Erfahrungen mit der DSGVO – Auswirkungen auf die Krankenhaus-IT

Das Datenschutzrecht hat mit der EU-Datenschutz-Grundverordnung (DSGVO) Anfang 2018 in der Öffentlichkeit hohe Wellen geschlagen. Im Jahr 2018 stand bei den Datenschutzaufsichtsbehörden die Beratung, gerade auch der Ärzteschaft, im Vordergrund. Jetzt werden seitens der Datenschutzaufsicht auch verstärkt Prüfungen durchgeführt und bereits die ersten Bußgelder verhängt. Welche Erkenntnisse kann man für die Praxis mitnehmen? Wer bislang noch nicht von Beschwerden, Prüfungen, Abmahnungen oder Bußgeldern betroffen war, sollte daraus keine Zukunftsprognose ableiten, sondern etwaige noch erforderliche Umsetzungsmaßnahmen angehen.

Große Gesundheitseinrichtungen, die als sogenannte kritische Infrastruktur angesehen werden, müssen zusätzlich zum Datenschutzrecht auch das IT-Sicherheitsgesetz (BSI-Gesetz) und die BSI-Kritisverordnung (§ 6 BSI-KritisV) beachten. Die „Handlungsempfehlungen zur Verbesserung der Informationssicherheit an Kliniken“[1] des Upkritis Branchenarbeitkreis medizinische Versorgung kann auch Nicht-Kritis-Einrichtungen eine gute Hilfestellung sein. Die Datenschutzkonferenz hält noch immer die Orientierungshilfe Krankenhausinformationssysteme, Stand März 2014, bereit. Aktueller ist die Technische Anlage - Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis der BÄK, KÄB.[2] Die DSGVO schreibt IT-Sicherheit nach dem Stand der Technik vor. Was das ist, ergibt sich aus dem aktuelle Grundschutzkompendium des BSI[3] (Bundesamt für Sicherheit in der Informationsgesellschaft).

Datenschutz richtig praktiziert, schützt nicht nur die Daten von Patienten und Beschäftigten, sondern auch die Ärzte und Krankenhäuser vor Imageverlust, Bußgeldern und strafbaren Verstößen gegen das Berufsgeheimnis. Dabei umfasst Datenschutz auch die Pflicht zu risikoangemessen technischen und organisatorischen Maßnahmen zum Schutz der Daten vor unberechtigter Kenntnisnahme und unbeabsichtigtem Verlust der Zugriffsmöglichkeit (IT-Sicherheit). Fehlende technische oder organisatorische Datenschutzmaßnahmen sind eines der Kriterien bei der Bemessung der Bußgeldhöhe nach der EU-Datenschutzgrundverordnung. Das Bußgeld kann – theoretisch – bis zu 10.000.000 Euro oder – falls das höhe ist – bis zu 2% des Jahresumsatzes betragen. Bei der Risikoabwägung kann sich also eine Investition in IT-Sicherheit durchaus lohnen, so dass Datenschutzpflichten auch zum hausinternen Argument für die Erhöhung des IT-Budgets werden können.

Welche fatalen Auswirkungen unzureichende Sensibilisierung der Beschäftigten gepaart mit unzureichender IT-Sicherheit eine Schadsoftware in einem Krankenhaus haben kann, zeigt der Fall des Klinikums Füstenfeldbruck. Der Mail-Trojaner Emotet hatte alle ca. 450 Rechner des Klinikums tagelang lahmgelegt. Bankkonten mussten gesperrt werden. Die Erreichbarkeit per E-Mail und Telefon war nicht mehr gegeben. Neue Patienten konnten – außer in extremen Notfällen – nicht mehr aufgenommen werden. Rettungswagen werden umgeleitet, Blutproben mussten per Hand beschriftet werden; alle Patientendaten müssen manuell erfasst werden und Datentransport erfolgt in der Papierakte des Patienten. Solch massiven Vorfälle rufen auch die Datenschutzaufsicht auf den Plan und führen zu verstärkten Prüfungen, auf die man sich mit den veröffentlichten Prüfungsfragebögen (s.u.) vorbereiten kann.

Die Gründe für Datenpannen, die im Regelfall der Datenschutzaufsicht und oft auch den Patienten zu melden sind, sind vielfältig: Cyberangriffe, Verlust/Diebstahl von Speichermedien, IT-Stillstand durch Stromausfall oder Erpressungssoftware, Fehlsendungen, fehlerhafte Löschung etc.[4]

Zunehmende Beschwerden

Mit der Pflicht, jeden über seine Rechte als Betroffener eine Datenverabeitung zu infomieren, ist auch das Know How und die Sensibilisierung der Beschäftigten und der Bevölkerung erheblich gestiegen, Damit geht einher eine Verunsicherung aber auch eine gestiegene Bereitschaft vermeintliche oder tatsächliche Datenschutzverstöße anzuzeigen. Bundesweit haben die Aufsichtsbehörden bis September 2018 über 11.000 Beschwerden gezählt. Die Zahl der Beschwerden ist geradezu explodiert: 3 bis 10-mal so hoch wie vor der DSGVO. Die Zahl der Mitarbeiter der Aufsichtsbehörden ist nicht im gleichen Maße gestiegen, so dass die Bearbeitung der Beschwerden teils mehrere Monate in Anspruch nimmt. Auch dies ist ein Grund, weshalb bislang nur vereinzelt etwas von den Auswirkungen der DSGVO zu hören ist.

Erste Bußgelder

Das erste bekannt gewordene Bußgeld unter der DSGVO wurde in Portugal verhängt. 400.000 Euro Bußgeld wurde gegen ein Krankenhaus festgesetzt, weil kein funktionierendes

Berechtigungskonzept vorlag. So gab es ca. 1.000 Ärzte-Accounts mit vollen Zugriffsrechten auf Patientendaten, aber nur ca. 300 Ärzte.

In Deutschland wurde ein Bußgeld von 20.000 Euro wegen fehlender Verschlüsselung von Accountdaten inkl. E-Mail-Adresse und Passwörtern verhängt. Die Daten sind gehackt und ins Internet gestellt worden.

5.000 Euro Bußgeld wurden gegen eine 2-Personenfirma verhängt, die mit ihrem Dienstleister keinen Vertrag zur Auftragsverarbeitung (AVV) geschlossen hatte. Im Gesundheitsbereich spielt in das Thema AVV das Thema Berufsgeheimnis, ärztliche Schweigepflicht, § 203 StGB, mit rein. Obwohl es auch zuvor praktiziert wurde, war bis zu einer Änderung der Strafnorm zum Berufsgeheimnis im Herbst 2017 die Einschaltung externer IT-Fachleute, Cloud-Dienste, Fernwartung, Aktenentsorgung etc. strafbar. Die Gesetzesänderung hat bewirkt, dass – sofern die Verpflichtung auf das Berufsgeheimnis erfolgt – der Einsatz Externer strafrechtlich zulässig ist. Datenschutzaufsichtsbehörden haben aber bereits angekündigt, dass sie nun auch verschärft im Gesundheitsbereich prüfen werden, ob die parallel notwendigen Verträge zur Auftragsverarbeitung abgeschlossen wurde und alle erforderlichen Regelungen, u.a. die zur IT-Sicherheit enthalten. Es gilt also alle externen Vertragspartner auf die Art der Leistung (AVV ja/nein) und Patientendaten (ja/nein) zu überprüfen und den Status der erforderlichen Verträge zu kontrollieren. Etwaige Fehler dürften im Gesundheitsbereich zu erheblich höheren Bußgelder führen.

80.000 Euro Bußgeld wurde auferlegt, weil Patientendaten im Internet zugänglich waren.

Datenschutzprüfungen

Die Datenschutzaufsichtsbehörden nehmen aufgrund von Beschwerden über Datenschutzverstöße einzelfallbezogene Prüfungen vor. Es gibt aber auch Prüfungen, bei denen die Aufsichtsbehörden „Verantwortliche" anschreiben und dazu auffordern, einen Fragebogen zum Stand der Umsetzung der DSGVO auszufüllen.5-4 Dabei zielten die ersten Prüfungen auf die allgemeine Umsetzung der DSGVO ab. Inzwischen werden auch spezielle Themen geprüft, z. B. die Umsetzung im Beschäftigtendatenschutz, Datenschutz auf Webseiten oder die IT-Sicherheit im Gesundheitsbereich – siehe das Beispiel des LDA Bayern.[5]

Wer die Prüfungsfragen auswertet, kann zielgerichteter die Datenschutzanforderungen umsetzen. Startpunkt für die noch fehlenden Umsetzungsmaßnahmen kann ein freiwilliges Datenschutz-Audit sein.

1 https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/Handlungsempfehlungen_Kliniken.pdf?__blob=publicationFile (Stand 27.07.2017)

2 Deutsches Ärzteblatt 22.06.2018

3 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html

4 Siehe online-Meldeformular der LDA Bayern: https://www.lda.bayern.de/de/datenpanne.html – LDA Hamburg, Orientierungshilfe zu Data-Breach-Meldungen nach Art. 33 DSGVO: https://datenschutz-hamburg.de/assets/pdf/2018.11.15_Data%20Breach_Vermerk_extern.pdf (Stand 3/2019).

5 https://www.datenschutz-recht-medizin.de/ransomware-arztpraxis-dsgvo/

Rechtsanwalt David Seiler verfügt über mehr als 22 Jahre Berufserfahrung als Anwalt. Er hat 2017 den Fachanwaltslehrgang IT-Recht erfolgreich abgeschlossen. Der Jurist ist als Autor, Dozent, Lehrbeauftragter (Datenschutzrecht, IT-Security Law), Gutachter und Datenschutzbeauftragter u. a. in größeren Arztpraxen und einer Ärztekammer tätig. Er berät bundesweit primär Unternehmen und Verbände. www.ds-law.eu