verschaffen und entsprechende, auf den Servern gespeicherte Daten abzugreifen. Aus diesem Grund ist es essenziell, dass sämtliche Software, die auf dem Smartphone installiert ist (und dazu gehört auch das Betriebssystem) stets auf dem aktuellen Sicherheitsstand ist. Datenverbindungen wie Bluetooth, WLAN etc. sollten nur aktiviert und genutzt werden, wenn sie wirklich benötigt werden. In allen anderen Fällen sollten diese Funktionen deaktiviert werden, was zusätzlich auch der Akkuleistung sehr zugute kommt. Ferner sollten so weit wie möglich auch alle „Dienste", besonders die „Backup-Cloud-Dienste" der Anbieter, aufgrund der vorstehend angesprochenen strafrechtlichen Relevanz von vornherein deaktiviert werden.

Bei großen Organisationen wie Krankenhäusern, MVZ etc., in denen Smartphones zum Einsatz kommen, sollten entsprechende Sicherheitskonzepte ausgearbeitet werden. Ferner sollte darüber nachgedacht werden, ob eine sog. Mobile Device Management (MDM) -Lösung, bei der die Nutzung bzw. der Nutzungsumfang der entsprechenden Smartphones halbwegs gesteuert werden kann, sinnvoll ist. In diesem Zusammenhang sei darauf hingewiesen, dass auch eine solche MDM-Lösung ein planvolles, organisatorisches Vorgehen inklusive entsprechender Regelungen erfordert.

Wie aufgezeigt, sind die zu treffenden technischen und organisatorischen Maßnahmen bei Smartphones und Co. nicht zu unterschätzen.

16.4 Der „Praxisauftritt" im Netz

Ein weiterer Bereich, der von einem Arzt auch nicht in seiner Relevanz unterschätzt werden sollte, ist sein „Praxisauftritt" im Internet. Mehr als die Hälfte der Arztpraxen in Deutschland verfügte nach einer Untersuchung der Stiftung Gesundheit aus dem Jahre 2015 über eine Internet-Präsenz (https://www.stiftung-gesundheit.de/pdf/studien/Aerzte_im_Zukunftsmarkt_Gesundheit-2015_eHealth-Studie.pdf). Im Jahre 2019 dürften

es praktisch alle sein. Denn keine Praxis kann sich noch leisten, nicht im Netz präsent zu sein.

Neben Informationen zur Praxis und zum Praxispersonal, den Tätigkeitsschwerpunkten, besonderen Qualifikationen usw. werden die Webseiten immer serviceorientierter. So ist bspw. zu beobachten, dass über den Webauftritt zunehmend auch (ärztliche) Serviceleistungen wie etwa die Vereinbarungen von Terminen oder die Anforderung von Rezepten angeboten werden.

Für über 70 % der Ärzte stellt die Praxis-Homepage nach dieser Studie eine der wichtigsten Marketingmaßnahmen dar, um sich ihren (potenziellen) „Kunden" gegenüber zu präsentieren. Auch dieser Anteil dürfte deutlich gestiegen sein.

Jedoch gilt es zu beachten, dass je mehr „Services" diese Webseite anbietet, umso mehr rechtliche Relevanz dieser Webseite zukommt. In diesen Fällen können die unterschiedlichsten rechtlichen Aspekte zu beachten sein.

Je nach Serviceangebot kann die Nichtbeachtung der einschlägigen Gesetze, die von der DSGVO, dem Telemediengesetz (TMG), dem Heilmittelwerbegesetz (HWG) bis hin zum Medizinprodukterecht reichen können, einschneidende rechtliche Konsequenzen mit sich bringen. So zeigt die vorstehend erwähnte Studie etwa auch, dass in etwa 10 % der Fälle bereits Abmahnungen wegen rechtlicher Verstöße gegen die Webseitenbetreiber erfolgten. Auch diese Zahl dürfte deutlich gestiegen sein. Gerade im Rahmen der DSGVO hatte ich mit diversen Abmahnungen zu tun.

Da die Webseite als Telemedium angesehen werden kann, muss diese zwingend immer ein Impressum mit den entsprechenden von § 5 TMG vorgesehenen Angaben enthalten. Falls in regelmäßigen zeitlichen Abständen Artikel erscheinen sollen, wie z. B. in einem Blog, so sollte in diesem Impressum ein redaktionell Verantwortlicher gem. § 55 Abs. 2 Rundfunkstaatsvertrag (RStV) benannt werden. Das Impressum sollte leicht erreichbar

sein. Die Rechtsprechung nimmt eine solche an, wenn man mit maximal zwei „Klicks" das Impressum leicht erreichen kann.

Um die Webseite ansprechend und freundlich zu gestalten, verwenden Ärzte gerne auch auf ihrer Webseite Bilder von sich und ihren Mitarbeitern und etwaige andere Fotos. Diesbezüglich gilt es immer penibel darauf zu achten, dass der Arzt diesbezüglich auch über die entsprechend notwendigen Rechte verfügt. Bei Veröffentlichungen von Bildern des Praxispersonals sollte die (explizite), schriftlich dokumentierte Einwilligung der Mitarbeiter eingeholt werden. Diesbezüglich sei auch darauf hingewiesen, dass Gerichte Einwilligungen von Mitarbeitern aufgrund des Machtungleichgewichts zwischen Arbeitgeber und Arbeitnehmern oftmals als unwirksam betrachtet haben. Aus diesem Grund muss alles unternommen werden, damit ein solcher Anschein erst gar nicht entsteht. Insbesondere sollte der Arzt die Mitarbeiter darüber aufklären, dass sie nicht verpflichtet sind, ihre Einwilligung zu erteilen und dass ein Versagen der Einwilligung keine beruflichen Konsequenzen nach sich zieht.

Die datenschutzrechtlichen Anforderungen, die sich auf einen Großteil der Datenverarbeitung der Homepage beziehen, bemessen sich zunächst maßgeblich an den Regelungen der DSGVO und des TMG, das in seinen datenschutzrechtlichen Bestimmungen möglicherweise bald von der sog. ePrivacy-Verordnung abgelöst werden wird. Wie aufgezeigt, können jedoch aufgrund der Tatsache, dass die Informationen, die aus den Daten extrahiert werden können, eine unterschiedliche „Qualität" besitzen, durchaus auch weitere Gesetze einschlägig sein. Unklar ist bislang auch, wie das Verhältnis der DSGVO zur TMG ist. Meiner Ansicht nach empfiehlt es sich, die allgemeinen Regeln der DSGVO als Maßgabe zu nehmen und zu prüfen, inwieweit das TMG andere/weitere Vorgaben beinhaltet. Grundsätzlich dürfte aber im datenschutzrechtlichen Bereich die DSGVO vorrangig gelten.

Das TMG regelt in §§ 12 ff. die datenschutzrechtlichen Anforderungen an den Anbieter einer Homepage (z. B. den Praxis-

inhaber) in Bezug auf die Rechte der Nutzer (wie z. B. der Patienten).

Besonders zu beachten sind in diesem Zusammenhang die Regelungen von §§ 13 und 15 TMG. Gem. § 13 ist der Webseitenbetreiber (sog. Diensteanbieter) verpflichtet, die Nutzer zu Beginn ihrer Nutzung über

- die Art,
- den Umfang und
- die Zwecke der Erhebung und Verwendung personenbezogener Daten sowie
- ggf. die Verarbeitung der Daten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums

zu unterrichten.

Diese Informationspflicht dürfte jedoch durch Art. 13 ersetzt/ergänzt werden. Mithin ist es nunmehr notwendig, dass jede Webseite in ihrer „Datenschutzerklärung" alle Informationen gem. Art. 13 hinsichtlich der Datenverarbeitung der Webseite auf eine transparente und nachvollziehbare Art und Weise darstellt. Hinsichtlich des konkreten Inhalts sei auf *Kapitel 9.3* verwiesen. Wie an diversen Stellen in diesem Buch aufgezeigt, lassen sich die ganzen gesetzlichen Anforderungen und insbesondere auch die Informationspflicht nach Art. 13 jedoch immer nur bei entsprechender Transparenz über die wahren Datenverarbeitungsvorgänge abbilden.

An dieser Stelle ein Hinweis: Die Datenschutzerklärung muss die **REALE** Datenverarbeitung auf der Webseite abbilden und in eine rechtliche Form gießen. Im Zuge des „DSGVO-Wahns" durfte ich um die 40–50 Datenschutzerklärungen von Webseiten überprüfen und anpassen. Dabei fiel mir bei JEDER dieser Webseiten auf, dass die bisherige Erklärung, auch wenn sie recht umfassend gewesen sein mag, niemals die wahre, technische Realität der Webseite erfasst hat. Denn so sind in ganz vielen „modernen" Webseiten oftmals viele externe Dienste eingebunden (bspw. von Google, Amazon und Co.), zu denen

der Nutzer bzw. der Browser des Nutzers beim Besuch der Webseite automatisch eine Verbindung aufbaut, Daten des Nutzers übermittelt und der Nutzer dieses praktisch nicht verhindern kann. Verantwortlich dafür ist die Arztpraxis als Betreiber der Webseite, die zwar für diese Datenübermittlung verantwortlich ist, jedoch davon oftmals gar keine Kenntnis hat.

Um eine Rechtskonformität der Webseite zu gewährleisten, gilt es daher immer, erst die komplette Datenverarbeitung der Webseite „technisch" zu analysieren. Erst wenn sämtliche Komponenten und Datenverbindungen der Webseite identifiziert wurden, sollte man mit der Erstellung der Datenschutzerklärung beginnen.

Da ein Arzt eine solch tiefgehende Analyse oftmals nicht selber durchführen kann, empfehle ich, dass er sich mit dem Webdesigner auseinandersetzt, der ihm seine Webseite erstellt hat. Der Webdesigner sollte eigentlich in der Lage sein, dem Arzt Auskunft über sämtliche von ihm eingebundene „Services" und Datenverbindungen zu geben. Wie leider jedoch meine Erfahrungen zeigen, wissen viele Webdesigner oftmals selber nicht, was sie alles für Services eingebunden haben bzw. welche Datenverbindungen alle im Hintergrund stattfinden. So traurig und unglaublich das klingen mag. Oftmals klicken Webdesigner bei der Erstellung der Webseite nach einer Art Baukastensystem einfach die technischen Komponenten zusammen und kümmern sich praktisch ausschließlich nur um das Design der Webseite. Dass die von ihnen eingesetzten technischen Komponenten jedoch möglicherweise nicht so gut miteinander harmonieren, ungewollte Funktionen mit sich bringen, ungewollte Datenverbindungen aufbauen usw. und dieses alles letzten Endes der (Rechts-) Sicherheit der Webseite nicht gerade zuträglich ist, wissen viele gar nicht. Wenn Ihnen daher Ihr Webdesigner keine klaren Auskünfte über ALLE von ihm eingesetzten „Services" geben und keine klaren Angaben darüber machen kann, welche Datenverbindungen alles beim Besuch der Web-

seite aufgemacht werden, sollten Sie sich, auch wenn es hart klingen mag, überlegen, ob dieser Webdesigner der richtige für Sie ist.

Das Problem, das viele IT-Sicherheitsexperten und ich persönlich bei der Einbindung externer Dienste sehen, ist, dass mit jeder Einbindung von externen Services automatisch die Angriffsfläche der Webseite vergrößert wird. Ferner steigt mit jeder Einbindung dieser Services automatisch das Risiko, dass damit neue Sicherheitslücken entstehen. Gerade weil die Anbieter dieser externen Dienste Daten der Besucher Ihrer Webseite erhalten, müssten Sie theoretisch mit diesen auch entsprechende Vereinbarungen hinsichtlich der Datenverarbeitung treffen (*vgl. Kapitel 17*). Da sich diese jedoch nicht auf solche Vereinbarungen einlassen, sollten Sie sich aufgrund der damit entstehenden Rechtsunsicherheit überlegen, ob dieser eingebundene „Service" wirklich notwendig ist oder man ggf. datenschutzfreundlichere Alternativen einsetzen sollte.

Wie vorstehend angesprochen, werden auch immer mehr „Dienstleistungen" über eine Praxiswebseite angeboten. Aus datenschutzrechtlicher Sicht lässt sich dazu anmerken, dass jede zusätzlich zum Informationszweck angebotene Dienstleistung auf der Webseite im Prinzip eine eigene Verarbeitung darstellt. Denn mit den zusätzlichen Services werden andere Zwecke verfolgt als die bloße Informationsverschaffung der Webseite als Zweck. Somit gilt es, sich insbesondere hinsichtlich der Datenschutzerklärungen (Art. 13) zu überlegen, wie man diese gestalten will. Meine Empfehlung lautet diesbezüglich, eine eigene Datenschutzerklärung zu verwenden. Denn das Aufführen dieser Informationen in der (Haupt-)Datenschutzerklärung der Webseite kann schnell dazu führen, dass diese Erklärung zu umfangreich und damit zu intransparent wird. Beliebte Services, für die man eine eigene Erklärung verwenden sollte, sind bspw. das Kontaktformular, Rezeptbestellung, Terminvereinbarung (falls externer Service), Bewerberportal usw.

Gerade bei Formularen wie dem Kontaktformular sollte man darauf achten, auch wirklich nur die Angaben abzufragen, die für den Zweck der Kontaktaufnahme notwendig sind (Datenminimierungsgrundsatz). In der Datenschutzerklärung zu diesem Service sollte man den gesetzlichen Anforderungen folgend darstellen, wieso diese Daten benötigt werden und wozu diese verwendet werden. Handelt es sich bei diesen Diensten um „externe" Dienste, muss ein Nutzer, wie z. B. ein Patient, bevor er diesen Diensten seine Daten preisgibt, explizit auf die Übermittlung und die Verarbeitung seiner Daten hingewiesen werden. Werden externe Dienste angeboten, die in Bezug zur ärztlichen Verschwiegenheitspflicht stehen, sollte man als Arzt diesen Dienstleister in die berufliche Verschwiegenheitspflicht einbinden (vgl. § 203 Abs. 4 StGB).

Werden Online-Formulare zur Übertragung von Daten an die Praxis (z. B. für Terminreservierung, Rezeptbestellungen, Mitteilungen) angeboten, so sollten diese Daten immer nur verschlüsselt mit einem anerkannten Verschlüsselungsstandard übertragen werden. Trotz der faktischen Verschlüsselung sollte ferner immer ein Hinweis auf den Sicherheitsstandard der Übermittlung (verschlüsselte Übertragung) und die Verwendung der übermittelten Daten und deren eventuelle Weitergabe erfolgen.

Durch das sog. IT-Sicherheitsgesetz ist nunmehr auch eine Regelung in das TMG gekommen, in der deutlich gemacht wird, dass jeder Webseitenbetreiber, der seine Webseite geschäftlich nutzt, die entsprechend nach dem Stand der Technik erforderlichen Maßnahmen ergreifen muss, um die Sicherheit der Datenverarbeitung und die Sicherheit der Besucher zu gewährleisten. Nichts Anderes dürfte auch die DSGVO in Art. 32 fordern, vielleicht sogar noch ein wenig „extensiver". Daraus folgt zwangsläufig, dass je mehr „Services" dem Nutzer mittels einer Webseite angeboten werden und je mehr sensible Daten die Nutzer dadurch von sich preisgeben, umso höhere Anforderungen an die Gewährleistung der Sicherheit dieser Webseite gestellt wer-

den müssen. Dieses bedingt auch, dass man die Webseite in regelmäßigen Abständen auf „Sicherheit“ ggf. durch Externe prüfen lassen sollte. Diese explizite, nunmehr gesetzlich verankerte Forderung in der DSGVO und dem TMG ist nur konsequent und trägt dem Bedrohungspotenzial, das von Webseiten ausgehen kann, Rechnung.

Die Arztpraxis - Datenschutz und Datensicherheit nach der neuen Datenschutzgrundverordnung
360 Seiten, Softcover, 978-3-609-10367-9, Verlag ecomed Medizin

Direkt zum Buch