Gesetzliche Änderungen

Gerade in jüngster Zeit hat sich viel verändert, denn unsere Regierung, wie auch die EU schaffen durch die immer stärker werdende Digitalisierung weitgehende Gesetze und Verordnungen im diesem Bereich. Zum Teil war das auch dringend notwendig, gerade wenn wir an den Datenschutz denken, teilweise ist aber die Bürokratie auch für kleine Unternehmen und Praxen damit erheblich angewachsen. Die **GoBD** war allerdings nicht ganz neu, im Prinzip wurden hier alte Verordnungen wie die GoBS auf den neusten Stand gebracht, z. B. war der **Z3 Zugriff** zuvor unter GDPdU zu finden. Auch schon zuvor mussten buchhaltungsrelevante Daten zehn Jahre aufbewahrt werden, es gibt jetzt allerdings Konkretisierungen und Verschärfungen. Teilweise um eine Prüfung zu erleichtern, teilweise um Steuerhinterziehung zu erschweren.

Ebenso hatten wir natürlich auch schon vor der **DSGVO** ein Bundesdatenschutzgesetz (BDSG) und eine entsprechende EU Richtlinie (Richtlinie 95/46/EG). Auch hier sind die neueren Verordnungen und Gesetze von weiteren Konkretisierungen und einigen Verschärfungen geprägt, dies mag auch der deutlich zunehmenden Digitalisierung geschuldet sein, ebenso eine Anhebung der Strafen, hier muss man leider anmerken, dass sich viele leider vorher nicht oder nicht ausreichend um den Datenschutz gekümmert haben, gerade in Hinblick auf die elektronische Verarbeitung. Es mag hierbei in Bezug auf kleine Unternehmen und Praxen weniger boshafte Absicht, als Unwissenheit gewesen sein. Nun ist das Thema aber sehr präsent, denn jeder Patient resp. Kunde hat sehr weitreichende Mittel, seine Rechte in Bezug auf seine Daten durchzusetzen und die Datenschutzbehörden nehmen dies deutlich ernster und kontrollieren schärfer.
Es war auch schon zuvor so, dass gesundheitsbezogene Daten unter besonderem Schutz gestanden haben und eben Praxen, obwohl sie ja eher kleinere Unternehmungen sind, hier eine besondere Belastung innerhalb der Umsetzung und Einhaltung haben, dennoch, denken Sie bitte immer daran, was es für den einzelnen bedeutet, wenn derartige Daten öffentlich werden.

Im Bezug zur DSGVO sind die Anforderungen an die IT Sicherheit deutlich gestiegen, denn gerade auch Viren und Trojaner können Daten ausspähen. Was erschwerend hinzukommt, ist eine deutliche Verschärfung der IT Angriffe auch auf kleinere Unternehmen und Praxen. Seit 2015 wurde dies besonders deutlich, weil es mehrere größere Angriffe mit erheblichen Schäden gab. Z. B. WannaCry (wurmartige Ausbreitung auf Geräten, die nicht alle Updates eingespielt hatten) Petya und NotPetya (gleiche Sicherheitslücke wie bei WannaCry, namens EternalBlue ausgenutzt, auch hier hätten zügige Updates einiges verhindert). Locky, ein Kryptotrojaner, der sich in Mailanhängen versteckt hat und Daten verschlüsselt, hier wurde beim Ausführen ein Makro aktiviert und in die gleiche Kerbe schlagen nun Gandcrab (Die kriminellen Macher dieser Schadsoftware haben angeben nicht weiter zu machen und es existiert von Bitdefender ein Entschlüsselungstool), sowie immer noch aktuell Emotet und das war nur die Spitze des Eisbergs, es existieren etliche andere. Aber wenn man sich Emotet ansieht, so haben wir gerade bei diesem Trojaner eine deutliche Steigerung im Angriffsvektor, denn dieser hat in mehreren Angriffswellen Outlook Adressbücher und Mails abgefischt. Die daraus resultierenden Kontakte und Mailthemen wurden von den Angreifern ausgewertet und fließen nun in die nächsten Angriffswellen hinein. Das heißt, Sie könnten Mails von bekannten Absendern mit durchaus sinnvollen Mailtexten erhalten, die auf eine frühere Konversation aufbauen. Gleich bleibt bislang nur, dass im Anhang der trügerischen Mail ein Word® Dokument angehängt ist, dass angeblich mit Klick auf "bearbeiten" oder "enable content" freigegeben werden sollte.
Dieser Klick allerdings ist verhängnisvoll, denn damit aktiveren Sie ein Makro und der Virus breitet sich auf Ihrem System aus. Zu diesem Zeitpunkt kann auch weitere Schadsoftware nachgeladen werden. Da sich die Signatur immer wieder ändert, werden Virenscanner sehr neue Varianten anfänglich nicht erkennen können. Seien Sie also auf der Hut, wenn Sie einen Mailanhang öffnen und mit einem Dialog nach weiteren Rechten gefragt werden. Besser nicht öffnen und mit dem angeblichen Absender Kontakt aufnehmen, hat schon so machen vor einer Infektion bewahrt. Das Bundesamt für Sicherheit in der Informationstechnik hat erneut Warnungen herausgegeben. Wir gehen auf dieses Thema später sehr viel genauer ein.

Auch das **Patientenrechtegesetz** hat weitreichende Anforderungen an Praxisinhaber. Auch hier werden Arbeitsabläufe angepasst werden müssen, etwa in Bezug zur Patientenkartei, bzw. Vertragsvereinbarungen und Aufklärung.

Hinzu kommt noch die nun in Kraft getretene **Kassensicherungsverordnung** die z. B. alle Abrechnungsprogramme, die Barzahlungen erfassen können per Definition

zu einem Kassensystem macht. Das haben viele übersehen, es steht im **Anwendererlass** unter **Nr. 1.2 zum §146a AO**. Die „Bonpflicht“ wurde im Januar 2020 dadurch populär, dass sich einige Bäcker und Metzger zu Wort meldeten und Berge von Bons in Schaufenster stellten um auf das Thema hinzuweisen. Die „Bonpflicht“ resp. **Belegausgabepflicht** gehört auch zur sog. KassenSichV also der Kassensicherungsverordnung. Auch Sie sind dazu verpflichtet einen Beleg auszugeben. Dieser muss aber nicht mit Thermopapier auf einem Bondrucker erzeugt werden. Wenn die geforderten Daten der sog. **TSE** (technische Sicherheitseinrichtung, später dazu mehr) auch mit auf die Rechnung gedruckt werden, ist diese Pflicht erfüllt. Wir merken jedoch bei diesem Thema, dass es ebenso wie die GoBD bei Einführung kaum bekannt ist und zusätzlich sowohl zeitlich als auch in ihrem Bekanntheitsgrad in der Bekämpfung der Corona Pandemie unterging. Aber durch Corona gab es auch weitere Verzögerungen, die Auswirkungen auf die Zertifizierung der TSE hatten, deswegen haben einige Bundesländer eine verlängerte Nichtaufgriffsregelung bis zum 31.03.2021 vereinbart. Längst aber nicht alle und die Vorgaben und Bedingungen um in die Verlängerung zu gehen, sind auch je nach Bundesland unterschiedlich. Zumindest aus der Sicht derjenigen, wie wir, die die Verordnung in einem Programm umsetzen müssen, ist diese fragmentierte Erleichterung gar keine. Denn z. B. Bremen spielt nicht mit und andere knüpfen starke Bedingungen an diese Erweiterung. Für uns bleibt es also beim 30.09.2020, denn wir können ja auch Kunden aus Bremen nicht in die Röhre gucken lassen und wenn das Programm für Bremen fertig sein muss, dann ist es nun mal fertiggestellt. Außerdem müssen wir dementsprechend zusätzlich unsere Kunden je nach Bundesland informieren und beraten. **Je mehr Daten und Unsicherheit im Umlauf sind, desto mehr Missverständnisse.** Wir hätten uns eine generelle Verschiebung aller Bundesländer auf den 31.03.2021 sehr gewünscht.

Für alle, die eine Internetseite betreiben, ist die doch nicht in Kraft getretene **e-Privacy** Verordnung noch nicht vom Tisch, denn es gibt zu Cookies nun weitreichende Vorgaben in den Richtlinien. Hier ist auch das letzte Wort noch nicht gesprochen, wir dürfen also gespannt sein, welche Auswirkungen das haben wird. Zusätzlich rüttelte der EuGH mit dem Kippen des **Privacy Shields** etliche Cloudanwender auf. Aber selbst eingebundene Dienste in Webseiten sind betroffen und selbst Software, von der man es eigentlich gar nicht denkt, kann betroffen sein.
In den nächsten Kapiteln gehen wir darauf genauer ein, auch werden wir einen kurzen Blick auf das **e-Health Gesetz** werfen, selbst wenn es bislang nur Ärzte betrifft.
Es gibt auch sehr schönes zu berichten, denn Abmahnungen gegen kleine Unternehmen und Vereine werden wohl erschwert.