Vorwort

Einführung in den Datenschutz

„Lauter und gewissenhaft werde ich mein Leben und meine Kunst bewahren […].Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach draußen tragen darf, werde ich schweigen und es geheim halten. Wenn ich diesen Eid erfülle und ihn nicht antaste, so möge ich mein Leben und meine Kunst genießen, gerühmt bei allen Menschen für alle Zeiten; wenn ich ihn aber übertrete und meineidig werde, soll das Gegenteil davon geschehen." *Eid des Hippokrates*

Schon Hippokrates wusste, welchen Stellenwert der Datenschutz im Arztberuf hat. Umso mehr gilt es heute, wo riesige Datenbestände über Patienten archiviert und zu vielen Seiten verbreitet werden.

Dieses Buch gibt dem Steuerberater der Inhaber einer Arzt- oder Zahnarztpraxis bzw. Heilberufler berät bzw. den Ärzten, Zahnärzten oder Heilberuflern einen ersten praktischen Einstieg zur Umsetzung des neuen europäischen Datenschutzrechts.

So unterschiedlich wie die jeweiligen Formen der Zusammenarbeit von Ärzten, Zahnärzten und Heilberuflern sind, so vielfältig sind jedoch auch die zu klärenden Detailfragen in den jeweiligen Arbeitsprozessen.

Die EU-Datenschutzgrundverordnung beinhaltet Rechenschafts- und Dokumentationspflichten über die Verarbeitung personenbezogener Daten und Datenströme in allen Organisationen gleich welcher Art. Bis dato etablierte Prozesse und Strukturen müssen unter Umständen hinterfragt und an die geforderten Regeln angepasst werden.

In den Medien wird die EU-Datenschutzgrundverordnung als großes Hindernis für die Berufsausübung gesehen, gleichzeitig wird Angst vor dem hohen Bußgeldrahmen angeführt. Richtig ist, dass die Durchsetzung von Bußgeldern durch die Landesdatenschutzbeauftragten einfacher geworden sein dürfte. Aber auf der anderen Seite müssen die Behörden auch sorgsam abwägen.

Hierzu sind bereits entsprechende Leitlinien, sogenannte Working-Papers für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679 vom 3.10.2017 der ARTIKEL-29-DATENSCHUTZGRUPPE veröffent-

licht worden (https://www.lfd.niedersachsen.de/startseite/dsgvo/leitlinien_art_29gruppe/).

Klargestellt werden muss, dass Abmahnungen wettbewerbsrechtlicher Natur sind. Das bedeutet, dass Abmahnungen dann rechtmäßig sind, wenn ein Datenschutzverstoß gegen das Wettbewerbsrecht (UWG) verstößt. Dies wird derzeit heftig in der Literatur diskutiert. Ob Mitbewerber Unterlassungsansprüche gegen Konkurrenten wegen Verstößen haben können ist zweifelhaft; allerdings wird dieser Streitpunkt wohl gerichtlich entschieden werden müssen. Entscheidend ist also, ob Datenschutz eine Marktverhaltensregelung darstellt und nicht nur eine Ordnungsvorschrift.

Da bereits in nahezu allen Praxen gesetzlich vorgegebene Qualitätsmanagementsysteme etabliert sind, kann zumindest auf bereits abgebildete Arbeitsprozesse zurückgegriffen werden. Grundsätzlich aber ist die Etablierung einer datenschutzkonformen Organisation neu und aufwendiger, weil in „Datenströmen" gedacht werden muss.

Die EU-Datenschutzverordnung geht davon aus, dass der Datenschutz personenbezogener Daten einem kontinuierlichen Verbesserungsprozess unterliegen. Dies liegt daran, dass die Informationstechnologie rasante Fortschritte macht. Datenschutz und Datensicherheit sind eng miteinander über sogenannte technisch-organisatorische Maßnahmen verknüpft.

Die positiven Aspekte der Einführung neuer Prozesse für den Datenschutz in der Praxis dürfen ebenfalls nicht übersehen werden. Durch die Durchleuchtung des Praxisbetriebs nach „Datenströmen" wird erhöhte Transparenz der Informations- und Datenverarbeitung geschaffen. Damit werden mögliche Schwachstellen, Fehler, Kostentreiber und Redundanzen im System aufgedeckt, die vorher vielleicht nicht offensichtlich waren.

Der besondere Fokus, den die EU-Datenschutzgrundverordnung auf die Technik setzt „privacy by default – Datenschutz durch konforme Voreinstellungen" und „privacy by design – Datenschutz durch Technikgestaltung" weist auf die Entwicklung für die Zukunft über die Einführung eines Datenschutz-Management-System (DSMS) hin zu einem umfassenden Information Security Management System (ISMS). ISMS, englisch für „Managementsystem für Informationssicherheit" ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Der Begriff wird im Standard ISO/IEC 27002 verwendet. ISO/IEC 27001 definiert ein ISMS. Der deutsche Anteil an dieser Normungsarbeit wird vom DIN NIA-01-27 IT-Sicherheitsverfahren betreut.

Weil im Schönbuch, im Juli 2018 **Harald Dauber**