Rechtsgrundlagen und Hinweise für die Zahnarztpraxis – Datenschutz- und Datensicherheits-Leitfaden für die Zahnarztpraxis-EDV

BUNDESZAHNÄRZTEKAMMER

KZBV
Kassenzahnärztliche Bundesvereinigung

Inhalt

Direktzugriff zu den Inhalten per Klick

1.0 Vorwort

Daten zu individuellen medizinischen Diagnosen, Befunden und Therapien sind immer sensible Daten. Die Verpflichtung auf einen sorgsamen Umgang mit diesen Daten ist aus gutem Grund Teil der Persönlichkeitsrechte, die jeder Bürger genießt. Die ärztliche Schweigepflicht, deren Verletzung nach dem Strafgesetzbuch geahndet wird, ist eine tragende Säule der Einhaltung dieser Persönlichkeitsrechte.

Auch in Zahnarztpraxen werden persönliche Daten heute in der Regel elektronisch verarbeitet und gespeichert. Das erleichtert die Praxisabläufe, bringt aber zugleich neue Verpflichtungen für Zahnarzt und Praxisteam mit sich. Bei der Dokumentation des Behandlungsgeschehens müssen ab dem 25.05.2018 die Auflagen des neuen Bundesdatenschutzgesetzes (BDSG) und vor allem die zum Teil verschärften Vorgaben in der für alle EU-Mitgliedsstaaten unmittelbar geltenden EU-Datenschutzgrundverordnung (EU-DSGVO) beachtet werden. Daher wurde der Leitfaden umfassend überarbeitet.

Ab dem 25. Mai 2018 gilt in allen Mitgliedsstaaten der Europäischen Union die EU-DSGVO. Ziel der EU-DSGVO ist es, eine europaweite Vereinheitlichung des Datenschutzrechts zu erreichen, die Rechte der von der Datenverarbeitung betroffenen Personen zu stärken und die Verantwortlichen bei Datenschutzverstößen empfindlich zu treffen. Gleichzeitig hat der Bundesgesetzgeber das alte durch das neue BDSG mit dem Willen ersetzt, das Recht an die EU-DSGVO anzupassen. Landesdatenschutzrechtliche Bestimmungen sollten ebenfalls bis zum 25.05.2018 Anpassungen erfahren. Die Auslegung der EU-DSGVO einschließlich ihrer 173 Erwägungsgründe und des neuen BDSG werden zukünftig nicht nur die zahnärztlichen Selbstverwaltungen, sondern auch die Datenschutzbehörden und die Gerichte beschäftigen. Dabei werden den Leitlinien des Europäischen Datenschutzausschusses als Nachfolger der sogenannten Artikel-29-Datenschutzgruppe, dem unabhängigen Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes, wenn auch keine rechtsverbindliche so aber sicherlich eine präjudizierende Wirkung zukommen. Die Leitlinien sind im Internet jederzeit abruf- und einsehbar. Viele Regelungen sind in Deutschland auch aus dem alten Datenschutzrecht bekannt. Dennoch kann sicherlich davon ausgegangen werden, dass dem neuen Datenschutzrecht eine breitere Aufmerksamkeit zuteil werden wird.

Ergänzend zu den folgenden Ausführungen können auch die Ausführungen in den Kurzpapieren der Datenschutzkonferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder herangezogen werden. Diese sind beispielsweise auf der Internetseite des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) veröffentlicht.

Die Einführung der Telematikinfrastruktur mit ihren neuen Anwendungen und Komponenten in die Praxen wirft neue Fragen auf. Für viele Praxen ist die Anbindung an die Telematikinfrastruktur der Anlass, sich noch intensiver mit Datenschutz und Datensicherheit zu beschäftigen. Dem trägt die Überarbeitung dieses Leitfadens Rechnung, welche die neue Technik mit ihren Herausforderungen und Chancen berücksichtigt.

Berlin/Köln, April 2018

Dr. Karl-Georg Pochhammer
Stellv. Vorsitzender des Vorstandes der KZBV

Jürgen Herbert
Vorstandsmitglied der BZÄK/Referent für Telematik

2.0 Grundsätze beim Einsatz von EDV in der Zahnarztpraxis

Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen[1] (Art. 9 Abs. 2 EU-DSGVO i.V.m. § 22 BDSG bzw. Art. 6 EU-DSGVO). Der Zahnarzt darf also die EDV im Rahmen des Behandlungsvertrages mit dem Patienten einsetzen. Für andere Zwecke darf er personenbezogene Patientendaten nur mit Zustimmung des Patienten verarbeiten. Bei der elektronischen Datenverarbeitung müssen die Daten vor unbefugtem Zugriff Dritter geschützt werden. Dies gilt zum Beispiel auch für das Reinigungspersonal der Praxis. Für besondere Schutz- und Sicherungsmaßnahmen zählt das BDSG in einer Anlage zu § 9 Abs. 1 BDSG verschiedene technische und organisatorische Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit auf. Dazu gehören z. B. die Zutritts- und Zugangskontrolle oder auch die Weitergabe- und Eingabekontrolle. Explizit wird die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren genannt.

Ab dem 25. Mai 2018 findet die Verpflichtung zur Ergreifung von geeigneten technischen und organisatorischen Maßnahmen ihre Rechtsgrundlage in Art. 25 EU-DSGVO und Art. 9 Abs. 2 EU-DSGVO i.V.m. § 22 Abs. 2 BDSG.

Einen angemessenen Sicherheitsstandard bei der elektronischen Datenverarbeitung in der Zahnarztpraxis einzuführen und konsequent zu praktizieren ist angesichts der stetig steigenden Komplexität der Anwendungen (Praxissoftware) und der Vernetzung mit externen Anbietern bzw. Dienstleistern nicht immer einfach.

Dabei spielen sowohl finanzielle Aspekte als auch die große Auswahl an Produkten im Bereich der IT-Sicherheit eine entscheidende Rolle. Fast alle hochwertigen Programme und Betriebssysteme verfügen über Sicherheitsmechanismen. Wer diese nicht nutzt bzw. die entsprechenden Hinweise in den Handbüchern nicht liest, verzichtet auf wichtigen Schutz zum Nulltarif. Er setzt sich außerdem einem erhöhten Haftungsrisiko beispielsweise bei „Datenklau“ oder Datenverlust aus.

Dieses Kapitel gibt einen kurzen und pragmatischen Überblick über wichtige IT-Sicherheitsmaßnahmen. Weitergehende Informationen zum „IT-Grundschutz“ bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI, www.bsi.de)

2.1 Umgang mit Kennwörtern und Qualität von Kennwörtern

Sehr häufig sind Schutzmechanismen abhängig von Benutzer- bzw. Kennwortabfragen. Grundsätzlich sollten die eingesetzten Abrechnungsprogramme, aber auch andere sensible Programme, durch Kennwörter geschützt werden.

Die Neigung, ein einfaches Kennwort zu vergeben bzw. ein voreingestelltes Kennwort nicht zu ändern, ist bei vielen Anwendern ausgeprägt. Effektiver Schutz ist so nicht möglich. Kennwörter sollten nicht zu kurz bzw. nicht zu leicht zu erraten sein. Das Kennwort sollte bestimmten Qualitätsanforderungen genügen, damit es nicht manuell oder automatisch (z. B. durch Hacker-Software) erraten werden kann. Ein optimales Kennwort sollte länger als sieben Zeichen sein, nicht im Wörterbuch vorkommen und keine Namen oder Geburtsdaten enthalten. Es sollte aus Sonderzeichen wie $, ?, (, &, Ziffern und einem Wechsel von Groß- und Kleinbuchstaben gebildet werden.

Kennwörter sollten außerdem regelmäßig geändert werden, um das Risiko zu minimieren, dass ein viel-

[1] Aus Gründen der Gleichbehandlung wird darauf hingewiesen, dass sich alle männlichen Personenbezeichnungen in diesem Leitfaden auch auf Frauen beziehen. Analog beziehen sich weibliche Personenbezeichnungen auch auf Männer.

leicht doch ausgespähtes Kennwort verwendet werden kann. Verlässt ein Mitarbeiter, zum Beispiel wegen Kündigung, die Praxis, ist die Zugriffsberechtigung sofort zu löschen oder zu ändern. Nach mehreren Versuchen, mit einem falschen Passwort in das System zu gelangen, sollte die Software den Zugriff automatisch sperren. In großen Praxen bietet es sich an, die Zugriffsrechte je nach Aufgabe des Mitarbeiters auf die tatsächlich erforderlichen Daten zu beschränken. Auch ist zu prüfen, inwieweit einzelne Mitarbeiter nur zum Lesen der Daten, nicht aber auch zu ihrer Veränderung berechtigt werden sollten. Ist ein Kennwort Unbefugten bekannt oder besteht auch nur der Verdacht, ist es unverzüglich zu ändern. Wenn ein Kennwort notiert wird, muss es sicher aufbewahrt werden. Ein Zettel unter der Schreibtischunterlage ist sicher nicht der geeignete Aufbewahrungsort.

Der Hersteller des Praxisverwaltungssystems (PVS) sollte in diesem Zusammenhang zusichern, dass er keine versteckten Kennwörter (sog. Backdoors) zu Wartungszwecken in sein Produkt eingebaut hat.

2.2 Virenschutz

Eine zuverlässige Virenschutz-Software ist unverzichtbar, unabhängig davon, ob ein System an das Internet angeschlossen ist oder nicht. Allein der Datenaustausch mittels Datenträger (CD, USB-Stick u. a.) birgt immense Gefahren. Die Installation eines Virenschutzprogramms ist daher unbedingt erforderlich. Es muss einen „Echtzeitschutz“ bieten und immer auf dem neuesten Stand gehalten werden. Vor der Anschaffung eines Virenschutzprogramms sollten Informationen über dessen Aktualisierungsmöglichkeiten eingeholt werden. Die Aktualisierung von Virenschutzprogrammen erfolgt in der Regel online.

Zu beachten ist, dass selbst ein regelmäßig aktualisiertes Virenschutzprogramm keinen absoluten Schutz bietet, da stets neue Viren auftauchen können, die das Programm noch nicht erkennen oder beseitigen kann.

Ausdrücklich muss in diesem Zusammenhang auf die Gefahren hingewiesen werden, die auch von „ganz normalen“ Text-, Bild- oder Datendateien ausgehen können. Es gibt spezialisierte Schadprogramme, die Schwachstellen von Anwendungsprogrammen oder des Betriebssystems ausnutzen und schon beim einfachen Aufruf der entsprechenden Datei aktiv werden können.

2.3 Benutzerkonten - Administrationsrechte

Betriebssysteme und andere Programme können Anwender nach Benutzern und Administratoren unterscheiden. Ein Administrator besitzt in der Regel Zugriff auf alle Systemebenen und bietet damit im Zweifelsfall auch Viren oder anderen Schadprogrammen eine Eintrittspforte. Oft arbeiten Anwender wissentlich oder unwissentlich in der Rolle eines Administrators am Rechner.

Daher sollten neben dem Konto des Administrators Benutzerkonten eingerichtet werden, die lediglich eingeschränkte Rechte besitzen. Diese Nutzerkonten mit eingeschränkten Rechten reichen in der Regel völlig aus, um die tägliche Arbeit am Rechner durchführen zu können. Für Änderungen an der Systemkonfiguration bzw. die Installation von neuer Software steht das Administratorkonto mit vollen Privilegien jederzeit zur Verfügung. Die in den neuen Windows-Betriebssystemen (ab Vista aufwärts) vorhandene „Benutzerkontensteuerung“ sollte genutzt und nicht deaktiviert werden. Bei der Anschaffung neuer Systeme sollte daher darauf geachtet werden, dass das zu Grunde liegende Betriebssystem eine entsprechende Sicherheitsfunktion bietet.

Ist unklar oder unbekannt, wie Benutzerkonten einzurichten bzw. zu konfigurieren sind oder wie mit der Benutzerkontensteuerung umzugehen ist, kann ein IT-Dienstleister oder auch der Software-

hersteller des PVS als Berater hinzugezogen werden. Er hilft auch bei der Einrichtung eines Servers. Dabei sind ggf. besondere Sicherheitsmaßnahmen wie das sog. „Härten" (das Entfernen von nicht benötigten Systemdiensten bzw. Betriebssystemsoftware) erforderlich, um einen effektiven Schutz des Servers gewährleisten zu können.

2.4 Datensicherung / Back-Up

Die Praxis- und Abrechnungsdaten müssen regelmäßig gesichert werden. Zum einen sind Aufbewahrungsfristen zu beachten, zum anderen ist ein Verlust der Behandlungsdaten zu verhindern. Ein simpler Hardwaredefekt kann zum Verlust der Daten des gesamten Quartals oder auch aller Daten der Festplatte führen. Auch Einbruch und Diebstahl von Rechnern oder Feuer können den totalen Verlust der Daten zur Folge haben. Deshalb sollte regelmäßig eine Datensicherung unter Verwendung einer marktüblichen Backup-Software auf transportablen Speichermedien (Bänder, externe Festplatten, Flash-Speicher [USB-Sticks], CDs oder DVDs) durchgeführt werden. Diese Speichermedien müssen wie die Rechner selbst gegen den Zugriff Unbefugter (körperlich und durch Kennwörter) geschützt werden. Für die Sicherung der Daten ist ein Konzept unumgänglich, das u. a. festlegt, wie oft die Datensicherung durchzuführen ist. Als Faustregel gilt: Je mehr Daten sich in kurzer Zeit ändern, umso häufiger ist eine Datensicherung notwendig. Dies kann eine tägliche oder eine wöchentliche Datensicherung bedeuten. Bei der Sicherung sollten stets mehrere Datenträger wechselweise zum Einsatz kommen. Für eine werktägliche Datensicherung empfiehlt sich die Verwendung von fünf Mediensätzen (Mo, Di, …, Fr.), für eine wöchentliche Datensicherung die Verwendung von vier bis fünf Mediensätzen (Woche 1, Woche 2 usw.), so dass die Datenträger erst nach dem Ende eines Sicherungszyklus wieder überschrieben werden.

Die Datensicherung sollte automatisiert erfolgen, sodass lediglich das Wechseln der Sicherungsmedien von Hand zu erfolgen hat. Für die Datensicherung ist eine verantwortliche Person (plus Vertreter) zu benennen, welche entsprechend unterwiesen und eingearbeitet die Datensicherung durchzuführen und zu protokollieren hat.
Nach der Datensicherung ist zu überprüfen, ob diese einwandfrei durchgeführt wurde. Eine geeignete Datensicherungssoftware sollte Mechanismen zur Verfügung stellen, die eine zuverlässige Kontrolle ermöglichen.

Um die Verfügbarkeit der Daten während der Aufbewahrungszeit sicherzustellen, müssen ausgelagerte Daten ggf. auf neue Datensicherungsmedien umkopiert werden.

Die Backup-Medien müssen unter Beachtung der gesetzlichen Vorschriften (siehe Kapitel 7, S. 27 ff.) an einem sicheren Ort aufbewahrt werden. Es empfiehlt sich, die Medien nicht in den Praxisräumen aufzubewahren, da sie im Falle eines Elementarschadens bzw. eines Diebstahls genauso verloren wären wie die Rechner selbst. Als Aufbewahrungsort eignet sich beispielsweise ein Datentresor außerhalb der Praxisräume.

Es ist heute unter Nutzung ausreichender Bandbreiten möglich, eine Datensicherung online im Internet, beispielsweise im Wege des Cloud-Computing, abzulegen. Verschiedene Anbieter bieten Speicherplatz im Internet zu geringen Kosten an. Wegen der Sensibilität der zu sichernden Daten ist jedoch prinzipiell davon abzuraten. Das Thema Cloud-Computing ist zudem relevant im Rahmen der Datenaufbewahrung bzw. der Dokumentation und Archivierung. Es wird deshalb in diesem Zusammenhang unter Kapitel 8.8.3 (S. 44) dargestellt.

2.5 Regelmäßige Sicherheitsupdates/Fernwartung

Neben den in Kapitel 2.2 (S. 5) angesprochenen Updates des Virenschutzprogramms sollten auch angebotene Aktualisierungen und Sicherheitsup-

dates des Betriebssystems und der Anwendungsprogramme regelmäßig durchgeführt werden. Die Hersteller sind entsprechend bemüht, entdeckte Sicherheitslücken zu schließen und veröffentlichen daher regelmäßig Sicherheitsupdates. Zur Betreuung der Updates sollte eine verantwortliche Person nebst Vertretung benannt und geschult werden.

Es ist inzwischen üblich, für das Praxisverwaltungssystem eine Fernwartung zu vereinbaren. Da hiermit zugleich sensible personenbezogene Daten zugreifbar werden, sind in diesem Fall einige Rahmenbedingungen zu beachten:

- Die Fernwartung muss vom Praxisrechner initiiert werden. Ein Zugriff von außen ohne vorherige Freischaltung am Praxisrechner ist unzulässig.
- Während der Dauer der Fernwartung, bei der unter Umständen auch personenbezogene Daten genutzt werden müssen, darf der Rechner nicht ausschließlich allein demjenigen überlassen werden, der die Wartungsarbeiten durchführt. Die Wartungsarbeiten sind für die gesamte Dauer am Praxisrechner zu beobachten, so dass ggf. bei Missbrauch sofort eingegriffen und beispielsweise die Verbindung getrennt werden kann.
- Nach Abschluss der Fernwartung ist der Rechner wieder vom Internet zu trennen, es sei denn, er ist entsprechend abgesichert (siehe Kapitel 3.1.5, S. 16).
- Da wie bereits erwähnt ggf. auch der Umgang mit personenbezogenen Daten notwendig sein kann, sind bei Auftragsvergabe an ein Unternehmen, das Fernwartung anbietet, die strengen Voraussetzungen des Art. 9 Abs. 1 EU-DSGVO i.V.m. § 22 Abs. 2 BDSG (siehe Kapitel 8.8, S. 42) zu beachten, was u.a. die Einforderung einer Verschwiegenheitserklärung vom jeweiligen Unternehmen beinhaltet.
- Es empfiehlt sich, den Umfang und den Zeitpunkt von Wartungstätigkeiten unter Angabe des Namens des Servicetechnikers zu protokollieren. Im Protokoll sollte auch die Neuinstallation von Programmen und Hardwareteilen dokumentiert werden.

2.6 Physischer Schutz, physische Umgebung

Um den unerwünschten Zugriff Dritter auf Daten der Praxis zu vermeiden, müssen Bildschirm, Tastatur, Maus, Kartenlesegerät, Konnektor, Drucker und Rechner so aufgestellt werden, dass sie für Unbefugte nicht zugänglich bzw. einsehbar sind. Das gilt auch für die Speichermedien zur Datensicherung. Wird der Arbeitsplatz verlassen, sollte der Computer manuell sofort gesperrt werden, so dass bei erneuter Nutzung erst das korrekte Kennwort wieder einzugeben ist. Neben der manuellen Direktsperrung kann auch der Bildschirmschoner zur Sperrung genutzt werden. Dieser wird nach einer einstellbaren (möglichst kurzen) Wartezeit aktiv und kann so konfiguriert werden, dass bei erneuter Nutzung des Rechners eine Kennwortabfrage erfolgt. Vor allem bei Rechnern in Behandlungsräumen sind diese Grundsätze unbedingt zu beachten.

Um zu verhindern, dass unbemerkt Daten kopiert werden, sollten USB-Anschlüsse und CD/DVD-Brenner gesperrt und nur im Bedarfsfall zur Nutzung freigegeben werden. Rechnersysteme können auch durch äußere Einflüsse Schaden nehmen. Zu hohe Temperaturen oder Spannungsspitzen in der Stromversorgung können die Systeme beschädigen oder gar zerstören. Ein Klimagerät sorgt für ausreichende Klimatisierung; eine unterbrechungsfreie Stromversorgung schützt vor Spannungsspitzen und vor Stromausfall.

2.7 Entsorgung von Systemen bzw. Datenträgern

Wohin mit dem alten Computer, dem alten System? Diese Frage scheint auf den ersten Blick einfach zu beantworten, ist aber im Hinblick auf die im Rechner verbauten Datenträger (Festplatten,

SSD-Speicher oder anderen ggf. vorhandenen Speichermedien) nicht ganz so einfach zu lösen.

Es gibt diverse angebotene Software, mit deren Hilfe Daten auf diesen Speichermedien gelöscht werden können, aber ob diese zuverlässig die gespeicherten Daten zerstören, ist vor allem für den Laien nicht nachvollziehbar.

Letztlich bleibt daher als sicherster Weg die physische Zerstörung der Datenträger.

Konkrete Informationen zur Entsorgung von Datenträgern bietet das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinem Grundschutzkatalog - Maßnahmenkatalog - M 2.167, zu finden im Internet auf der Webseite: https://www.bsi.bund.de.

Ebenfalls im Internet sind Firmen zu finden, die sich auf die Entsorgung von Datenträgern spezialisiert haben. Hierbei ist darauf zu achten, dass diese die Entsorgung/Vernichtung schriftlich ggf. durch ein Zertifikat nachweisen.

Auch offensichtlich defekte Datenträger sind oft mit Hilfe spezieller Techniken und spezieller Software noch lesbar. So können beispielsweise gelöschte Daten wiederhergestellt werden. Vor der Entsorgung von Datenträgern oder auch des alten PCs ist daher mit Hilfe von geeigneter Software bzw. durch physische Zerstörung der Datenträger sicherzustellen, dass diese im Nachhinein nicht wieder gelesen werden können.

2.8 Notwendige Weitergabe von Datenträgern an externe Dritte

Unter bestimmten Umständen kann es notwendig sein, Datenträger an externe Dritte weiter zu geben. So kann beispielsweise der Hersteller des PVS-Systems Daten anfordern, um Probleme oder Fehler in der Software nachvollziehen zu können. Vor der Weitergabe dieser Daten sollten diese entsprechend verschlüsselt werden. Dem Empfänger der Daten ist dann der verwendete Schlüssel auf getrenntem Wege mitzuteilen, so dass nur er mit Hilfe des erhaltenen Schlüssels die Daten entschlüsseln und nutzen kann. Der Empfänger der Datensendung sollte sich darüber hinaus vorab zur Geheimhaltung und Verschwiegenheit schriftlich verpflichten.

Das beschriebene grundsätzliche Verfahren gilt unabhängig vom Format des Datenträgers, also für die alte Diskette genauso wie für die Festplatte, den USB-Stick oder optische Datenträger wie die CD.

Auch hier bietet das Bundesamt für Sicherheit in der Informationstechnologie (BSI) in seinem Maßnahmenkatalog unter M 4.433 entsprechende Informationen an. Diese sind im Internetangebot des BSI unter: https://www.bsi.bund.de zu finden.

Unter bestimmten Bedingungen kann es vorkommen, dass ein Datenträger nicht mehr verschlüsselt werden kann. Dies kann z. B. bei einem defekten Datenträger der Fall sein, welcher aber noch unverzichtbare Daten enthält.
Hier bieten diverse Dienstleister die Reparatur von beschädigten Datenträgern an. In diesem Fall ist es physisch nicht möglich, den Datenträger vor dem Versand zu verschlüsseln. Daher ist die schriftliche Versicherung des Dienstleisters zur Geheimhaltung und Verschwiegenheit unabdingbar erforderlich. Von Dienstleistern, welche diese schriftliche Erklärung nicht vorab abgeben, ist abzuraten.

2.9 Einweisung und Schulung, Verantwortlichkeit

Der Zahnarzt ist nach § 7 Abs. 3 der Musterberufsordnung für Zahnärzte (MBO) der Bundeszahnärztekammer sowie nach der entsprechen-

den Regelung in der jeweiligen Berufsordnung der zuständigen Landeszahnärztekammer verpflichtet, alle in der Praxis tätigen Personen über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies schriftlich festzuhalten.

Zusätzlich sind die Mitarbeiter, die mit der Datenverarbeitung beschäftigt sind, gemäß § 5 BDSG (ab Mai 2018: § 53 BDSG) bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Die Verschwiegenheitspflicht und das Datengeheimnis bestehen für die Verpflichteten auch nach Beendigung ihrer Tätigkeit fort.

Um einen störungsfreien Betrieb der IT-Umgebung in der Praxis zu gewährleisten, sind Sach- und Fachkenntnis nötig. Das Personal, das mit Betrieb und Pflege der IT betraut ist, sollte die notwendigen Einweisungen absolviert haben. Dazu sind in der Regel keine kostspieligen Seminare erforderlich. Softwarehäuser bzw. Systembetreuer helfen ggf., die notwendigen Einweisungen und Schulungen durchzuführen.
Neben diesem „Basiswissen" ist die Festlegung von Verantwortlichkeiten für die Betreuung der IT-Systeme elementar. Festzulegen ist u. a., wer zuständig ist für:

- die Einhaltung der Sicherheitsvorschriften,
- die Aktualisierung des Virenschutzes,
- die Datensicherung,
- die Sicherheitsupdates.

2.10 Verschlüsselung

Mobile Rechner (Notebooks oder PDAs etc.), Datenträger, aber auch stationäre Rechner können gestohlen werden. In diesem Fall sind die darauf gespeicherten Patientendaten Unberechtigten zugänglich. Will man auch für diese Fälle die größtmögliche Sicherheit für Patientendaten erreichen, kann man den Einsatz von Verschlüsselung erwägen. Die Datenträger der entsprechenden Geräte können vollständig verschlüsselt werden, so dass nur die vorgesehenen berechtigten Personen aus der Praxis sie entschlüsseln können. Dies gilt für alle Datenträger/Medien z. B. auch für Datenträger/Medien, die Datensicherungen enthalten.

Beim Einsatz von Verschlüsselung müssen jedoch auch weiterführende Aspekte wie die geeigneten Algorithmen, Schlüssellängen sowie die Prozeduren und Maßnahmen für das Schlüsselmanagement betrachtet werden, so dass neben der Sicherheit der Daten auch deren Verfügbarkeit gewährleistet werden kann. Bei einer Entscheidung für den Einsatz von Verschlüsselung sollte fachlicher Rat unbedingt in Anspruch genommen werden.

2.11 Abkündigung / Laufzeitende der Software

Auch Software, also Applikationen von Herstellern oder auch Betriebssysteme haben eine begrenzte Lebensdauer. Das gefällt in der Regel nicht, ist die gewohnte Arbeitsumgebung doch so vertraut und gut eingespielt. Aktuellstes Beispiel hierfür ist das „Lebensende" von „Windows XP". Microsoft als Hersteller dieses Betriebssystems hat im April 2014 nach einer Laufzeit von dreizehn Jahren den Support für „XP" eingestellt.

Was bedeutet dies nun konkret für den Fall, dass wie in unserem Beispiel „Windows XP" noch auf einem oder mehreren Rechnern installiert ist? Hört der Rechner gar auf zu funktionieren? Was ist zu tun? Vorab sei bemerkt, dass die Antworten sich nicht nur auf unser Beispiel „Windows XP" beziehen, sondern zu einem großen Teil allgemein gültig für jede Software stehen, welche vom Hersteller nicht mehr unterstützt wird.

Die anscheinend gute Nachricht am Anfang: Der Rechner läuft weiter und alles scheint so in Ordnung zu sein wie es das immer schon war. Doch

es ist nur scheinbar alles gut. Die Hersteller von Software arbeiten stetig daran, ihre Software zu verbessern, Fehler zu bereinigen und mögliche Sicherheitslücken zu schließen. Stellt nun der Hersteller den Support für eines seiner Produkte offiziell ein, so werden eben keine Fehlerkorrekturen und Verbesserungen in das Produkt eingepflegt und vor allem keine Sicherheitslücken mehr geschlossen. Konkret bedeutet dies für unser Beispiel „Windows XP", dass es auf dem Stand vor der Abkündigung des Supports bleibt und bleiben wird.

In der Vergangenheit war zu einem gewissen Teil sicherlich durch die lange Laufzeit bedingt „Windows XP" das am meisten von Hackern angegriffene Ziel. Kein anderes Betriebssystem, keine andere Software wurde so oft durch Angriffe aus dem Internet mit Viren, Trojanern, Spamsoftware und anderem Ungeziefer bzw. Schädlingen attackiert. Es gibt konkrete Vermutungen und Anzeichen dafür, dass noch Sicherheitslücken vorhanden sind, die bis zum Supportende nicht von Microsoft geschlossen wurden. Es ist also anzunehmen, dass die Angriffe auf genau diese Lücken nun nach dem Ende des Supports zunehmen werden und sehr wahrscheinlich Schaden auf bzw. in dem nun schutzlosen Rechner anrichten werden.

Leider beschränkt sich der dann angerichtete Schaden nicht nur auf den Rechner an sich. Dramatischer sind die Folgen wie sie etwa bei Datendiebstahl, Ausspähen von Kennworten, Mitschneiden von PIN-Nummern etc. entstehen können.

Die Konsequenz des bisher Geschilderten ist klar: **Abgekündigte Software vor allem wie in unserem Beispiel genannt „Windows XP" als Betriebssystem soll nicht weiter betrieben werden und ist zu ersetzen!**

Auch gute Virenscanner bzw. gut abgesicherte Internetzugänge hindern nicht vor einem Befall des Systems mit Schadsoftware. Es ist dabei zu beachten, dass Schadsoftware auch auf anderen Wegen (USB-Sticks, CDs, externe Festplatten ...) auf den Rechner gelangen können.

Allerdings ist bei rein offline betriebenen Systemen ein durch die Schadsoftware verursachter Datenausgang nicht zu erwarten. Bei Systemen, die nicht und auch nicht zeitweise an das Internet angebunden sind (offline), kann abgekündigte Software und damit auch das als Beispiel genannte „Windows XP" weiter betrieben werden. Es ist dabei jedoch sicherzustellen, dass das System vollständig und damit auch physikalisch vom Internet getrennt ist. Ein Systemwechsel auf neuere Betriebssysteme ist in diesem Fall lediglich zu empfehlen.

3.0 Nutzung des Internets

Mit Einführung der Telematikinfrastruktur ergeben sich neue Möglichkeiten zur Online-Kommunikation, die technisch zwar auch das Internet als Infrastrukturkomponente nutzen, dabei jedoch das Praxisnetz oder die Praxisarbeitsplätze nicht direkt mit dem Internet verbinden. Wenn eine Internetanbindung gewünscht ist, kann ein „sicherer Internetzugang" als zusätzlich angebotener Dienst explizit freigeschaltet werden.

Zur Nutzung der Komponenten und Dienste der Telematikinfrastruktur in den Praxen werden die PVS-Systeme durch einen sicherheitszertifizierten Konnektor über VPN-Verbindungen mit der Telematikinfrastruktur verbunden. Um jegliche Online-Anbindung der PVS-Systeme zu vermeiden, besteht die Möglichkeit zur Nutzung des sogenannten Standalone-Szenarios mit zwei Konnektoren. Hierbei ist nur einer der beiden Konnektoren, an welchen ein zusätzliches Kartenterminal angeschlossen ist, mit der Telematikinfrastruktur zur Prüfung und Aktualisierung der Versichertenstammdaten verbunden. Die technische Umsetzung dieser Lösung ist weiter unten ausgeführt.

Die Anbieter der VPN-Zugangsdienste zur Telematikinfrastruktur müssen auch einen sicheren Internetzugang anbieten. Der Zahnarzt kann sich entscheiden, ob er diesen Dienst nutzen will.

Damit wird der Zugang zu Internetdiensten z. B. zur Online-Recherche, zur Bestellung von Praxismaterial oder ähnlichem zusätzlich durch ein sicheres Gateway abgesichert.

Ist ein Internetzugang unabhängig von der Telematikinfrastruktur notwendig oder erwünscht, gelten die bestehenden und im Folgenden aufgeführten Empfehlungen.

Grundsätzlich sollte der Zugang zum Internet mit Hilfe eines Routers (eines Gerätes zum Verbindungsaufbau in das Internet) und einer Firewall erfolgen, die den Datenverkehr in und aus dem Internet regelt. Die Konfiguration des Routers, vor allem aber der Firewall, sollte nur durchführen, wer gute Fachkenntnisse hat. Häufig wird als Firewall von verschiedenen Anbietern eine Software angeboten, die auf dem jeweiligen Rechner installiert Firewall-Funktionalitäten bieten soll. Bei diesen Lösungen handelt es sich jedoch nicht um einen Schutz der gesamten Praxis-Infrastruktur, sondern lediglich um den Schutz des einzelnen Rechners. Um die gesamte Praxis-Infrastruktur zu schützen, empfiehlt sich der Einsatz einer dedizierten Firewall-/Proxylösung an zentraler Stelle. Bei der Auswahl geeigneter Produkte sollte fachlicher Rat unbedingt in Anspruch genommen werden.

Insbesondere ein drahtloses Praxisnetzwerk kann Sicherheitslücken aufweisen. Hierbei ist zu beachten, dass das Netzwerk durch Unbefugte außerhalb der Praxisräume angewählt werden kann, wenn keine zusätzlichen Sicherungsmaßnahmen - insbesondere dem Einsatz von ausreichend sicheren kryptografischen Verschlüsselungsverfahren - ergriffen werden und damit kein ausreichender Passwortschutz (möglichst durch Verschlüsselung mittels WPA2-Verfahren) besteht. Hier ist in besonderer Weise der Nutzung durch Dritte vorzubeugen.

Eine Möglichkeit zur Kommunikation mit der KZV und sogar zur Nutzung des Internets ist ein „Intranet“ in Form eines virtuellen privaten Netzwerks (VPN). Das bedeutet, dass jeder Kontakt zu anderen Teilnehmern dieses VPNs über eine geschützte Verbindung läuft. Einige VPN-Anbieter sichern über die „private“ Kommunikation zu bekannten Teilnehmern hinaus auch den Zugriff auf das Internet ab (durch Vergabe dynamischer Rechner-Adressen, Firewalls etc.). Daher sollte ein VPN nur in Absprache mit der KZV genutzt werden, um sicherzugehen, dass das VPN ausreichenden Sicherheitsstandards genügt.

Firewalls ermöglichen in der Regel im Übrigen auch das Filtern von URLs, also den von den Nutzern aufgerufenen Internetseiten. Daher kann als zusätzlicher Schutz diese Funktion genutzt werden, um die zur Nutzung freigegebenen Internetseiten einzuschränken und um damit natürlich das Sicherheitsniveau zu erhöhen.

Leider ist die manuelle Pflege solcher Listen mit einem recht hohen zeitlichen und damit auch ggf. personellen Aufwand verbunden.

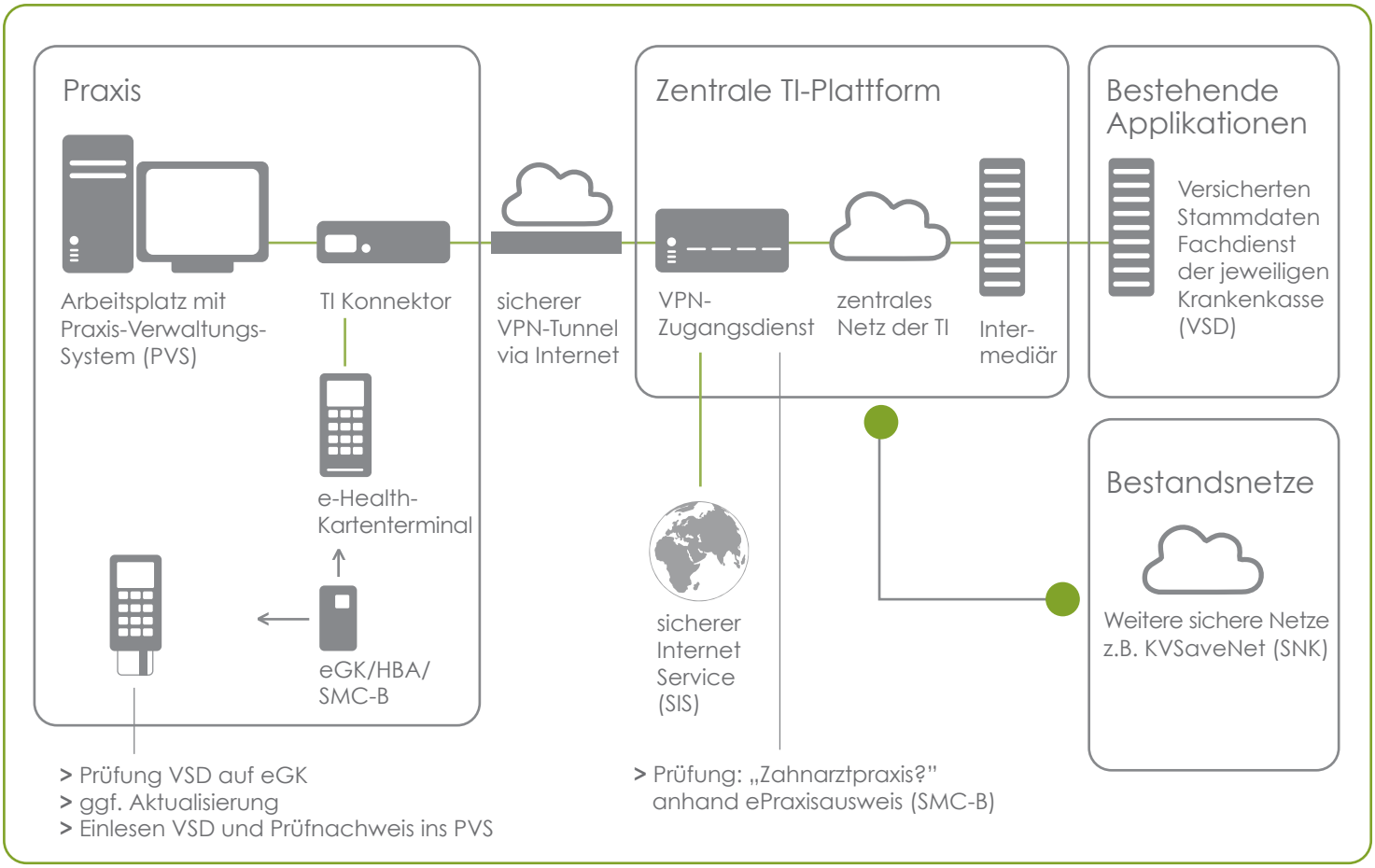
Um dies zu umgehen, aber auch gleichzeitig die Filterfunktionalität für aufgerufene Internetseiten nutzen zu können, empfiehlt sich der Einsatz einer Firewall eines Herstellers, der diese Funktion z. B. mit Begriffen wie „ContentFiltering“ oder ähnlichen umschreibt. Diese „ContentFilter“ verwenden in der Regel eine Datenbank, in der ggf. mehrere Millionen klassifizierter Einträge vorhanden sind. So kann bei Aufruf einer Webseite entschieden werden, ob diese Seite möglicherweise gefährlichen Inhalt beherbergt oder nicht erwünschte Inhalte (Drogen, Waffen ...) enthält. Die auf der Firewall befindliche lokale Datenbank wird automatisch aktualisiert, um so stets zeitnah einen optimalen Schutz bieten zu können.

Um eine Kommunikation mit bestimmten Partnern (z. B. der KZV) immer zu gewährleisten, sollte die Adresse (IP-Adresse) des beabsichtigten Kommunikationspartners in einer sog. „WhiteList“ (Liste freigeschalteter IP-Adressen) fest eingetragen werden.

3.1 Netzwerk-Varianten und Anbindung an das Internet

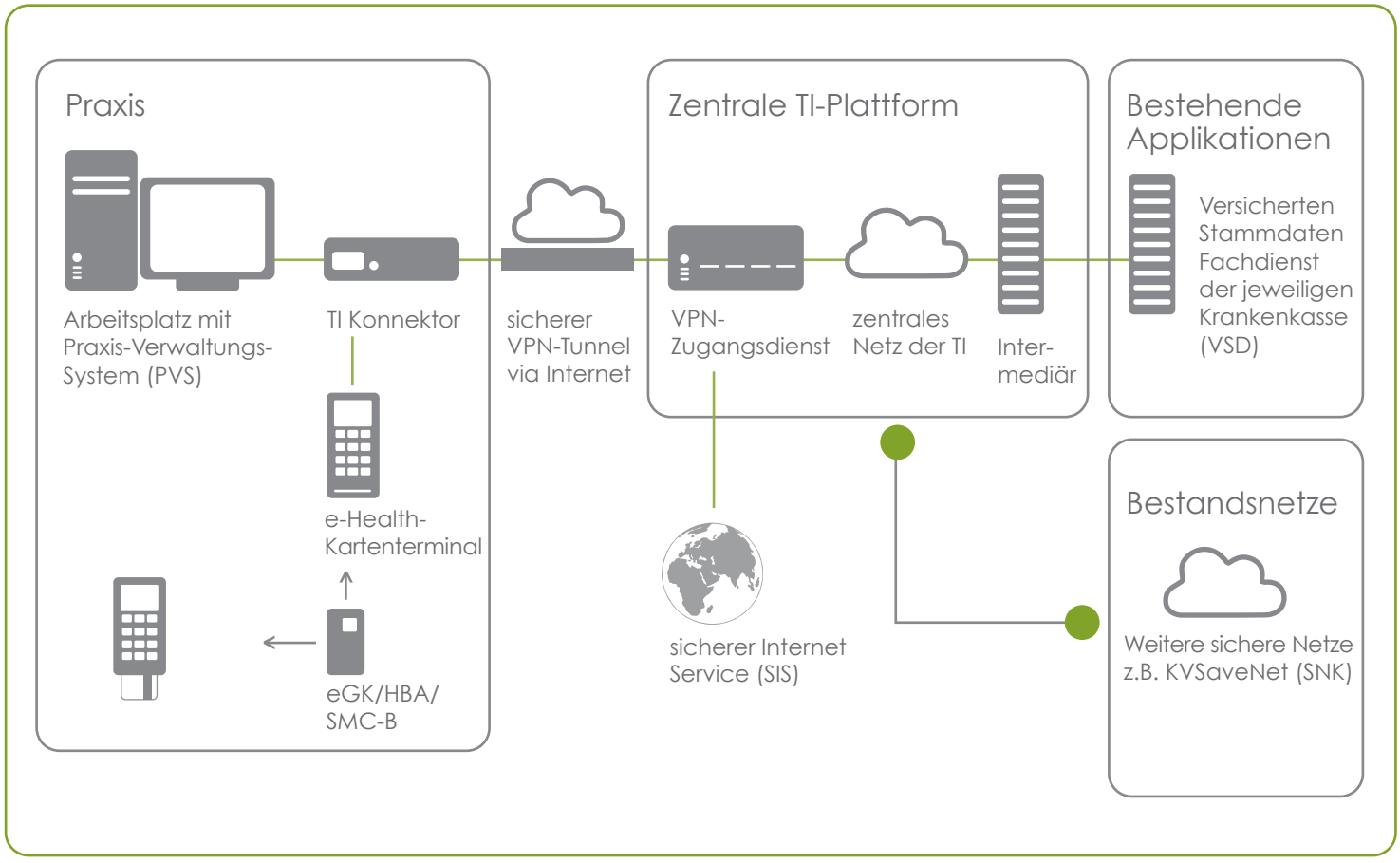
3.1.1 Telematikinfrastruktur: Anbindung an die Telematikinfrastruktur über den Konnektor (sicher)

Der von der gematik zugelassene und vom Bundesamt für Sicherheit in der Informationstechnologie zertifizierte Konnektor verfügt über zahleiche Sicherheitsfunktionen. Er schützt sowohl das Praxisnetzwerk gegen Angriffe von außen (Firewall Funktion) und sorgt durch die Verbindung mit dem VPN-Zugangsdienst für eine sichere Anbindung an die Telematikinfrastruktur. Ein direkter Zugang in das Internet ist zunächst nicht möglich. Dies kann jedoch bei Bedarf über den weiter unten beschriebenen zusätzlichen Dienst „sicheren Internetzugang“ ermöglicht werden.



3.1.2 Telematikinfrastruktur: Nutzung eines sicheren Internetzugangs (SIS) (sicher)

VPN-Zugangsdiensteanbieter sind dazu verpflichtet, auch einen sicheren Internetzugang zusätzlich anzubieten. Durch ein Sicherheits-Gateway als Schutzmaßnahme ist somit ein sicherer Zugang auch zu Internetdiensten, z. B. zur Fachrecherche, möglich. Dies entspricht der oben beschriebenen „Nutzung eines VPN-Gateways", bei dem die tatsächlich implementierten Schutzmaßnahmen durch gematik-Spezifikationen vorgegeben sind und im Rahmen der Zulassung geprüft werden.

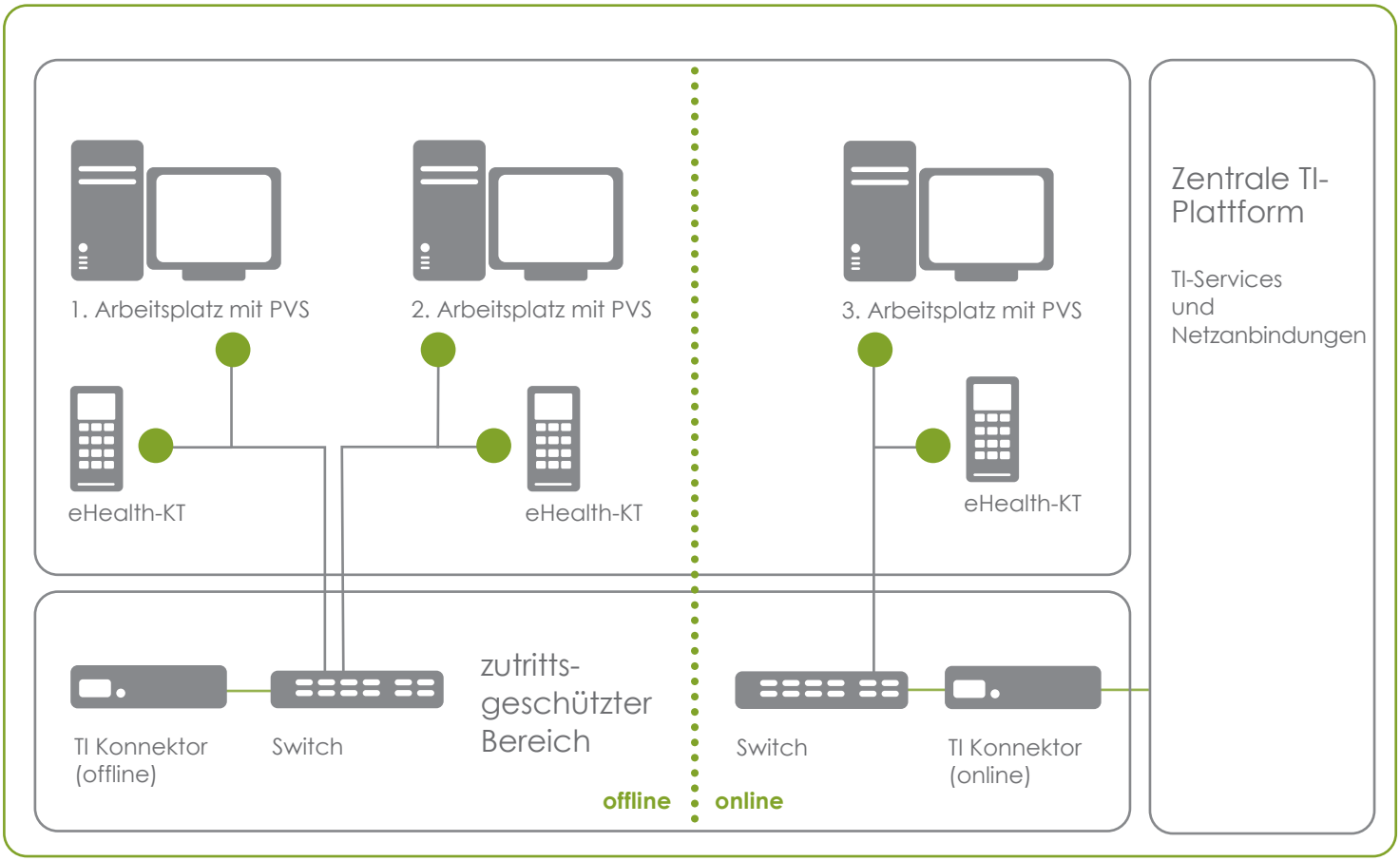


3.1.3 Telematikinfrastruktur: Standalone-Szenario mit physischer Trennung (sicher)

Neben der direkten Anbindung des Praxisverwaltungssystems besteht für die Zahnarztpraxis alternativ die Möglichkeit, die gesetzlich vorgegebene Online-Prüfung und Aktualisierung der Versichertenstammdaten vollständig getrennt vom Praxisverwaltungssystem vorzunehmen. Bei dieser in der Grafik veranschaulichten Lösung werden jedoch zwei Konnektoren und Kartenterminals benötigt und die elektronische Gesundheitskarte muss zweimal gesteckt werden.

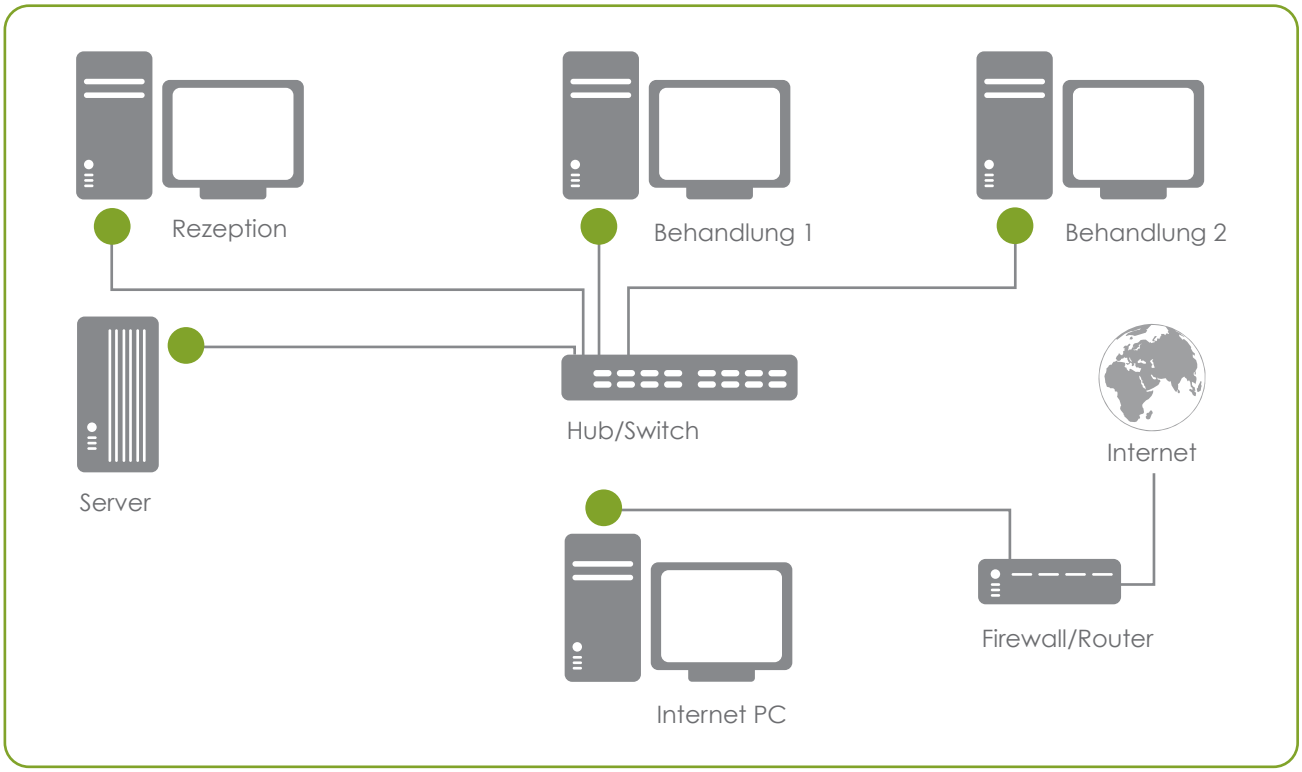
Zunächst wird die eGK in das Kartenterminal gesteckt, welches mit dem Konnektor verbunden ist, der Zugang zur Telematikinfrastruktur hat. Die Versichertenstammdaten werden auf Aktualität und Gültigkeit geprüft und ggf. aktualisiert. Anschließend muss die eGK in das zweite Kartenterminal gesteckt werden. Dieses ist mit dem Konnektor verbunden, welcher seinerseits mit dem PVS verbunden ist und keine Online-Anbindung hat. Nun können von dort die ggf. aktualisierten Stammdaten in das PVS eingelesen werden.

Die Nutzung des Internets von Systemen im Praxisnetz ist in diesem Szenario nicht gewünscht und auch nicht möglich.



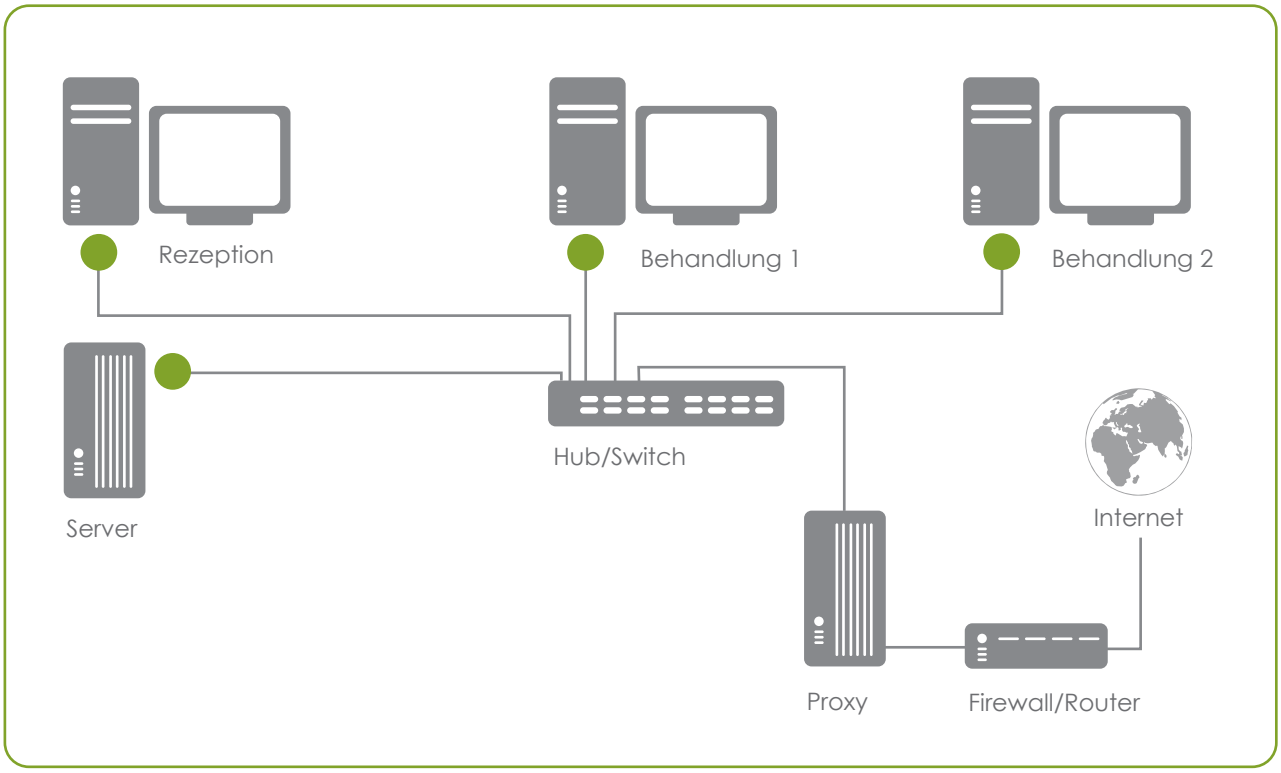
3.1.4
Nutzung eines eigenen unabhängigen „Internet-PCs“ (sicher)

Die sicherste Möglichkeit, die Praxis an das Internet anzubinden, bietet das folgende Szenario: Alle Rechner im Praxisnetz sind miteinander verbunden und nutzen einen gemeinsamen Server zur Datenhaltung der Praxis- und Patientendaten. Zusätzlich wird ein einzelner Rechner betrieben, der keine Netzwerkverbindung zu den anderen Praxis-Rechnern und damit auch keinen Zugriff auf Patienten- bzw. Praxisdaten hat. Dieser isolierte Rechner (der „Internet-PC“) hat jedoch als einziger eine Verbindung mit dem Internet.



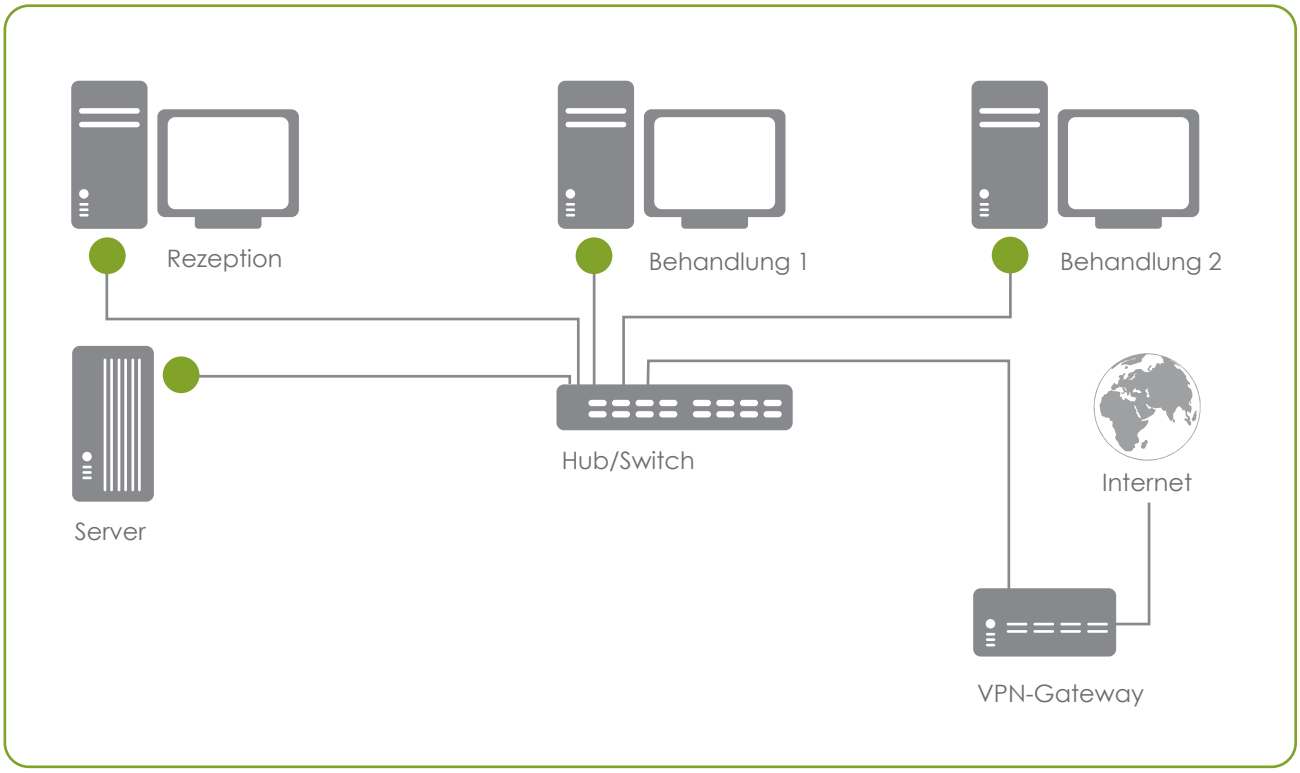
3.1.5
Nutzung eines Proxy-Servers (nahezu sicher)

In diesem Fall haben alle Rechner in der Praxis Zugang zum Internet. Kein Rechner kommuniziert jedoch direkt mit dem Internet. Alle Anfragen in das Internet und alle Antworten aus dem Internet werden über einen sogenannten „Proxy“-Rechner vermittelt. Der Proxy sendet die Anfragen jedes Praxisrechners in das Internet und verteilt die Antworten aus dem Internet entsprechend an die anfragenden Praxisrechner. Es sollte nur ein Proxy zum Einsatz kommen, der Internet- und Mailverkehr filtert und so das Risiko einer Infektion durch Schadsoftware minimiert.



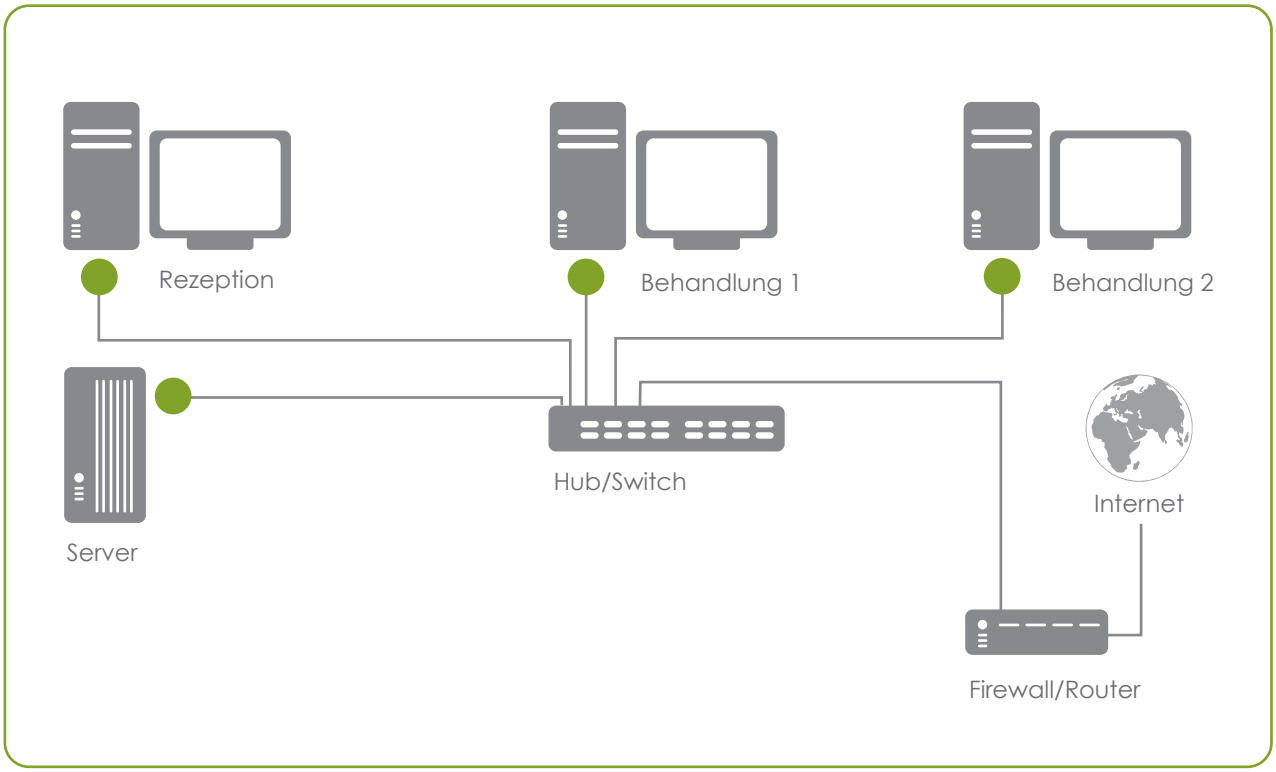
3.1.6
Nutzung eines VPN-Gateways (nahezu sicher)

Bei dieser Kommunikationsform haben alle Rechner in der Praxis Zugang zum Internet. Alle Anfragen in das Internet und alle Antworten aus dem Internet werden über ein sog. VPN-Gateway mit diversen Schutzmechanismen (Firewall, Intrusion Prävention, Virenschutz) geleitet. Mit dem Kommunikationspartner (z. B. KZVen) können gesicherte, verschlüsselte Verbindungen mittels VPN-Techniken realisiert werden. Die Sicherheit liegt hier in der Verantwortung des Betreibers des VPN-Gateways.



3.1.7 Direkte Anbindung an das Internet (unsicher)

Die letzte Möglichkeit besteht darin, dass alle Rechner in der Praxis eine direkte Verbindung in das Internet haben und direkt an das Internet ihre Anfragen senden bzw. aus dem Internet ihre Antworten empfangen. Von dieser Variante ist aus Sicherheitsgründen abzuraten.



3.2 Umgang mit E-Mail-Programmen und Webbrowsern

Die Nutzung eines Internet-Browsers und eines E-Mail-Programms ist grundsätzlich mit großen Risiken verbunden. Die meisten Infektionen eines Rechners mit schädlicher Software finden beim Webbrowser durch Nutzung von aktiven Komponenten wie z. B. ActiveX, Scriptsprachen und Multimedia-Plugins statt. Die modernen Browser bieten die Möglichkeit, die Nutzung von aktiven Komponenten einzuschränken bzw. zu untersagen. Dies sollte so weit wie möglich genutzt werden, um das Risiko der Infektion durch Schadsoftware zu minimieren. Darüber hinaus sollten keine unbekannten Webseiten besucht werden. Dies gilt vor allem für Webseiten, die beispielsweise kostenlos Software, Filme, Musik oder Ähnliches anbieten. Jede Infektion eines Rechners, der auch Zugriff auf die Praxis- bzw. Patientendaten hat, bedeutet ein nicht zu kalkulierendes Risiko.

Bei der Nutzung des E-Mail-Programms ist darauf zu achten, dass E-Mails nach Empfang nicht automatisch geöffnet angezeigt werden. Dies kann entsprechend im E-Mail-Programm konfiguriert werden. Empfangene Dateianhänge sollten nicht arglos geöffnet werden. Von ihnen geht eine große Infektionsgefahr für den Rechner aus. Im Zweifelsfall ist vor dem Öffnen eines Anhangs Kontakt mit dem Absender der E-Mail aufzunehmen, um abzuklären, ob der Anhang gefahrlos geöffnet werden kann. E-Mails gänzlich unbekannter Absender mit einem unbekannten Betreff sollten nicht geöffnet und ggf. direkt gelöscht werden.

Schließlich sollten sich Empfänger und Absender in den Fällen, in denen sie per E-Mail Informationen bezogen auf konkrete Patienten austauschen, im Vorfeld entweder auf ein geeignetes Pseudonym für den jeweiligen Patienten verständigen und/oder eine geeignete Verschlüsselung der E-Mails vereinbaren.

3.3 Telemedizinische Entwicklungen

Telemedizin bezeichnet den Einsatz von Telekommunikations- und Informationstechnologien im Gesundheitswesen zur Überwindung einer räumlichen Trennung zwischen Patient und behandelndem (Zahn-)Arzt sowie zwischen mehreren Ärzten, zum Beispiel durch Teleradiologie. Mit der zu erwartenden Entwicklung von telemedizinischen Anwendungen in der Zukunft werden auch neue Strukturen geschaffen, wobei jedoch eingesetzte technische Systeme so gestaltet bleiben müssen, dass die bewährte Vertrauensbeziehung zwischen Arzt und Patient sichergestellt bleibt. Grundsätzlich bleiben also dieselben datenschutzrechtlichen Rahmenbedingungen gültig wie außerhalb der Telemedizin. Auch wenn zum heutigen Zeitpunkt telemedizinische Anwendungen in der zahnärztlichen Praxis noch eine untergeordnete Rolle spielen, können sich durch die Verfügbarkeit neuer Techniken zukünftig auch telemedizinische Methoden durchaus im Praxisalltag etablieren. Dadurch ergeben sich aber auch dann neue Fragestellungen.

3.4 Bereitstellung von Patientendaten über Datennetze

Patienten können ihre Daten nur im Einzelfall für einen Zugriff konkret bestimmter, außerhalb der Praxis tätiger Dritter freigeben. Eine allgemeine Bereitstellung von Patientendaten in einem Datennetz durch einen Arzt oder Zahnarzt ist hingegen nach der gegenwärtigen Rechtslage grundsätzlich nicht zulässig.

Wichtig ist zu beachten, dass eine Offenbarung von Patientendaten auch dadurch erfolgt, dass Dritten ein elektronischer Datenabruf ermöglicht wird.

4.0 Anforderungen an die Praxissoftware

4.1 Verwendung zugelassener Praxisverwaltungssoftware bei vertragszahnärztlicher Tätigkeit

Für die Abrechnung vertragszahnärztlicher Leistungen darf nur ein Praxisverwaltungssystem (PVS) eingesetzt werden, das die Eignungsfeststellung der Prüfstelle der KZBV erhalten hat. Die Verwendung eines PVS, mit dem der Vertragszahnarzt Leistungen zum Zweck der Abrechnung erfasst, speichert und verarbeitet, bedarf der Genehmigung durch die zuständige Kassenzahnärztliche Vereinigung (KZV). Der Vertragszahnarzt gibt der KZV das eingesetzte PVS und die jeweils verwendete Programmversion bekannt, damit die KZV überprüfen kann, ob das PVS für die vertragszahnärztliche Abrechnung geeignet ist. Der Vertragszahnarzt hat seiner KZV bei jeder elektronischen Abrechnung zu bestätigen, dass die genehmigte Programmversion angewandt wurde. Nähere Informationen zu Praxisverwaltungssystemen mit Eignungsfeststellung sind unter www.kzbv.de zu finden bzw. werden von der zuständigen KZV bereitgehalten.

4.2 Anforderungen bedingt durch die Praxis-Organisationsform

4.2.1 Neuanschaffung eines Praxisverwaltungssystems

Bei der Planung einer Neuanschaffung eines Praxisverwaltungssystems sollte die Organisationsform der Praxis berücksichtigt werden:

Einzelpraxis
Bei einer Einzelpraxis mit einem Einzelplatzsystem oder einem Mehrplatzsystem, bei dem die EDV-Arbeitsplätze untereinander vernetzt sind, wird auf denselben Datenbestand zugegriffen.

Berufsausübungsgemeinschaft (früher: Gemeinschaftspraxis)
Bei einer Berufsausübungsgemeinschaft schließt der Patient grundsätzlich mit allen Zahnärzten gemeinschaftlich einen Behandlungsvertrag. Die Zahnärzte sind zur gegenseitigen Vertretung berechtigt und insoweit auch von der ärztlichen Schweigepflicht befreit.
Die EDV-Arbeitsplätze sind untereinander vernetzt, arbeiten mit demselben Praxisverwaltungssystem und greifen ebenfalls auf denselben Datenbestand zu. Bei der KZV wird eine gemeinsame Abrechnung eingereicht.

Ausnahmen liegen vor, wenn ein Patient entsprechend dem Grundsatz der freien Arztwahl ausdrücklich nur mit einem der Zahnärzte einen Behandlungsvertrag schließt. In diesen, in der Praxis eher seltenen Fällen gilt die ärztliche Schweigepflicht auch gegenüber den Kollegen in der Berufsausübungsgemeinschaft. Dies erfordert entsprechende organisatorische und technische Maßnahmen, die eine eindeutige Zuordnung und Beschränkung der Zugriffsrechte auf die Patientendaten durch den behandelnden Zahnarzt und das Praxispersonal ermöglichen.

Bilden bereits niedergelassene Zahnärzte oder bildet ein bereits niedergelassener Zahnarzt mit einem Zahnarzt, der noch nicht über einen eigenen Patientenstamm verfügt, eine Berufsausübungsgemeinschaft, kann nicht ohne Weiteres angenommen werden, dass die bisherigen Patienten der Einzelpraxis mit einer gemeinsamen Behandlung durch die Mitglieder der neu gebildeten Praxis einverstanden sind. Eine Zusammenführung dieser Patientendaten sollte erst

dann erfolgen, wenn der Patient der gemeinsamen Behandlung nicht widerspricht oder aber ausdrücklich zugestimmt hat. Dieses Vorgehen ist analog bei der Erweiterung bestehender Berufsausübungsgemeinschaft zu empfehlen.

Bei der Auflösung von Berufsausübungsgemeinschaften hat der Partner, der die Gemeinschaftspraxis verlässt und damit keinen Zugriff mehr auf die Praxis-EDV und die Patientenkartei hat, ein legitimes Interesse an den gemeinsamen Patientendaten. Dies gilt zumindest dann, wenn der ausscheidende Zahnarzt seine Tätigkeit an anderer Stelle weiter ausüben will und sich die Patienten bei ihm in Behandlung begeben.

Praxisgemeinschaften

Jede an der Praxisgemeinschaft teilnehmende Praxis ist rechtlich selbstständig und muss deshalb eine eigene Dokumentation und einen eigenen Datenbestand führen. Im Verhältnis zu den Partnern der Praxisgemeinschaft gilt die ärztliche Schweigepflicht.

Bei einer Praxisgemeinschaft wird für jeden Zahnarzt eine eigene Abrechnung erstellt. Auch hier wird ein gemeinsames Praxisverwaltungssystem genutzt, es muss jedoch mandantenfähig sein, d. h. für jeden Zahnarzt eine eigene Patientendatenverwaltung und Abrechnung vorsehen. Dabei muss gewährleistet sein, dass die Datenbestände der in der Praxisgemeinschaft tätigen Zahnärzte nicht gegenseitig eingesehen werden können. Im Falle der Vertretung muss der Zahnarzt eine Einwilligung von seinen Patienten einholen, dass sein Kollege ggf. in die Patientendaten Einsicht nehmen kann. Grundsätzlich muss über geeignete Zugriffsschutzmechanismen sichergestellt werden, dass nur berechtigte Personen Zugriff auf die jeweiligen Daten haben.

Medizinisches Versorgungszentrum (MVZ)

Auch vom MVZ sind die Regelungen zur ärztlichen Schweigepflicht und zum Datenschutz zu beachten.

Allerdings können sich aufgrund der inneren Organisation eines MVZ besondere Anforderungen hinsichtlich des Schutzes der Patientendaten ergeben. Es wird daher empfohlen, bereits in der Planungsphase in Zusammenarbeit mit der jeweiligen Datenschutzaufsichtsbehörde auf Landesebene ein individuelles Datenschutzkonzept zu erarbeiten. Entsprechendes gilt für in einem MVZ zugelassene Zahnärzte.

Einrichtungen zur integrierten und besonderen Versorgung

Nach den Regelungen zur „Besonderen Versorgung“ können Krankenkassen u. a. mit Vertragszahnärzten und Kassen(zahn)ärztlichen Vereinigungen Verträge über eine besondere Versorgung von Versicherten abschließen, die eine interdisziplinär fachübergreifende Versorgung (integrierte Versorgung) sowie besondere ambulante ärztliche Versorgung ermöglichen (ausführlich § 140 a SGB V).

Bei den Versorgungsformen nach § 140 a SGB V erfolgt die Teilnahme des Patienten und des Arztes auf freiwilliger Basis.

Auch in diesen Fällen gestaltet sich die Sicherstellung der ärztlichen Schweigepflicht und des Datenschutzes sehr komplex. Es wird daher empfohlen, bereits in der Planungsphase in Zusammenarbeit mit der jeweiligen Datenschutzaufsichtsbehörde ein individuelles Datenschutzkonzept zu erarbeiten. Für den Bereich der integrierten Versorgung werden bestimmte Grundanforderungen in § 140 a Abs. 5 SGB V definiert.

4.2.2 Weiterverwendung des Praxisverwaltungssystems

Ist eine Neuanschaffung nicht geplant und wird das vorhandene PVS weiter genutzt, so sollte es in punkto Datenschutz und Datensicherheit kritisch geprüft und nötigenfalls nachgebessert werden.

4.2.3 Änderung der Praxis-Organisationsform oder Wechsel des Praxisverwaltungssystems

Der Zahnarzt sollte darauf achten, dass die in seinem Praxisverwaltungssystem gespeicherten Patienten- und Leistungsdaten im Notfall mit gängigen EDV-Standardwerkzeugen darstell- und verarbeitbar sind. Damit wird sichergestellt, dass diese Daten bei einem Systemwechsel nicht verloren gehen. Die PVS-Hersteller sind verpflichtet, die „Schnittstelle zum Austausch zahnärztlicher Patientendaten" in ihr System zu integrieren. Hiermit wird sichergestellt, dass die Festlegung in § 291 d SGB V, ärztliche Patientendaten über den Zeitraum von 10 Jahren nach Abschluss der Behandlung aufzubewahren, entsprochen wird.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften liegt beim Zahnarzt. Er muss daher ein besonderes Augenmerk auf den Datenschutz und auch die Datensicherheit legen. Hierzu ist ein zuverlässiges Datensicherungskonzept unerlässlich, da der Zahnarzt während der vorgeschriebenen Aufbewahrungsfrist (in der Regel zehn Jahre, § 10 Abs. 5 MBO) in der Lage sein muss, seine Abrechnungsdaten auch nach Wechsel des Praxisverwaltungssystems lesbar und verfügbar zu halten, siehe hierzu Kapitel 2.4, S. 6.

5.0 Anforderungen an die Hardwarekomponenten

5.1 PC(s)

Die Anforderungen an die Hardware hängen von der Praxisgröße und der Art der Praxis ab, aber auch von der eingesetzten Software. Bei der Anschaffung eines oder mehrerer PCs sollte darauf geachtet werden, dass ein aktuelles und leistungsfähiges Modell mit möglichst aktuellem Betriebssystem erworben wird. Die Hersteller von Praxissoftware sollten genaue Angaben bezüglich der Leistungsfähigkeit der zu verwendenden Hardware und der unterstützten Betriebssysteme machen können.

Für den „Mehrplatzbetrieb", also den Einsatz von Rechnerarbeitsplätzen in den Behandlungsräumen, und vor allem für die „karteilose" Praxis gelten zusätzliche Anforderungen. Dabei ist besonders zu beachten, dass ein zentraler Rechner (der Server) die Daten vorhält. An ihn sind hinsichtlich Betriebssystem, Stabilität und Sicherheit bzw. Redundanz bei der Datenhaltung besondere Anforderungen zu stellen. Keinesfalls sollte dieser Server gleichzeitig als Arbeitsplatz genutzt werden, auch wenn dadurch ein Rechner eingespart werden könnte. Der Server ist ein zentrales Element, er darf beispielsweise nicht abgeschaltet werden. Nutzt man ihn als Arbeitsplatz, sind seine Stabilität und Sicherheit nicht gewährleistet. Bei Vernetzung der Praxisräume oder Auswahl eines geeigneten Serverbetriebssystems ist es empfehlenswert, sich ggf. durch externe Dienstleister beraten zu lassen bzw. den Vorgaben des PVS-Herstellers zu folgen. In jedem Fall sind vorher Informationen vom jeweiligen Softwareanbieter einzuholen.

Egal ob „Einplatz- oder Mehrplatzbetrieb", eine organisierte und funktionierende Datensicherung (siehe auch Kapitel 2.4, S. 6) ist unumgänglich.

5.2 Drucker

Die Auswahl des Druckers ist abhängig von den Anforderungen in der Praxis. Ein Laserdrucker oder ein Tintenstrahldrucker sollte gewählt werden, wenn Blankoformularbedruckung vorgesehen ist. Welche Drucker vom Praxisverwaltungsprogramm unterstützt werden, ist mit dem jeweiligen PVS-Hersteller zu klären.

5.3 Stationäre Kartenterminals

Mit dem Online-Rollout der Telematikinfrastruktur werden neue, zertifizierte Kartenterminals, sog. eHealth Terminals benötigt. Der Einsatz von nicht zertifizierten Kartenterminals zur Nutzung der Dienste der TI ist nicht zulässig. Eine Übersicht über die zum jeweiligen Zeitpunkt zertifizierten Produkte wird von der gematik auf deren Webseite veröffentlicht.

eHealth-Kartenterminals werden zukünftig mittels Netzwerkanschlüssen in das Netzwerk der Praxis integriert und von dem dort vorhandenen Konnektor verwaltet. Die direkte Anbindung an ein PVS-System über USB-Anschlüsse ist nicht mehr möglich. Die alten, stationären Kartenterminals können mit der neuen Telematikinfrastruktur und dem Konnektor nicht mehr genutzt werden. Die neuen Kartenterminals verfügen über eigene austauschbare, aber mittels Siegel geschützte Gerätekarten (gSMC-KT) mit besonderer Sicherheitsfunktion zur Identifizierung und Betrieb des Kartenterminals innerhalb der TI. Neben der eGK werden auch die neuen Kartenterminals noch Krankenversichertenkarten einlesen können. Die Krankenversichertenkarte ist zwar seit dem 01.01.2015 kein gültiger Versicherungsnachweis für gesetzlich Krankenversicherte mehr, wird jedoch für Patienten, die bei sonstigen Kostenträgern, wie z. B. Polizei versichert sind, weiterhin genutzt.

Die Kartenterminals verfügen über ein Siegel, welches insbesondere bei längerer Nicht-Nutzung auf Unversehrtheit kontrolliert werden sollte, um Manipulationen an der Hardware durch unbefugte Dritte zu vermeiden. Im Falle einer Beschädigung des Siegels ist das Gerät nicht mehr zu verwenden.

5.4 Mobile Kartenterminals

Zukünftig werden auch neue mobile Kartenterminals für Praxen erforderlich, die mobile Behandlungen unterstützen sollen. Sobald die neuen Kartenterminals verfügbar sind, werden die zugelassenen Geräte auf der Webseite der gematik veröffentlicht.

5.5 Konnektor

Der Konnektor ist eine Hardwarebox, welche sowohl die Verbindung zur Telematikinfrastruktur durch eine gesicherte VPN-Verbindung aufbaut als auch das Netzwerk der Praxis vor Zugriffen von außen schützen kann und damit Firewall-Funktionen bietet. Neben dieser technischen Absicherung müssen dennoch die in diesem Leitfaden aufgeführten organisatorischen Maßnahmen (Zugangsschutz, Länge und Ausgestaltung von Passwörtern etc.) selbstverständlich weiterhin beachtet werden. Konnektoren sind vom Bundesamt für Sicherheit in der Informationstechnik sicherheitszertifiziert und von der gematik zugelassen. Sie verfügen wie die neuen Kartenterminals auch über ein Siegel, welches regelmäßig auf Unversehrtheit zu kontrollieren ist, um Manipulationen am Gerät erkennen zu können.

Im Falle einer Siegelbeschädigung ist das Gerät nicht mehr zu verwenden. Dies gilt auch, wenn andere Hinweise auf eine Öffnung oder sonstige Manipulation des Gerätes erkennbar sind.

6.0 Online-Übertragung der Abrechnungsdaten / ZOD / elektronischer Zahnarztausweis / eGK

6.1 Online-Übertragung der Abrechnungsdaten in der Zahnarztpraxis

Alle KZVen streben die flächendeckende Online-Übermittlung der Abrechnungsdaten aus den Zahnarztpraxen an und treiben diese durch Schaffung entsprechender Anreize oder durch mittelfristige Verpflichtung der Praxen voran.

Um maximalen Schutz des Praxissystems zu gewährleisten, sollte die Übermittlung der Abrechnungsdaten (wie auch alle übrigen Online-Anwendungen) von einem separaten PC (siehe hierzu Kapitel 3.1.4, S. 15) oder bei Anbindung des PVS an die TI unter Nutzung des sicheren Internetzugangs, wie ein VPN-Zugangsdiensteanbieter dies anbieten wird, erfolgen. (siehe hierzu Kapitel 3.1.2, S. 13) Unabhängig davon, von welchem Rechner aus die Übermittlung erfolgt, sollten die nachfolgend aufgeführten Schutzmaßnahmen ergriffen werden.

Grundlage für die Abrechnung ist das ordnungsgemäße Einbringen der Abrechnungsdaten in die Systeme der zuständigen KZV. Über die sichere Online-Anbindung des Praxissystems hinaus sind bei der Online-Abrechnung daher folgende Eckpunkte zu beachten:

1. Es ist sicherzustellen, dass der Empfänger der Abrechnungsdaten zweifelsfrei die zuständige KZV ist. Falls die Abrechnungsdaten auf einem Portal abgelegt werden, wird durch die KZV sichergestellt, dass jeder berechtigte Zahnarzt nur auf seine Daten Zugriff hat (durch sichere, idealerweise Hardware-basierte Authentisierungsmaßnahmen).

2. Da Abrechnungsdaten in der Regel personenbezogene und damit sensible Daten sind, müssen sie während der Übertragung nach aktuellen Sicherheitsstandards verschlüsselt sein.

3. Sobald die Abrechnungsdateien ohne begleitende Papierunterlagen übermittelt werden, auf denen der Zahnarzt die Ordnungsmäßigkeit der abgerechneten Leistungen per Unterschrift bestätigt hat („papierlose Abrechnung"), ist die Abrechnungsdatei nach Auffassung der KZBV qualifiziert zu signieren, um die Rechtssicherheit für diese Form des Abrechnungsweges zwischen KZVen und Praxen zu gewährleisten. Die geeigneten Instrumente dazu sind vorhanden (ZOD-Karte, elektronischer Zahnarztausweis). Die jeweilige KZV entscheidet, wie zu verfahren ist.

Die KZV kann Auskunft darüber geben, ob und wie die oben beschriebenen Bedingungen gewährleistet sind, nach welchen Verfahren die Online-Abrechnung ermöglicht wird, und welche Verhaltensregeln der Zahnarzt beachten muss.

6.2 Der elektronische Zahnarztausweis

Der elektronische Zahnarztausweis (eZahnarztausweis) ist der elektronische Heilberufsausweis (HBA) für Zahnärzte. Er weist den Ausweisinhaber sowohl optisch als auch elektronisch als Zahnarzt aus. Letzteres ist notwendig, da der Gesetzgeber vorgegeben hat, dass ein Zugriff auf die Daten der elektronischen Gesundheitskarte (eGK) grundsätzlich nur durch Berechtigte erfolgen darf. Je nach Anwendung sind dies z. B. Zahnärzte, Ärzte oder Apotheker. Daher müssen diese Berechtigten mit einem entsprechenden elektronischen Ausweis ausgestattet sein.

Neben seiner Sichtausweisfunktion stellt er Sicherheitswerkzeug für die elektronische Kommunikation mit Dritten dar. Der eZahnarztausweis ermöglicht seinem Inhaber eine rechtssichere elektronische Kommunikation mittels qualifizierter elektronischer Signatur sowie die verlässliche Authentisierung gegenüber Dritten.

Die qualifizierte elektronische Signatur stellt eine rechtssichere elektronische Unterschrift dar. Sie kann im Rahmen der papierlosen Abrechnung erforderlich sein (je nach Vorgabe der KZV, siehe hierzu Kapitel 6.1, S. 24).

Mit Hilfe der Ver- und Entschlüsselungsfunktion kann zusätzlich ein sicherer Versand elektronischer Dokumente vorgenommen werden, so dass Dritte keinen Zugriff auf vertrauliche Inhalte haben. Der eZahnarztausweis kann damit zur vertraulichen Übermittlung schützenswerter Daten (elektronische Arztbriefe, Abrechnungsdaten etc.) und zur sicheren Anmeldung an Online-Portalen von Kammern und KZVen eingesetzt werden.

Die jeweiligen (Landes-)Zahnärztekammern sind die Herausgeber des eZahnarztausweises. Die Zahnärztekammer Saarlands hat als erste Kammer 2013 mit der Ausgabe von eZahnarztausweisen begonnen, mittlerweile ist er in allen Kammerbereichen verfügbar bzw. in Vorbereitung. Die Zahnärztekammern werden ihre Mitglieder über den Ausgabeprozess sowie die Antragsverfahren informieren.

In einigen Kammerbereichen sind noch ZOD-Karten im Feld oder werden durch die zuständige KZV ausgegeben. Diese sind mit dem eZahnarztausweis technisch weitgehend identisch und sollen für die entsprechenden Anwendungen (auch in der Telematik-Infrastruktur) bis zum Ablauf ihrer Gültigkeit eingesetzt werden können, so dass Investitionssicherheit für den Zahnarzt gegeben ist.

Ab Verfügbarkeit der medizinischen Anwendungen in den Praxen (Notfalldaten, el. Medikationsplan, Arzneimitteltherapiesicherheit) ist das Vorhandensein eines HBA und damit eines eZahnarztausweises (oder ZOD-Karte) in der Praxis verpflichtend.

Hinweise:

1. Der eZahnarztausweis (oder ZOD-Karte) dient dem Schutz der Daten beim Transport (Verschlüsselung, Signatur). Sie ersetzt jedoch nicht die sichere Online-Anbindung eines Computers zum Schutz der dort gespeicherten Daten (siehe Kapitel 3, S. 10 ff.).

2. Der Schutz der Daten beim Transport kann auch durch spezielle Protokolle gewährleistet werden, die automatisch vom angewählten Anbieter zur Verfügung gestellt werden („https-Protokoll“, zu erkennen an entsprechender Kennzeichnung im Browser). Die Abrechnungsportale der KZVen wickeln die Übertragung der Abrechnungsdaten in der Regel über dieses Protokoll[2] ab.
Auch dieses Verfahren schützt nur den Transport von Daten und kann eine sichere Online-Anbindung nicht ersetzen.

3. Die sichere Online-Anbindung eines Computers (siehe Kapitel 3, S. 10 ff.) schützt diesen und die darauf befindlichen Daten vor Angriffen. Sie ersetzt nicht den Schutz der Daten beim Transport. Dies kann „streckenbezogen“ durch eine „geschützte Leitung“ (SSL-Verbindung) oder ein Virtuelles Privates Netzwerk (VPN)[3] vom jeweiligen Anbieter (z. B. der KZV) gewährleistet werden (siehe Punkt 2)

[2] Der Unterschied zwischen dem Einsatz technischer Protokolle und der Verschlüsselung durch Signaturkarten (z. B. ZOD-Karte) liegt darin, dass technische Protokolle die Verbindung (und alle über diese Verbindung übermittelten Daten) zwischen zwei Computern absichern, während eine Verschlüsselung durch Signaturkarten daten- und personenbezogen erfolgt. Die Daten bleiben also im zweiten Fall auf dem Empfangsrechner im verschlüsselten Zustand gespeichert, bis die Person, für die die Daten bestimmt sind, diese mit ihrer Signaturkarte entschlüsselt.
[3] Je nach technischer Ausstattung (Router, Firewall etc., s. Kapitel 3) kann mit einem VPN auch die sichere Online-Anbindung gewährleistet werden.

oder „datenbezogen“ durch den Sender erfolgen (siehe Punkt 1). Ob der eingerichtete Schutz ausreichend ist, müsste vom Sender (also dem Zahnarzt) jeweils genau überprüft bzw. beim Portalbetreiber erfragt werden.

4. Eine „geschützte Leitung“ (SSL-Verbindung) allein gewährleistet nicht die sichere Identifizierung des Kommunikationspartners beim Zugriff auf ein Online-Portal (z. B. Einsicht in persönliche Abrechnungskonten bei der KZV). Allenfalls kann „das Online-Portal“ den auf die Portal-Daten zugreifenden PC identifizieren, jedoch nicht die Person, die ihn bedient. Zuverlässige Sicherheit bei der Authentifizierung und damit die Vermeidung unbefugter Zugriffe auf ein Online-Portal bieten nur Hardwarebasierte Methoden wie z. B. – nach dem Konzept „Besitz und Wissen“ – die Chipkartentechnologie in Verbindung mit einer persönlichen Identifikationsnummer (eZahnarztausweis und PIN)[4].

5. Bis zur Verfügbarkeit eines eHealth-Konnektors (mit Einführung der medizinischen Anwendungen in der Telematik-Infrastruktur) sind zum Einsatz des eZahnarztausweises / der ZOD-Karte ein geeignetes Kartenlesegerät sowie ggf. entsprechende Software für Verschlüsselung und Signatur erforderlich. Diese Komponenten sind in der Regel bei dem entsprechenden Anbieter erhältlich. Die Notwendigkeit einer entsprechenden Software kann bei der zuständigen KZV erfragt werden.

6.3 Telematikinfrastruktur und elektronische Gesundheitskarte

Bereits seit dem 01.01.2015 ist die eGK grundsätzlich alleiniger Versicherungsnachweis für die Versicherten in der gesetzlichen Krankenversicherung. Die auf der eGK gespeicherten Versichertenstammdaten werden in den Arzt- und Zahnarztpraxen regelmäßig online geprüft und ggf. aktualisiert, sobald die erforderlichen technischen und vertraglichen Voraussetzungen geschaffen worden sind. Das erstmalige Entstehen der Verpflichtung seitens der Praxen ist vom Gesetzgeber in § 291 Abs. 2 b SGB V näher geregelt worden. Praxen, die die Prüfung ab dem dort festgelegten Zeitpunkt nicht durchführen, droht eine Kürzung des Honorars.

Die Gesellschafterversammlung der gematik hat den Beschluss zur Einführung der Telematikinfrastruktur am 01.06.2017 gefasst.
Wie bereits bei den Komponenten ausgeführt, erfolgt die sichere Online-Anbindung des Praxisverwaltungssystems über eine Hardwarebox, den sogenannten "Konnektor". Dieser Konnektor sollte an einem Ort aufbewahrt werden, zu dem Unbefugte keinen Zutritt haben. Ein eigener Raum oder bauliche Maßnahmen sind in der Regel jedoch nicht erforderlich. Es bietet sich an, den Konnektor z. B. dort aufzustellen, wo auch der Praxis-Server steht. Die zugelassenen Geräte findet man auf der Seite der gematik. Für den Zugang zur Telematikinfrastruktur benötigt man den elektronischen Praxisausweis, bestellbar über die KZV. Fragen beantwortet die zuständige KZV oder der PVS-Hersteller.

Zusätzlich verfügt der Konnektor wie auch die Kartenterminals über ein Siegel. Dies ist regelmäßig auf Beschädigung zu prüfen, um auszuschließen, dass Unbefugte die Geräte manipuliert haben. Ist das Siegel gebrochen, sollte das Gerät nicht mehr verwendet werden und ein Ersatzgerät ist zu beschaffen.

Damit nur berechtigte Praxen Zugang zur Telematikinfrastruktur erhalten können, wird dies durch einen elektronischen Praxisausweis sichergestellt. Dabei handelt es sich um eine sog. SMC-B. Dies ist

[4] Siehe auch Entschließung der 81. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2011: "Mindestanforderungen an den technischen Datenschutz bei der Anbindung von Praxis-EDV-Systemen an medizinische Netze", Referenz www.bfdi.bund.de
Der Datenschutzkontrollausschuss der Vertreterversammlung der KZBV empfiehlt, in der Zahnarztpraxis zur sicheren Authentisierung am Online-Abrechnungsportal der KZV mittelfristig entweder qualifizierte Signaturkarten (ZOD-Karte oder elektronischer Zahnarztausweis) oder Hardware-VPN-Lösungen einzusetzen.

eine kleine Karte, welche ähnlich der SIM-Karte eines Handys in ein Kartenterminal gesteckt wird. Die Freischaltung der Karte erfolgt durch eine PIN. Ein freigeschalteter elektronischer Praxisausweis ist die Basis, damit ein Konnektor online gehen kann und eine Verbindung mit der Telematikinfrastruktur aufgebaut wird. Elektronische Praxisausweise werden von der zuständigen KZV ausgegeben[5].

Vor dem Behandlungsbeginn sollte der elektronische Praxisausweis durch PIN-Eingabe freigeschaltet werden. Die PIN des elektronischen Praxisausweises sollte an einem sicheren Ort aufbewahrt und nur vertraulich, z. B. an das berechtigte Praxispersonal, weitergegeben werden. Wird eine PIN auch anderen bekannt, ist diese umgehend unmittelbar zu ändern. Eine verlorengegangene oder gestohlene Karte ist unmittelbar zu sperren und eine neue zu beantragen.

Neben der bereits beschriebenen Online-Anwendung werden medizinische Anwendungen der elektronischen Gesundheitskarte (z. B. Notfalldatenmanagement, elektronischer Medikationsplan, Arzneimitteltherapiesicherheit) konzipiert und entsprechende Feldtests vorbereitet.

7.0 Rechtsgrundlagen

7.1 Grundlagen der (zahn-)ärztlichen Schweigepflicht

Die zahnärztliche Schweigepflicht gilt umfassend für das besondere Vertrauensverhältnis zwischen Zahnarzt und Patient. Sie ist strafbewehrt (§ 203 Strafgesetzbuch (StGB)) und festgeschriebene Berufspflicht (§ 7 MBO der Bundeszahnärztekammer i.V.m. der entsprechenden Regelung in der jeweiligen Berufsordnung der (Landes-)Zahnärztekammer). Danach haben Zahnärzte die Pflicht, über alles, was ihnen in ihrer Eigenschaft als Zahnarzt anvertraut und bekannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren.

Die zahnärztliche Schweigepflicht umfasst alle Informationen und Daten, die mit der zahnärztlichen Behandlung in Zusammenhang stehen. Dazu gehören die Art der Krankheit, deren Verlauf, Anamnese (Familienanamnese), Therapie und Prognose, körperliche und geistige Feststellungen, Patientendaten in Akten und auf elektronischen Datenträgern, Untersuchungsmaterial und Untersuchungsergebnisse. Ferner werden sämtliche im Rahmen der Behandlung gemachten Angaben über persönliche, familiäre, berufliche, wirtschaftliche und finanzielle Gegebenheiten, auch wenn diese keinen direkten Bezug zu einer Krankheit haben, von der zahnärztlichen Schweigepflicht umfasst. Schon der Name oder die Tatsache der Behandlung des Patienten stellen Patientengeheimnisse dar.

Das Patientengeheimnis besteht auch nach Abschluss der Behandlung fort und gilt über den Tod des Patienten hinaus. Eine Ausnahme hiervon regelt § 630 g Abs. 3 BGB. Die Erben des verstorbenen Patienten dürfen bei der Wahrnehmung vermögensrechtlicher Interessen Einsicht in die Patientenakten nehmen bzw. elektronische Abschriften von der Patientenakte verlangen, soweit der Einsichtnahme der ausdrückliche oder mutmaßliche Wille des Patienten oder sonstige erhebliche Rechte Dritter nicht entgegenstehen. Gleiches gilt für die nächsten Angehörigen des Patienten, soweit sie immaterielle Interessen geltend machen.

7.2 Schweigepflicht als Berufspflicht

Der Zahnarzt hat die Pflicht, über alles, was ihm in seiner Eigenschaft als Zahnarzt anvertraut und be-

[5] Mehr Infos zur Telematik-Infrastruktur und zum el. Praxisausweis finden Sie unter www.kzbv.de.

kannt geworden ist, gegenüber Dritten Verschwiegenheit zu wahren. Er ist zur Offenbarung lediglich dann befugt, soweit er von dem Betroffenen oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde oder soweit die Offenbarung zum Schutze eines höheren Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben davon unberührt. Der Zahnarzt hat alle in der Praxis tätigen Personen über die gesetzliche Pflicht zur Verschwiegenheit zu belehren und dies zu dokumentieren. (siehe insbesondere Art. 5 und 24 EU-DSGVO sowie § 7 MBO der Bundeszahnärztekammer i.V.m. der entsprechenden Regelung in der jeweiligen Berufsordnung der Landeszahnärztekammer, vgl. auch hierzu Kommentar zur Muster-Berufsordnung der Bundeszahnärztekammer). Die Berufsaufsicht obliegt den zuständigen Zahnärztekammern.

7.3 Schweigepflicht gem. § 203 StGB, Verletzung von Privatgeheimnissen

§ 203 StGB stellt die Verletzung von Privatgeheimnissen durch Zahnärzte und Angehörige anderer Berufsgruppen, die in einem besonderen Vertrauensverhältnis zum Patienten stehen, unter Strafe. Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ein Patientengeheimnis, das ihm aufgrund seiner Stellung anvertraut oder sonst bekannt geworden ist, unbefugt offenbart. § 203 StGB hat einige Änderungen erfahren, die zum 09.11.2017 in Kraft getreten sind. Dadurch sind offene Rechtsfragen durch den Gesetzgeber geklärt worden.

7.3.1 Straftatbestand

Zahnärzte sind bei ihrer beruflichen Tätigkeit auf die berufliche Hilfeleistung anderer Personen angewiesen. Je nach Art der Tätigkeit haben diese auch die Möglichkeit, von den geschützten Geheimnissen Kenntnis zu erlangen. Als Beispiele können hier das zahnärztliche Praxispersonal oder der externe IT-Dienstleister genannt werden.

Soweit diese Tätigkeiten durch das angestellte Personal des Zahnarztes wahrgenommen werden, liegt kein Offenbaren des Geheimnisses vor, § 203 Absatz 3 Satz 1 StGB. Das eigene Personal ist der Sphäre des Zahnarztes zuzuordnen, so dass keine für das Offenbaren erforderliche „Hinausgabe von Tatsachen aus dem Kreis des Wissenden oder der zum Wissen Berufenen“ erfolgte. Angestellte Praxismitarbeiter sind berufsmäßig tätige Gehilfen.

Wenn durch den Zahnarzt fremde Geheimnisse gegenüber sonstigen Personen offenbart werden, die an seiner beruflichen oder dienstlichen Tätigkeit mitwirken und soweit dies (gemeint ist die Offenbarung) für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist, liegt nach neuer Gesetzeslage ein befugtes Offenbaren und damit keine strafbare Handlung vor. Es ist deshalb nunmehr rechtssicher möglich, beispielsweise einen externen IT-Dienstleister für die Wartung der EDV/IT zu beauftragen, ohne in die Gefahr der eigenen Strafbarkeit zu kommen. Allerdings besteht hierbei die Verpflichtung, den sonstigen mitwirkenden Personenkreis zur Geheimhaltung zu verpflichten. Trägt der Zahnarzt dafür die Sorge nicht und die sonstige mitwirkende Person offenbart unbefugt ein Geheimnis, macht er sich fortan selbst strafbar, § 203 Absatz 4 Nummer 1 StGB. Zugleich ist strafbar, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person bekannt geworden ist.

Werden weitere Zahnärzte/Ärzte in die konkrete Behandlung eines Patienten miteinbezogen (Bsp: Überweisung an MKG-Chirurgen), ist dies regelmäßig strafrechtlich unbedenklich. Will der Patient hingegen seinen „Hauszahnarzt“ wech-

seln und der neue Zahnarzt fragt nach den bisherigen Behandlungsdaten, ist eine Weitergabe regelmäßig nur mit einer Entbindung der Schweigepflicht bzw. einer Einwilligung des Patienten möglich.

7.3.2 Entbindung von der Schweigepflicht

Der Zahnarzt ist zur Offenbarung auch befugt, soweit er von dem Betroffenen oder seinem gesetzlichen Vertreter von der Schweigepflicht entbunden wurde oder soweit das Offenbaren zum Schutze eines höheren Rechtsgutes erforderlich ist. Gesetzliche Aussage- und Anzeigepflichten bleiben davon unberührt. Die Verschwiegenheitspflicht gilt für alle in der Praxis tätigen Personen, die hierüber nachweislich zu belehren sind.

Der Zahnarzt ist nicht an die Schweigepflicht gebunden, wenn und soweit ihn der Patient davon ausdrücklich entbunden hat. Ob eine durch schlüssiges Verhalten erfolgte Schweigepflichtentbindung zukünftig ebenfalls ausreichen wird, ist in Anbetracht der Tatsache, dass das Datenschutzrecht (siehe dazu Kapitel 8.3, S. 34) eine konkludente Einwilligung jedenfalls in die Weitergabe von Gesundheitsdaten nicht mehr ausreichen lässt, zumindest zweifelhaft. Aus Gründen der Beweissicherung und der dem Zahnarzt obliegenden Nachweisführungspflicht nach dem Datenschutzrecht empfiehlt sich daher eine schriftliche Entbindungserklärung des Patienten einzuholen. Auch Minderjährige und psychisch Kranke können wirksam einwilligen, wenn und soweit sie über die erforderliche Einsichtsfähigkeit im Einzelfall verfügen.

Der Zahnarzt ist zur Offenbarung von Patientendaten des Weiteren befugt, wenn und soweit diese von der sogenannten mutmaßlichen Einwilligung des Patienten gedeckt ist. Ein solcher Fall kann zum Beispiel vorliegen, wenn der Patient bewusstlos, nicht erreichbar oder verstorben ist und der Zahnarzt aufgrund der gegebenen Umstände, bestimmter Anhaltspunkte, im Interesse des Patienten von dessen Einverständnis ausgehen kann.

Gestattet ist auch die Weitergabe von Patientengeheimnissen in rechtfertigenden Situationen des Notstands. Ein solcher liegt nur vor, wenn die Offenbarung von Patientengeheimnissen zur Abwendung gegenwärtiger ernstlicher Gefahren für Leib oder Leben oder ähnlich gewichtiger Rechtsgüter erforderlich ist und die Gefährdung nicht auf andere Weise abgewendet werden kann (Güterabwägungsprinzip). Die Rechtsprechung verlangt daher immer, dass der Offenbarung ein (erfolgloser) Versuch des Zahnarztes vorausgeht, den Patienten dazu zu bewegen, selbst entsprechend tätig zu werden beziehungsweise bestimmte Handlungen zu unterlassen. Beispiel: Hinweise auf Misshandlung oder entwürdigende Behandlung (Verletzungen im Mund- oder Gesichtsbereich) von Kindern durch Eltern kann die Offenbarung gegenüber Dritten (Jugendamt oder Polizei) rechtfertigen. Kein höherrangiges Rechtsgut stellt dagegen das alleinige Strafverfolgungsinteresse des Staates dar.

Eine Offenbarung von Patientendaten zur Wahrnehmung eigener berechtigter Interessen kann im Einzelfall zulässig sein, soweit die Offenbarung der Patientendaten im Verhältnis zur eigenen Interessenswahrnehmung als angemessenes Mittel angesehen werden kann, zum Beispiel bei Regressverfahren oder Schadenersatzklagen. Die Wahrnehmung eigener berechtigter Interessen liegt auch vor, wenn ein Zahnarzt einem Patienten selbst, also ohne Einschaltung einer privatärztlichen Verrechnungsstelle, ärztliche oder zahnärztliche Leistungen in Rechnung gestellt hat und diese Forderung nach erfolgloser schriftlicher Mahnung einem Rechtsanwalt oder einem Inkassobüro zur Eintreibung übergibt. Der Zahnarzt sollte bei der Mahnung deutlich auf

diese Folge der Nichtzahlung der Forderung hinweisen. Eine Datenübermittlung ohne Einwilligung ist aber nicht zulässig, wenn der Zahnarzt zum Einzug der Forderung diese an Dritte (Inkassobüro etc.) abtritt.

7.3.3 Anforderungen an den Schutz der Patientendaten und der (zahn)ärztlichen Schweigepflicht bei der Behandlung in Pflegeheimen

In der „Pflegeheimsituation" gelten prinzipiell dieselben Anforderungen an den Schutz der Patientendaten und an die (zahn)ärztliche Schweigepflicht wie in der normalen „Praxissituation".

Daraus folgt, dass der Zahnarzt diese Pflichten allgemein und daher auch bei der Beratung, Untersuchung und Behandlung von Patienten in Pflegeheimen zu beachten hat. Eine gesonderte gesetzliche Erlaubnis für diese spezielle Behandlungssituation gibt es nicht. Daher sollte beispielsweise darauf geachtet werden, dass die dortige Beratung, Untersuchung oder Behandlung organisatorisch nach Möglichkeit so gestaltet wird, dass auch hier Dritte keine Möglichkeit zur Kenntnisnahme der Patientendaten erhalten. Zahnmedizinische Behandlungen sollten daher idealerweise in abgetrennten Räumlichkeiten oder Einzelzimmern erfolgen. Ferner sollten Zahnärzte und zahnmedizinisches Personal gegenüber anderen Heimbewohnern oder deren Angehörigen oder sonstigen Heimbesuchern auf Verschwiegenheit achten. Beispielsweise sollten insoweit allgemein wahrnehmbare Zurufe von Patientendaten unterlassen werden.

7.3.4 Schweigepflicht in strafrechtlichen Verfahren

Bei strafrechtlichen Ermittlungsverfahren gegen einen Zahnarzt dürfen Patientenunterlagen, die als Beweismittel von Bedeutung sein können, beschlagnahmt werden, wenn der Zahnarzt sie nicht freiwillig herausgibt. Die Beschlagnahme muss, außer wenn Gefahr im Verzug ist, ein Richter anordnen, der im Einzelfall das Interesse an der Wahrheitsermittlung mit dem Verschwiegenheits- und Datenschutzinteresse des Patienten abzuwägen hat. Die Beschlagnahmeanordnung kann je nach Ermittlungsgegenstand einzelne Patientenunterlagen, bestimmte Fall-/Abrechnungskonstellationen oder die gesamten Patientenakten umfassen.

Ist dagegen der Patient der Beschuldigte oder das Opfer einer Straftat, hat der Zahnarzt ein Zeugnisverweigerungsrecht. Er darf Unterlagen nicht herausgeben, soweit und solange der Patient ihn nicht von der Schweigepflicht entbindet. Das Zeugnisverweigerungsrecht des Zahnarztes gemäß § 53 Strafprozessordnung (StPO) und das Beschlagnahmeverbot der Patientenakten (§ 97 StPO) sind Ausfluss der zahnärztlichen Schweigepflicht. Das Zeugnis- bzw. Auskunftsverweigerungsrecht des Zahnarztes wird jedoch durch die Regelungen des Bundeskriminalamtgesetzes (BKA-G) eingeschränkt. Danach sind Zahnärzte zur Offenbarung von Berufsgeheimnissen verpflichtet, wenn dies zur Terrorismusbekämpfung erforderlich ist.

In diesem Zusammenhang bleibt auch festzuhalten, dass die Befugnisse der Datenschutzbehörden gegenüber Zahnärzten wie auch gegenüber den anderen in § 203 Absatz 1 StGB genannten Berufsgeheimnisträgern eingeschränkt sind. Die Datenschutzbehörden dürfen weder Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, noch Zugang zu den Geschäftsräumen, ein-

schließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters verlangen, soweit dies zu einem Verstoß gegen die Geheimhaltungspflichten des Zahnarztes führen würde.

8.0 Datenschutzrechtliche Grundlagen

Zu beachten ist, dass die Regelungen der EU-DSGVO und des neuen BDSG erst ab dem 25.05.2018 unmittelbar anwendbar sind. Bis zu diesem Zeitpunkt besteht die aktuelle Rechtslage unverändert fort.

Das neue Datenschutzrecht gilt auch für die Zahnarztpraxis. Der Zahnarzt, das Praxispersonal aber auch weitere an der Tätigkeit des Zahnarztes mitwirkenden Personen, die nicht der unmittelbaren Sphäre des Zahnarztes angehören (z. B. externe IT-Dienstleister), sind deshalb verpflichtet, die Vorschriften der EU-DSGVO und des BDSG zu beachten. Neben den bekannten Organisationspflichten muss die Zahnarztpraxis nunmehr jederzeit nachweisen können, dass sie bei der Verarbeitung personenbezogener Daten sowohl die in der Verordnung verankerten Datenschutzgrundsätze als auch die technisch-organisatorischen Anforderungen einhalten. Es wird bereits deshalb dazu geraten, ein risikoangemessenes Datenschutz-Managementsystem in der Zahnarztpraxis zu führen bzw. einzuführen, das insbesondere folgende Punkte berücksichtigt:

Erfassen aller datenschutzrelevanten Vorgänge samt ihrer jeweiligen Datenschutzrisiken

Dokumentation der relevanten Verarbeitungsvorgänge, Verstöße, Maßnahmen etc.

Implementierung interner Datenschutz- und IT-Sicherheitsrichtlinien (Kontrolle, Optimierung, regelmäßige Datenschutzschulungen der Mitarbeiter)

Der Datenschutz ergänzt die Regelungen zur (zahn)ärztlichen Schweigepflicht, die sich aus dem Berufs- und Strafrecht ergeben (vgl. dazu unter Kapitel 7.0, S. 27 ff.).

8.1 Wichtige datenschutzrechtliche Begriffe

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Bei „Gesundheitsdaten“ handelt es sich um eine besondere Kategorie von personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Der Begriff der „Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Eine „Einwilligung“ der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

„Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Weitere Begriffsdefinitionen finden sich in Art. 4 EU-DSGVO sowie in § 2 BDSG.

8.2 Datenverarbeitung in der Zahnarztpraxis

In der Zahnarztpraxis werden regelmäßig die unterschiedlichsten Daten verarbeitet. Der Zahnarzt ist verpflichtet, eine Patientenakte zu führen, in der sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse aufzuzeichnen sind. Da es sich dabei regelmäßig um Gesundheitsdaten handelt, verarbeitet der Zahnarzt eben genau diese mit jeder zahnärztlichen Behandlung. Insbesondere wegen des Zusammenhangs zur Abrechnung der zahnärztlichen Leistungen bzw. des Rechts der gesetzlichen Krankenversicherung stehen die Patientendaten auch in engem Bezug zu den Sozialdaten. Der Zahnarzt verarbeitet aber auch im weiteren Geschäftsbetrieb regelmäßig personenbezogene Daten, wie z.B. in der Buchhaltung. Regelmäßig bestehen zudem vertragliche Beziehungen zu Dritten, wie z.B. Lieferanten, Dentallaboren Reinigungsfirmen, Software- oder Abrechnungsfirmen etc., die mit einer Verarbeitung von personenbezogenen Daten einhergehen. Auch beschäftigt eine Praxis regelmäßig Mitarbeiter, so dass im Rahmen der zu Grunde liegenden Arbeitsverhältnisse Beschäftigtendaten beispielsweise bei der Lohnbuchhaltung verarbeitet werden. Ganz überwiegend ist die Verarbeitung der unterschiedlichen Daten bereits gesetzlich erlaubt und bedarf daher keiner ausdrücklichen Einwilligung durch die betroffene Person.

8.2.1 Verarbeitung von personenbezogenen Daten

Eine Verarbeitung personenbezogener Daten ist nach Art. 6 EU-DSGVO rechtmäßig, wenn eine der dort genannten Bedingungen erfüllt ist. Neben der Einwilligung sind für die Zahnarztpraxis insbesondere folgende weitere Bedingungen für eine rechtmäßige Verarbeitung von personenbezogenen Daten relevant:

- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich,
- die Verarbeitung erfolgt auf Anfrage der betroffenen Person;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.

8.2.2 Verarbeitung von Beschäftigtendaten

Bei der Verarbeitung von Beschäftigtendaten ist Art. 88 EU-DSGVO und § 26 BDSG zu berücksichtigen. Danach dürfen grundsätzlich personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnis-

ses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zu beachten ist, dass in § 26 Absatz 2 BDSG besondere Anforderungen an die Freiwilligkeit der Einwilligung (siehe dazu Kapitel 8.3, S. 34) gestellt werden, sofern die Verarbeitung auf einer Einwilligung beruht.

8.2.3 Verarbeitung von Gesundheitsdaten

Unter den Voraussetzungen des Art. 9 EU-DSGVO i.V.m. § 22 BDSG ist eine Verarbeitung von Gesundheitsdaten zulässig. Hervorzuheben ist die zulässige Verarbeitung, die für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von (zahn-)ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden. In diesen Fällen ist die Verarbeitung auch ohne Einwilligung des Patienten zulässig.

8.2.4 Verarbeitung von Sozialdaten nach SGB V

Die Verarbeitung von Daten, die zur Abrechnung der zahnärztlichen Leistungen bzw. aus dem Recht der gesetzlichen Krankenversicherung folgen, richtet sich nach den besonderen Datenschutzregelungen im SGB I, SGB V und SGB X.

Die Grundnorm der Datenschutzregelungen stellt § 35 Abs. 1 SGB I dar, der einen Anspruch auf Wahrung des Sozialgeheimnisses für jedermann und damit auch für die Patienten konstituiert. Sonderregelungen zu Teilbereichen finden sich in den §§ 284 – 305 b SGB V (Grundsätze der Datenverwendung in der GKV bzgl. der Versicherungs- und Leistungsdaten). Die Vorschriften der Sozialgesetzbücher regeln im Wesentlichen die Grundsätze für die Erhebung, Verarbeitung und Nutzung überwiegend administrativer Daten, nicht jedoch die speziellen Voraussetzungen für die Zulässigkeit der Verarbeitung von Patientendaten sowie Krankheitsbildern der Patienten. Für diesen Bereich ist – wie zuvor geschildert - auf die EU-DSGVO und das BDSG zu verweisen.

Es sind bereits einige Regelungen aus dem SGB I und X an die EU-DSGVO angepasst worden. Weiterhin gibt es Informationen dazu, dass der deutsche Gesetzgeber Anpassungen insbesondere im SGB V vornehmen wird.

8.2.5 Datenschutzfolgenabschätzung

Das Datenschutzrecht sieht unter den Voraussetzungen des Art. 35 EU-DSGVO eine Pflicht zur Durchführung einer Datenschutzfolgenabschätzung vor. Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss der Verantwortliche in der Zahnarztpraxis vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Diese Pflicht besteht insbesondere bei Praxen, die eine umfangreiche Verarbeitung von Gesundheitsdaten durchführen (siehe dazu Kapitel 8.4, S. 35).

8.3 Die Einwilligung in die Datenverarbeitung

Auch in der Zahnarztpraxis kann es notwendig sein, eine Einwilligung für eine Datenverarbeitung einzuholen. Beispielsweise kann eine Abrechnung der erbrachten zahnärztlichen Leistung durch einen Dritten u. a. nur mit einer entsprechenden Einwilligung des Patienten erfolgen. Gerade vorformulierte Einwilligungserklärungen können Ungenauigkeiten aufweisen, denn eine rechtmäßige Einwilligung ist nach Art. 7 EU-DSGVO an bestimmte Voraussetzungen geknüpft. Eine Einwilligung in die Verarbeitung von Daten muss danach grundsätzlich

- durch eine eindeutige bestätigende Handlung,
- freiwillig,
- für einen konkreten Fall,
- bezogen auf einen oder mehrere bestimmte Zwecken,
- bezogen auf die bestimmte Verarbeitung,
- in informierter und verständlicher Weise,
- in Kenntnis der Tatsache, dass die Einwilligung jederzeit widerrufen werden kann,

erfolgen.

Eine in der Praxis genutzte vorformulierte Einwilligung sollte vom verantwortlichen Zahnarzt in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache gefasst sein und keine missbräuchlichen Klauseln beinhalten. Dies gilt erst Recht, wenn von einer schriftlichen Einwilligungserklärung mehrere Sachverhalte erfasst sind oder werden sollen. Diese müssen für die einwilligende Person klar voneinander unterscheidbar sein. Damit die betroffene Person in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte sie mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Eine Einwilligung erfolgt nur dann freiwillig, wenn eine echte oder freie Wahl bestanden hat und die betroffene Person in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Daher ist eine datenschutzrechtliche Einwilligung, die etwa die zahnärztliche Behandlung von der Einwilligung abhängig macht, kritisch zu betrachten und nicht zu empfehlen, vgl. auch Art. 7 Abs. 4 EU-DSGVO.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

Die betroffene Person ist vor Abgabe der Einwilligung davon in Kenntnis zu setzen, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen (vgl. Art. 7 Abs. 3 EU-DSGVO). Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung jedoch nicht berührt.

Der verantwortliche Zahnarzt muss im Streitfalle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten rechtmäßig eingewilligt hat. Es sind daher schriftliche Einwilligungserklärungen vorzugswürdig, obwohl das Recht auch elektronisch abgegebene oder mündliche Einwilligungen als ausreichend erachtet. Da eine Einwilligung durch eine eindeutige bestätigende Handlung erfolgen muss, kann eine Einwilligung etwa durch schlüssiges Verhalten wegen möglicher Mehrdeutigkeit regelmäßig nicht angenommen, bei Gesundheitsdaten wegen der Formulierung in Art. 9 Absatz 2 a) EU-DSGVO („ausdrücklich“) sogar ganz ausgeschlossen werden. Es ist deshalb auch anzunehmen, dass die bisherige Rechtsprechung fortbestehen wird. Diese verlangt, dass sich eine Einwilligung in die Verarbeitung von Gesundheitsdaten auch ausdrücklich auf diese beziehen

muss. Teile einer Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen die EU-DSGVO darstellen. Blanko-Einwilligungen sind unzulässig.

Innerhalb der Praxis sollte für eine sachgerechte Dokumentation der Einwilligungen Sorge getragen werden. Bereits vorliegende Einwilligungen sollten überprüft werden, ob diese auch unter der EU-DSGVO wirksam bleiben oder nach Maßgabe des neuen Rechts nochmals einzuholen sind. Voraussetzung für ein Fortwirken soll sein, dass die „Art der bereits erteilten Einwilligung" den Bedingungen der EU-DSGVO entspricht. Anzunehmen sein dürfte daher, dass eine Vielzahl von bisher rechtmäßigen Einwilligungen in der Zahnarztpraxis auch weiterhin rechtmäßig sein dürften. Die EU-DSGVO sieht schließlich kein Verwirken von Einwilligungen vor. Empfohlen wird derzeit als „Best Practice", dass Einwilligungen „regelmäßig" aufgefrischt werden sollten.

Die Verarbeitung von Gesundheitsdaten ist schließlich ohne Einwilligung erlaubt, wenn sie zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist und die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben.

8.4 Datenschutzbeauftragter

Die Rolle des Datenschutzbeauftragten als zentrale Anlaufstelle für Betroffene, Verantwortliche, Auftragsverarbeiter und Aufsichtsbehörden ist durch die EU-DSGVO gestärkt worden. Sie ist zugleich Ausdruck des in Art. 5 EU-DSGVO verankerten datenschutzrechtlichen Transparenzgrundsatzes.

8.4.1 Pflicht zur Benennung eines Datenschutzbeauftragten

Für Praxisformen besteht in der Regel nach § 38 BDSG i.V.m. Art. 37 EU-DSGVO eine Pflicht zur Benennung eines Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Ob in einer Praxis diese geforderte Mindestanzahl von Beschäftigten tatsächlich erreicht und damit die Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht, kann unter Zuhilfenahme der folgenden Kriterien herausgefunden werden.

Bei der Ermittlung der Personenanzahl kommt es allein auf die tatsächliche Anzahl der tätigen Personen an. Die Art der Beschäftigung (z. B. Voll- oder Teilzeit, Auszubildende, Praktikanten, Leiharbeit) ist hierfür unerheblich. Vereinfacht gesagt sind "Köpfe" zu zählen. Die Anzahl von mindestens zehn Beschäftigten, die auf Dauer personenbezogene Daten automatisiert verarbeiten, muss „in der Regel" gegeben sein. Vorübergehende Änderungen (Überschreitungen oder Unterschreitungen) des Personalbestands sind daher unschädlich. Ausgenommen werden können deshalb Personen, die nur zufällig im Rahmen der Erledigung anderer Aufgaben mit der Verarbeitung personenbezogener Daten zu tun haben (z. B. Wartungstechniker; kurzfristiger Entlastungsassistent; Mitarbeiter eines externen Dentallabors). Die automatisierte Verarbeitung personenbezogener Daten muss aber nicht Hauptaufgabe der beschäftigten Person sein, um „ständig" zur Personenanzahl hinzugezählt werden zu müssen. Auf den Anteil bzw. Umfang der Verarbeitung an der gesamten Arbeit kommt es nicht an. Mitarbeiter sollten daher auch berücksichtigt werden, die über einen PC-Arbeitsplatz oder PC-Zugang verfügen. Für eine „ständige" Beschäftigung müssen die Mitarbeiter ihre Aufgaben auf unbestimmte bzw. längere Zeit ausüben, d. h. immer, wenn sie anfällt.

Wann dies im Einzelnen der Fall sein wird, hängt von den konkreten Umständen in der Zahnarztpraxis ab. Eine automatisierte Verarbeitung liegt vor, wenn die Verarbeitung mit Hilfe von Datenverarbeitungsanlagen, also in der Regel mit Computern, erfolgt.

Sind in der Regel in der Praxis weniger als 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, ist auch weiterhin kein Datenschutzbeauftragter zu bestellen. Sofern andere Auffassungen vertreten werden, ist dem entgegenzuhalten, dass eine Verpflichtung zur Benennung eines Datenschutzbeauftragten auch unterhalb der 10-Personen-Regel nur dann besteht, wenn der Verantwortliche Verarbeitungen vornimmt, die einer Datenschutz-Folgenabschätzung nach Art. 35 EU-DSGVO unterliegen. Dies ergibt sich aus § 38 Abs. 1 Satz 2 BDSG. Der Bundesgesetzgeber hat jedoch mit seiner Festlegung, einen Datenschutzbeauftragten verpflichtend erst ab einer Personenzahl von mindestens 10 Personen benennen zu müssen, nicht nur von der Möglichkeit Gebrauch gemacht, von der EU-DSGVO abzuweichen, sondern zugleich die Wertung getroffen, dass eine umfangreiche Datenverarbeitung i.S.d. Art. 37 Satz 1 Ziffer c) EU-DSGVO regelmäßig erst mit der Personenanzahl von 10 Personen einhergehen dürfte. In der Begründung des Regierungsentwurfs finden sich zu § 38 Abs. 1 Satz 2 BDSG zudem keine anderslautenden Ausführungen (BT-Drucksache 18-11325 vom 24.2.2017, S.107), sodass davon auszugehen ist, dass der Gesetzgeber es schlicht bei der bisherigen Rechtslage belassen wollte und mit dem Verweis auf Art. 35 EU-DSGVO keine Ausweitung der Benennungspflicht beabsichtigt gewesen ist. Auch schränkt der Erwägungsgrund 91 der EU-DSGVO das Kriterium der „umfangreichen“ Datenverarbeitung dahingehend ein, dass „die Verarbeitung personenbezogener Daten nicht als umfangreich gelten sollte, wenn die Verarbeitung personenbezogene Daten von Patienten ... betrifft und durch einen einzelnen Arzt, ... erfolgt.“ Auch hier lässt sich die gesetzgeberische Wertung schlussfolgern, dass erst ab einer Beschäftigungsgröße von 10 Personen von einer umfangreichen Datenverarbeitung auszugehen sein wird. Denn Sinn und Zweck ist es gewesen, dass eine „umfangreiche" Datenverarbeitung erst dann gegeben ist, wenn die Verarbeitung von Gesundheitsdaten das übliche Maß bei Weitem übersteigt. So dient die 10-Personen-Regel in diesem Sinne schließlich auch der Rechtssicherheit.

8.4.2 Benennung eines Datenschutzbeauftragten

Die Benennung eines Datenschutzbeauftragten sollte unverzüglich erfolgen, sobald die Pflicht zur Benennung besteht. Freiwillig kann ein Datenschutzbeauftragter jederzeit benannt werden. Der Wortlaut der EU-DSGVO und des BDSG spricht nur noch von einer Benennung des Datenschutzbeauftragten. Eine schriftliche Bestellung, entsprechend den Bestimmungen des alten BDSG, ist ab dem 25.05.2018 daher nicht mehr erforderlich. Gleichwohl empfiehlt es sich aus Gründen der Rechtssicherheit und der deutlich gestiegenen Nachweispflichten, die Benennung zum Datenschutzbeauftragten in geeigneter Form zu dokumentieren und die wesentlichen Aufgaben des Datenschutzbeauftragten festzuhalten, wie z.B. Zeitpunkt der Wirksamkeit der Benennung, die übernommenen gesetzlichen und gegebenenfalls zusätzlich vertraglich vereinbarten Aufgaben, das zur Verfügung gestellte Zeitkontingent, die zur Verfügung gestellten Ressourcen. Bereits bestehende Bestellungsurkunden sind ggf. auf Konformität mit dem neuen Recht zu überprüfen und ggf. anzupassen.

Als Datenschutzbeauftragter kommen Mitarbeiter der Praxis in Betracht. Ebenso ist aber eine externe Lösung durch einen entsprechenden Dienstleistungsanbieter möglich. Welche Variante vorzugswürdig ist, hängt nicht zuletzt von den konkreten Umständen in der Zahnarztpraxis

ab. Die Tätigkeit des Datenschutzbeauftragten darf jedenfalls in keinem Interessenkonflikt mit der eigentlichen Tätigkeit in der Zahnarztpraxis stehen. Dies führt regelmäßig dazu, dass weder der Praxisinhaber noch der IT-Verantwortliche der Praxis gleichzeitig Datenschutzbeauftragter sein können.

Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde, der jeweiligen Landesdatenschutzbehörde, mitzuteilen. Dabei bietet es sich an, die Kontaktmöglichkeiten sowohl innerhalb der Zahnarztpraxis (z. B. per E-Mail, Informationsrundschreiben, Intranet, Organigramm oder Aushang) als auch für Patienten (z. B. Webseite, Kundeninformation) hinreichend zu kommunizieren. Hierzu wird empfohlen, eine postalische Adresse sowie eine entsprechend gewidmete E-Mail-Adresse und Telefonnummer anzugeben. Nicht zwingend ist demgegenüber die Veröffentlichung oder Mitteilung des Namens des Datenschutzbeauftragten. Gleichwohl wird die Bekanntgabe des Namens gegenüber der Aufsichtsbehörde und den Beschäftigten vom unabhängigen Beratungsgremium der Europäischen Kommission empfohlen.

Soweit ein betrieblicher Datenschutzbeauftragter aufgrund der Mitarbeiterzahl nicht zu bestellen ist und tatsächlich auch nicht bestellt wurde, obliegen dessen Aufgaben unmittelbar der Praxisleitung.

8.4.3 Qualifikation des Datenschutzbeauftragten

Der Datenschutzbeauftragte wird nach Art. 37 Abs. 5 EU-DSGVO aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die Aufgaben gemäß Art. 39 EU-DSGVO zu erfüllen, benannt. Das Maß des erforderlichen Fachwissens bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung in der Zahnarztpraxis und dem Schutzbedarf der personenbezogenen Daten, die die Praxis erhebt und verwendet. Der Datenschutzbeauftragte sollte allgemeine Kenntnisse über die Arbeitsabläufe sowie Kenntnisse über die Datenverarbeitung in der Praxis haben. Er muss die gesetzlichen Regelungen kennen und anwenden können. Die erforderlichen Qualifikationsanforderungen können insbesondere durch den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung erlangt sein. Um eventuell zu Beginn der Bestellung noch bestehende Informationsdefizite auszugleichen, empfiehlt sich der Besuch von geeigneten Fortbildungsveranstaltungen. Der Besuch solcher Veranstaltungen ist auch nach der Bestellung angezeigt, um auf dem aktuellen, erforderlichen Informationsstand zu bleiben, und um sich Kenntnisse über die sich ändernden rechtlichen und technischen Entwicklungen anzueignen. Zu den persönlichen Eigenschaften sollten beispielsweise Integrität und ein ausgeprägtes Berufsethos zählen.

8.4.4 Aufgaben des Datenschutzbeauftragten

Dem Datenschutzbeauftragten obliegen nach Art. 39 EU-DSGVO zumindest folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten aus dem geltenden Datenschutzrecht

- Überwachung der Einhaltung der rechtlichen Bestimmungen sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den

Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen

- Auf Anfrage Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 EU-DSGVO
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 EU-DSGVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der EU-DSGVO im Zusammenhang stehenden Fragen.

8.4.5 Stellung des Datenschutzbeauftragten

Nach Art. 38 der EU-DSGVO ist in der Zahnarztpraxis dafür Sorge zu tragen, dass der Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“ wird. Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben zu unterstützen, indem ihm die für die Erfüllung der Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung gestellt werden. Es muss sichergestellt werden, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der Praxisleitung.

Ist der Datenschutzbeauftragte gleichzeitig Arbeitnehmer, so genießt er Kündigungsschutz. Die Abberufung des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 BGB zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass der Arbeitgeber zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

Der Datenschutzbeauftragte ist zur Verschwiegenheit verpflichtet und bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden. Er genießt unter den Voraussetzungen des § 38 Abs. 2, i.V.m. § 6 Abs. 6 BDSG ein Zeugnisverweigerungsrecht.

8.5 Verzeichnis von Verarbeitungstätigkeiten

Jeder Zahnarzt ist nach Art. 30 EU-DSGVO verpflichtet ein Verzeichnis aller in seinen Zuständigkeitsbereich fallenden Verarbeitungstätigkeiten mit personenbezogenen Daten zu erstellen und zu führen. Art. 30 EU-DSGVO ersetzt die bisher nach dem alten Datenschutzrecht als Verfahrensverzeichnis, Verfahrensbeschreibung oder Dateibeschreibung bekannten Dokumentationspflichten. Der Aufsichtsbehörde müssen die Verzeichnisse der Verarbeitungstätigkeiten auf Verlangen zur Verfügung gestellt werden. Ordnungswidrig handelt zukünftig, wer vorsätzlich oder fahrlässig entgegen Art. 30 Absatz 1 EU-DSGVO ein Auskunftsverlangen der Aufsichtsbehörde nicht richtig behandelt. Zum Nachweis der Einhaltung dieser Verordnung sollte der Ver-

antwortliche in der Zahnarztpraxis deshalb ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen.

Als Verfahren gelten beispielsweise:

- (elektronische) Patientenakten;
- (Zahn-)arztinformationssysteme;
- elektronische Diktier- und Spracherkennungsprogramme;
- Buchhaltungssoftware;
- Software zur Versendung und Verwaltung von E-Mails;
- Adressdatenbanken;
- Software zur Terminverwaltung;
- (elektronische) Personalakten.

Für die Verzeichnisse von Verarbeitungstätigkeiten ist keine bestimmte Form vorgeschrieben. Sie können als Word- oder Exceldatei geführt werden und müssen folgende Angaben enthalten:

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls erforderlich);
- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten);
- die Art der verarbeiteten Daten;
- die möglichen Empfänger der Daten, an die Daten übermittelt werden (z. B. Kassenzahnärztliche Vereinigungen, Krankenkassen, Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- wenn möglich, Löschfristen;
- wenn möglich, technische und organisatorische Maßnahmen der Datensicherheit gem. Art. 32 EU-DSGVO

Die Erstellung der Verzeichnisse kann ein mühsamer Prozess sein, da es meist gar nicht so einfach ist, den Überblick darüber zu gewinnen, welche Datenverarbeitungsprozesse es in der Praxis gibt. Dies gilt umso mehr, wenn Zahnärzte und Mitarbeiter beruflich Smartphones, Tablets und Laptops nutzen. Auch Programme auf derartigen Endgeräten können als Verarbeitungstätigkeit i.S.d. Art. 30 EU-DSGVO zählen, für die die Pflicht zur Führung eines entsprechenden Verzeichnisses gilt. Wenn erstmalig Verzeichnisse von Verarbeitungstätigkeiten angelegt werden, ist dies nach aller Erfahrung mit einem hilfreichen Klärungsprozess verbunden. Denn stets sind die Verarbeitungszwecke zu definieren und die Festlegung von Löschfristen gibt Anlass, Daten nicht unüberlegt für alle Ewigkeit auf Datenträgern „verstauben“ zu lassen. Wenn Verzeichnisse von Verarbeitungstätigkeiten angelegt werden, ist dies ein guter Anlass, über die Effizienz, Nachvollziehbarkeit und Sinnhaftigkeit der eigenen Datenverwaltung nachzudenken. Dies kann nicht nur dem Schutz von Patientendaten und der Datensicherheit dienen, sondern auch der Effizienz der Arbeitsabläufe in der Praxis.

8.6 Patienteninformationen zur Datenverarbeitung

Den verantwortlichen Zahnarzt treffen nach Art. 13 und 14 EU-DSGVO umfassende Informationspflichten. Patienten und andere betroffene Personen sollen über alle relevanten Informationen der Datenverarbeitung unterrichtet werden, um eine faire und transparente Datenverarbeitung zu gewährleisten. Die Datenschutzbestimmungen auf Praxis-Websites müssen diesen Anforderungen genügen. Auch empfehlen sich allgemeine „Hinweise zur Datenverarbeitung“, die jeder Patient vor der ersten Behandlung erhalten und unterschreiben sollte. Die neuen Informationspflichten umfassen unter anderem

- den Namen und die Kontaktdaten der Praxis;
- den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten (falls vorhanden);
- die Art der verarbeiteten Daten;

- die Zwecke der Datenverarbeitung;
- die Art der Personen, deren Daten verarbeitet werden (Patienten, Beschäftigte oder Lieferanten);
- die möglichen Empfänger der Daten, an die die Daten übermittelt werden (z. B. Krankenkassen und Verrechnungsstellen);
- die Übermittlung von Daten in die USA oder in ein anderes Land außerhalb der EU (z. B. bei der Nutzung von Webmail-Diensten oder anderen Cloud-Diensten);
- Löschfristen;
- die datenschutzrechtlichen Ansprüche des Patienten (Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht, Datenübertragbarkeit);
- das Recht des Patienten auf Widerruf einer Einwilligung;
- das Recht des Patienten auf Beschwerde bei einer Datenschutzbehörde.

Die EU-DSGVO und das neue BDSG sehen zwar Ausnahmeregelungen von der Informationspflicht vor, die aber in der Zahnarztpraxis regelmäßig nicht einschlägig sein dürften. Da ein Verstoß gegen die Informationspflichten bußgeldbewehrt ist, ist anzuraten, den Informationspflichten in der Praxis beispielsweise durch allgemeine Hinweise zum Datenschutz in der Zahnarztpraxis gerecht zu werden. Die Informationen sollten in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in klarer und einfacher Sprache zur Verfügung gestellt werden. Insbesondere bei der Nutzung einer Onlineterminvergabe sind die Informationen auch auf der Praxiswebsite zu veröffentlichen. Die Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden. Innerhalb der Praxis bietet sich eine Information direkt am Empfangstresen in schriftlicher Form an. Zum Nachweis der Information ist es ratsam, diese vom Patienten gegenzeichnen zu lassen oder zumindest den erfolgten Hinweis entsprechend zu dokumentieren. Informationen nach den Art. 13 und 14 EU-DSGVO müssen zum Zeitpunkt der Erhebung von der Praxis den betroffenen Personen mitgeteilt bzw. unentgeltlich zur Verfügung gestellt werden.

8.7 Datenschutzrechte der betroffenen Personen

In den Art. 15 bis 22, 34 EU-DSGVO bzw. §§ 34 bis 37 BDSG sind weitere Rechte der betroffenen Personen geregelt. Diesen Regelungen sind die in Art. 12 EU-DSGVO festgelegten Grundsätze gemein.

Werden die Rechte der Patienten aus dem Datenschutzrecht geltend gemacht, müssen von der Zahnarztpraxis alle danach erforderlichen Informationen und Mitteilungen, die sich auf die Datenverarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache gegeben werden. Sie können schriftlich oder in anderer Form, gegebenenfalls also auch elektronisch, erfolgen. Falls vom Patienten verlangt, kann die Information auch mündlich erteilt werden, sofern die Identität des Patienten in anderer Form nachgewiesen wurde.

Werden Rechte aus den Art. 15 bis 22 EU-DSGVO geltend gemacht, ist die betroffene Person über die ergriffenen Maßnahmen grundsätzlich unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden.

Alle Mitteilungen und Maßnahmen gemäß den Art. 15 bis 22 und Art. 34 EU-DSGVO müssen grundsätzlich unentgeltlich zur Verfügung gestellt werden.

In der Praxis sollte eine Umgangsweise mit der Ausübung von Rechten von Patienten festgelegt werden, die den dargestellten Anforderungen genügt und die einer betroffenen Person die Ausübung ihrer Rechte erleichtert.

8.7.1 Anspruch auf Auskunft und Berichtigung

Jeder Patient hat nach Maßgabe des Art. 15 EU-DSGVO i.V.m. § 34 BDSG das Recht, eine Bestätigung darüber zu verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat der Patient ein Recht auf Auskunft über diese personenbezogenen Daten und u. a. auf folgende Informationen:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

Eine derartige Auskunftsfunktion sollte in der Regel die Praxis-Software von vornherein mit vorsehen. Die zu erteilende Auskunft muss für den Patienten lesbar sein, Kürzel und Schlüssel müssen also erklärt werden – entweder durch ein entsprechendes Verzeichnis oder eine eigene Langtext-Fassung als Auskunftsversion des EDV-Ausdrucks. Das Auskunftsrecht versetzt den Patienten in die Lage, unrichtige Daten zu erkennen. Er hat einen gesetzlichen Anspruch auf eine Berichtigung unrichtiger und Vervollständigung unvollständiger Daten nach Art. 16 EU-DSGVO.

8.7.2 Recht auf Löschung von Daten

Es besteht für Patienten grundsätzlich ein Recht auf Löschung ihrer Daten unter den Voraussetzungen des Art. 17 Abs. 1 EU-DSGVO. Eine damit einhergehende Pflicht zur Löschung entfällt in der Zahnarztpraxis aber regelmäßig im Hinblick auf die Patientenakte nach § 17 Absatz 3 EU-DSGVO i.V.m. § 35 Absatz 3 BDSG Ein Zahnarzt ist aus zivil- und berufsrechtlichen Gründen verpflichtet, die Patientenakte und damit die dazugehörigen Daten nach Abschluss der Behandlung aufzubewahren. Für andere Bereiche bestehen oftmals ebenfalls Aufbewahrungspflichten, die ein etwaiges Recht auf Löschen entfallen lassen. Dienen die Daten zudem zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, müssen sie ebenfalls nicht gelöscht werden. Bestehen keine entsprechenden Verpflichtungen zur Aufbewahrung mehr, müssen die Daten sodann gelöscht werden.

8.7.3 Recht auf Einschränkung der Verarbeitung und Datenübertragbarkeit; Widerspruchsrecht

Das Recht auf Einschränkung der Datenverarbeitung bzw. auf Datenübertragbarkeit („Datenportabilität“) spielt in der zahnärztlichen Praxis eine eher untergeordnete Rolle. Sie werden dennoch erwähnt, da auch diese Rechte unter die in Kapitel 8.6 (S. 39) beschriebenen Informationspflichten fallen. Die Voraussetzungen des Rechts auf Einschränkung der Datenverarbeitung sind in Art. 18 EU-DSGVO festgelegt. Regelmäßig fußt die zahnärztliche Behandlung auf einem Behandlungsvertrag, so dass man die

Annahme haben könnte, ein Recht auf Datenübertragbarkeit bestünde. Tatsächlich unterliegt der Zahnarzt aber der berufs- und zivilrechtlichen Dokumentationspflicht, so dass die Verarbeitung von Patientendaten zur Erfüllung einer rechtlichen Verpflichtung erfolgt. Für diesen Fall sieht der Erwägungsgrund 68 der EU-DSGVO gerade vor, dass ein Recht auf Datenübertragbarkeit nicht bestehen soll. Ein Widerspruchsrecht aus Art. 21 EU-DSGVO, § 36 BDSG ist ebenso wenig praxisrelevant.

8.7.4 Mitteilungspflichten

Eine Verletzung des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 EU-DSGVO ist vom Verantwortlichen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der zuständigen Datenschutzbehörde mitzuteilen. Dies gilt nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Der Verantwortliche teilt allen Empfängern, denen personenbezogene Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Art. 16, Art. 17 Absatz 1 und Art. 18 EU-DSGVO mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

8.8 Datenverarbeitung im Auftrag/ „Outsourcing“

Aus organisatorischen, verwaltungstechnischen aber auch aus wirtschaftlichen Gründen kann die Auslagerung von bestimmten Aufgaben wie Rechnungsstellung, IT-Wartung, Archivierung, Aktenvernichtung usw. auf spezialisierte Personen / Dienstleister, die außerhalb der Sphäre des Zahnarztes tätig sind, von erheblichem Interesse sein.

Da mit einer solchen Auslagerung die Verarbeitung von Patientendaten verbunden ist, müssen beim Outsourcing nicht nur die datenschutzrechtlichen Bestimmungen, sondern auch die dem Zahnarzt obliegenden Geheimhaltungspflichten eingehalten werden. Dies gilt auch, wenn bspw. zahntechnische Leistungen durch ein gewerbliches Labor erbracht und zu diesem Zwecke personenbezogene Patientendaten an das Labor übermittelt werden. Auch ist eine Codierung der Daten (Pseudonymisierung) zu empfehlen, gegebenenfalls ist das gewerbliche Labor entsprechend zur Verschwiegenheit zu verpflichten.

Die Einschaltung von anderen Personen zur Ausführung bestimmter unterstützender Aufgaben ist im Rahmen der Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO möglich, wenn die Datenverarbeitung auf der Basis eines zwischen dem Zahnarzt als Auftraggeber und dem Auftragnehmer geschlossenen Vertrages (z. B. Geschäftsbesorgungs-, Werk- oder Dienstvertrag) erfolgt und die Verantwortung für die Verarbeitung von Patientendaten - diese erstreckt sich vor allem auf die Kontroll- und Weisungspflichten - beim Auftraggeber und damit beim Zahnarzt verbleibt. Hiervon ist regelmäßig dann auszugehen, wenn der Auftragnehmer als „verlängerter Arm“ des Auftraggebers agiert.

8.8.1 Gesetzliche Anforderungen

Eine datenschutzrechtlich zulässige Auftragsdatenverarbeitung setzt voraus, dass die datenschutzrechtlichen Vorgaben aus den Art. 28 und 29 EU-DSGVO beachtet werden.

Die Auftragsdatenverarbeitung hat auf der Grundlage einer **schriftlichen Vereinbarung** zu erfolgen, kann aber **auch auf elektronischem Wege** abgeschlossen werden (s. Art. 28 Abs. 9 EU-DSGVO).

Zu den in dem Vertrag **zu regelnden Inhalten** gehören u. a.:

Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die zu treffenden technischen und organisatorischen Maßnahmen, die Kontroll- und Weisungsrechte des Auftraggebers insbesondere in Bezug auf die Einhaltung von technischen und organisatorischen Maßnahmen sowie weitere Rechte und Pflichten der Vertragsparteien.

Der Vertrag kann entweder durch **individuellen Vertrag oder unter Nutzung von Standardvertragsklauseln** geschlossen werden (s. Art. 28 Abs. 6 EU-DSGVO).

Die Übertragung der Datenverarbeitung auf Dritte sollte der Zahnarzt jedoch aus folgenden Gründen genau abwägen:

- der Zahnarzt ist verantwortlich für die datenschutzkonforme Datenverarbeitung auch wenn die tatsächliche Datenverarbeitung durch einen Dritten erfolgt,
- Verstöße gegen datenschutzrechtliche Bestimmungen können sanktioniert werden. Je nach Einzelfall und Schwere des Verstoßes können Geldbußen in Höhe von bis zu 20 Mio. Euro oder 4 % des erzielten Jahresumsatzes, je nachdem welcher Betrag höher ist, verhängt werden.

Von der Auftragsdatenverarbeitung zu unterscheiden ist die sog. **Funktionsübertragung**. Diese liegt dann vor, wenn der Auftragnehmer über einen eigenständigen Entscheidungsspielraum verfügt und die Daten für eigene Zwecke erhebt, verarbeitet oder nutzt. In diesem Fall liegt keine Datenweitergabe zwecks Auftragsdatenverarbeitung vor, sondern eine Datenübermittlung an Dritte, die einer gesonderten Einwilligung des Patienten bedarf (siehe dazu unter Kapitel 7.3.2, S. 29).
Hierunter fallen z. B. Tätigkeiten von Inkassobüros, sofern alle Forderungen zu einem Preis gekauft werden und das Ausfallrisiko beim Dienstleister liegt.

Als Berufsgeheimnisträger hat der Zahnarzt auch die Spezialregelungen des § 203 StGB zu beachten (siehe dazu unter Kapitel 7.3, S. 28).

8.8.2 Privat(zahn-)ärztliche Verrechnungsstellen (PVS)

Während die Datenübermittlung an die KZVen auf der Basis von Rechtsvorschriften des SGB V erfolgt, ist diejenige an die Privatärztlichen Verrechnungsstellen (PVS) freiwillig.

Datenschutzrechtlich ist dies nur dann eine Auftragsdatenverarbeitung, wenn das „Outsourcing“ lediglich die Erstellung und das Versenden von Rechnungen betrifft. Regelmäßig wird der Einzug bzw. das Inkasso der Rechnungen jedoch ebenfalls durch die PVS erfolgen. In diesem Falle ist kein Raum für eine Auftragsdatenverarbeitung. Unerheblich ist dabei, welche Form des Inkassos gewählt wird. Aufgrund der vollständigen Funktionsübertragung liegt datenschutzrechtlich eine Datenübermittlung vor. Die Patienten müssen deshalb der Datenweitergabe zugestimmt haben, egal ob sie elektronisch oder „klassisch“ auf

dem Papierweg erfolgt. Aufgrund der oftmals schwierigen Abgrenzung Auftragsdatenverarbeitung/Datenübermittlung ist eine schriftliche Einwilligung in die Datenweitergabe anzuraten, wenn eine Privatzahnärztliche Abrechnungsstelle in Anspruch genommen werden soll.

Die gleiche Problematik stellt sich im Zusammenhang mit der externen Archivierung von Patientendaten (siehe dazu unter Kapitel 8.9.1, S. 46). Auch hier ist rechtlich von einer Datenübermittlung auszugehen, da ein bestimmter Aufgaben- bzw. Pflichtenbereich des Zahnarztes – die Archivierung - vollständig von einem externen Anbieter übernommen wird.

8.8.3 Cloud-Computing

Im Zuge der technischen Neuerungen ergeben sich immer wieder neue Formen der Datensicherung und -speicherung. In den letzten Jahren wurden verstärkt Angebote bezüglich Datenspeicherung, Datensicherung oder gar des virtuellen Betriebs Ihrer Anwendungen im Netz (Cloud) gemacht. Bei der Nutzung solcher **Cloud-Dienste** wird die eigene benötigte IT-Infrastruktur dabei ganz oder teilweise in eine andere, meist über das Internet erreichbare Rechnerlandschaft übertragen und dort betrieben.

Diese Risiken muss der Cloud-Nutzer sorgfältig prüfen, wenn er in Betracht zieht, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen.

Eine Hilfestellung für die Entscheidung für oder wider Cloud-Computing bietet das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebene Broschüre „Sichere Nutzung von Cloud-Diensten – Schritt für Schritt von der Strategie bis zum Vertragsende“ (abrufbar unter https://www.bsi.bund.de).
Mit der Nutzung derartiger Cloud-basierter IT-Dienste bezüglich personenbezogener Patientendaten sind derzeit allerdings eine Vielzahl rechtlicher Unsicherheiten verbunden, und zwar sowohl im Hinblick auf das Datenschutzrecht als auch die (zahn)ärztliche Schweigepflicht.

Cloud-Computing wird von der h. M. in der Rechtsliteratur und den Aufsichtsbehörden **grundsätzlich** als Unterfall der **Auftragsdatenverarbeitung** nach Art. 28 EU-DSGVO eingestuft. Es ist jedoch stark vom jeweiligen Einzelfall abhängig, ob es sich beim Cloud-Computing um eine Auftragsdatenverarbeitung oder eine **Funktionsübertragung** handelt. Im Falle einer Datenübermittlung an Dritte (in diesem Falle den Cloud-Anbieter) bedürfte es im Falle personenbezogener Daten einer gesetzlichen Übermittlungsbefugnis, deren Vorliegen aber zumindest zweifelhaft ist, oder einer schriftlichen Einwilligung sämtlicher Patienten. Letzteres ist regelmäßig mit erheblichen praktischen Problemen verbunden (siehe ergänzend hierzu Kapitel 8.3, S. 34).

Ebenso ist rechtlich ungeklärt, ob und inwieweit eine (wirksame) Verschlüsselung der Daten vor Übermittlung in die Cloud zur Folge hat, dass sie als anonyme Daten gewertet werden müssten und dadurch dem Datenschutzrecht entzogen wären.

Im Falle einer **Auftragsdatenverarbeitung** durch den Cloud-Dienstleister (z. B. in Form des Speicherns) könnte eine Datenübermittlung an diesen zwar grundsätzlich gestattet sein. Problematisch und vom Zahnarzt besonders zu prüfen sind jedoch folgende Aspekte / Fragen:

- Wo – an welchem Ort – werden die Daten verarbeitet?
- Kann ich als für die Verarbeitung der Daten verantwortliche Stelle aufgrund des virtuellen Charakters des Cloud-Computings den Kontroll- und Weisungspflichten im gebotenen Umfang nachkommen?
- Schaltet der Cloud-Anbieter bei der Erfüllung seiner Aufgaben andere Subunternehmer ein?

Angesichts der Tatsache, dass beim Cloud-Computing regelmäßig auf weltweit verstreute Server zurückgegriffen wird, ist aber bereits diese Voraussetzung für eine verantwortliche Auftragsdatenverarbeitung zweifelhaft.

Zudem sind die für eine Auftragsdatenverarbeitung an den Auftraggeber (Zahnarzt) gestellten, gesetzlichen Anforderungen praktisch kaum zu erfüllen, z. B. hinsichtlich sorgfältiger Auswahl sowie späterer Kontrolle des Diensteanbieters. Überdies steht der Auftraggeber auch weiterhin in der vollen datenschutzrechtlichen Verantwortung und er muss „Herr der Daten" bleiben.

Cloud-Anbieter nutzen aber vielfach ausländische Subunternehmer, die wiederum den Cloud-Anbietern IT-Ressourcen zur Verfügung stellen. Es ist deshalb für den Nutzer regelmäßig nur sehr schwer zu überschauen, an welchem Ort der Welt seine Daten tatsächlich gerade gespeichert und ob in die Datenverarbeitung andere von ihm nicht beauftragte Dienstleister einbezogen sind.

Der Zahnarzt hat daher genau zu prüfen, mit welchen Maßnahmen der Cloud Anbieter die datenschutzrechtlichen Risiken des Cloud-Computings absichert. Seiner Kontrollverpflichtung könnte der Zahnarzt dann genügen, wenn er entsprechende Zertifizierungen unabhängiger Stellen vorweisen kann, aus denen sich insbesondere die Einhaltung der Datensicherheit ergibt. Die Entwicklung von harmonisierten Standards für Clouds und gegenseitigen Anerkennung von nationalen Zertifikaten wird derzeit vom Bundesministerium für Wirtschaft und Energie (BMWi) mit Vertretern europäischer Cloud-Initiativen aus einigen EU-Ländern diskutiert.

Daneben stellt sich auf Grundlage eines Urteils des Bundessozialgerichts vom 10.12.2008 auch die grundsätzliche Frage, ob für die Datenweitergabe von Patientendaten durch Leistungserbringer überhaupt eine Auftragsdatenverarbeitung möglich bzw. zulässig ist, solange eine solche nicht eigens im Sozialgesetzbuch V vorgesehen ist.

Neben diesen datenschutzrechtlichen Unwägbarkeiten des Cloud-Computings ist ferner zu beachten, dass unabhängig vom Vorliegen einer Auftragsdatenverarbeitung in der Datenübertragung in die Cloud unter Umständen ein **Offenbaren eines Berufsgeheimnisses** im Sinne des § 203 StGB gesehen werden kann, der Zahnarzt somit also gegen seine **Schweigepflicht** verstoßen könnte (siehe hierzu Kapitel 7.3, S. 28).

Die Speicherung von steuerlich relevanten Daten in grenzüberschreitenden Cloud-Diensten unterliegt zudem folgenden Besonderheiten. § 146 Abs. 2 S. 1 Abgabenordnung (AO) schreibt vor, dass diese Daten grundsätzlich nur im Inland zu führen und aufzubewahren sind. Die Finanzbehörde kann zwar auf Antrag bewilligen, dass die Speicherung in einem Mitgliedstaat der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums mit Amtshilfeübereinkommen (EWR) archiviert werden können. Dies bedarf aber ebenso einer Zustimmung durch die ausländische Finanzbehörde. Zudem muss die deutsche Finanzbehörde auf die Dokumente zugreifen können. Nach § 148 AO dürfen **steuerrechtliche Unterlagen** außerhalb des EU/EWR-Raumes nach Bewilligung der Finanzbehörde nur aufbewahrt werden, wenn das Aufbewahren im Inland für den Steuerpflichtigen Härten mit sich brächte und die Besteuerung nicht beeinträchtigt wird.

Vor dem Hintergrund all dieser derzeit ungeklärten Rechtsfragen und damit verbundenen Unsicherheiten sollte der Zahnarzt sorgfältig prüfen, cloudbasierte IT-Dienste für die Speicherung oder gar sonstige Verarbeitung von Patientendaten in Anspruch zu nehmen.

8.9 Dokumentation, Archivierung und Vernichtung

8.9.1 Dokumentation und Archivierung

Für den Zahnarzt besteht eine berufsrechtliche und gesetzliche Verpflichtung zur Dokumentation, die in den Berufsordnungen der (Landes-)Zahnärztekammern bzw. § 630 f BGB konkretisiert wird. Demnach ist der Zahnarzt verpflichtet, in der Patientenakte sämtliche aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlichen Maßnahmen und deren Ergebnisse, insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen und Aufklärung für jeden Patienten getrennt zu dokumentieren.

Bei der Dokumentation der Einwilligung des Patienten bzw. dessen Aufklärung in die Behandlung bietet sich aufgrund der erheblichen Beweislastbedeutung an, bspw. auch den Namen der anwesenden ZFA zu dokumentieren. Ebenso bietet sich u. U. je nach Einzelfall an, die Einwilligung schriftlich einholen zu lassen und den Patienten die Tatsache, dass mündlich aufgeklärt wurde, gegenzeichnen zu lassen.

Die Gesamtdokumentation ist für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen (s. § 630 f Abs. 3 BGB).

Die Patientenakte kann entweder in Papierform oder elektronisch geführt werden. Berichtigungen und Änderungen von Eintragungen sind nur zulässig, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind (s. § 630 f Abs. 1 BGB).

Bei elektronischer Führung der Patientenakte muss gewährleistet sein, dass in allen Fällen, also auch bei einem Wechsel zu einem anderen Praxisverwaltungssystem die Daten nicht verloren gehen. Das Praxisverwaltungssystem muss die Nachvollziehbarkeit der Veränderung gewährleisten. Beim Einscannen von Dokumenten ist die vom BSI im April 2013 veröffentlichte und im März 2017 aktualisierte Richtlinie zum ersetzenden Scannen von Dokumenten (sog. BSI-TR-Resiscan 03138, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html) zu beachten. In dieser sind die technischen und organisatorischen Anforderungen für Scanprozesse und -produkte beschrieben, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Zahnärztliche Dokumentationen haben unabhängig davon, ob sie in Papier- oder elektronischer Form vorliegen, Urkundenqualität. Die Regelungen in §§ 630 f, 630 h Abs. 3 BGB sehen eine Dokumentation der Behandlung vor und enthalten entsprechende Beweislastregelungen. Daher ist eine Dokumentation, insbesondere der Patientenakten, zumindest auch in Papierform nach wie vor vorzugswürdig und zu empfehlen. Zum einen stellt sich bei der elektronischen Speicherung die Frage, ob bei einer nachträglichen Änderung bzw. Berichtigung einer Patientenakte der ursprüngliche Inhalt der elektronischen Akte weiterhin erkennbar bleibt, zum anderen kann ein möglicher Datenverlust zu einer Beweisnot für den Zahnarzt führen, da nicht dokumentierte Maßnahmen innerhalb einer Behandlung die Vermutung begründen, dass diese Maßnahmen tatsächlich nicht getroffen wurden. Deshalb ist auch nicht zu empfehlen, Patientenakten in Papierform nach der elektronischen Speicherung zu vernichten.

Beim Umgang mit zahnärztlichen Dokumentationen jeglicher Art sind zudem die Bestimmungen über die ärztliche Schweigepflicht und den Datenschutz zu beachten. Der Zahnarzt muss daher technisch und organisatorisch sicherstellen, dass

Unbefugte Dritte weder im Empfangsbereich noch in den Behandlungsräumen Zugriff oder Einblick in die Dokumentation oder andere Patientendaten erhalten (siehe Kapitel 2.6, S. 7).
Nach Aufgabe oder Übergabe der Praxis hat der Zahnarzt unter Beachtung der datenschutzrechtlichen Bestimmungen seine zahnärztlichen Dokumentationen aufzubewahren oder dafür Sorge zu tragen, dass sie ordnungsgemäß verwahrt werden.

Zahnärzten, denen bei einer Praxisaufgabe oder Praxisübergabe zahnärztliche Dokumentationen in Verwahrung gegeben werden, müssen diese Unterlagen getrennt von den eigenen Unterlagen unter Verschluss halten und dürfen sie nur mit Einverständnis der Patienten einsehen oder weitergeben. Hinsichtlich der Besonderheiten der papierlosen Abrechnung zwischen Zahnarztpraxis und KZV (siehe Kapitel 6.1, Nr. 3, S. 24) ist zu berücksichtigen, dass die Abrechnungsdatei ebenfalls den gesetzlichen und vertraglichen Aufbewahrungsfristen unterliegt. Im Hinblick auf die Tatsache, dass ein Papierdokument in diesen Fällen fehlt, stellt die unter 6.2 (S. 24) empfohlene elektronische Signatur eine wirksame Möglichkeit des Integritätsschutzes der elektronischen Datei dar.

8.9.2 Aktenvernichtung

Wenn nach Ablauf der vorgeschriebenen Aufbewahrungsfristen die Patientendaten nicht mehr gebraucht werden, z. B. weil keine weitere Behandlung des Patienten zu erwarten ist, sind die Unterlagen ordnungsgemäß zu vernichten. Sie müssen daher entweder in einem eigenen Schredder zerkleinert (nach DIN 32757, Sicherheitsstufe 3-4) oder einem Aktenvernichtungsunternehmen übergeben werden. Wenn zur Aktenvernichtung ein Unternehmen eingeschaltet wird, findet datenschutzrechtlich eine Datenverarbeitung im Auftrag statt.

Der Zahnarzt bleibt die verantwortliche Stelle. Ihm obliegt es zu kontrollieren, ob der Auftrag datenschutzgerecht erledigt wurde. Um die Einhaltung der ärztlichen Schweigepflicht zu gewährleisten, sollten die Patientendaten in einem abgeschlossenen Behältnis, das in der Regel vom Unternehmen zur Verfügung gestellt wird, zur Vernichtung gegeben werden. Auch im Rahmen des eigentlichen Vernichtungsvorgangs durch das beauftragte Unternehmen ist die Kenntnisnahme von Patientendaten durch dessen Mitarbeiter auszuschließen. Ergänzend hierzu wird auf die Ausführungen in Kapitel 8.8, S. 42, verwiesen.

8.10 Checkliste Datenschutz

Die folgende Checkliste stellt die wesentlichen Fragestellungen zusammen, die im Zusammenhang mit der EU-DSGVO bzw. des BDSG in der Zahnarztpraxis zu stellen sind. Sie soll der Übersicht und der Strukturierung innerhalb der Zahnarztpraxis für einen Umgang mit dem Datenschutz dienen. Sie ist dabei praktische Hilfe. Da jede Zahnarztpraxis individuelle Besonderheiten aufweisen kann, können je nach Anforderungen weitere Fragen zu beantworten sein.

A. Verantwortung in der Zahnarztpraxis:	Ja	Nein
Wird in der Zahnarztpraxis bereits Datenschutz gelebt, bspw. durch das Vorhandensein eines Datenschutzkonzepts, Sicherheitsanweisungen etc.?		
Brauchen sie in der Zahnarztpraxis einen betrieblichen Datenschutzbeauftragten? (wenn nein angekreuzt wird, bietet sich an, die Gründe dafür festzuhalten)		
Wenn ja, ist er schon gem. Art. 37 Abs. 7 EU-DSGVO der zuständigen Aufsichtsbehörde gemeldet?		
B. Verarbeitungsverzeichnisse nach Art. 30 EU-DSGVO		
Führen Sie in Ihrer Zahnarztpraxis ein oder mehrere Verzeichnisse Ihrer Verarbeitungstätigkeiten gem. Art. 30 EU-DSGVO?		
Ist bei Ihnen sichergestellt, dass datenschutzrechtliche Belange bei Änderungen in der Zahnarztpraxis Berücksichtigung finden?		
Gibt es ein Konzept zur Löschung von Daten?		
C. Einbindung externer Unternehmen (Dienstleister, gewerbliches Labor etc.)		
Sind in ihrer Zahnarztpraxis externe Dritte zur Erledigung der Aufgaben eingebunden (gewerbliches Labor, externe IT-Dienstleister, Lohnbuchhaltung etc.)?		
Wenn ja, haben Sie eine Übersicht über die Zusammenarbeit mit Dritten?		
Werden insbesondere Patientendaten zwischen Ihnen und diesen externe Dritten ausgetauscht?		
Wenn ja, haben Sie mit allen diesen Dritten die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 EU-DSGVO abgeschlossen?		
Sind Dritte (aber auch Angestellte) zur Geheimhaltung verpflichtet worden?		
D. Informationspflichten		
Weisen Sie in ihrer Praxis auf die Informationen aus den Art. 13 und 14 EU-DSGVO hin?		
Sofern Ihre Zahnarztpraxis auch über eine eigene Homepage verfügt, ist diese den Anforderungen der EU-DSGVO bzw. des BDSG anzupassen?		
E. Anpassungen von Musterformularen		
Benutzen sie Musterformulare für Einwilligungen in die Datenverarbeitung (Schweigepflichtentbindungen, Einwilligung zur Abrechnung privatzahnärztlicher Leistungen durch Dritte, Auftragsdatenverarbeitungsverträge etc.)		
Wenn ja, sind diese ggf. anzupassen?		
Können sie erteilte Einwilligungen notfalls nachweisen?		
F. Umgang mit Betroffenenrechte		
Gibt es in Ihrer Zahnarztpraxis eine bestimmte Verfahrensweise, wie mit den Betroffenenrechten umgegangen werden soll?		
G. Umgang mit Risiken / Sicherheitsmaßnahmen		
Gibt es in Ihrer Praxis ein System, das ggf. nachweisen kann, dass ihre Datenverarbeitung den Anforderungen gerecht wird?		
Nutzen Sie Systeme zum Schutze und zur Sicherheit ihrer Datenverarbeitung?		
Werden diese Systeme turnusmäßig überprüft und aktualisiert?		
Müssen sie eine Datenschutzfolgenabschätzung durchführen?		
H. Umgang mit Datenschutzverletzungen		
Haben sie in Ihrer Praxis ein System eingeführt, wie Datenschutzverletzungen erkannt werden können bzw. mit Datenschutzverletzungen umzugehen ist?		
Haben Sie festgelegt, wer potentielle Datenschutzverletzungen der zuständigen Behörde innerhalb von 72 Stunden mitteilen soll?		

9.0 Anhang

9.1 Weitere Quellen zum Datenschutz und zur Datensicherheit

Quellen im Internet:
BfDI: **www.bfdi.bund.de**
BSI für Bürger: **www.bsi-fuer-buerger.de**

9.2 Glossar

ActiveX
Im Internet Explorer genutzte Möglichkeit, Inhalte aktiv (und ggf. missbräuchlich) zu steuern

Administrator
Nutzer mit den umfassendsten Berechtigungen auf dem Computer, kann daher wesentliche Systemänderungen durchführen

Authentisierung
Nachweis der Identität und Zugriffsberechtigung, z. B. bei Anmeldung an einem KZV-Portal durch eine ZOD-Karte

Backdoor
Zugriffsmöglichkeit auf Software und Daten durch einen Zugang, welcher dem Nutzer nicht bekannt ist und welchen er nicht kontrollieren kann

Benutzerkonto
Verknüpft Nutzer und ihre Berechtigungen auf dem Computer, z. B. um Zugriff zur Änderung von Dateien nur speziellen Nutzern zu erlauben

Datensicherung
Regelmäßige Kopien von wichtigen Daten auf externe Medien (Festplatten, CDs, DVDs)

Datenverschlüsselung
Z. B. Verschlüsselung von Dokumenten, welche dann auch verschlüsselt auf einem Rechner oder Datenträger abgelegt werden können

eGK
Elektronische Gesundheitskarte

Firewall
Regelt und beschränkt den Datenverkehr in und aus dem Internet. Soll das Ausspähen des Rechners verhindern.

Hacker
Person oder Gruppe, welche unbefugt auf einen Rechner oder auf Daten zugreift und hierzu gezielt Sicherungsmaßnahmen umgeht, z. B. zur Spionage oder zur Schädigung

https-Protokoll
Hyper**T**ext **T**ransfer **P**rotocol **S**ecure (dt. sicheres Hypertext-Übertragungsprotokoll), Verfahren, um Daten im World Wide Web abhörsicher zu übertragen. Es wird zur Transportverschlüsselung und zur Authentifizierung der Kommunikation zwischen Webserver und Browser im Internet verwendet.

Konnektor
Hardwarebox der Telematikinfrastruktur mit Sicherheitsfunktionen, zugelassen von der gematik und zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik

KZBV
Kassenzahnärztliche Bundesvereinigung

KZV
Kassenzahnärztliche Vereinigung

Multimedia Plugins
Z. B. Player zum Abspielen von Flashfilmen. Können Eintritt von Schadsoftware bieten.

PIN
Persönliche **I**dentifikations**n**ummer

Proxy
Einrichtung, die stellvertretend für den eigentlichen Nutzerrechner im Internet Anfragen stellt und Daten stellvertretend für diesen entgegennimmt. Dadurch werden die dahinterliegenden Rechner „verschleiert".

PVS
Praxisverwaltungssystem

Router
Technisches Gerät, um Daten in Netzwerken zielgerichtet zu übertragen und einen Verbindungsaufbau zum Internet durchzuführen

SIS
Abkürzung für "sicheres Internet", eines optionalen Dienstes eines VPN-Zugangsdiensteanbieters der Telematikinfrastruktur

SSL-Verbindung
Secure **S**ockets **L**ayer, (hybrides) Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet

Transportverschlüsselung
Während des Transportes sind die Daten verschlüsselt, liegen berechtigten Empfänger dann jedoch unverschlüsselt vor

Trojaner
Schadsoftware, kann Daten löschen, verändern oder abhorchen (z. B. Passwörter)

Virenschutzprogramm
Programm auf dem Rechner, welches vor Schadsoftware (Viren, Trojaner) schützt

Virus
Schadsoftware, kann Daten löschen, verändern oder ausspähen (z. B. Passwörter)

VPN-Zugangsdiensteanbieter
Anbieter, welcher einen zur Online-Anbindung an die Telematikinfrastruktur sicheren Dienst bereitstellt

WhiteList
Liste freigeschalteter IP-Adressen

ZOD
Zahnärzte **O**nline **D**eutschland:
Sicherheitsinfrastruktur für Zahnärzte auf der Basis qualifizierter Signaturkarten

Impressum

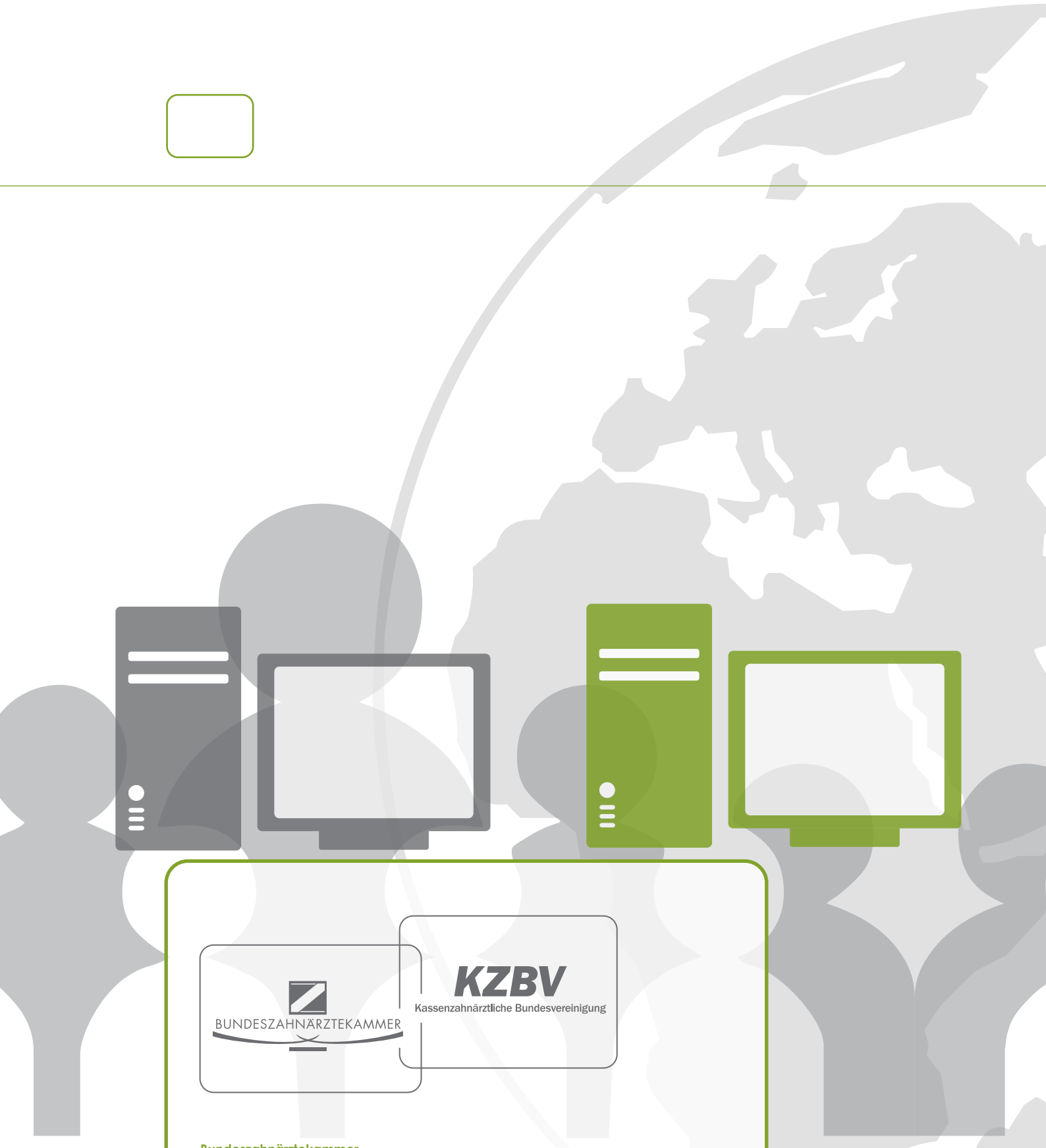
Herausgeber

Bundeszahnärztekammer (BZÄK)

Kassenzahnärztliche Bundesvereinigung (KZBV)

Gestaltung/Grafiken

tobedesign



Bundeszahnärztekammer
Arbeitsgemeinschaft der Deutschen Zahnärztekammern e.V. (BZÄK)
Chausseestraße 13 | 10115 Berlin
Telefon: +49 30 40005-0 | Fax: +49 30 40005-200
E-Mail: info@bzaek.de | www.bzaek.de

Kassenzahnärztliche Bundesvereinigung
Universitätsstr. 73 | 50931 Köln
Telefon: +49 221 4001-0 | Fax: +49 221 4040-35
E-Mail: post@kzbv.de | www.kzbv.de