arztgeheimnis fallen, wären dementsprechend dem Anwendungsbereich des BDSG vollständig entzogen. Übrig blieben lediglich Daten ohne jeglichen Bezug zur eigentlichen zahnärztlichen Tätigkeit, wie dies bei Daten des Büropersonales und beispielsweise bei Lieferantendaten der Fall sein mag.

Die herrschende Meinung vertritt hingegen die Ansicht, dass die Anwendung des BDSG durch die Regelung des zahnärztlichen Berufsrechts grundsätzlich nicht verdrängt, sondern lediglich ergänzt wird. Die Subsidiarität tritt bezogen auf den Zahnarzt nur dann ein, wenn die spezielleren Regelungen des zahnärztlichen Berufsrechtes inhaltlich einen Reglungsgegenstand des BDSG umfassen. Werden bestimmte Sachverhalte durch die spezifischen Regelungen hingegen nicht erfasst, so bleibt das BDSG anwendbar.

Da die Zahnärzteschaft in heutiger Zeit fast vollständig automatisiert Daten verarbeitet, sind auch Zahnärzte damit grundsätzlich potenzielle Adressaten der datenschutzrechtlichen Normen des BDSG. Die Anwendung des Datenschutzrechtes ist daher nur dort begrenzt, wo das Berufsgeheimnis vorgeht. Im Einzelnen ergibt sich damit nachfolgendes Bild:

a. Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten?

Nach § 4f BDSG besteht für nicht-öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten und hierzu mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Aus dem zahnärztlichen Berufsrecht und dem hier geschützten Vertrauensverhältnis zwischen Zahnarzt und Patient

herzuleiten, diese Verpflichtung träfe die Zahnärzteschaft grundsätzlich nicht, erscheint fernliegend. Vielmehr sind auch Zahnärzte, die die Voraussetzung des § 4f BDSG erfüllen, grundsätzlich dazu verpflichtet, einen betrieblichen Datenschutzbeauftragten zu bestellen, der die zahnärztliche Datenverarbeitung im Hinblick auf die dem Berufsgeheimnis unterliegenden Daten zu beaufsichtigen hat (ausführlich hierzu im Teil 2 unter 1.).

b. Auskunfts- und Benachrichtigungspflichten gegenüber dem Patienten?

Gemäß § 34 Abs. 1 BDSG hat die verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten, den Empfängern, an die Daten weitergegeben werden, und den Zweck der Datenspeicherung zu erteilen. Nach § 33 Abs. 1 BDSG ist der Betroffene für den Fall, dass erstmals personenbezogene Daten für eigene Zwecke ohne seine Kenntnis gespeichert werden, von der Speicherung zu benachrichtigen (§ 33 Abs. 1 BDSG). Die Benachrichtigungspflicht besteht nicht, wenn der Betroffene auf andere Weise Kenntnis von der Speicherung seiner personenbezogenen Daten erlangt oder die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

Auch die vorgenannten Auskunfts- und Benachrichtigungspflichten gegenüber dem Patienten verstoßen nicht gegen die Geheimhaltungspflichten des zahnärztlichen Berufsrechts. §§ 33, 34 BDSG sind mithin im Arzt-Patienten-Verhältnis grundsätzlich anwendbar. Da die Speicherung der personenbezogenen Patientendaten einer gesetzlichen Aufbewahrungspflicht folgt (§ 12 Abs. 1 MBOZ – 10 Jahre), muss der Patient über die erstmalige Erhebung der Daten jedoch nicht gesondert informiert werden (§ 33 Abs. 2 BDSG). Hinzu kommt, dass Patienten bei der Begründung von Behandlungsverhältnissen in aller Regel freiwillig eine Vielzahl personenbezogener Daten über sich preisgeben und eine Datenerhebung ohne Kenntnis des Betroffenen grundsätzlich nicht stattfindet.

c. Auskunftspflichten gegenüber Datenschutzkontrollinstanzen?

Nach § 38 BDSG wird die Ausführung des BDSG durch die Aufsichtsbehörden der Länder kontrolliert. Die der Kontrolle unterliegenden privaten Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde gemäß § 38 Abs. 3 BDSG auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft solcher Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der ZPO bezeichneten

Angehörigen der Gefahr strafrechtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

Vor allem die Datenschutzbeauftragten der Länder sind der Ansicht, die Auskunftspflicht des § 38 BDSG treffe auch den Zahnarzt. Dies ergebe sich aus einer Zusammenschau des § 38 Abs. 4 Satz 3 BDSG i. V. m. § 24 Abs. 6 BDSG und § 2 Nr. 2 BDSG. Den Datenschutzkontrollinstanzen stünden daher umfassende Auskunfts- und Besichtigungsansprüche zu.

Meines Erachtens greift diese Auffassung jedoch zu kurz. In diesem Zusammenhang greift die Vorschrift des § 1 Abs. 3 Satz 2 BDSG zum Schutz der beruflichen Geheimhaltungspflichten des Zahnarztes ein. Diese verbietet es, Daten, die Berufsgeheimnissen unterliegen, gegenüber den Datenschutzkontrollinstanzen aufzudecken. Sie verbietet den Datenschutzkontrollinstanzen auch, diese Daten etwa durch andere Kontrollmaßnahmen zu erhalten. Ohne einen solchen Schutz bliebe das Berufsgeheimnis nicht unberührt. Eine Auskunftsverpflichtung des Zahnarztes gegenüber den Datenschutzbehörden besteht daher nicht. Bei Auskunftspflichten verdrängt § 1 Abs. 3 Satz 2 BDSG vielmehr die in § 38 Abs. 3 BDSG grundsätzlich enthaltene Auskunftsverpflichtung. Über der zahnärztlichen Schweigepflicht unterliegende Daten dürfen Zahnärzte und ihre Mitarbeiter den Datenschutzkontrollinstanzen keine Auskunft erteilen. Sie können sich insoweit auf das ihnen nach dem zahnärztlichen Berufsrecht zustehende Verschwiegenheitsrecht zurückziehen.

Auch die in § 38 Abs. 4 BDSG vorgesehenen sonstigen Betretungs-, Prüfungs- und Einsichtsrechte der Datenschutzkontrollinstanzen bestehen gegenüber Zahnärzten grundsätzlich nicht. Auch insoweit geht die zahnärztliche Verschwiegenheitsverpflichtung den Befugnissen der Datenschutzkontrollbehörden nach § 38 Abs. 4 BDSG vor. Nur so kann das Vertrauensverhältnis zwischen Zahnarzt und Patient wirksam geschützt werden.

d. Vorrang sozialrechtlicher Spezialgesetze

Soweit es um die Verarbeitung von Daten im Rahmen der gesetzlichen Krankenversicherung geht, finden die Bestimmungen des BDSG ebenfalls keine Anwendung. Somit kommt insbesondere ein Rückgriff auf die nach den allgemeinen Regelungen des BDSG für eine Datenverarbeitung in privaten Unternehmen (§§ 4 Abs. 1, 4a i.V.m. § 28 Abs. 6 BDSG) mögliche Einwilligung als Ermächtigungsgrundlage für eine Datenverarbeitung und Datenweitergabe nicht in Betracht. Zwar sieht auch § 67d i.V.m. § 67b Abs. 1 SGB X eine

Einwilligung als Ermächtigungsgrundlage vor, doch findet diese Regelung nur auf die in § 35 Abs. 1 SGB I genannten Stellen Anwendung, zu denen der Zahnarzt gerade nicht gehört.

e. Zusammenfassung

Finden die spezialgesetzlichen Regelungen keine Anwendung und widerspricht auch die zahnärztliche Verschwiegenheitspflicht einer Anwendung des BDSG nicht, finden die Vorschriften des Gesetzes mithin auch auf den Zahnarzt und die im Rahmen seiner Tätigkeit stattfindenden Datenerhebungs- und –verarbeitungsvorgänge Anwendung. Dementsprechend ist die Erhebung, Verarbeitung und Nutzung personenbezogener Patientendaten gemäß § 4 BDSG grundsätzlich nur zulässig, soweit das BDSG oder andere Rechtsvorschriften dies erlauben oder der Betroffene in die vorbeschriebenen Vorgänge eingewilligt hat. Gemäß § 4 Abs. 2 BDSG gilt der sogenannte Grundsatz der Direkterhebung, nach dem personenbezogene Daten grundsätzlich unmittelbar beim Betroffenen zu erheben sind. Die hiermit verbundene Transparenz der Datenerhebung soll sicherstellen, dass die Daten nur mit Kenntnis und Mitwirkung des Betroffenen beschafft werden und erfüllt damit zugleich die Anforderungen des Bundesverfassungsgerichts an die Wahrung des Rechts auf informationelle Selbstbestimmung. Die (Patienten-)Datenerhebung bedarf daher, dies ist zunächst festzuhalten, entweder der gesetzlichen Erlaubnis oder der Einwilligung des Betroffenen.

5. Datenschutzgrundsätze

Für die Verwendung besonderer Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG sieht § 28 Abs. 7 BDSG besondere Regelungen vor. Dessen Zielrichtung ist es, alle gesundheitsbezogenen Dienstleistungen einzubeziehen. § 28 Abs. 7 Satz 1 BDSG nennt abschließend die Zwecke, zu denen eine Erhebung von Daten **ohne Einwilligung** des Betroffenen (Patienten) erlaubt ist. Im Einzelnen sind dies:

- Gesundheitsvorsorge
- Medizinische Diagnostik
- Gesundheitsversorgung
- Behandlung
- Verwaltung von Gesundheitsdiensten

Zum Bereich der Verwaltung von Gesundheitsdiensten sind das Abrechnungswesen und die Buchhaltung zu zählen. Der Bezug von Daten zum Gesundheitsbereich führt für sich

gesehen aber noch keine Erlaubnis zur Verwendung der Daten herbei, denn das Gesetz verlangt zudem ausdrücklich die Erforderlichkeit der Datenerhebung. Ist eine solche nicht gegeben, bedarf es generell der Zustimmung des betroffenen Patienten.
Unzulässig ist dementsprechend beispielsweise eine Weitergabe sensitiver Daten an Anbieter von Dokumentationsdienstleistungen, zum Beispiel zwecks Mikroverfilmung von Patientendaten aus einer Zahnarztpraxis. Nicht zulässig ist auch die einwilligungslose Übermittlung von Daten an (gewerbliche) Verrechnungsstellen oder Inkassobüros.

a. Datenverarbeitung nur durch Personen, die einer Geheimhaltungspflicht unterliegen

Eine Verarbeitung der Daten ist auch nur dann zulässig, wenn die Daten in allen Phasen der Verarbeitung durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Erfasst hiervon ist der in § 203 Abs. 1 Nr. 1 StGB genannte Personenkreis einschließlich des Hilfspersonals, für welches eine entsprechende Geheimhaltungspflicht gilt. Insoweit geht die herrschende Meinung in der juristischen Literatur davon aus, dass lediglich „berufsmäßig tätige Gehilfen“, die organisatorisch in die Praxis eingegliedert sein müssen, von der Privilegierung des § 203 Abs. 3 Satz 2 StGB profitieren. Die betreffenden Personen müssen danach aus Sicht des Zahnarztes, in seinen organisatorischen und weisungsgebundenen internen Bereich der vertrauensbegründenden Sonderbeziehung einbezogen sein, was externe Dienstleister, die etwa ein Outsourcing von Schreib-, Telefon- oder EDV-Diensten anbieten, aufgrund ihrer „Selbstständigkeit“ grundsätzlich nicht sein könnten. Externe Dienstleister seinen dementsprechend **keine berufsmäßig tätigen Gehilfen** des Zahnarztes, sodass eine Auftragsdurchführung durch diese auf Grundlage des § 203 StGB strafbar sein könne.

Andere gehen davon aus, dass auch externer Dienstleister als Gehilfen des Zahnarztes im Sinne von § 203 Abs. 3 Satz 2 StGB eingeordnet werden können. Hierfür sei jedoch erforderlich, dass der Zahnarzt die externen Dienstleister in einer Art und Weise in seine Verschwiegenheitsverpflichtung einbindet, die die Wahrung der durch § 203 StGB geschützten Patienteninteressen rechtfertigt. Dies könne beispielsweise durch eine Verschwiegenheitsverpflichtung geschehen, die auch allen Mitarbeitern des externen Dienstleisters auferlegt wird. Des Weiteren empfehle sich die Vereinbarung von Vertragsstrafen für den Fall der Zuwiderhandlung, welche ebenfalls dazu geeignet sind, Zuwiderhandlungen im Vorfeld auszuschließen bzw. die Gefahr solcher Zuwiderhandlungen im Vorfeld erheblich zu minimieren.

Weder die Rechtsprechung noch der Gesetzgeber haben sich bislang abschließend dazu geäußert, welcher der vorgenannten Auffassungen gefolgt werden soll. Im Interesse der Zahnärzteschaft bleibt zu hoffen, dass die Meinung den Vorzug erlangt, die ein weites Verständnis des Gehilfenbegriffes favorisiert. Als Begründung für diese Ansicht kann herangezogen werden, dass auch andere Gesetzesvorschriften, die Gehilfentätigkeiten regeln (so etwa § 278 BGB. § 53a stopp, § 11 BDSG) eine organisatorische Einbindung in die Praxis des Zahnarztes oder ein festes Dienst- oder Arbeitsverhältnis nicht voraussetzen. Maßgeblich für die Gehilfeneigenschaft des Dienstleisters ist hier allein, ob der Zahnarzt über eine hinreichende Steuerungsmacht im Sinne einer effektiven Kontrollmöglichkeit verfügt. Solange eine solche in der konkreten Ausgestaltung des Vertragsverhältnisses zwischen dem Zahnarzt und dem Dienstleister verankert ist, sehe ich eine Strafbarkeit nicht als gegeben an. Um dies sicherzustellen, sind Verträge mit externen Dienstleistern jedoch sorgsam auszuhandeln und vor allem auf die Kontrollmöglichkeiten zu achten (ausführlich hierzu im Teil 2 unter 3.).

b. Verwendung nur im Rahmen des Erhebungszwecks

Die Erhebung, Verarbeitung und/oder Nutzung personenbezogener Daten ist zudem grundsätzlich nur im Rahmen zuvor festzulegender Zwecke ohne Einwilligung des Betroffenen zulässig (§ 28 Abs. 8 Satz 1 BDSG). Dementsprechend ist z. B. die "anlasslose" Sammlung von personenbezogenen Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken unzulässig. Die Zweckbindung haftet den personenbezogenen Daten grundsätzlich dauerhaft an. Sie kann nur in bestimmten, eng begrenzten Ausnahmefällen durchbrochen werden.

Dies bereitet insbesondere immer dann Probleme, wenn Patientendaten an Dritte übermittelt werden sollen. Eine solche Übermittlung ist nur zulässig, wenn sie entweder durch eine gesetzliche Vorschrift, durch die Einwilligung des Patienten oder aber durch einen besonderen Rechtfertigungsgrund legitimiert ist. Dies gilt grundsätzlich auch bei der Übermittlung von Daten an andere Ärzte und/oder Zahnärzte.

Gesetzliche Übermittlungsbefugnisse und -pflichten finden sich insbesondere

- für die Übermittlung personenbezogener Daten an die Kassenzahnärztlichen Vereinigungen, beispielsweise zu Zwecken der Abrechnungs- oder Wirtschaftlichkeitsprüfung

- für die Übermittlung an die Krankenkasse, beispielsweise wenn es um die Übermittlung von Arbeitsunfähigkeitsbescheinigung geht
- für die Übermittlung nach dem Infektionsschutzgesetz (§§ 6 ff. IfSG)
- für die Übermittlung nach der Röntgenverordnung (§ 17 a RöV, § 28 Abs. 8 RöV).

Soweit keine gesetzliche Übermittlungsbefugnis vorliegt, bedarf es entweder der konkreten Einwilligung des Patienten oder einer sonstigen Rechtfertigung. Eine solche kann ausnahmsweise gegeben sein, wenn eine nicht anders abwendbare Gefahr für ein höherwertiges Rechtsgut, wie Leben, Gesundheit und Freiheit, abgewehrt werden soll oder der Zahnarzt im Rahmen der Wahrnehmung berechtigter Interessen, etwa bei strafrechtlichen Ermittlungsverfahren, gegen ihn selbst oder aber auch im Rahmen der Durchsetzung zivilrechtlicher Ansprüche gegen den Patienten darauf angewiesen ist, die ihm anvertrauten Patientendaten zu offenbaren.

Ein solcher Fall liegt jedenfalls dann nicht vor, wenn die Weitergabe der personenbezogenen Daten beispielsweise im Rahmen einer Praxisveräußerung stattfindet. Zwar kann ähnlich wie im Falle des Verkaufs eines Einzelhandelsunternehmens auch hier ein berechtigtes Interesse des Praxisübernehmers am – zumeist essentiellen – Patientenstamm nicht von der Hand gewiesen werden. Dennoch scheitert eine einwilligungslose Übermittlung hier grundsätzlich an den schutzwürdigen Betroffeneninteressen.

Der Bundesgerichtshof verlangt vor der (offenen) Weitergabe der Patientenunterlagen an einen Nachfolger (Übernehmer) daher die Zustimmung der Patienten in „eindeutiger und unmissverständlicher Weise“. Eine Bestimmung in einem entsprechenden Kaufvertrag, die den Veräußerer auch ohne Einwilligung der betroffenen Patienten verpflichtet, die Patientenkartei zu übergeben, verletzt das informationelle Selbstbestimmungsrecht der Patienten und die ärztliche Schweigepflicht; sie ist wegen Verstoßes gegen ein gesetzliches Verbot nichtig (§ 134 BGB). Auch die Annahme eines stillschweigenden oder durch schlüssiges Handeln erklärten Einverständnisses des Patienten in die Weitergabe seiner Unterlagen scheidet im Regelfall aus.

Hier hat sich in der Vergangenheit das so genannte „Zwei-Schrank-Modell“ etabliert. Grundlage dieses Modells ist ein doppeltes Karteischranksystem. Der Veräußerer übergibt dem Käufer den verschlossenen Karteikartenschrank mit den gesamten Behandlungsunterlagen, an denen der Veräußerer zunächst das Eigentum behält. Die Parteien vereinbaren im Kaufvertrag eine Verwahrungsklausel, in der sich der Käufer

verpflichtet, die Alt-Kartei für den Veräußerer zu verwahren und auf diese oder Teile von ihr nur dann Zugriff zu nehmen, wenn der Patient ihrer Nutzung durch den Käufer schriftlich zugestimmt hat oder wenn er durch sein Erscheinen zur Behandlung in der Praxis schlüssig zum Ausdruck bringt, dass er eine Nutzung der Alt-Kartei durch den Käufer wünscht und billigt. Erst wenn der Patient auf diese Weise sein Einverständnis zur Nutzung der Alt-Kartei erklärt, darf diese entnommen werden und in die laufende Patientenkartei der erworbenen Praxis eingebracht werden.

c. Anforderungen an die Einwilligung des Patienten

Mit Ausnahme der vorstehend beschriebenen Fallgruppen, in denen die Datenerhebung und -verwendung auch ohne Einwilligung des Patienten möglich und zulässig ist, bedürfen die sonstigen Erhebungs-, Speicherungs- und Verwendungsvorgänge gemäß § 4 BDSG stets der Einwilligung des betroffenen Patienten.

aa. Allgemeine Anforderungen, § 4a BDSG

Die Vorschrift des § 4a BDSG regelt verbindlich und unabdingbar, welchen Voraussetzungen eine Einwilligung in die Verarbeitung und Nutzung personenbezogener Daten genügen muss, wenn sie wirksam sein soll.

Nach § 4 Abs. 1 BDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit der Betroffene eingewilligt hat. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und der Betroffene auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hingewiesen wird.

Die Einwilligung bedarf grundsätzlich der Schriftform (§ 126 BGB), soweit nicht wegen besonderer Umstände eine andere Form angemessen ist.

bb. Freiwilligkeit

Mit Blick auf den Schutzzweck des Datenschutzrechtes, der auf die Wahrung der informationellen Selbstbestimmung des Betroffenen gerichtet ist, normiert § 4a BDSG, dass die Einwilligung nur wirksam ist, soweit sie auf der freien Entscheidung des Betroffenen beruht. Dieses Erfordernis der Freiwilligkeit stellt eines der wesentlichen Anforderungen an

eine wirksame Einwilligungserklärung dar. Nach den verfassungsrechtlichen Grundlagen steht dem Einzelnen grundsätzlich frei, selbst zu entscheiden, welchen Dritten er seine Daten offenbaren möchte.

Der Betroffene muss tatsächlich die Möglichkeit haben, selbst darüber zu befinden, ob und unter welchen Bedingungen die sich auf seine Person beziehenden Angaben benutzt werden dürfen. Daran fehlt es, wenn sich der Betroffene in einer Situation befindet, die ihm keine Möglichkeit zu einer eigenen, selbstständigen Stellungnahme lässt, die Einwilligung also nur dazu dienen würde, einen scheinbar von ihm gebilligten Vorgang rechtlich abzusichern. Insbesondere gilt dies in Fällen, in denen Leistungen auf dem Spiel stehen, die für den Betroffenen unentbehrlich sind.

Im Arzt-Patienten-Verhältnis sieht das Bundessozialgericht (BSG) in diesem Zusammenhang insbesondere Probleme, soweit es sich um Einwilligungserklärungen handelt, die im Rahmen medizinischer Notfallbehandlungen eingeholt werden. Hier wird sich der Patient häufig in einer Situation befinden, in der er in seiner freien Willensbildung deutlich eingeschränkt ist, was nach Ansicht des BSG dafür spricht, eine Datennutzung kraft Einwilligung nicht pauschal, sondern nur in ausdrücklich normierten Fällen zuzulassen. Patienten sind - insbesondere in Notfallsituationen - zumindest subjektiv oftmals nicht frei in ihrer Entscheidung für oder gegen die Einwilligung. Sie können den berechtigten Eindruck haben, im Interesse einer schnellen und guten (Notfall-) Versorgung die ihnen von dem Leistungserbringer vorgelegte Erklärung unterschreiben zu sollen.

Auch in unterversorgten ländlichen Gebieten oder bei der Inanspruchnahme besonders spezialisierter Fachärzte dürfte eine freie Entscheidungsmöglichkeit allenfalls theoretischer Natur sein. Vor einer solchen zumindest subjektiven Zwangslage sind die Patienten geschützt, solange keine gesetzliche Regelung existiert, welche die Datenweitergabe durch Leistungserbringer im Krankenversicherungsrecht grundsätzlich zulässt - und den Patienten damit zumutet, einem Wunsch des Leistungserbringers nach Einwilligung in eine Datenweitergabe ggf. ausdrücklich zu widersprechen.

cc. Konkrete Zweckbindung/Bestimmtheit

Für die Wirksamkeit der datenschutzrechtlichen Einwilligung ist es weiterhin notwendig, dass die datenerhebende Stelle den Betroffenen **vor Erteilung der Einwilligung** über die beabsichtigte Verwendung informiert, denn der Betroffene kann einer Verarbeitung seiner personenbezogenen Daten nur insoweit rechtswirksam zustimmen, als Klarheit über Zweck

und Reichweite seiner Einwilligung besteht; d. h. er muss wissen, worüber er eine Erklärung abgibt.

Der Zahnarzt hat den Patienten daher umfassend und rechtzeitig über Zweck, Art und Umfang der geplanten Datenverarbeitung zu informieren. Darunter fallen auch Informationen über die Rechte der Betroffenen, Löschfristen sowie Informationen zur verantwortlichen Stelle und deren technisch-organisatorischen Maßnahmen zur Regelung der zugriffsberechtigten Personen, wobei diese nach herrschender Meinung nicht namentlich genannt werden müssen, sondern es ausreichend sein soll, diese mit einer Funktionsbeschreibung (z. B. Administrator) anzugeben. Des Weiteren ist der Betroffene auch über mögliche Empfänger der Daten zu informieren.

Allgemein gehaltene Erklärungen, wie „der Patient stimmt der Verarbeitung seiner personenbezogenen Daten, welche im Rahmen der Vertragsabwicklung anfallen, zu“ oder „der Patient ist mit jeder Form der Datenverarbeitung einverstanden“, sind keinesfalls ausreichend und müssen wesentlich detaillierter formuliert werden.

Rechtsprechung und Literatur verlangen insoweit eine „informierte Einwilligung“. Die Einwilligungserklärung muss daher so bestimmt sein, dass die Art der personenbezogenen Daten und der Zweck der Erhebung oder Verwendung sowie im Falle der Übermittlung etwaige Empfänger hinreichend genau benannt werden. Weiterhin hat die Einwilligung „für den konkreten Fall und in Kenntnis der Sachlage“ zu erfolgen.

Für eine informierte Einwilligungserklärung sind daher nachfolgende Fragen zu beantworten:

- Welche Daten werden vom Betroffenen erhoben?
- Welche Angaben sind zwingend erforderlich und warum, welche Angaben sind hingegen lediglich optional?
- Werden die Daten neben dem eigentlichen Verwendungszweck auch für Marketing- und Werbezwecke (beispielsweise Praxisnewsletter) verwendet?
- Werden die Daten noch zu weiteren Zwecken verwendet und wenn ja, zu welchen?
- Kann der Verwendung dazu widersprochen werden?
- Werden die Daten an Dritte weitergegeben?
- Wie erfolgt die Datenverwendung innerhalb der Zahnarztpraxis?
- Wer greift innerhalb der Zahnarztpraxis auf die Daten tatsächlich zu?

dd. Formerfordernisse

Die datenschutzrechtliche Einwilligung bedarf schließlich grundsätzlich der Schriftform. Dies soll verhindern, dass der Betroffene vorschnell und ohne nähere Überlegungen über die Folgen seiner Einwilligungserklärung in die Verarbeitung seiner personenbezogenen Daten einwilligt.

Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung zudem gemäß § 4a Abs. 1 Satz 4 BDSG im äußeren Erscheinungsbild aus den anderen Erklärungen hervorzuheben. Vor allem bei der Erhebung von Daten auf Formularen soll so verhindert werden, dass der Betroffene die Einwilligung übersieht. Daher ist die gesetzlich vorgeschriebene Hervorhebung Wirksamkeitsvoraussetzung.

Die Einwilligungserklärung ist mithin abgesetzt von den anderen Erklärungen an deutlich sichtbarer Stelle aufzunehmen. Sie darf nicht an versteckter Stelle mitten in einem vorformulierten Text untergebracht werden. In der Praxis kann der Hervorhebungspflicht beispielsweise dadurch genügt werden, dass die datenschutzrechtliche Einwilligungsklausel fett gedruckt und entsprechend überschrieben („Datenschutzrechtliche Einwilligungsklausel“) vom übrigen Text abgesetzt wird. Nicht ausreichend soll nach Aufsicht der Bayerischen Aufsichtsbehörde in ihrem Tätigkeitsbericht von 2006 beispielsweise die Formulierung „Datenschutzklausel“, „Hinweis“ bzw. „Erklärung zum Datenschutz“ sein. Denn das Wort „Einwilligung“ bzw. „Einwilligungserklärung“ oder „Einwilligungsklausel“ müsse bereits in der Überschrift vorkommen, um der Hervorhebungspflicht zu genügen.

Des Weiteren empfiehlt es sich, die datenschutzrechtliche Einwilligung – soll sie mit anderen Erklärungen zusammen abgegeben werden – auch optisch vom sonstigen Text abzuheben. Dies kann z. B. durch eine Hervorhebung, etwa durch Sperrschrift, Unterstreichung, Einrahmung, Verwendung anderer Schrifttypen, durch Trennlinien oder ähnliches geschehen.

Haftungsfalle Datenschutz - Bestandsaufnahme und Handlungsempfehlungen für die Zahnarztpraxis, Teil 2

In Teil 1 dieses Beitrages wurden die wesentlichen Grundlagen des Datenschutzrechtes aufgezeigt, die durch den Zahnarzt beim Umgang mit Patientendaten zu beachten sind. Nachfolgend sollen diese Grundlagen auf einzelne Fallkonstellationen angewendet werden. Dabei konzentriert sich der Beitrag auf die Themenkomplexe, Datenschutzbeauftragter, Online-Bestellungen von Praxismaterial, elektronische Behandlungsdokumentation und das Outsourcing in der Zahnarztpraxis.

1. Bestellung eines Datenschutzbeauftragten

Im ersten Teil dieses Beitrages habe ich dargestellt, dass auch den Zahnarzt grundsätzlich eine Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten treffen kann. Diese grundsätzliche Verpflichtung trifft jedoch, insoweit ist dem Leitfaden „Vorgaben zu Datenschutz- und Datensicherheit für die Zahnarztpraxis-EDV“ der KZBV und der BZÄK ausdrücklich zu widersprechen, nicht bereits deshalb jeden Zahnarzt, weil diese im Rahmen ihrer Behandlungstätigkeit zwangsläufig besondere Arten personenbezogener Daten verarbeiten. Im Leitfaden der KZBV und der BZÄK heißt es insoweit missverständlich:

> *„Soweit in der Zahnarztpraxis eine elektronische Patientenakte ohne Einwilligung der Patienten geführt wird, ist unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen ein Beauftragter für den Datenschutz zu bestellen (§ 4f Abs. 1 Satz 6 BDSG). Allerdings ist das Speichern von Patientendaten mittels EDV im Rahmen der Zweckbestimmung des Patientenvertrags zulässig. Einer gesonderten Einwilligung der Patienten bedarf es in diesen Fällen nicht.“*

Diese Ausführungen werden durch das BDSG nicht untermauert, insbesondere kann eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragen nicht aus 4f Abs. 1 Satz 6 BDSG hergeleitet werden. Die knappen Ausführungen im Leitfaden sind daher entsprechend zu ergänzen.

a. Funktion des Datenschutzbeauftragten

Hierzu scheint es zunächst erforderlich, die Person und die Aufgaben des betrieblichen Datenschutzbeauftragten näher zu beleuchten, um dann auf diejenigen Fallkonstellationen

einzugehen, in denen eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten tatsächlich eingreift.

Die Aufgabe und Tätigkeit eines Datenschutzbeauftragten wird in den §§ 4f und 4g BDSG geregelt. Der Beauftragte für Datenschutz wirkt nach der gesetzgeberischen Intention auf die Einhaltung des BDSG und anderer Datenschutz-Gesetze hin (SGB V, TMG, TKG, etc.). Die zentrale Aufgabe ist dabei die Kontrolle und Überwachung der ordnungsgemäßen Datenverarbeitung.

In dieser Funktion soll der Datenschutzbeauftragte auf die Einhaltung der Datenschutzbestimmungen hinwirken, indem er betriebsinterne Datenschutzvorgänge prüft und beurteilt, ob die zur Sicherung des Rechtes auf informationelle Selbstbestimmung getroffenen Maßnahmen ausreichen oder Verbesserungsmöglichkeiten bestehen. Dabei hat er neben der Zulässigkeit der Datenverarbeitung, auch die getroffenen Schutzmechanismen, insbesondere die EDV und das Netzwerk zu bewerten, was gleichsam ein gewisses technisches Verständnis erfordert. Die Prüfung und Überwachung hat in regelmäßigen Abständen nach eigenem Ermessen zu erfolgen. Sobald neue Verfahren in einem Betrieb eingeführt werden, ist der Datenschutzbeauftragte hierüber vorab zu informieren und in die Entscheidungsfindung einzubeziehen. Ein wesentliches Augenmerk liegt dabei darauf, dass ausschließlich Befugte eine nur auf den Zweck beschränkte Verarbeitung vornehmen können und dass der Eigentümer der Daten sein Selbstbestimmungsrecht auf Auskunft, Korrektur, Sperrung und Löschung wahrnehmen kann. Schließlich obliegt dem betrieblichen Datenschutzbeauftragten auch die Schulung der Mitarbeiter, um diese für die Belange des Datenschutzes zu sensibilisieren. Im Rahmen dieser Schulungstätigkeit hat der Datenschutzbeauftragte vor allem über mögliche Änderungen im Bereich der Datenschutzgesetzgebung zu informieren, soweit diese vom Unternehmen zu beachten sind. Den Datenschutzbeauftragten trifft damit gleichsam eine Verpflichtung, sich durch geeignete Fortbildungen und das Studium aktueller Gesetzgebungsvorhaben auf dem Laufenden zu halten.

Da der Datenschutzbeauftragte in seinem Funktionsbereich nicht immer populäre Entscheidungen trifft, sieht das Gesetz seine Weisungsfreiheit und Unabhängig von Vorgesetzten in seinen Funktionsbereichen vor. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden und ist direkt der Geschäftsleitung unterstellt. Seit der Novellierung des BDSG im Jahre 2009 ist der Datenschutzbeauftragte zudem mit einem verbesserten Kündigungsschutz ausgestattet (§ 4f Abs. 3 BDSG) und kann, solange er seine Funktion innehat, lediglich außerordentlich gekündigt werden. Dieser

Kündigungsschutz bleibt auch nach einer Abberufung als betrieblicher Datenschutzbeauftragter für ein weiteres Jahr nach der Beendigung der Bestellung bestehen.

Die Bestellung eines internen Datenschutzbeauftragten hat in der Regel für einen gewissen Zeitraum zu erfolgen, um sicherzustellen, dass er seine Tätigkeit im angemessenen Umfang ausführen kann. Je nach Bundesland werden dabei Zeiträume zwischen 3 und 5 Jahren als angemessen angesehen.

b. Allgemeine Anforderungen an den betrieblichen Datenschutzbeauftragen

Gerade in kleineren Betrieben (wie der Zahnarztpraxis), die sonst keinen verschärften Kündigungsvorschriften unterliegen, verleitet der gesetzlich angeordnete Kündigungsschutz oft dazu, Familienangehörige als Datenschutzbeauftragte einzusetzen, um sich die Freiheit der Personalgestaltung auch in Zukunft zu belassen. Dieser Gedanke ist vorschnell und sollte in aller Regel gleich wieder verworfen werden.

Zum Datenschutzbeauftragten darf nämlich nur bestellt werden, wer die notwendige Fachkunde und Zuverlässigkeit besitzt. Ende vergangenen Jahres hat der sog. Düsseldorfer Kreis hohe Mindestanforderungen zur erforderlichen Fachkunde und den Rahmenbedingungen für betriebliche Datenschutzbeauftragte beschlossen (abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Mindestanforderungen_an_Datenschutzbeauftragte/Mindestanforderungen_an_DSB_nach_4f_II_und_III_BDSG.pdf). Der Düsseldorfer Kreis ist das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Die einzelnen auf Landesebene zuständigen Aufsichtsbehörden koordinieren hier ihr Vorgehen und setzen dessen Beschlüsse in aller Regel konsequent um. Die hier formulierten Anforderungen der Aufsichtsbehörden sollten daher genau beachten, da andernfalls Geldbußen nach § 43 Abs. 1 Nr. 2 BDSG von bis zu 50.000 Euro drohen.

Unabhängig von der jeweiligen Branche und Größe des Unternehmens muss jeder Datenschutzbeauftragte über erhebliches Wissen im Datenschutzrecht verfügen. Dies umfasst unter anderem Grundkenntnisse zu den verfassungsrechtlich garantierten Persönlichkeitsrechten der von Datenverarbeitungen Betroffenen und der Mitarbeiter des Unternehmens. Zudem erfordert die Bestellung zum Datenschutzbeauftragten umfassende Kenntnisse der für das Unternehmen – die Praxis – einschlägigen Regelungen des BDSG und der Spezialgesetze. Hierzu ist das Unternehmen verpflichtet (§ 4f Abs. 3 Satz 7 BDSG,

§ 4f Abs. 2 BDSG), dem betrieblichen Datenschutzbeauftragten für die Erhaltung seiner Fachkunde die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

Die erforderliche Zuverlässigkeit erfordert, dass kein Interessenkonflikt bei der Wahrnehmung der Funktion besteht. Ein solcher besteht vor allem bei allen Personen, die ein eigenes Interesse am Unternehmen (etwa wegen Beteiligung an seinem Vermögen wie z. B. Teilhaber oder Gesellschafter) oder Leitungsfunktion haben. Geschäftsführer oder der Abteilungsleiter, vor allem der Personal- oder der IT-Abteilung, scheiden deshalb regelmäßig aus. Auch andere Personen außerhalb des Betriebes können ausscheiden, wie beispielsweise der Firmenanwalt oder Familienangehörige.

c. Auswahl des Datenschutzbeauftragten

Wegen vorgenannter Anforderungen an die Person des betrieblichen Datenschutzbeauftragten und des Umstandes, dass die Aufsichtsbehörden die Fachkunde des Datenschutzbeauftragten prüfen, sich nachweisen lassen und in berechtigten Fällen auch die unwirksame Bestellung feststellen oder den Datenschutzbeauftragten sogar von seiner Bestellung entheben können, bereitet seine Bestellung oftmals "praktische Schwierigkeiten". Die ehemalige Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Bettina Sokol, formulierte dies in ihrem 17. Datenschutzbericht wie folgt:

> *"Grundsätzlich ist die Möglichkeit für die Bestellung externer Beauftragter [...] oft eine praktikable Lösung, da sie häufig selbst nicht über Personal verfügen, das die für Datenschutzbeauftragte erforderliche fachliche Eignung hat. Hierfür wurde die Möglichkeit zur Bestellung eines externen Datenschutzbeauftragten geschaffen, welche mittlerweile auch durch die Berufsbezeichnungen "Fachkraft für Datenschutz und Datenschutzbeauftragter" klar definiert wurde."*

Jeder Zahnarzt, den eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten trifft, sollte daher darüber nachdenken, ob es nicht sinnvoller erscheint, einen externen Datenschutzbeauftragten zu bestellen. Fachkräfte für Datenschutz sind in aller Regel durch entsprechende Zertifizierungen, beispielsweise des TÜV, der IHK oder der DEKRA, ausgewiesen und bieten ihre Dienstleistungen am Markt an. Ein externer Datenschutzbeauftragter kann aufgrund von Erweiterungen des StGB (§ 203 Abs. 2a StGB) auch für Geheimnisträger, wie Zahnärzte, tätig werden, da ihm ein entsprechendes Recht

zur Aussageverweigerung zukommt und auch das strafprozessuale Beschlagnahmeverbot auf diesen ausgeweitet wurde.

Der mit einem externen Datenschutzbeauftragten zu schließende Dienstvertrag muss so ausgestaltet sein, dass eine unabhängige Erfüllung der gesetzlichen Aufgaben gewährleistet wird. Dies soll durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet werden. Der Düsseldorfer Kreis empfiehlt grundsätzlich eine Vertragslaufzeit von mindestens vier Jahren, bei Erstverträgen wird wegen der Notwendigkeit der Überprüfung der Eignung grundsätzlich eine Vertragslaufzeit von ein bis zwei Jahren empfohlen. Bei Bestellung eines externen Datenschutzbeauftragten müssen Unternehmen eine bedarfsgerechte Leistungserbringung sicherstellen. Auch externe Datenschutzbeauftragte müssen ihre Leistungen daher in angemessenem Umfang in der beauftragenden verantwortlichen Stelle selbst erbringen. Hierfür sollen Zahnarzt und externer Datenschutzbeauftragter ein angemessenes Zeitbudget konkret vereinbaren und vertraglich festgelegen.

Die Kosten der Beauftragung eines befähigten externen Datenschutzbeauftragten belaufen sich auf Beträge zwischen 3.000,00 und 10.000,00 € im Jahr und differieren stark danach, welche Fachkenntnisse hier im Einzelnen vorhanden sind.

Wer einen innerbetrieblichen (angestellten) Datenschutzbeauftragten bestellen möchte, hat für seine fachliche Qualifikation und fortlaufende Weiterbildung Sorge zu tragen. Die hier auflaufenden Kosten können daher erheblich sein.

d. Wen trifft die Verpflichtung zu Bestellung eines Datenschutzbeauftragen?

Anders als im Leitfaden der KZBV und der BZÄK formuliert, trifft die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten hingegen **nicht jeden Zahnarzt**, der in seiner Praxis eine elektronische Patientendokumentation vorhält. Eine solche Verpflichtung sieht das BDSG nicht vor.

Zunächst gilt vielmehr § 4f S. 2 und 3 BDSG, der nicht-öffentlichen Stellen, in denen mehr als neuen Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten auferlegt. Eine automatisierte Verarbeitung liegt vor, wenn die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen erfolgt (§ 3 Abs. 2 BDSG). Eine Datenverarbeitungsanlage ist

eine Einrichtung, die Daten nach vorgegebenen Programmen und Verfahren verarbeitet. In der Regel sind damit Computer im weitesten Sinne gemeint, auf denen personenbezogene Daten gespeichert und/oder bearbeitet werden. Zuzugestehen ist dem Leitfaden damit, dass Zahnärzte, die in Ihrer Praxis eine elektronische Patientendatenverwaltung (elektronische Karteikarte) verwenden, automatisierte Datenverarbeitungsvorgänge vornehmen. Sie sind damit grundsätzlich Adressaten der in § 4f normierten Verpflichtungen.

Die Pflicht gilt, sobald **mind. 10 Personen regelmäßig** mit der automatisierten Verarbeitung beschäftigt sind. Hierunter fallen nicht nur Vollzeitkräfte, sondern auch freie Mitarbeiter, Auszubildende, Leiharbeiter, Praktikanten und Volontäre. **Nur kurzeitige Beschäftigte sind nicht zu berücksichtigen** (bspw. Urlaubsvertretungen). Sobald innerhalb einer Zahnarztpraxis damit ständig mehr als 10 Personen, einschließlich des zahnärztlichen Personals und des Praxisinhabers, Zugriff auf die elektronische Patientendatenverwaltung haben, hat die Praxis einen betrieblichen Datenschutzbeauftragten zu bestellen. In den Fällen, in denen keine elektronische Patientenakte geführt wird, greift diese Verpflichtung erst, wenn mindestens 20 Personen innerhalb der Zahnarztpraxis beschäftigt werden (§ 4f Abs. 1 S. 3 BDSG).

Des Weiteren sieht § 4f BDSG grundsätzlich eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten vor, soweit besondere personenbezogene Daten im Sinne des § 3 Abs. 9 BDSG automatisiert verarbeitet werden. Sicherlich, der Zahnarzt verarbeitet mit Patientendaten stets derartige besondere personenbezogene Daten. Dennoch gilt die Verpflichtung zur Bestellung eines Datenschutzbeauftragten auch in diesen Fällen nur grundsätzlich und gerade nicht generell. Dies ist bedingt durch den in § 4f Abs. 1 S. 6 BDSG normierten Hinweis darauf, dass nur dann eine Verpflichtung besteht, wenn im Rahmen der Datenverarbeitung eine sog. Vorabkontrolle im Sinne des § 4d Abs. 5 BDSG zu erfolgen hat. Dies jedoch ist nicht bereits dann der Fall, wenn besondere personenbezogene Daten automatisiert verarbeitet werden.

Vielmehr trifft die Verpflichtung zur Durchführung einer Vorabkontrolle und die damit einhergehende Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten nur denjenigen, der die Datenverarbeitung dieser besonderen Daten weder aufgrund einer gesetzlichen Verpflichtung, noch im Rahmen der Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen vornimmt.

Beide alternativ genannten Ausnahmefälle dürften im Rahmen der Datenerhebung und –verarbeitung durch den Zahnarzt jedoch regelmäßig gegeben sein.

Bereits seit 01.01.2008 sind Zahnärzte per Gesetz verpflichtet, ihre Leistungen auf elektronischem Weg abzurechnen. Deshalb verarbeiten die KZVen ausschließlich digitale Abrechnungen weiter, d.h., die an der vertragszahnärztlichen Versorgung teilnehmenden Zahnärzte **müssen** die Aufstellung ihrer medizinischen Leistungen elektronisch einreichen und mithin personenbezogene Patientendaten elektronisch verarbeiten (§ 295 SGB V).

Des Weiteren wird sich die Zulässigkeit der (einwilligungslosen) elektronischen Patientendokumentation bereits aus dem Wesen des Behandlungsvertrages und mithin aus einem rechtsgeschäftlichen Schuldverhältnis ergeben. Wie in Teil 1 diesen Beitrages bereits dargelegt, normiert § 28 Abs. 7 Satz 1 BDSG, dass die Erhebung besonderer personenbezogener Daten **ohne Einwilligung** des Betroffenen (Patienten) erlaubt ist, soweit diese zum Zwecke der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung, der Behandlung und/oder der Verwaltung von Gesundheitsdiensten erforderlich ist, wobei zum Bereich der Verwaltung von Gesundheitsdiensten auch das Abrechnungswesen und die Buchhaltung zu zählen sind. Die Patientendokumentation dient mithin der Durchführung der eigentlichen Behandlungsleistung und mithin dem Behandlungsvertrag als solchem. Soweit es nicht um besondere Arten personenbezogener Daten geht, ergibt sich die Berechtigung zur Erhebung, Speicherung, Verarbeitung und Nutzung der personenbezogenen Daten aus § 28 Abs. 1 Satz Nr. 1 BDSG.

Genau in diesen Fällen sieht das BDSG eine Verpflichtung zur Vorabkontrolle gerade nicht vor. Ist eine Verpflichtung zur Vorabkontrolle jedoch nicht gegeben, besteht auch eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten aus § 4f Abs. 1 S. 6 BDSG nicht.

Insoweit begründet allein die Tatsache, dass besondere Arten personenbezogener Daten automatisiert verarbeitet werden also keine generelle Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten.

Dies gilt soweit und solange die automatisiert erhobenen und verarbeiteten Daten allein zum Zweck der Durchführung der zahnärztlichen Behandlung verwendet werden.

In diesem Fall ist auch die Einholung der von KZBV und BZÄK formulierten Einwilligung in die Führung einer elektronischen Patientenkartei m.E. nicht erforderlich, wenn nicht sogar überflüssig.

In diesem Fall ist auch die automatisierte Verarbeitungen vor ihrer Inbetriebnahme nicht der zuständigen Aufsichtsbehörde zu melden (§ 4d Abs. 3 BDSG).

e. Pflichten des Datenschutzbeauftragen gegenüber Dritten

Ist der Zahnarzt nach Vorgenanntem zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet, was – wie gezeigt – in aller Regel nur dann der Fall sein wird, wenn er ständig mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Patientendaten betraut, treffen den Datenschutzbeauftragten sowie den Zahnarzt selbst eine Reihe von Verpflichtungen, deren Kenntnis insbesondere dann, wenn nicht auf einen externen Datenschutzbeauftragten zurückgegriffen wird, notwendig ist.

Nach § 4e BDSG muss jede private Stelle, die eine Meldepflicht nach § 4d BDSG trifft, den Umgang mit diesen Daten dokumentieren. Eine Meldepflicht besteht jedenfalls dann, wenn eine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten besteht. Für diese Dokumentation hat sich die Bezeichnung "Verfahrensverzeichnis" oder "Verfahrensübersicht" eingebürgert.

Gemäß § 4g Abs. 2 S. 1 BDSG ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 BDSG genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen (häufig bezeichnet als "internes Verfahrensverzeichnis").

Soweit im Unternehmen ein Datenschutzbeauftragter ernannt ist, hat dieser gemäß § 4g Abs. 2 S. 2 BDSG Teile dieses "internen Verfahrensverzeichnisses" (konkret die Angaben nach § 4e Satz 1 Nr. 1 bis 8 BDSG) auf Antrag jedermann in geeigneter Weise verfügbar zu machen. Man spricht insoweit häufig vom "öffentlichen Verfahrensverzeichnis". Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle (dem Zahnarzt) zu diesem Zweck eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Hierbei handelt es sich um Angaben über:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Wird das Verfahrensverzeichnis nicht oder nicht ordnungsgemäß geführt, ist mit einem Einschreiten der Aufsichtsbehörden zu rechnen, die häufig von Dritten informiert werden, wenn ein Unternehmen auf Anfrage kein Verfahrensverzeichnis vorlegen kann. Die Aufsichtsbehörden haben ausweislich des § 38 Abs. 4 BDSG einen Anspruch auf Einsicht des Verfahrensverzeichnisses. Liegt kein ordnungsgemäßes Verfahrensverzeichnis vor kann dies auch die Verhängung eines Zwangsgeldes zur Folge haben, um die Erstellung eines Verzeichnisses zu veranlassen.

2. „Onlinebestellungen“ von Praxismaterial

Im Steuerrecht besteht nach § 147 AO eine eigene Aufbewahrungspflicht für steuerrelevante Belege. Diese gilt für alle Buchführungs- und Aufzeichnungspflichtigen im Sinne der §§ 140, 141 AO, also auch für Zahnärzte als Freiberufler. Ein steuerrelevanter Beleg liegt – ein-fach gesagt – immer dann vor, wenn die Belege, Buchungen oder Berechnungen die Steuerlast mindern können.

Geschäftsprozesse werden zunehmend durch E-Mail-Kommunikation abgewickelt. E-Mail-Dokumente sind nach den Grundsätzen des Steuerrechtes zu archivieren, soweit sie steuer-relevante Belege enthalten. Nach § 147 Abs. 6 AO ist die Finanzbehörde berechtigt, im Rahmen einer Außenprüfung Einsicht in die gespeicherten Daten zu nehmen und das Datenverarbeitungssystem zur Prüfung dieser Unterlagen zu nutzen. Der Steuerpflichtige

muss die steuerlich relevante E-Mail-Kommunikation elektronisch archivieren und sicherstellen, dass die Dokumente während der Aufbewahrungsfrist maschinell ausgelesen werden können. E-Mail-Kommunikation mit steuerlich relevantem Inhalt muss damit während der gesamten gesetzlichen Aufbewahrungsfrist elektronisch archiviert werden. Auf diese elektronisch vorzuhaltenden steuerrelevanten Belege hat die Finanzverwaltung im Rahmen von Betriebsprüfungen weitgehende Zugriffsrechte, die sich auch auf die Datenverarbeitungssysteme erstrecken, die die steuerrelevanten Belege enthalten (§ 147 Abs. 6 Satz 1 AO). Bewahrt der Steuerpflichtige Belege elektronisch auf, so hat die Finanzverwaltung ein umfassendes Datenzugriffsrecht. Dies beinhaltet als erstes das Recht auf Lesbarmachung am Bildschirm und nicht etwa nur das Recht auf Ausdruck von digital gespeicherten Belegen. Die Finanzverwaltung und nicht der Steuerpflichtige soll entscheiden dürfen, welche Belege und Daten vorgelegt und überprüft werden.

Die vorgenannten Grundsätze können dann an Relevanz gewinnen, wenn – wie in vielen Zahnarztpraxen bereits üblich – Praxismaterial nicht nur per Telefax, sondern auch online bestellt wird. Gelangen Fakturierungen und sonstige steuerrelevante Rechnungen im Rahmen des Onlinebestellvorganges in digitaler Form (per E-Mail) in die Zahnarztpraxis, kann sich eine Konfliktlage zwischen der zahnärztlichen Verschwiegenheitsverpflichtung und dem Einsichtsrecht der Finanzbehörden „am Bildschirm“ ergeben. Dies kann insbesondere dann der Fall sein, wenn Bestellungen nicht über ein konkretes, nur für die Abwicklung von Materialbestellungen eingerichtetes Postfach, sondern vielmehr über das zentrale E-Mail-Postfach der Praxis erfolgen. In diesen Postfächern kann sich nämlich auch Kommunikation mit Patienten befinden, die unstreitig der Verschwiegenheitsverpflichtung unterliegt.

Nach nicht rechtskräftiger Auffassung des Finanzgerichtes Nürnberg ist die elektronische Betriebsprüfung auch bei einem Berufsgeheimnisträger grundsätzlich zulässig. Das Finanzgericht kommt zu dem Ergebnis, dass die Finanzverwaltung die elektronische Betriebsprüfung auch bei Berufsgeheimnisträgern durchführen dürfe (hier Steuerberater). Diese könnten sich gegenüber der Finanzverwaltung nicht darauf berufen, aus den vorzulegenden Daten könnten geschützte Mandantendaten ersichtlich sein. Nach Auffassung des FG Nürnberg ist es vielmehr Aufgabe des Berufsgeheimnisträgers, seine Datenbestände so zu organisieren, dass bei einer zulässigen Einsichtnahme in die steuerlich relevanten Datenbestände keine geschützten Bereiche tangiert werden. So sei der Datenzugriff nicht deshalb ermessenswidrig, weil bei dem Steuerpflichtigen eine Trennung zwischen ungeschützten und geschützten Daten nicht möglich sei. Nach den Grundsätzen ordnungsgemäßer Buchhaltung sei ein effizientes internes Kontrollsystem vorgeschrieben, nach dem sensible Informationen des Unternehmens gegen unberechtigte Kenntnisnahme

zu schützen und unberechtigte Veränderung durch wirksame Zugriffs- bzw. Zugangskontrollen zu unterbinden sind. Auch das BDSG verlange die Trennung der Daten nach den Verwendungszwecken und deren zweckgebundene Verarbeitung. Entsprechend diesen Vorgaben verfügten heute nahezu alle im Einsatz befindlichen Betriebssysteme und datenverarbeitungsgeschützten Buchführungssysteme über Möglichkeiten, den Zugriff auf die prüfungsrelevanten Bereiche im Sinne des § 147 Abs. 1 AO zu beschränken. Sollte ein Datenverarbeitungssystem eine Trennung der Daten nicht zulassen, könne dies nicht zur rechtlichen Unzulässigkeit des Datenzugriffes führen. Anderenfalls könnte derjenige, der eine nicht den allgemeinen Anforderungen entsprechende Software benutzt eine praktisch wirksame Außenprüfung verhindern. Dem Berufsgeheimnisträger ist nach Auffassung des FG Nürnberg jedenfalls durchaus möglich, bei der Erfassung der Geschäftsvorfälle und der Erstellung der Belege, die Trennung der verschwiegenheitspflichtigen Angaben von den steuer- und buchführungsrelevanten Daten herbeizuführen. Wenn er diesbezüglich „seine Hausaufgaben“ nicht gemacht habe, könne er hiermit eine zulässige Prüfungshandlung nicht blockieren.

Das vorgenannte Urteil beleuchtet das Spannungsverhältnis zwischen Betriebsprüfungen bei Berufsgeheimnisträgern und deren Pflicht zur Verschwiegenheit. Nach § 193 Abs. 1 Alt. 2 AO ist eine Außenprüfung zwar auch bei Berufsgeheimnisträgern möglich, dieser Grundsatz kollidiert aber mit der beruflichen Verschwiegenheitspflicht, bei Anwälten gemäß § 53a BRAO, § 2 BORA sowie den Auskunftsverweigerungsrechten nach § 102 Abs. 1 AO. Die daraus entstehende Grundsatzfrage, ob bei einem Berufsgeheimnisträger überhaupt eine Betriebsprüfung angeordnet werden kann oder ob seine Praxis nicht vielmehr „prüfungsfreie Zone“ bzw. „finanzamtsfreier Raum“ ist, hat der Bundesfinanzhof bereits verneint.

Mit Urteil vom 28. Oktober 2009 ging der Bundesfinanzhof sogar einen großen Schritt weiter und gab einen Rahmen vor, welche (Papier-)Unterlagen ein Berufsgeheimnisträger bei einer ihn betreffenden Betriebsprüfung wegen seiner Verschwiegenheitspflicht zurückbehalten muss. Danach darf der Berufsgeheimnisträger nur nicht patientenbezogene Unterlagen und diejenigen Unterlagen vorlegen, bei denen die Patienten auf eine Geheimhaltung verzichtet haben. Alle anderen Unterlagen müsse der Berufsgeheimnisträger schwärzen bzw. vollständig zurückbehalten.

Die Entscheidung des FG Nürnberg, gegen welche die Revision anhängig ist, geht nun noch einen Schritt weiter und befasst sich mit der Frage, inwieweit die Finanzverwaltung im Rahmen einer Außenprüfung bei einem Berufsgeheimnisträger auf Unterlagen, die mit Hilfe eines Datenverarbeitungssystems erstellt worden sind, zugreifen darf. Die Ausführungen des

FG Nürnberg hätten – für den Fall, dass der Bundesfinanzhof die Rechtsprechung bestätigt – dabei weitreichende Konsequenzen.

Um Schwierigkeiten, die sich aus dem vorbeschriebenen Spannungsverhältnis ergeben, zu vermeiden, empfiehlt sich daher entweder Zugriffsbeschränkungen auf die steuerlich relevanten Dokumente sicherzustellen, z. B. durch eindeutige Indexkriterien wie Buchungsdatum und Zugriffsbeschränkungen. Zudem ist zu beachten, dass sichergestellt werden muss, dass z. B. bei Personaldokumenten, die der Betriebsprüfer auch nicht versehentlich zu Gesicht bekommen darf, eine besondere Schutzvorkehrung eingerichtet wird.

Speziell in Bezug auf Bestellungen von Praxismaterial und die daraus resultierenden digitalen Rechnungsbelege, die die Finanzverwaltung grundsätzlich so einsehen kann, wie sie in die Praxis gelangt sind, empfiehlt es sich in jedem Fall eine Trennung der Bestellvorgänge von der Patientenpost vorzunehmen. Hier scheint aus meiner Sicht die Einrichtung eines eigenen E-Mail-Postfaches für Bestellungen (beispielsweise bestellungen@praxis-mustermann.de) sinnvoll und notwendig.

3. Outsourcing in der Zahnarztpraxis

Auch im Zahnarztleben hat das "Outsourcing" zwischenzeitlich an Bedeutung gewonnen. Virtual Offices, externe Schreibbüros, virtuelle Sekretariate etc. stoßen auch beim Zahnarzt mehr und mehr auf Interesse. Externe Abrechnungs- und EDV-Dienstleister werden in zahlreichen Praxen eingesetzt. Wer als Zahnarzt externe Dienstleister durch das Outsourcing mit Patientendaten in Berührung bringt, etwa im Wege der Auslagerung von elektronischen Aktenbeständen oder weil der externe Dienstleister als Telefonzentrale des Zahnarztes fungiert, vollzieht datenschutzrechtlich relevante Vorgänge in Bezug auf die in seiner Praxis befindlichen personenbezogenen Daten.

Eine Einwilligung der Betroffenen, d. h. der Patienten, liegt dabei regelmäßig nicht vor. Oftmals ist dem Patienten die Art und Weise der Büroorganisation des Zahnarztes viel-mehr gar nicht bekannt. Wer in der Zahnarztpraxis von Zahnarzt Dr. Mustermann anruft, geht (jedenfalls noch) davon aus, dass er auch in der Zahnarztpraxis Dr. Mustermann landet und nicht etwa in einer Telefonzentrale, die durch ein selbstständiges Unternehmen betrieben wird. Der Anrufer wird daher in der Regel davon ausgehen, dass die ihm am Telefon entgegentretenden Personen in die betriebliche Organisation des Zahnarztes im Rahmen

bestehender Beschäftigungsverhältnisse und damit im Rahmen der diesen Beschäftigten zustehenden Verschwiegenheitsverpflichtungen und Rechte einbezogen sind. Tatsächlich handelt es sich hier jedoch um externe Dienstleister, die von den Privilegierungen des zahnärztlichen Berufsstandes gerade nicht profitieren.

Besondere spezialgesetzliche Tatbestände, die eine Übermittlung der Patientendaten an Dritte und deren Speicherung und Nutzung gestatten würden, existieren nicht. Zulässig ist der Datenumgang mit Patientendaten daher nur dann, wenn das Verhältnis zwischen dem Zahnarzt und dem externen Dienstleister als sog. Auftragsdatenverarbeitung im Sinne von § 11 BDSG ausgestaltet ist.

Eine Auftragsdatenverarbeitung liegt vor, wenn personenbezogene Daten durch eine andere verantwortliche Stelle im Auftrag erhoben, verarbeitet oder genutzt werden (§ 11 BDSG). Die andere Stelle muss dabei den Weisungen des Auftraggebers unterworfen sein und darf keine eigene Entscheidungsbefugnis darüber besitzen, wie sie mit den Daten umgeht (im Gegensatz zur sogenannten Funktionsübertragung). Der Auftragnehmer ist zudem sorgfältig auszuwählen, der Auftrag muss schriftlich erteilt werden und der Auftraggeber muss den Auftragnehmer umfassend kontrollieren können und seine Kontrollen schriftlich dokumentieren. Die einzelnen Mindestvertragsklauseln einer entsprechenden Auftragsdatenverarbeitungsvereinbarung können beispielsweise im Internet unter http://www.bitkom.org/files/documents/Mustervertragsanlage_zur_Auftragsdatenverarbeitung_v_3_0.pdf heruntergeladen werden.

Vergibt der Zahnarzt Aufträge an externe Dienstleister ohne eine solche oder im Rahmen einer unzureichenden Auftragsdatenverarbeitungsvereinbarung, stellt dies gleichzeitig eine Ordnungswidrigkeit dar, die gemäß § 43 Abs. 1 Nr. 2b BDSG mit Bußgeldern in Höhe von bis zu 50.000,00 Euro sanktioniert werden kann.

Verstöße des Dienstleisters bei der Auftragsdatenverarbeitung sind in der Regel (zivilrechtliche) Vertragsverletzungen, die nach den allgemeinen Regelungen zu Schadensersatz führen können. Es empfiehlt sich darüber hinaus, Verstöße des Dienstleisters mit einer entsprechenden Vertragsstrafe zu sanktionieren, um sicherzustellen, dass derartigen Verstößen entgegengewirkt wird. Eine Formulierung könnte etwa wie folgt ausgestaltet sein:

> *„Der Auftragnehmer verpflichtet sich bei Zuwiderhandlung gegen die normierten Verpflichtungen zu einer Vertragsstrafe, die ggf. der Höhe nach vor dem zuständigen Gericht zu überprüfen ist, von nicht unter 50.000,00 EUR pro nachgewiesenem Fall der Zuwiderhandlung unter Ausschluss des Fortsetzungszusammenhangs. Mit der Zahlung*

der Vertragsstrafe wird die Geltendmachung des Anspruchs auf Unterlassung oder eines darüber hinausgehenden Schadensersatzes bei entsprechendem Nachweis nicht ausgeschlossen. Die Vertragsstrafe wird auf einen möglichen Schadensersatz angerechnet."

Ob ein Verstoß gegen § 11 BDSG darüber hinaus über die Vorschriften der §§ 3, 4 Nr. 11 UWG auch wettbewerbsrechtlich geahndet werden kann, ist bislang noch nicht entschieden. Es spricht jedoch viel dafür, auch die Vorschrift des § 11 BDSG als Marktverhaltensregelung im Sinne des § 4 Nr. 11 UWG einzustufen, denn hier geht es nicht nur darum, Rechtssicherheit für Auftraggeber und Auftragnehmer zu schaffen, sondern auch Sicherheit für die Betroffenen zu erreichen. Es ist daher nicht ausgeschlossen, dass § 11 BDSG von Gerichten als Marktverhaltensregelung im Sinne des § 4 Nr. 11 BDSG eingestuft wird. In diesem Fall würden Verstöße gegen die Vorschriften zur Auftragsdatenverarbeitung gleichzeitig die Gefahr der wettbewerbsrechtlichen Inanspruchnahme nach sich ziehen.

Auch aus diesem Grunde erscheint es sinnvoll, einzurichtende oder bereits eingerichtete Auftragsdatenverarbeitungen auf ihre Rechtssicherheit und rechtliche Zulässigkeit hin zu über-prüfen.

4. Anforderungen an die elektronische Behandlungsdokumentation

Die Behandlungsdokumentation stellt einen wichtigen, rechtserheblichen Beleg im Rahmen der Rechtfertigung des ärztlichen Vorgehens dar.

Die klassische Karteikarte auf Papier hat dabei den Vorteil, dass sie eine Urkunde, genauer eine Privaturkunde, i.S.d. §§ 415 ff. ZPO darstellt und ihr damit eine Beweissicherungsfunktion zukommt. Dies bedeutet zwar nicht, dass der Inhalt der Urkunde als richtig angenommen wird, sie besitzt also keine materielle Beweiskraft. Vielmehr bleibt dies der richterlichen Beweiswürdigung vorbehalten. Meist wird aber, so zeigt es sich in der Praxis der Rechtsprechung, davon ausgegangen, dass die dokumentierten Handlungen auch tatsächlich in der Art wie beschrieben, vorgenommen wurden. Der Beweiswert ist damit höher anzusetzen, als es die vorherigen Ausführungen vermuten lassen. Der Einwand der Manipulationsmöglichkeit kann zudem dadurch entkräftet werden, dass allein durch die einfache Inaugenscheinnahme Veränderungen, wie Streichungen, Zufügungen oder Neuerrichtung der Akte, meist schon ohne weiteres wahrnehmbar sind. Bestimmte Indizien, wie die Benutzung nur eines einzigen Stiftes bei mehrmonatigen Aufzeichnungen, können dabei leicht zu einer Überführung der Manipulation führen. Auch gibt es heutzutage die Möglichkeit, das Alter von Aufzeichnungen durch einen Gutachter bestimmen zu lassen.

Diese Vorteile der Papierakte sind bei der elektronischen Akte schwerer zu verwirklichen. Elektronische Dokumente sind nachträglich einfach veränderbar ohne Spuren zu hinterlassen, sowohl in Bezug auf die Daten selbst, also den Inhalt, als auch bezüglich des Alters der Dokumente. Problematisch ist auch das Merkmal der Originalität bei eingescannten Objekten.

Allein die Datensicherung in regelmäßigen Abständen ist hierfür keinesfalls ausreichend. Die Gegenseite, also Patient oder Krankenversicherer, wird sich im Prozess sowohl bei Fragen der Begründung des Honoraranspruches als auch bei Haftungsfragen immer darauf berufen, dass die angeführte Dokumentation nachträglich erstellt oder geändert wurde, um die entscheidenden Punkte einzuführen oder zu löschen. Die Beweisfunktion wird damit vollständig in Frage gestellt.

Das OLG Koblenz hat einen solchen Fall gerade zu bescheiden. Dem Arzt liegt dabei lediglich eine nicht besonders gesicherte elektronische Behandlungsdokumentation vor. Das OLG zeigt dabei wohl die Tendenz, dies nicht als entlastendes Beweismittel anzuerkennen. Der Beweis seitens des Arztes muss daher anders erbracht werden, wobei fraglich ist, wie dies tatsächlich möglich sein soll.

Die einzig bisher erfolgte, rechtssichere Lösung, stellt das Verfahren mittels einer qualifiziert elektronischen Signatur mit qualifiziert elektronischen Zeitstempeln dar. Hierunter versteht man mit elektronischen Informationen verknüpfte Daten, mit denen der Unterzeichner / Signaturersteller identifiziert und die Integrität der signierten elektronischen Information überprüft werden kann.

Insoweit ist die Aussage im Leitfaden der KZBV und der BZÄK dahingehend, dass die zahnärztliche Dokumentation auch auf elektronischen Datenträgern „Urkundsqualität“ habe und „der Beweiswert einer elektronischen Behandlungsdokumentation nicht dadurch gemindert werde, dass ein Praxisverwaltungssystem verwendet wird, das nicht gegen nachträgliche Veränderbarkeit der gespeicherten Patientendaten gesichert ist“ (Leitfaden, S. 22) zumindest kritisch zu sehen (ausführlich zu dieser Problematik unter: http://www.ddn-online.net/uploads/smartsection/454_ddn_0609_kazemi.pdf).

Dr. Robert Kazemi
(Rechtsanwalt)