Hochschule für Angewandte Wissenschaften Hamburg
*Hamburg University of Applied Sciences*

**BACHELORARBEIT**

# Datenschutzanforderungen in der Medizintechnik


Vorgelegt von

Alexander Ivan Jücker

[redacted]

Studiengang Medizintechnik

Fakultät Life Sciences


Betreuung der Arbeit durch

Prof. Dr. Udo van Stevendaal

Prof. Dr. Bernd Flick

Linz, im August 2021

# EIDESSTATTLICHE ERKLÄRUNG

Ich, Alexander Ivan Jücker, [redacted], versichere hiermit, dass ich die vorliegende Bachelorarbeit mit dem Thema

*Datenschutzanforderungen in der Medizintechnik*

ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Quellen und Hilfsmittel verwendet habe. Wörtliche oder dem Sinn entnommene Stellen sind unter Angabe der Quelle kenntlich gemacht.

.....

Alexander Ivan Jücker

Linz, 30. August 2021

# KURZFASSUNG

Diese Arbeit behandelt das Thema der Datenschutzanforderungen in der Medizintechnik. Im Rahmen dieser Arbeit beziehen sich diese Anforderungen aus der Reformierung der europäischen Richtlinien für Medizinprodukte und des Datenschutzes zu den Verordnungen Medical Device Regulation (MDR) und Datenschutz-Grundverordnung (DSGVO). Nach einer Einleitung in relevante Begrifflichkeiten für Datensicherheit und Datenschutz, arbeitet eine genaue Analyse beider Verordnungstexte ihre Ziele und Strategien zur Verbesserung der Datensicherheit und des Datenschutzes heraus. Des Weiteren sollen die daraus formulierten Grundsätze sowie Sicherheits- und Leistungsanforderungen hervorgehoben werden, als auch die Maßnahmen, die von Herstellern und Betreibern von Medizinprodukten umgesetzt werden müssen. Dabei nennt die Arbeit auch Leitlinien und Normen, die Herstellern und Betreibern als Hilfestellung zur Compliance dienen können. Im Fokus eines typischen Anwendungsfeldes der Medizingeräte, dem medizinischen IT-Netzwerk eines Krankenhauses, werden auch die Probleme für Datensicherheit und Datenschutz sowie die Verantwortlichkeiten innerhalb des Zusammenwirkens von Hersteller und Betreiber erörtert. U. a. aus diesen Problemen, für das Gesundheitswesen als wichtiger Infrastrukturbereich, hat sich eine nationale Gesetzgebung zur IT-Sicherheit ergeben, die auch betrachtet wird. Neben integrierter Software, wird auch die eigenständige Software als Medizinprodukt behandelt. Dabei wird aufgezeigt, wie beide Verordnungen, als auch die nationale Politik, die bisherigen Probleme dieses Anwendungsfeldes aufzugreifen. Die Diskussion, welche Auswirkungen die Anforderungen an Datensicherheit und Datenschutz auf den Medizinproduktemarkt haben, bildet den Abschluss dieser Arbeit.

# ABSTRACT

This thesis deals with the topic of data protection requirements in medical technology. In the context of this work, these requirements relate to the reform of the European directives for medical devices and data protection to the Medical Device Regulation (MDR) and the General Data Protection Regulation (GDPR). After an introduction into relevant terminology for data security and data protection, a detailed analysis of both regulation texts elaborates their goals and strategies for improving data security and data protection. Furthermore, the principles formulated on the basis of them, security and performance requirements, as well as the measures that must be implemented by manufacturers and operators of medical devices, will be highlighted. The thesis also mentions guidelines and standards that can serve as an aid to compliance for manufacturers and operators. Focusing on a typical application field of medical devices, the medical IT network of a hospital, the problems for data security and data protection, as well as the responsibilities within the interaction of manufacturer and operator, are discussed. Out of these problems and further ones for the health service, as an important infrastructure sector, a national legislation for IT security resulted. In addition to integrated software, stand-alone software as a medical device is also considered. It is shown, how both regulations, as well as national policy, take up the past problems inside this application field. A discussion about the effect, which the requirements for data security and data protection have on medical device market, finishes this thesis.

# INHALTSVERZEICHNIS

# 1 EINLEITUNG

Die Digitalisierungstechnologien unserer heutigen Zeit halten zunehmend Einzug in das Gesundheitssystem. Während Märkte anderer Branchen, wie z. B. der Unterhaltungsindustrie, fließend mit dem Strom dieser Technologien mitschwimmen können, ist dies in der Medizinprodukt-Branche undenkbar. Viel zu riskant würden sich Produkte bei einem unregulierten Eintritt und unkontrollierten Veränderungen des Marktes auf die Patientensicherheit auswirken. Umso verzwickter ist jedoch die Situation, wenn man bedenkt wie schnell sich diese elektronischen Technologien modernisieren. Mit ihren immer kürzer und frequenter werdenden Entwicklungsintervallen stehen sie in Kontrast zu komplexen Infrastrukturen des Gesundheitswesens, einem sehr sensiblen Markt, langen politischen Entscheidungswegen, umfangreichen regulatorischen Anpassungen und mehrjährigen Produktlebenszyklen medizintechnischer Geräte. Durch diese Diskrepanz kann eine Gefahr für die Sicherheit entstehen. Diese Gefahr besteht auch für die Sicherheit und den Schutz von Daten, die durch Medizinprodukte verarbeitet werden. Dabei unterstützen Software-Programme mit Algorithmen bei der Zusammenführung der Daten zu Informationen, die die Grundlage der medizinischen Diagnostik und Ausrichtung von therapeutischen Behandlungen bilden. Aus diesem Grund kommt diesen Daten ein hoher Stellenwert zu, was sie schützenswert macht. Es braucht daher verbindliche und einheitliche Regeln für den Umgang mit Daten, als auch für die Konformität der Informationstechnik und ihren Maßnahmen zur Sicherung der verarbeitenden Daten. Den rechtlichen Rahmen dafür schaffte die EU-Regierung durch die Reformierung aus den europäischen Richtlinien für Medizinprodukte und Datenschutz zu den Verordnungen Medical Device Regulation (MDR) und Datenschutz-Grundverordnung (DSGVO). Im Folgenden werden die Ziele und Strategien beider Verordnungen zur Verbesserung der Datensicherheit und des Datenschutzes herausgearbeitet. Des Weiteren wurden aus Ihnen Anforderungen formuliert, die für Hersteller und Betreiber von Medizinprodukten verbindlich umzusetzen sind.

# 2 EINFÜHRUNG IN DEN DATENSCHUTZ

Der Begriff des Datenschutzes kann sehr weit gefasst werden, da unter diesen jegliche Arten von Daten fallen, die schützenswert sein können. Daten werden als einzelne Attribute zu einer Information zugeordnet. Somit können Daten als Teil einer Information verstanden werden. Der Datenschutz hat die zentrale Aufgabe jedes einzelne Individuum insofern zu schützen, dass diesem kein persönlicher Schaden entsteht. Andernfalls würde dies die Verletzung seines Persönlichkeitsrechtes, als menschliches Grundrecht, bedeuten. Im Hinblick auf die Datensicherheit entsteht ein persönlicher Schaden, wenn die Daten unerlaubt erhoben und zur Erschließung personenbezogener Informationen verarbeitet werden. Unerlaubt wäre dies in einer Art und Weise, die das betreffende Individuum nicht wollen würde [1].

Die Maßnahmen für den Datenschutz können sich also insofern komplex gestalten, je komplexer auch der Umfang an zu verarbeitenden Daten wird. Denn damit steigt auch die Zahl der Möglichkeiten auf personenbezogene Informationen rückzuschließen. Dieser genannte Umfang an Daten bildet sich in einem informationsverarbeitenden System aus, welches in seinen Anforderungen größer aufgefasst werden muss. Dieses System soll insofern funktionssicher sein, dass es nur solche Zustände annimmt, die zu keiner unerlaubten Veränderung oder Gewinnung von Informationen führen. Dies beschreibt die, dem Datenschutz übergeordnete, IT-Sicherheit, Informationssicherheit oder Datensicherheit. Sie trägt die Schutzziele der Verfügbarkeit, Vertraulichkeit und Integrität [1].

- **Verfügbarkeit**

Unabhängig von der genauen Beschaffenheit eines informationsverarbeitenden Systems, gilt es als funktionssicher, wenn die Daten oder Informationen wie vorhergesehen genutzt werden können und von diesem Zustand nicht abgewichen wird. Dafür müssen die Daten, mit der ein autorisierter Anwender arbeiten soll, zu jedem Zeitpunkt vorhanden und zugänglich sein. Dies beschreibt das Schutzziel der Verfügbarkeit [1].

- **Vertraulichkeit**

Sind Daten oder Informationen als vertraulich zu behandeln, da ihre Schutzwürdigkeit dementsprechend eingestuft wurde, so dürfen sie nicht herausgegeben werden. Der vorhergesehene Zustand des informationsverarbeitenden Systems ist nur dann hergestellt, wenn ausschließlich befugte Anwender den Zugang in zulässiger Weise erhalten. Dies beschreibt das Schutzziel der Vertraulichkeit [1].

- **Integrität**

Das Schutzziel der Integrität ist insofern wichtig, als dass es die Richtigkeit einer Information sicherstellt. Ein funktionssicheres informationsverarbeitendes System kann dafür nur jenes sein, das nur vollständige und korrekte, auch unversehrt genannte, Daten beinhält. Aus falschen oder unerlaubt manipulierten Attributen würden sich falsche und nicht integre Informationen ableiten lassen [1].

- **Compliance**

Erläuterte Schutzziele bilden die Grundlage für den Aufbau eines funktionsgemäßen, und damit sicheren, informationsverarbeitenden Systems. Compliance bedeutet hierbei, dass dieser Aufbau auch geltende Gesetze und Regeln, z. B. abgemachte Verträge, berücksichtigen muss [1].

- **Medizinisches IT-Netzwerk**

Im Zuge des technologischen Fortschritts entwickelten sich informationsverarbeitende Systeme, die zunehmend computergestützte Prozesse zur digitalen Datenverarbeitung nutzten. Die Vorteile in der Effizienz und Wirtschaftlichkeit der Erhebung, Verwaltung und Auswertung von Daten, die kurzen Innovationszyklen sowie die weitere Schaffung von kabelgebundenen und drahtlosen Kommunikationsmöglichkeiten von Informationssystemen begünstigten die Erweiterung zu informationstechnischen Netzwerken.

Auch in die Entwicklung von Medizintechnik hielt dieser Fortschritt gleichermaßen Einzug, durch Einbindung von Softwareprogrammen für die digitale Datenverarbeitung und Schnittstellen-Technologien für die Vernetzung zu einem medizinischen IT-Netzwerk.

Nach Norm EN IEC 80001-1 definiert sich diese besondere Art eines Netzwerkes dadurch, dass mindestens ein Medizinprodukt in dieses eingegliedert ist. Medizin- und Informationstechnik agieren hierbei miteinander, wodurch sich aus mehrerer Hinsicht der Regulierungsgrad erhöht. Denn nicht nur die Pflicht zur Gewährleistung der physischen Unversehrtheit von Patienten, Anwendern und Dritten besteht. Sobald Medizinprodukte in ein IT-Netzwerk integriert werden, obliegt hierbei auch die Verantwortung zur Einhaltung des Datenschutzes und der Datensicherheit auf beiden Seiten. Auf der Seite des Betreibers der medizinischen Netzwerkorganisation, z. B. Gesundheitsdienstleister sowie des Herstellers der eingebundenen Medizinprodukte [2].

Datenschutz-, aber auch gleichzeitig Medizinprodukt-Regulierungen greifen hierbei mit gleicher Bestimmtheit ein, um die Sicherheit einzuhalten. Denn die, in diesem Kontext erhobenen und zu verarbeitenden, Gesundheitsdaten sind als besondere Art personenbezogener Daten einzuordnen und gelten als besonders schützenswert [3]. Die Verfehlung der Datensicherheits-Schutzziele kann aber auch gleichzeitig nicht nur ein unmittelbares Risiko für die persönliche, sondern auch physische, Patientensicherheit darstellen.

Welche Regulierungen die Datensicherheit, als Beitrag zur Patientensicherheit, betreffen, soll in den nachfolgenden Abschnitten vertieft werden.

# 3 RECHT UND ANWENDUNG DES DATENSCHUTZES

Da der Datenschutz in der Medizintechnik durch die Rechtsprechung erst umsetzbar werden kann, ist es wichtig auf den rechtlichen Hintergrund genauer einzugehen. Dabei sind als wichtigste zentrale Regularien auf europäischer Ebene die Verordnungen Medical Device Regulation und Datenschutz-Grundverordnung zu nennen. Aus diesen Verordnungen ergeben sich Maßnahmen, die in praktische Anwendungsfelder von Medizinprodukten übertragen werden.

## 3.1 EUROPÄISCHE MEDICAL DEVICE REGULATION (MDR)

Eine dieser erwähnten Regulierungen wird durch die europäische Verordnung (2017/745), Medical Device Regulation (MDR), gestellt. Sie ist am 25. Mai 2017 offiziell in Kraft getreten. Nach einer Übergangsfrist von zwei Jahren, sowie einer Pandemie bedingten Verschiebung um ein weiteres Jahr, muss die Verordnung seit 26. Mai 2021 bereits in die nationalen Bestimmungen jedes EU-Mitgliedsstaates übertragen worden sein. Dies ist insofern erforderlich geworden, da die neue EU-Regulierung als Verordnung einen unmittelbar verbindlichen Charakter hat und sich somit einheitlich über nationale gesetzliche Regelungen stellt. Im Gegensatz dazu waren die vorherigen Medizinprodukt-Richtlinien insofern nur in ihren zu erreichenden Zielen für den adressierten Staat verbindlich umzusetzen. In Deutschland wurde dies, nach eigenem Ermessen des Landes, in das Medizinproduktegesetz (MPG) umgesetzt. Dies hatte, so wie in jedem anderen EU-Mitgliedsstaat auch, das Resultat uneinheitlicher Gesetzmäßigkeiten [4].

Dieser Zustand wurde somit per EU-Verordnung, durch die Ablösung der bisher für die EU geltenden drei Richtlinien für Medizinprodukte, korrigiert:

• Richtlinie 93/42/EWG für allgemeine Medizinprodukte (MDD),

• Richtlinie 98/79/EG für in-vitro Diagnostik Medizinprodukte (IVDD),

• Richtlinie 90/385/EWG für aktive implantierbare medizinische Geräte (AIMDD) [2].

Die Richtlinien für allgemeine Medizinprodukte und aktive implantierbare medizinische Geräte wurden zu einer Verordnung zusammengeführt [2]. Die andere Richtlinie für in-vitro Diagnostik

Medizinprodukte IVDR ist eine eigene Verordnung mit eigenem Geltungsbeginn ab dem 26. Mai 2022 [5]. Auf diese soll in der Arbeit nicht weiter eingegangen werden.

Die genaue Auseinandersetzung mit der MDR ist für Hersteller von Medizinprodukten so wichtig, da sie den rechtlichen Rahmen zur Zulassung der Medizinprodukte im europäischen Wirtschaftsraum gibt. Eine Zulassung bedeutet, dass die Konformität mit diesen rechtlichen Rahmenbedingungen gewährleistet ist, was wiederum durch eine CE-Kennzeichnung (französisch für Conformité Européenne) für das Produkt signalisiert wird [4].

Eine genaue Betrachtung der MDR soll Aufschluss darüber geben, ob und welche Maßnahmen zum Datenschutz von der europäischen Regierung angeordnet wurden. Dies wäre eine direkte Orientierungsmöglichkeit für einen Medizinprodukt-Hersteller.

Die MDR strukturiert sich in Erwägungsgründe, einen Hauptteil aus zehn Kapiteln sowie siebzehn weiteren Anhängen, dargestellt in Abbildung 1 [4].


**Abb. 1** ***Gliederung der MDR (eigene Darstellung)*** **[4]**

Mittels ihrer Erwägungsgründe macht die Verordnung deutlich, dass der Rechtsrahmen aus den Richtlinien 93/42/EWG für allgemeine Medizinprodukte und 90/385/EWG für aktive

implantierbare medizinische Geräte besteht. Jedoch musste dieser überarbeitet werden, um dem technologischen Fortschritt gerecht zu werden. Vor allem die zunehmende Zahl an digitalen Gesundheitsanwendungen machten diesen Schritt der Anpassung notwendig, um die Zulassung auch in diesem Bereich stärker regulieren zu können. [4] Aus diesem Grund wäre zu erwarten, dass innerhalb dieser Erwägungsgründe auch das Ziel des Datenschutzes genannt wird. Dieser kann schließlich, wie bereits erläutert, auch unmittelbar zur Sicherheit des Patienten beitragen.

Aus den 101 Erwägungsgründen wurden in einer Analyse 30 Zielkategorien festgestellt, aus denen sich die Begründung zur Einführung der neuen MDR ergeben. Das Ergebnis der Analyse ist in Abbildung 2 zu sehen [4].

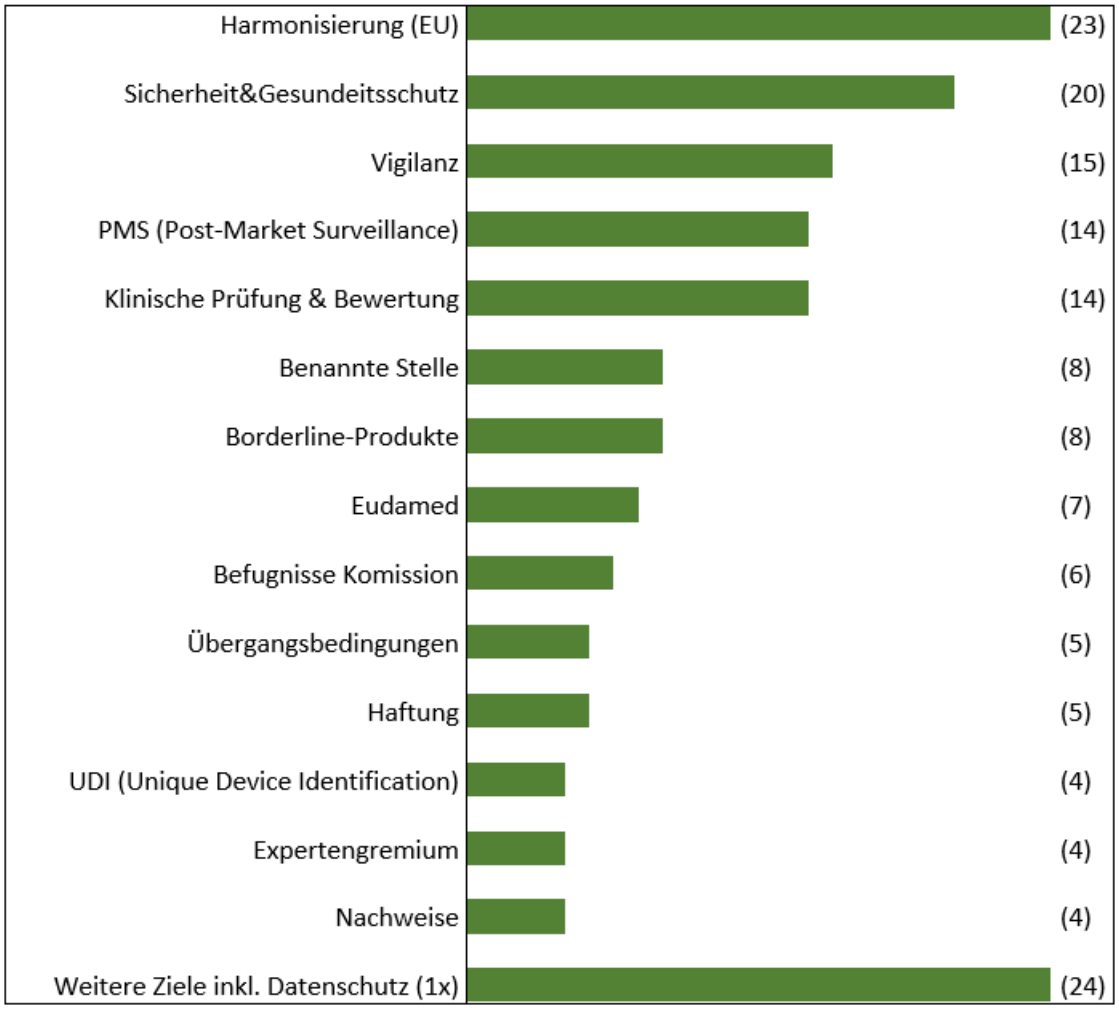


**Abb. 2** ***Zielkategorien der Erwägungsgründe aus der MDR, Analyse-Ergebnis (eigene Darstellung)*** **[4]**

Mit einer Nennung in Erwägungsgrund Nummer 47 fällt der Datenschutz in die zusammengefasste Kategorie der weiteren Ziele, da dieser weniger als vier Mal erwähnt wird. Erwähnungsgrund 47 bezieht sich auf die Datenerfassung und Verarbeitung innerhalb der elektronischen EUDAMED Datenbank [6]. Diese Datenbank wurde mit der MDR als verpflichtende Anforderung eingeführt. Die EUDAMED (European Databank on Medical Devices) hat den Zweck alle Medizinprodukte, die sich auf dem EU-Markt befinden, zu erfassen. Hierzu gehören auch u. a. Informationen, Dokumente, Bescheinigungen, gemeldete Zwischenfälle, klinische Prüfungen und Wirtschaftsakteure, z. B. Hersteller und Bevollmächtigte, die in Verbindung mit dem eindeutig registrierten Produkt stehen. Damit wird die Überwachung des Marktes durch die zuständigen Behörden verbessert, da die Produktinformationen europaweit über eine einheitliche Plattform verfügbar sind [7] [8].

Somit ist erkennbar, dass der Datenschutz nicht als maßgeblicher Beweggrund zur Einführung der MDR gesehen wird. Er ist zumindest nicht als Erwägungsgrund konkret genannt. Vielmehr kann als größte Motivation zur neuen MDR die Harmonisierung von Vorschriften innerhalb der europäischen Union betrachtet werden. Danach die Stärkung der Sicherheit und des Gesundheitsschutzes, gefolgt von Verbesserungen der Marktüberwachung [4].

Mit entsprechender Strenge sind die Schwerpunkte der Zielsetzung auch im nachfolgenden Verlauf des MDR-Textes wiederzufinden. Um als verbindliche Verordnung auch unmittelbar und einheitlich in jedes nationale Recht übertragbar zu sein, wurden die gesetzlichen Mindestanforderungen detaillierter gefasst. So sind diese in die Anforderungen für die Benannten Stellen nach einheitlicheren Abläufe und Unterlagen, als auch in die der klinischen Bewertung, Prüfung, Marktbeobachtung, Vigilanz sowie technischen Dokumentation mit eingeflossen [4].

So ist in diesem Zusammenhang für die Betrachtung aus Datenschutzsicht, besonders der Anhang I der MDR zu erwähnen, in dem die grundlegenden Sicherheits- und Leistungsanforderungen spezifiziert werden. Die zunehmende Einbeziehung von informationsverarbeitender Software in Medizinprodukten hat auch in der MDR zur Aufnahme neuer Anforderungen an die IT-Sicherheit geführt [4].

So wird in Abs 14.2.d) von den Risiken gesprochen, die aus einer eventuell negativen Wechselwirkung zwischen Software und dem IT-Netzwerk entstehen können. Diese Risiken müssen die Hersteller bei der Auslegung und Herstellung ihrer Produkte soweit wie möglich reduzieren bis ganz ausschließen [6].

Abs 14.5 betont zudem, dass bei Auslegung und Herstellung die Zuverlässigkeit und Sicherheit bei der Kompatibilität zwischen Medizinprodukten, aber auch Nicht-Medizinprodukten, eingehalten werden muss [6].

In Abs 17.4. macht die Verordnung deutlich, dass die Hersteller für den bestimmungsgemäßen Betrieb ihrer Software Mindestanforderungen festlegen müssen. Hierbei wird die geforderte Datensicherheit nicht nur auf die Hardware zurückgeführt, sondern soll auch in den Eigenschaften der IT-Netzwerke sowie IT-Sicherheitsmaßnahmen, inklusive des Schutzes vor unbefugtem Zugriff, Berücksichtigung finden [4].

Nach Absatz 18.8 sind die Medizinprodukte so auszulegen und herzustellen, dass sie so weit wie möglich vor unbefugtem Zugriff geschützt sind, da dieser den bestimmungsgemäßen Betrieb des Produkts beeinträchtigen könnte [6].

Abs 17.2 spezifiziert weiter die grundlegende Sicherheits- und Leistungsanforderung an Medizinprodukte mit Software, dass sie entsprechend nach dem Stand der Technik entwickelt und hergestellt werden müssen [9].

Daraus lässt sich ableiten, dass für die europäische Regierung auch die Datensicherheit als Teil zur Erfüllung der Zielsetzung für mehr Sicherheit und Wirksamkeit der Medizinprodukte gesehen wird. Die Hersteller haben somit ihre Produkte auch datentechnisch sicher zu gestalten, um eine Konformität erlangen zu können [4].

Die Sicherheit wird für den gesamten Produktlebenszyklus durch ein Risikomanagement des Herstellers eingeschätzt, welches Teil des verpflichtenden Qualitätsmanagementsystems ist. Hierbei werden die Risiken miteinbezogen, die, nach Abs 2 Anhang I der MDR, in vertretbarem Verhältnis zum klinischen Nutzen stehen sollen. In Übertragung auf die IT-Sicherheit sind dies die Patientenrisiken, die aus der Verletzung der drei Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit folgen könnten [4].

Für weitere Vertiefungen können den Herstellern die Anforderungen aus den folgenden Normen helfen, die einen Bezug zur Datensicherheit bei Medizinprodukten herstellen. Das Risikomanagement bei Medizinprodukten aus ISO 14971, der Software-Lebenszyklus bei Medizinprodukten aus IEC 62304, das Qualitätsmanagement für Medizinprodukte aus ISO 13485, der Standard IEC 60601-1 zu medizinischen elektrischen Geräten sowie der Standard IEC 60601-4-5, der die Datensicherheit bei netzwerkintegrierten Medizinprodukten behandelt. [4]

Im Konformitätsbewertungsverfahren werden die Medizinprodukte, auf Grundlage der Zweckbestimmung sowie nach Potenzial der identifizierten Risiken, in vier Risikoklassen I (niedrig), IIa (mittel), IIb (erhöht) und III (hoch) eingeteilt. Dieses Verfahren erfolgt unterschiedlich eingängig, je höher die Risikoklasse ausfällt. Aus den Neuerungen im Konformitätsbewertungsverfahren kann dabei festgehalten werden, dass der europäischen Regierung die sicherheitsrelevante Tragweite eigenständiger Medizinprodukt-Software deutlich bewusster geworden ist. Für diese gilt die neue Regel 11 Anhang VIII der MDR, welche eine höhere Risikoklassifizierung vorsieht, als es in der vorherigen Richtlinie der Fall war [4]. Eigenständige Medizinproduktesoftware (z. B. mobile medizinische Apps) hatten nach der Regel 12 der Medizinprodukt-Richtlinie eine Einstufung in Risikoklasse I erhalten [10].

Software, die in ein Medizinprodukt eingebettet ist, wird entsprechend des insgesamten Risikopotenzials der Einheit bewertet. Genauso, wie nun auch die eigenständige Software, mindestens in die Klasse IIa der nichtaktiven und aktiven Medizinprodukte. Sollte die Einbindung von Software in ein aktiv implantierbares Medizinprodukt bestehen, so gehört die Einteilung immer in die Klasse III [1].

Damit wird deutlich, dass datenschutzrechtliche Maßnahmen nicht nur im eingangs erwähnten Kontext des medizinischen IT-Netzwerkes bestehen müssen, sondern auch für eigenständige Software, die als Medizinprodukt gilt.

Die besondere Stellungnahme in der MDR zur Datensicherheit setzte die europäische Kommission weiter fort. Im Dezember 2019 veröffentlichte die MDCG (Medical Device Coordination Group) den Leitfaden „Guidance on Cybersecurity for Medical Devices“. Dieser gibt den Medizinprodukt-Herstellern eine Übersicht über Anforderungen, Erklärungen zu Begriffen und schlägt Konzepte und Gestaltungsmöglichkeiten zur Datensicherheit vor, um die grundlegenden Datensicherheitsanforderungen aus Anhang I der MDR erfüllen zu können [11] [12].

Einen Hauptaspekt der Leitlinien bildet die Risikoprävention der Informationssicherheit. Sie schließt darin die Betriebssicherheit, Informationssicherheit mit ihrem Datenschutz sowie die Effektivität der Sicherheitsmechanismen der Medizinprodukte mit ein. Dazu gehören vor allem die Konstruktionssicherheit, das Datensicherheitsrisikomanagement, die Berücksichtigung von Sicherheitsleistung, Standardverfahren zur Beurteilung von Sicherheitsrisiken, die Risiko-Nutzen-Analyse für Sicherheitsaspekte, die Erfüllung von Mindestanforderungen der Datensicherheit, die Validierung und Verifizierung über den gesamten Produktlebenszyklus,

Sicherheitsaspekte bei Dokumentation und Gebrauchsanweisung sowie die andauernde Überwachung von Schwachstellen und deren Behebung. [11]

In weiterer Auseinandersetzung hat die Arbeitsgruppe des International Medical Device Regulators Forum im März 2020 mit den „Principles and Practices for Medical Device Cybersecurity“ die Sicherheitsaspekte weltweit harmonisiert [11].

Ebenfalls auf europäischer Ebene wurde die Bedeutung der Cybersicherheit im Gesundheitswesen, durch Inkrafttreten der EU-Verordnung 2019/881, unterstrichen. Diese schaffte im April 2019 die Agentur für Cybersicherheit (ENISA) und führte eine neue Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ein. Das Hauptziel der Verordnung ist, die Informationssicherheit bereits in die Entwicklung von Produkten, Diensten und Prozessen verbindlich zu machen [13]. Im Januar 2021 veröffentlichte sie ein Dokument, das Organisationen des Gesundheitswesens zur Einhaltung aller erforderlichen Sicherheitsmaßnahmen bei Nutzung von externen Cloud-Diensten, zur Datensammlung durch medizinische Geräte, bewegen soll. Die Veröffentlichung dieses Dokuments macht deutlich, wie stark das Risiko, durch die Bedrohung des unrechtmäßigen Eindringens von außen, für die IT-Sicherheit zugenommen hat.

Nachdem die MDR Software, als Umgebung sensibler Datenverarbeitung, in ihrem Risikopotenzial höherstellt sowie die Datensicherheit als eine relevante Anforderung zur Erreichung der Sicherheit und des Gesundheitsschutzes anerkennt, stellt die Medizinprodukt-Verordnung explizit ein Kapitel, welches u. a. den Datenschutz direkt anspricht (Kapitel IX, siehe Abbildung 1). In Artikel 110 (1) der MDR heißt es demnach: „Bei der Verarbeitung personenbezogener Daten im Rahmen der Durchführung dieser Verordnung beachten die Mitgliedstaaten die Richtlinie 95/46/EG.“ [6]

Die Richtlinie 95/46/EG bezeichnet die im Jahr 1995 erlassene EU-Datenschutz-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Mit verbindlichem Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung DSGVO, per EU-Verordnung Nr. 2016/679, wurde sie am 25. Mai 2018 abgelöst [14]. Die MDR verweist damit auf die für alle Mitgliedsstaaten verbindliche Überführung der DSGVO in ihre nationalen Datenschutzgesetze. Diese müssen, laut MDR, auch in Bezug auf alle datenverarbeitenden Medizinprodukte Berücksichtigung finden, die für den EU-Markt zugelassen werden.

## 3.2 EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Die DSGVO stellt Grundsätze, Begriffsdefinitionen und Mindestanforderungen an den Datenschutz für sämtliche Lebenssachverhalte, in denen personenbezogene Daten verarbeitet werden. Auch berücksichtigt es die Dateisysteme, in die gespeichert werden soll [14]. Dadurch werden die Hersteller, wie auch Betreiber von Medizinprodukten durch die Verordnung angesprochen, da eingebettete bzw. eigenständige Medizinprodukt-Software und Gesundheitsdienstleistungs-Verwaltungssysteme personenbezogene Daten verarbeiten. In diesen Anwendungsfeldern der Datenverarbeitung gilt es die Arten von Daten noch weiter zu unterscheiden.

Nach Art 4 Z 1 der DSGVO bedeutet personenbezogen, dass alle Informationen auf eine betroffene Person bezogen werden können und durch besondere Kennung oder Merkmale auf dessen physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Identität zurückgeschlossen werden kann [15].

Eine besondere Kategorie der personenbezogenen Daten bilden die sensiblen Daten, die, nach Art 9 Abs 1, auf die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, aber auch auf die sexuelle Orientierung und die Gesundheit schließen lassen [15]. Mit Letzterem sind die Gesundheitsdaten gemeint, welche in praktischer Anwendung, durch Medizinprodukt-Software oder Verwaltung bei Gesundheitsdienstleistern, besonders vorkommen. Diese Differenzierung ist nötig, da sensible Daten einem noch stärkeren Schutzbedürfnis unterliegen, da, nach Erwähnungsgrund 51 der DSGVO, mit ihrer Verarbeitung erhebliche Risiken für Grundrechte und Grundfreiheiten, z. B. informationelle Selbstbestimmung, auftreten können [15]. Dies macht die hohe Bedeutsamkeit sicherer Datenschutzmaßnahmen und die Verantwortung klar, der sich Hersteller und Betreiber von Medizinprodukten bewusst sein müssen. Nicht zuletzt, da die Sanktionsmöglichkeiten bei Verstößen sehr hoch ausfallen können. In Art 8, 11, 25 bis 39, 42 und 43 der DSGVO werden Pflichten für Verantwortliche oder Auftragsverarbeiter beschrieben, deren Verletzung, je nach Bedingungen und Ermessen, Strafzahlungen von bis zu 10 Mio. € oder 2 % des weltweit erwirtschafteten Gesamtumsatzes des abgelaufenen Wirtschaftsjahres bedeuten können [14].

### 3.2.1 RELEVANTE GRUNDSÄTZE UND PFLICHTEN AUS DER DSGVO

Die eingangs erwähnten Schutzziele der Informationssicherheit, Verfügbarkeit, Vertraulichkeit und Integrität werden durch Art 5 DSGVO in ihren Grundsätzen für die Verarbeitung

personenbezogener Daten aufgegriffen und dem Verantwortlichen rechtsbindend zur Einhaltung zugewiesen. Dieser hat dafür Sorge zu tragen, dass nachvollziehbar ist welche Daten zu welchem Zweck erhoben und verarbeitet werden („Transparenz“). Der Zweck zur Verarbeitung muss genau und rechtmäßig festgelegt sein („Zweckbindung“), denn nach diesem richtet sich die Angemessenheit der notwendigen Datenmenge („Datenminimierung“). Die Daten müssen stets sachlich korrekt und, falls erforderlich, aktuell gehalten werden. Unrichtige Daten dürfen nicht vorhanden sein. Dafür müssen Maßnahmen zur unverzüglichen Löschung oder Korrektur getroffen werden („Richtigkeit“). Die Daten dürfen zeitlich nicht unbegrenzt in einer Form gespeichert sein, die eine Identifizierung des Betroffenen möglich macht. Dieser Zustand begrenzt sich lediglich auf die Zeit der Datenverarbeitung, bis der vereinbarte Zweck erfüllt wurde. Für Archivzwecke oder statistische Zwecke gibt es Sonderregelungen („Speicherbegrenzung“). Die Datenverarbeitung ist durch geeignete technische und organisatorische Maßnahmen so zu gestalten, dass die Sicherheit der personenbezogenen Daten gewährleistet werden kann. Als Gefahren für die Datensicherheit werden die unbefugte oder unrechtmäßige Verarbeitung, unbeabsichtigte Zerstörung, Schädigung oder der Verlust genannt („Integrität und Vertraulichkeit“) [16].

Ein Grundsatz, der in Anwendung mit Medizinprodukten berücksichtigt werden muss, ist die nach Art 7 DSGVO einzuholende ausdrückliche Einwilligung des Betroffenen zur Erhebung und Verarbeitung seiner Daten. Er muss freiwillig und in Kenntnis der Sachlage, durch eine eindeutig bestätigende Handlung, seine Zustimmung geben. Jedes Einwilligungsformular muss in einer klar verständlichen Sprache verfasst sein und die betroffene Person muss über die erhobenen Daten sowie deren Verwendung aufgeklärt werden. Die Einwilligung ist besonders wichtig für die Gesundheitsdaten, als besondere Kategorie personenbezogener Daten, die ohne ausdrückliche Einwilligung nicht erhoben oder verarbeitet werden dürfen. Die Verarbeitung von Daten einer besonderen Kategorie ist nur unter bestimmten Umständen zulässig, wie in Artikel 9 DSGVO dargelegt wird [16].

Weiter in der DSGVO ergeben sich auch konkrete organisatorische Pflichten für jede datenverarbeitende Stelle. Darunter fällt Art 30 DSGVO, der Verantwortliche und Auftragsverarbeiter dazu verpflichtet ein aktualisiertes Verzeichnis all ihrer Datenverarbeitungstätigkeiten anzufertigen. Dem Betroffenen müssen, nach Art 13 DSGVO, Informationen über den Verantwortlichen, die Zwecke der Verarbeitung, Speicherdauer, Absichtserklärungen sowie weitere Aufklärungen zu verschiedenen Rechten des Betroffenen zukommen. In der Regel werden diese Informationen dem Betroffenen in Form einer Datenschutzerklärung oder Datenschutzbestimmung kommuniziert. Sollte es zu Verletzungen

des Schutzes personenbezogener Daten kommen, so ist der Verantwortliche, nach Art 33 DSGVO, verpflichtet diese an die Aufsichtsbehörde weiterzuleiten. Sollte sich ein hohes Risiko für den Betroffenen ergeben, so muss diesem auch eine Meldung zukommen. Der Auftragsverarbeiter hat bei Kenntnis von Datenschutzverletzungen den Verantwortlichen zu informieren [16].

Besonders interessant für die Integration von technischen Datenschutzmaßnahmen in die Entwicklung von Medizinprodukten oder organisatorischen Datenverwaltungssystemen ist der Art 25 DSGVO. Hierbei muss sich die Gestaltung der Technik danach richten die Sicherheit der Daten gewährleisten zu können. Diese Anforderung wird auch als privacy by design bezeichnet. Welche Schutzmaßnahmen hierbei konkret anzuwenden sind wird in der DSGVO weitestgehend offen gelassen. Den Herstellern solche Freiräume zu lassen, bei gleichzeitigem Verweis auf den Stand der Technik, ergibt insofern Sinn, dass die Verordnung mit den schnellen technischen Entwicklungen der Datensicherheit beständig bleiben kann. Es werden zeitlos gültige Datenschutzmaßnahmen, wie die Pseudonymisierung, genannt [17]. Nach Art 4 DSGVO, ist dies eine Weise, in der die Datenverarbeitung erfolgen kann. Dabei können personenbezogene Daten ohne zusätzliche Informationen nicht mehr dem Betroffenen zugeordnet werden. Dies entsteht durch das Austauschen von Daten, die eine Identifikation des Betroffenen möglich machen würden, mit einem Ersatz, einem sogenannten Pseudonym. Die zusätzlich erforderlichen Informationen zur Zuordnung zwischen Betroffenem und den Pseudonymen werden getrennt voneinander gespeichert. Durch technische und organisatorische Maßnahmen soll die Verbindung zwischen den Daten auf ihre zugehörige Person nicht direkt möglich gemacht werden [16] [18]. Auch in Erwägungsgrund Nr. 78 zu geeigneten technischen und organisatorische Maßnahmen findet sich kein weiterer Hinweis auf weitere konkrete Hinweise zur Umsetzung. An anderen Stellen der Gesetzgebung werden die Verschlüsselung sowie die Anonymisierung der Daten genannt [17]. Im Gegensatz zur Pseudonymisierung werden alle identifizierenden Merkmale aus personenbezogenen Daten nicht ausgetauscht, sondern gelöscht, sodass diese nicht mehr oder nur mit sehr hohem Aufwand dem Betroffenen wieder zuordenbar sind [18].

Neben dem Datenschutz durch Technikgestaltung, nennt der gleiche Art 25 DSGVO auch den Datenschutz durch datenschutzfreundliche Voreinstellungen, auch privacy by default genannt. Der Verantwortliche hat die Datenverarbeitung so voreinzustellen, dass nur die zur Verarbeitung erforderlichen Daten genutzt werden. Privacy by default entspricht somit dem Datenschutzgrundsatz der Datenminimierung [19].

Insgesamt soll durch die technischen und organisatorischen Maßnahmen ein dem Risiko angemessenes Sicherheitsniveau der Verarbeitung erzielt werden (Art 32 DSGVO). Dies schließt die Pseudonymisierung und Verschlüsselung personenbezogener Daten mit ein. Auch die anfangs erwähnten Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) sind in den Ansprüchen an ein belastbares Datenverarbeitungs-System wiederzufinden. Sollte es zu einem physischen oder technischen Ausfall des verarbeitenden Systems kommen, so müssen gesetzte Maßnahmen die Verfügbarkeit und den Zugang zu den personenbezogenen Daten schnell wiederherstellen können. Abschließend müssen auch alle Maßnahmen auf ihre Wirksamkeit fortlaufend überprüft, bewertet und evaluiert werden [16].

Soweit lässt sich zusammenfassen, dass die Datenschutz-Grundverordnung auf zwei Säulen aufbaut, um das zentrale Ziel, den Schutz natürlicher Personen, zu erreichen: Grundsätze, Begriffsdefinitionen und Mindestanforderungen für die Verarbeitung personenbezogener Daten sowie die Sicherung der Grundrechte und Grundfreiheiten.
Die DSGVO geht jedoch noch weiter und ergänzt die beiden Säulen durch eine dritte des Risikomanagements für den Datenschutz. Gemeint ist konkret die, in Art 35 Abs 1 DSGVO, genannte Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung. Diese muss durch den Verantwortlichen bereits im Vorfeld durchgeführt werden. Hierbei müssen Risiken sowie ihre Folgen, die durch die Verarbeitung personenbezogener Daten entstehen können, analysiert und bewertet werden. Der Fokus der Bewertung wird hierbei auf mögliche Risiken und Folgen der Datenverarbeitung durch neue Technologien gelenkt, die nach Art, Umfang, Umstand oder Zweck der Verarbeitung entstehen können [14].

Nach Art 35 Abs 7 DSGVO muss die Folgeabschätzung ein Mindestmaß an Informationen enthalten. So ist eine systematische Beschreibung der Datenverarbeitungsvorgänge und der Zwecke der Verarbeitung nötig. Hinzu kommt eine Bewertung der Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung. Zur besseren rechtlichen Einordnung liefert die DSGVO hierzu mehrere Grundsätze für den Datenschutz, z. B. die Datenminimierung, sowie auch für die persönlichen Rechte der Betroffenen, z. B. das Recht auf Information oder auf Auskunft und Berichtigung der Daten. Als drittes wird die Folgenabschätzung für die Grundrechte und Grundfreiheiten genannt. Hierbei muss der Verantwortliche ermitteln, welche Auswirkungen es für einen Betroffenen hat, wenn seine personenbezogenen Daten gestohlen, beschädigt, gelöscht, missbraucht oder manipuliert werden. Abschließend sind Maßnahmen, darunter auch Sicherheitsmaßnahmen, festzulegen, die zum Schutz personenbezogener Daten

angemessen sind sowie der Nachweis erbracht werden, dass die Verordnung eingehalten wird [16].

Die Forderung eines Risikomanagements wird also aus den beiden Verordnungen deutlich. Dabei spricht die MDR deutlicher die Datensicherheit an, während sie für den Schutz personenbezogener Daten und zusammenhängender Grundrechte bzw. Grundfreiheiten auf die DSGVO verweist. Da der Datenschutz ein Teilbereich der Datensicherheit ist, kann über Letztere an das Risikomanagement herangeführt werden.

## 3.3 MEDIZINPRODUKTE IN EINER IT-UMGEBUNG

Besonders bei der Implementierung von Medizinprodukten in eine IT-Netzwerkumgebung, wie sie beispielsweise in einem Krankenhaus auftritt, stellt sich beim Zusammenwirken von Hersteller und Betreiber die Frage nach den Verantwortlichkeiten zum Datenschutz. So wäre der Medizinprodukt-Hersteller, hinsichtlich seiner Produkte, nicht direkt von der DSGVO als Verantwortlicher betroffen. Er ist in diesem Fall ein Auftragsverarbeiter. Er entwickelt seine Produkte für das Krankenhaus des Betreibers, der als Auftragsverantwortlicher damit auch vor der DSGVO als Verantwortlicher der Datenverarbeitung gilt. Denn u. a. über die Medizinprodukte erfolgt die Datenerhebung für das Krankenhaus als Leistungserbringer. Dieser bestimmt die Mittel und den Zweck der Datenverarbeitung, um dem Patienten, mittels ihrer gewonnenen Informationen, adäquate Gesundheitsbehandlungen anbieten zu können [20]. Diese Schlussfolgerung bedeutet jedoch nicht, dass der Hersteller die gesamte Datenschutzarbeit auf den Krankenhausbetreiber legen kann. Denn, wie schon ausgeführt, greift die DSGVO bereits in die Gestaltung der Technik ein und nimmt dadurch Bezug auf die Entwicklung und Auslegung der Medizinprodukte. In ihren technischen Vorgängen der Datenverarbeitung soll der Datenschutz nach Stand der Technik berücksichtigt werden. Damit soll der Hersteller sicherstellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind ihren Datenschutzpflichten nachzukommen [16]. Beschriebener DSGVO Erwägungsgrund Nr. 78 zu geeigneten technischen und organisatorischen Maßnahmen zeigt also auf, dass der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter zusammenarbeiten müssen. Diese Entscheidung erscheint sinnvoll, denn der Hersteller des Medizinproduktes weiß genau in welcher Art und Weise die personenbezogenen Daten verarbeitet werden. Der Hersteller entwickelt nach den Datenschutzanforderungen, führt für sein Produkt die Datenschutzfolgenabschätzung durch und gibt seine Ergebnisse an den Betreiber weiter. Diese kann er, im Hinblick auf die Datensicherheit, bei der Konzeption und dem Aufbau der Krankenhaus-Netzwerkumgebung mitberücksichtigen. So gesehen ergibt sich für den

Hersteller die Beteiligung an der Erfüllung der Ansprüche an ein datensicheres Gesamtsystem des Betreibers.

Das Zusammenwirken von Betreiber und Hersteller wird nicht nur durch die DSGVO motiviert, sondern auch durch die MDR. Um ihr zentrales Ziel zur Stärkung der Patientensicherheit durch Maßnahmen zur Datensicherheit verfolgen zu können, muss die Abstimmung zwischen Betreiber und Hersteller noch besser ineinandergreifen. Bei immer komplexer werdenden Datenverarbeitungsnetzwerken der Gesundheitsdienstleister würden die Gefahren für den Patienten andernfalls größer werden. Dabei lassen sich die allgemeinen Schutzziele und Maßnahmen für die Informationssicherheit aus der MDR und DSGVO auf die real möglichen Gefährdungsszenarien abbilden. Das Kritische an diesen Szenarien ist, dass die Gesundheit des Patienten unmittelbar von der Verfügbarkeit, Vertraulichkeit und Integrität seiner Daten innerhalb des verarbeitenden Netzwerks abhängen kann. Die Schwierigkeit ist gleichzeitig jedoch, dass sich bei solchen Gefährdungsszenarien Hersteller wie auch Betreiber innerhalb ihrer jeweiligen Konformität aufhalten möchten, um rechtlich abgesichert zu sein. Gerade bei einem so sensiblen Thema, wie dem Schutz von Gesundheitsdaten in umfangreichen IT-Netzwerken mit Medizinprodukten, wurde in der Vergangenheit die Verantwortlichkeit auf die jeweils andere Partei geschoben. So sahen die Hersteller von Medizinprodukten oftmals nicht eine Zuständigkeit für die IT-Netzwerke der Betreiber zu haben, in die ihre Produkte integriert wurden. Die Betreiber wiederum beklagten sich, dass sie, durch diese mangelnde Berücksichtigung der Hersteller, ihre Absicherungsaufgaben für die Medizinprodukte innerhalb ihres Netzwerkes gar nicht übernehmen konnten. Eine große Herausforderung resultierte also daraus, dass der Betreiber äußerst vorsichtig mit Modifikationen bei der Integration der Medizinprodukte in seine Netzwerkumgebung umgehen musste. Diese können die Beeinträchtigung der Funktionsfähigkeit des Medizinproduktes mit sich ziehen und damit auch regulatorisch als Eigenherstellung gelten. Der Betreiber würde die volle Rechtsverantwortung für das modifizierte Medizinprodukt übernehmen müssen. Er müsste sogar dafür ein eigenständiges Konformitätsverfahren durchführen, um nachzuweisen, dass durch seine Änderungen keine neuen relevanten Risiken für die Patientensicherheit entstehen. Dieser Aufwand kann durch die Zweckbestimmung des Herstellers vermieden werden. Je nachdem inwieweit er dabei die Integration in Netzwerke datensicherheitstechnisch berücksichtigt hat für sein Produkt. So dürfte der erforderliche Anpassungsbedarf der Medizintechniksoftware in Sachen Informationssicherheit für den Betreiber deutlich kurzlebiger erfolgen, als der Hersteller durch Firmware- und vor allem Sicherheitsupdates tatsächlich validiert und freigibt. Dem in Relation steht, in Anbetracht der rein mechanischen oder elektrischen Sicherheit, die deutlich längere Auslegung der Betriebsdauer des Geräts selbst über mehrere Jahre hinweg

[21]. Dem Betreiber bleibt oftmals keine andere Alternative als das Abwarten auf sicherheitsrelevante Updates oder Freigaben durch den Hersteller. Aus Sicht der Informationssicherheit birgt dieses verzögerte Schließen von Sicherheitslücken immer die Gefahr, dass die Netzwerke, und auch die darin befindlichen Medizingeräte, besonders angreifbar von außen sein können. Ein sogenannter Hacker-Angriff könnte Gesundheitsdaten abgreifen, manipulieren, löschen oder sogar ganz die Funktionsfähigkeit der Medizinprodukte beeinflussen, was unmittelbar die Patientensicherheit gefährdet. Besonders riskant wirken hierbei Teile der Software, die der Hersteller nicht selbst entwickelt hat, sondern von weiterer Seite miteinbezieht. So kann z. B. ein hinzugekauftes Betriebssystem als Basis der Softwarestruktur des Medizinprodukte-Herstellers dienen. Auf die Entwicklung solcher Fremdsoftware hat er jedoch keinen großen Einfluss und muss auch wiederum auf diesen Hersteller warten, bis dieser bekannt gewordene Sicherheitslücken schließt [21].

Die gesetzlichen Regelungen durch das Medizinproduktegesetz MPG bzw. die Medizinprodukte-Betreiberverordnung MPBetreibV waren für solche Streitfragen zwischen Hersteller und Betreiber zu unklar formuliert und wiesen im praktischen Anwendungsfeld vernetzter Medizinprodukte in IT-Umgebungen massive Schwachstellen auf. Auch bei Zuhilfenahme von Normen, z. B. zur Einordnung und Bewertung neuester IT-Entwicklungen in der Patientenbehandlung, entstanden oftmals schwer zu lösende Widersprüche [21].

Die Reformierung durch die Medizinprodukt-Verordnung setzt an dieses Problem an, in dem sie den Rahmen zur Medizinprodukt-Einstufung weit größer fasst für Software, die im Gesundheitsbereich zur Patientenbehandlung genutzt wird. Dies war vor der Reformierung ein Problem [21].

Außerdem war u. a. die mangelnde gesetzlich klare Berücksichtigung des Anteils, den der Datenschutz am Patientenschutz haben kann, ein Problem. Aus dem MPG oder der MPBetreibV heraus war dieser nicht explizit zur Konformität vorgesehen. Aus diesem Grund konnte die Verpflichtung zum Schutz der Patientendaten für den Hersteller nur mittelbar hergeleitet werden. Der Versuch des Gesetzgebers diese Regelungslücke aufzufangen, in dem er in § 2 Abs 4 MPG u. a. vorgibt, dass die Rechtsvorschriften über die Geheimhaltung und den Datenschutz unberührt bleiben, löste das hauptsächliche Problem jedoch nicht [21]. Verdeutlichen tut dies das Beispiel der direkt relevanten harmonisierten Norm DIN EN 62304 für Medizinprodukte-Software, die Herstellern als Orientierung dienen soll. Die Norm unterstreicht die Problematik in der zu eng ausgeführten Begriffsdefinition der Sicherheit durch die unzureichende Rückführung auf die rein mechanisch und/oder elektrisch ordnungsgemäße

Funktionsweise. Sie definiert, dass eine Software regelkonform entwickelt wurde, und damit als sicher gilt, wenn ihre Funktionalität korrekte Ergebnisse liefert. Daraus impliziert die Norm, dass kein unzulässiges Risiko für die Patientensicherheit besteht. Die hierbei fehlende Miteinbeziehung der Datensicherheit verursacht im Szenario eines Hacker-Angriffs, bei dem als Beispiel Patientendaten manipuliert wurden, dass die Medizinprodukte-Software weiterhin als konform gilt. Da sie die korrekte Verarbeitung aus den veränderten Daten durchführt, funktioniert sie trotzdem ordnungsgemäß, obwohl für den Patienten ein potenziell unmittelbares Sicherheitsrisiko entstanden ist. Um als sicher zu gelten, muss also eine Software die korrekte Verarbeitung der korrekten Daten gewährleisten können [21].

Erst im Zuge der zunehmenden Vernetzung von Medizintechnik im Trend der Digitalisierung des Gesundheitswesens ergänzte sich die Informationssicherheit, und damit auch der miteingeschlossene Datenschutz, zum verbindlichen Verständnis eines sicheren Medizinproduktes. Die Konformität als „sicher für den Patienten“ zu gelten ist, durch die Reformierung zur MDR, nicht mehr rein auf die mechanisch und/oder elektrisch ordnungsgemäße Funktionsweise des einzelnen Medizinproduktes zurückführbar.

Dies schließt die Informationssicherheit, und die damit verbundene Berücksichtigung des Medizinproduktes in Netzwerkumgebungen, verbindlich in das Qualitätsmanagement des Herstellers ein, innerhalb dessen er seine Software regelmäßig auf bekannte relevante Sicherheitslücken zu untersuchen und anzupassen hat. Als Teil des Qualitätsmanagements, wirkt hierbei das Risikomanagement zur laufenden Evaluierung von möglichen informationstechnischen Risiken auch mit ein. Umso nötiger und eingängiger muss dies durch den Hersteller erfolgen, wenn er selbst zum direkten Verantwortlichen für den Datenschutz wird. Dies wäre z. B. der Fall, wenn er auf eigenen Servern oder über einen internetbasierten Speicher, einer Cloud, personenbezogene Daten verarbeiten würde, die das Medizinprodukt erhoben hat [22].

Ansonsten ist in der Regel der Betreiber als Verantwortlicher zu sehen. Er ist aber auf die Zuarbeit durch den Medizinprodukt-Hersteller angewiesen. Diese Unterstützung kommt in Form von Produkten, die bereits in sich mit informationssicheren Verarbeitungsprozessen konzipiert und entwickelt wurden. Vorgaben von getroffenen Datensicherheits-Schutzmaßnahmen und datenschutzfreundlichen Voreinstellungen leisten einen wesentlichen Beitrag zur Konformität des Medizinproduktes. Der Hersteller muss klare Aussagen treffen, wie und in welcher Umgebung, als auch mit welchen Komponenten seine Software eingesetzt werden soll. Die Ergebnisse des Risikomanagements zur Gefahreneinschätzung der

Datensicherheit, als auch insbesondere die der Datenschutzfolgeabschätzung, sind für den Betreiber essentielle Informationen. Diese müssen alle in die Zweckbestimmung und Gebrauchsanweisung mit aufgenommen werden. Nur so erhält der Betreiber die nötige rechtliche Legitimation, als Verantwortlicher des gesamten datenverarbeitenden Netzwerkes seiner Gesundheitseinrichtung, die vielzähligen weiteren organisatorischen und technischen Maßnahmen auch ergreifen zu dürfen, um das Patientenrisiko auf einem angemessenen Datenschutzniveau zu halten [22]. Als eine der wichtigsten Maßnahmen ist hierbei, neben der Ausfallsicherheit der Infrastruktur, die Abschirmung des Netzwerks vor äußeren Gefahren zu nennen. Da technisch verarbeitete Patientendaten zunehmend relevanter für die medizinische Diagnostik und Behandlung werden, steigt auch das Interesse von Cyber-Kriminellen daran. Gesundheitsdaten, als digitales Abbild des Patienten, können kriminelle Umsätze bringen, wodurch im Lauf der Zeit Datendiebstahl und Erpressungsversuche durch Verschlüsselung von Daten bekannt geworden sind [21]. Aber es müssen nicht immer nur Cyber-Kriminelle sein. Unter die möglichen Angreifer können auch Personen fallen, die im Auftrag von Regierungen zur Datenspionage handeln. Auch Einzelpersonen können aus politischen Zielen heraus, als sogenannte Hacktivists, agieren [23]. Wirksame Methoden gegen Schadsoftware können hierbei die Netzwerksegmentierung, das Einbauen von Firewalls mit definierten Regeln oder der Einsatz von Intrusion-Prevention-Systemen IPS oder Intrusion-Detection-Systemen IDS sein, die bekannte Malware und Angriffe erkennen und abwenden [21]. Zur Unterstützung bei der Integration der Medizinprodukte, als auch dem Betreiben des medizinischen IT-Netzwerks, existiert ein gesetzter Standard durch die nicht harmonisierte Norm DIN EN 80001-1. Zur Verbindung eines Medizinproduktes mit einem weiteren oder auch einem Nicht- Medizinprodukt kann die Norm DIN EN ISO 14971 herangezogen werden [24].

Um Gegenmaßnahmen setzen zu können, müssen davor die Schwachstellen identifiziert werden. Die DIN EN 80001-1 empfiehlt daher dem Betreiber die Durchführung eines Risikomanagements. Dabei teilt man die Risiken in zwei Kategorien ein. Die erste Kategorie besteht aus den Risiken, die vom Medizinprodukt und seiner Software innerhalb des Netzwerks ausgehen können. Die zweite Kategorie deckt die Risiken ab, die von der Anbindung der Medizinprodukte an das Internet ausgehen können. Diese Verbindung vom Betreiber zum Hersteller ist zur Fernwartung nötig. Als Methode für ein Risikomanagement nach DIN EN 80001-1 kann eine FMEA Analyse gewählt werden. FMEA steht hierbei für Failure Mode and Effects Analysis und wertet die Eintrittswahrscheinlichkeit der möglichen Fehler und ihren Einfluss aus. Sind die Risiken identifiziert, ausgewertet und durch Maßnahmen auf ein vertretbares Restrisiko reduziert worden, so muss der verantwortliche Risikomanager des medizinischen IT-Netzwerkes, diese Restrisiken freigeben [23].

Deutlich schwieriger gestaltet sich das Risikomanagement für die Fernwartungsverbindung am Medizinprodukt. Durch die direkte Verbindung mit dem Internet stellt das Medizinprodukt ein mögliches Einfallstor für den Angriff von außen dar [23]. Die Art und Weise, wie dieser Angriff aussehen kann, kann sehr vielfältig sein. So versuchen sich Angreifer über ungezielte, dafür vielzählige, Methoden Zugang in das Netzwerk zu verschaffen. So können sie Späh- und Schadsoftware, sogenannte Malware, durch Internetseiten, infizierte E-Mails oder Anwendungen, wie z. B. Apps, über die Benutzer innerhalb des Netzwerks einschleusen. Des Weiteren können Denial-of-Service-Angriffe oder E-Mail-Bomben Störungen des Datenverkehrs oder die Netzwerkverfügbarkeit beeinträchtigen. Gezieltere Attacken können über persönliche Gespräche oder über soziale Medien mit den Verwaltern oder Benutzern des Netzwerks erfolgen, wodurch Informationen über das Krankenhausnetzwerk besorgt werden (Social Engineering). Über den Zugang zum WLAN Netzwerk bietet sich dem Angreifer außerdem die Möglichkeit den Netzwerkverkehr zu verfolgen, um gesendete Informationen abzugreifen (War Driving). Noch gezieltere Angriffe können durch das Ausnutzen von Software-Schwachstellen in ihrem Quellcode erfolgen, so genannten Exploits. Hierbei könnten, mittels logischer Bomben oder Backdoors, ein direkter Zugang zu den Gesundheitsdaten hergestellt werden oder weitere Veränderungen in den Quellcodes eingeschleust werden [24]. Besonders gefährlich kann eine polymorphe Bedrohung aus dem Internet werden. Dies ist eine Attacke auf das medizinische IT-Netzwerk durch die Kombination mehrerer der beschriebenen Angriffsformen bei ständig wechselnder Erscheinungsform der Schadsoftware. Die Medizinprodukte sind für den Angriff so lukrativ, da die Angreifer über die Fernwartungsanbindung einen Zugang über das Internet erhalten können und sich, von der Software des Medizinproduktes aus, auf weitere vernetzte Medizingeräte oder PCs mit Software innerhalb des Netzwerks verbreiten können. Umso ungünstiger ist dabei die bereits erwähnte Tatsache, dass Medizinprodukt-Hersteller auf die Verwendung von Microsoft, als Basis ihres Software-Betriebssystem, setzen. Dies liegt an der Monopolstellung von Microsoft für Betriebssysteme und an der Favorisierung durch die Hersteller. Innerhalb eines medizinischen IT-Netzwerkes verwenden im Durchschnitt neun von zehn Medizinprodukte mit Software Microsoft als Betriebssystem. Noch ungünstiger wird es in diesem Zusammenhang, dass viele dieser Medizinprodukt-Computer nicht an sogenannte Patchmanagement-Systeme des Betreibers angeschlossen sind [23]. Durch diese Systeme steuert der Betreiber strategisch das Einspielen von Software-Aktualisierungen, sogenannten Patches. Diese können Korrekturen von Programmfehlern vornehmen oder Sicherheitslücken schließen, die nach Marktstart bekannt geworden sind [25]. Sie sind damit unerlässlich für den Schutz gegen Cyber-Attacken. Jedoch wird durch die Hersteller oftmals der Anschluss ihrer

Computer und Server an die Patchmanagement-Systeme des Betreibers nicht unterstützt oder untersagt, aufgrund der bereits ausgeführten regulatorischen Problematik [23].
Der deutsche Gesetzgeber erwirkt in dieser Lage insofern einen Druck zu einer Lösungsfindung, als dass er das Gefährdungspotenzial durch die Cyber-Problematik für die kritische Infrastruktur erkannt hat und Maßnahmen dagegen gesetzlich fordert. So sieht das geltende IT- Sicherheitsgesetz in § 8a Abs 1 für Fernwartungseinrichtungen in medizinischen IT-Netzwerken eine besonders technologische Ausgereiftheit vor, um Cyber-Angreifer abzuwehren. Die Lösungsfindung dafür liegt jedoch primär beim Gesundheitsdienstleister, der vom Gesetz als Betreiber einer kritischen Infrastruktur adressiert wird [23].

## 3.4 IT-SICHERHEITSGESETZ

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme ist im Juli 2015 in Kraft getreten und gilt für kritische Sektoren der Infrastruktur, die vor allem im Krisenfall gesellschaftlich essentiell sind. Seit Juni 2017 zählt dazu auch das Gesundheitswesen. Das Gesetz wird ergänzt durch die Kritische-Infrastruktur-Verordnung BSI-KritisV, mittels der transparente Kriterien für das Gesundheitswesen verbindlich formuliert wurden [26].

Dabei hat der Gesundheitsdienstleister, für die Erbringung seines gesellschaftlich relevanten Beitrags, sein medizinisches IT-Netzwerk nach dem Stand der Technik adäquat abzusichern. Dies wird alle zwei Jahre durch das Bundesamt für Sicherheit in der Informationstechnik BSI als zuständige Behörde überprüft. Diese Beweispflicht, in Form von Risikomanagement, Gefährdungsanalyse, Maßnahmen und Dokumentation, erhöht den technischen und administrativen Aufwand des Betreibers nochmal mehr [27]. Der Betreiber kann diese Maßnahmen nach der BSI-Leitlinie zum branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus B3S ausrichten, da sich die Überprüfung nach dieser Leitlinie richtet. Dieser Standard gibt in Kapitel 6.4.6 einen Bezug auf die medizinischen Risiken der Medizintechnik innerhalb eines Krankenhausnetzwerks und setzt dahingehend das Risikomanagement und die Gefährdungsanalyse nach DIN EN 80001-1 (Informationssicherheit von Medizingeräten) verbindlich für das Datensicherheitsmanagement fest. Zur Umsetzung genannter Maßnahmen können auch die DIN ISO/ IEC 27001 für Informationssicherheits-Managementsysteme sowie weitere Standards der ISO/IEC 80001-Serie hinzugezogen werden [26]. An dieser Stelle ist anzumerken, dass Punkt 3.5 und 3.6 der DIN EN 80001-1 den Medizinprodukt-Hersteller dazu verpflichtet den Betreiber mit der Herausgabe von Informationen zu unterstützen [28]. Über die Verbindung zum IT-Sicherheitsgesetz besteht somit für den Hersteller eine indirekte gesetzliche Mitverantwortung.

Im Kern des Risikomanagements werden die Risiken auf Risiko-Objekte bezogen und die Verantwortlichen dieser identifiziert. Die identifizierten Bedrohungen und Schwachstellen der Risiko-Objekte werden, je nach Bewertung, durch Parameter, wie Eintrittswahrscheinlichkeit und Schadenspotenzial, in Risikokriterien eingeordnet, woraus sich die Gefährlichkeitseinschätzung ergibt. Daraus werden Vorgehensweisen zur Behandlung, Kommunikation und Überwachung der Risiken gesetzt, die zur Sicherstellung der medizinischen Versorgung beitragen sollen. Diese medizinische Versorgung umfasst die Betrachtungsbereiche der Patientensicherheit, Behandlungseffektivität und des Versorgungsniveaus. Die Patientensicherheit betreffend wird u. a. der Ausfall kritischer Medizintechnik genannt, was auf einen Bezug zur mechanischen und/oder elektrischen Sicherheit schließt. Interessant für den Datenschutz ist die Gefährdungsanalyse, die das Risikomanagement ergänzt. Neben allgemeinen externen Bedrohungsszenarien und internen strukturellen Schwachstellen, werden hierbei branchenspezifische Gefährdungen betrachtet. Dies können z. B. das Nichtvorhandensein relevanter Systeme für den Behandlungsprozess, die fehlende Verfügbarkeit oder Veränderung medizinisch relevanter Daten, der Vertraulichkeitsverlust von Patienten- oder Behandlungsinformationen, als auch die Manipulation von IT-Systemen oder Medizintechnik sein [26].

## 3.5 Herstellerübergreifende Vernetzung von Medizingeräten

Die, durch das Risikomanagement und die Gefährdungsanalyse betrachteten Bereiche, zeigen im Ergebnis auf, dass Maßnahmen für die Informationssicherheit nicht nur nach außen hin, sondern auch nach innen im Netzwerk gesetzt werden müssen. So kann Medizintechnik nicht nur in ihrer Vernetzung aus dem Netzwerk heraus, sondern auch in ihrer Vernetzung untereinander innerhalb des Netzwerks für Gefährdungen der Informationssicherheit sorgen. So verursachen herstellerabhängig unterschiedliche Schnittstellenstandards heterogene technische Infrastrukturen innerhalb des Netzwerks. Es resultieren, statt der Integration in ein großes homogenes Verbund-Netzwerk, mehrere vereinzelte Teilnetzwerke. Zwischen ihren Datenübertragungsbrüchen müssen durch den Betreiber anderweitige Überbrückungen geschaffen werden. Im umständlichsten Fall ist die Übertragung der Patientendaten dann nur noch manuell lösbar. So müssen z. B. Befunddaten ausgedruckt und händisch in das Krankenhausinformationssystem eingegeben werden, auch wenn sie im Medizingerät elektronisch vorhanden sind. Dies ist für den Datenschutz insofern gefährlich, da an diesen Stellen die Datenverfügbarkeit eingeschränkt werden kann oder Daten fehlerhaft übertragen werden können. Die herstellerübergreifende Vernetzung und die darauf aufbauende Kommunikation zwischen Medizingeräten gestaltet sich so schwierig, da die Geräte jeweils

über unterschiedliche proprietäre Schnittstellen verfügen oder diese nur den Datenaustausch in eine Richtung (unidirektional) mit den Informationssystemen zulassen. Die Möglichkeit für ein Verbund-Netzwerk zum vollumfänglichen geräteübergreifenden Datentransfer durch eine bidirektionale Kommunikation wird durch solche Medizingeräte eingeschränkt. Auch die Datensicherheit leidet durch mögliche Bedienungs- oder Systemfehler, aufgrund unterschiedlicher Bedienungsoberflächen und nicht einheitlichen Kommunikations- und Sicherheitskonzepten [29]. Zur Lösung dieses Problems formte sich ein Zusammenschluss aus führenden Medizinprodukt-Herstellern, der 2016 in die Gründung des Vereins OR.NET mündete. Aus dieser Initiative heraus wurde ein neuer internationaler Schnittstellen-Standard IEEE 11073 SDC (Service-oriented Device Connectivity) etabliert und Anfang 2019 veröffentlicht. Dieser setzt sich aus drei Teilstandards zur Spezifikation eines Kommunikationsprotokolls mit definierter Syntax, semantischen Interoperabilität sowie deren kombinierter Anwendung zusammen und soll als Grundlage für die Interoperabilität herstellerübergreifender Medizinprodukte dienen. Geräte, die diesen Standard verwenden, können relevante Kommunikationsparameter, wie z. B. Kanal, Sicherheitsniveau und Taktung, untereinander abklären, bevor die eigentliche Datenübertragung ausgeführt wird. Durch diese Vorbereitung gelangt ein sicherer und verzögerungsfreierer Datenaustausch. Als einer der ersten großen Medizinprodukt-Hersteller führte Dräger diesen Standard in seine Produktentwicklungen mit ein [29] [30].

## 3.6 SOFTWARE ALS MEDIZINPRODUKT

Neben Software, die in ein Medizinprodukt mit eingebettet ist („embedded“), kann die eigenständige („stand-alone“) Software auch als Medizinprodukt qualifiziert werden (Software as Medical Device SaMD). Dies definiert das Medizinproduktegesetz MPG in seinen Begriffsbestimmungen unter § 3. Ein Problem war dabei, dass nach der vorherigen Richtlinie 93/42/EWG über Medizinprodukte solche Software in die Risikoklasse I eingestuft wurde. Für diese Risikoklasse durfte ein Medizinprodukt-Hersteller die Konformität seines Produktes ohne Hinzunahme einer Benannten Stelle erklären. Je nach Zweckbestimmung des Herstellers, ob sie den Begriffsdefinitionen eines Medizinproduktes nach § 3 MPG entspricht, wurde die Abgrenzung zu eigenständiger Software, die kein Medizinprodukt ist, hergestellt. So ist es auch oftmals vorkommen, dass die Hersteller ihre Software-Produkte als Medical Apps eingestuft haben. Sie stellen keine Medizinprodukte dar und wurden über Plattformen, wie dem Google Play- oder Apple Store, vertrieben. Hatten die verantwortlichen Unternehmen dieser Medical Apps ihren Sitz im EU-Ausland, so war die Überwachung schwieriger [31].

Dieses Problemfeld vergrößerte sich, aufgrund des Wunsches der Gesellschaft nach mehr Selbstbestimmtheit bei der eigenen Gesundheit und der daraus resultierenden Nachfrage nach Lösungen einer personalisierten Medizin. Dies ist am eingängigsten durch den Trend von elektronischen Gesundheitshelfern, z. B. sogenannten Wearables oder Smartphone-Apps zur Messung und Auswertung diverser Körperparameter, zu beobachten. Die EU-Regierung sah in diesem verstärkten Auftreten eines nichtregulierten Marktbereiches ein Sicherheitsproblem und griff dieses in der Reformierung zur MDR gesondert auf, durch die vorgesetzte Kategorisierung von Medizinprodukt-Software in höhere Risikoklassen. Diese Maßnahme schafft zwar ein besseres Instrument zur Überwachung des Marktzugangs, jedoch kann es diesen für viele digitale Medizinprodukte auch gleichzeitig pauschal hemmen. Besonders trifft die Start-Ups und kleinen Unternehmen. Ihre Produkte haben in ihrer Vielzahl und hohen Innovationskraft einen besonderen Anteil auf die Entwicklung des digitalen Gesundheitswesens. Diesen Gedanken griff die Bundesregierung im November 2019 durch das Digitale-Versorgung-Gesetz DVG auf. Dieses Gesetz hat das zentrale Ziel die Digitalisierung und Innovationskraft in Deutschland zu stärken. Des Weiteren soll das Gesundheitssystem effizienter und versorgungssicherer gemacht werden, der digitaltechnische Infrastrukturausbau, wie u. a. an der Telematikinfrastruktur, soll angetrieben werden und eine bessere Verfügbarkeit digitaler Gesundheitsanwendungen muss gewährleistet werden [32]. Versicherte erhalten durch das Gesetz erstmalig einen Anspruch auf die Versorgung mit ärztlich verschriebenen digitalen Gesundheitsanwendungen. Deren Anerkennung und Erstattung bei den Krankenkassen wird durch ein beschleunigtes Erstattungsverfahren erleichtert. Im Rahmen dieses Fast-Track-Verfahrens können digitale Gesundheitsanwendungen nach der Konformitätserklärung zum Medizinprodukt sowie nach einer bis zu dreimonatigen Prüfung durch das Bundesinstitut für Arzneimittel und Medizinprodukte BfArM vorläufig in ein Verzeichnis für digitale Gesundheitsanwendungen aufgenommen werden. Dadurch sind die Produkte sofort für die Patienten verfügbar. Innerhalb einer Frist von zwölf Monaten hat der Hersteller Zeit einen Nachweis zu erbringen, dass sein Produkt einen positiven Beitrag zur Versorgung und Effektivität des Gesundheitssystems leistet. In dieser Phase können bereits Leistungen mit den Versicherern abgerechnet werden. Die Anforderungen an die Medizinprodukte, um sich für dieses Verfahren zu qualifizieren und erstattungsfähig zu sein, werden seit April 2020 in der Verordnung des DVG (Digitale-Gesundheitsanwendungen-Verordnung DiGAV) genauer spezifiziert. Als Hilfestellung zur Erfüllung dieser Anforderungen dient eine Leitlinie des BfArM [4]. Während aus der DVG der Datenschutz und die Datensicherheit nur allgemein gefordert wurden, gehen aus der Verordnung in § 4 DiGAV die Anforderungen diesbezüglich hinsichtlich Produktbeschaffenheit

und Organisation hervor. Dabei müssen die Produkte die gesetzlichen Datenschutzvorgaben und Anforderungen an die Informationssicherheit durch Maßnahmen nach dem aktuellen Stand der Technik gewährleisten. Die personenbezogenen Daten dürfen durch die digitalen Gesundheitsanwendungen erst durch Einwilligung des Versicherten nach den Bestimmungen der DSGVO und danach nur zu definierten Zwecken verarbeitet werden. Eine Verwendung darüber hinaus, insbesondere für Werbezwecke, wird verboten. Des Weiteren wird die Verarbeitung geografisch nur auf die EU beschränkt und alle an der Datenverarbeitung beteiligten Personen im Unternehmen des Herstellers verpflichten sich zur Verschwiegenheit. Die Verordnung stellt außerdem in Anlage 1 einen Fragebogen. Durch die Beantwortung von Fragen zum Datenschutz und zur Datensicherheit muss der Hersteller die Erfüllung der Anforderungen nach § 4 erklären [33].

Mit der gezielten Weiterführung des Digitale-Versorgung-Gesetzes in Bereiche des Gesundheitswesens, spezifiziert und steigert der Gesetzgeber die Anforderungen an den Datenschutz. So geht z. B. aus dem Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz DVPMG die stärkere Miteinbeziehung des BSI und BfArM hervor. Ab Juni 2022 wird das BSI befugt sein die Anforderungen an die Datensicherheit der Medizinprodukte jährlich zu überprüfen und zu diesem Zweck ein Prüfverfahren und Zertifikat festzulegen. Diese Zertifizierung bestätigt, dass die Anforderungen erfüllt wurden, im Sinne des DSGVO Artikels 42 [34]. In diesem wird eine Zertifizierung als Nachweis gefordert, dass die Vorgaben der DSGVO, nach ISO/IEC 27011, im Umgang mit personenbezogenen Daten eingehalten werden. Dabei kann ein Informationssicherheits-Managementsystem zur besseren Darlegung des konformen Umgangs mit personenbezogenen Daten von Vorteil sein. Bei der Implementierung unterstützt die DIN ISO/ IEC 27001. Die ISO/IEC 27701 ergänzt dabei durch weitere Anleitungen zur organisatorischen Weiterentwicklung und Prozessoptimierung des Managementsystems im Bereich des Datenschutzes [11] [35].

Durch das BfArM kann auch der Nachweis dieses Zertifikats verlangt werden, sowie Penetrationstests und Sicherheitsgutachten von neuen, aber auch bereits in das Verzeichnis aufgenommenen, digitalen Gesundheitsanwendungen [34].

# 4 SCHLUSSFOLGERUNG

Die Betrachtungen in dieser Arbeit haben aufgezeigt welchen großen Stellenwert die Datensicherheit und der damit verbundene Datenschutz in der Politik entwickelt hat. Dies spiegelt sich am deutlichsten durch die Reformierung zur gesetzlichen Regulierung von Medizinprodukten und Datenschutz auf europäischer Ebene wieder. Es ist das Bestreben zu mehr Vereinheitlichung eines stellenweise ungenügend harmonisch regulierten Marktes innerhalb des europäischen Wirtschaftsraumes. Die bisherigen EU-Richtlinien 93/42/EWG für allgemeine Medizinprodukte (MDD), 90/385/EWG für aktive implantierbare medizinische Geräte (AIMDD) und 95/46/EG für den Datenschutz, stellten nur zu erreichende Ziele verbindlich, jedoch nicht deren Umsetzung. Diese lag bei der nationalen Gesetzgebung jedes Mitgliedsstaates nach eigenem Ermessen zur Regelsetzung. Durch die Aufwertung der Richtlinien zu Verordnungen schaffte die EU-Regierung einen Hebelarm, um Maßnahmen verbindlicher und einheitlicher einführen zu können, aber auch um einen größeren Nachdruck erzeugen zu können in der Strafverfolgung mittels stärkerer Sanktionierung.

Im Hinblick auf die Entwicklung zu einem digitalisierten Gesundheitswesen, nimmt sich die MDR dem wachsenden Anteil an informationsverarbeitender Medizinprodukt-Software an und spezifiziert grundlegende Sicherheits- und Leistungsanforderungen an die Datensicherheit. Aus diesen ist eine Strategie zu erkennen die zentralen Schutzziele der IT-Sicherheit von Verfügbarkeit, Vertraulichkeit und Integrität der Daten in die Auslegung eines bestimmungsgemäßen Gebrauchs, und damit in die Konformität für Produkt- und Patientensicherheit, zu setzen. Um also als sicheres Medizinprodukt gelten zu dürfen, reicht es nicht mehr nur die rein mechanischen und/oder elektrischen Risiken in die Entwicklung und Auslegung miteinzubeziehen. In ausdrücklicher Verbindung zur DSGVO, setzt die MDR bewusst an diese Stelle an und verpflichtet den Hersteller zu einer Mitberücksichtigung von Datensicherheits- und Datenschutzrisiken in seinem Risikomanagement. Einerseits die Mitberücksichtigung von Risiken für den Patienten, nicht nur in seiner physischen, sondern auch in seiner persönlichen Gestalt. Denn die zunehmende Technologisierung im Gesundheitswesen bringt eine größere Datenverfügbarkeit mit sich, auf die sich die moderne individuelle Medizin stützt. Umso mehr entsteht dadurch ein digitales Abbild des Patienten, das als schützenswert zu erachten ist. Nicht umsonst erhalten Gesundheitsdaten einen besonders sensiblen Schutzstatus, dessen Wichtigkeit durch die Grundrechte und Grundfreiheit des Menschen untermauert wird. Die DSGVO nimmt sich diesem Schutz an und setzt dafür die verbindlichen Rahmenbedingungen. So spezifiziert sie wiederum grundlegende

Sicherheits- und Leistungsanforderungen an den Datenschutz. Sie ergänzt die MDR dabei insofern gut, da sie auch zentrale Grundsätze für den Hersteller nennt, Pflichten daraus verbindlich ableitet und sie genauso in den bestimmungsgemäßen Gebrauch zur Gewährleistung der Produkt- und Patientensicherheit miteinfließen lässt. Die zentralen Grundsätze der Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit wirken sich in die Gestaltung der Anwendbarkeit und der Technik, die sich als privacy by default und privacy by design bezeichnen lassen. Ersteres meint den Datenschutz nach außen. Das Medizinprodukt ist nach Stand der Technik so zu gestalten, dass es bereits in seinen Voreinstellungen datenschutzfreundlich bedienbar ist bzw. unerlaubten Anwendern eine Bedienung erst gar nicht möglich macht. Zweites meint den Datenschutz nach innen, also das Medizinprodukt nach Stand der Technik so zu gestalten, dass es durch seine technische Beschaffenheit die Sicherheit der Daten und Einhaltung der Datenschutzziele bei der Datenverarbeitung gewährleisten kann .

Für das Risikomanagement des Herstellers ergibt sich die weitere Mitberücksichtigung von Risiken für Datensicherheit und Datenschutz innerhalb des Anwendungsfelds seines Medizinproduktes. So können sich Auslegung und Entwicklung der Medizinprodukte an vorangegangenen Evaluierungen zu Risiken durch die Implementierung in bestehende medizinische IT-Netzwerke, vor allem aufgrund mangelnder Netzwerk-Interoperabilität und Vulnerabilität gegen Cyber-Angriffe, ausrichten. Der Hersteller erstellt aus seinem Risikomanagement eine angepasste Zweckbestimmung und teilt dem Betreiber alle Ergebnisse und Informationen mit. Dies bietet dem Betreiber mehr rechtliche Legitimation organisatorische und technische Maßnahmen für den Datenschutz ergreifen zu dürfen. Als Verantwortlicher der Datenverarbeitung ist er zu dieser technischen Gestaltung seines Netzwerkes, nach der privacy by design Vorgabe, verpflichtet. Als Auftragsverarbeiter der Daten unterstützt ihn der Hersteller dabei durch datenschutzkonforme Produkte, mit denen der Betreiber diese Vorgaben erfüllen kann. Bei zukünftigen Ausschreibungen der Betreiber werden daher eher Hersteller gewinnen, die datenschutzfreundliche Produkte anbieten. Durch die Schaffung einer solchen Marktsituation erkennt man die gute Hebelwirkung auf die Hersteller zugunsten des Datenschutzes, die die beiden EU-Regulierungen im Zusammenspiel erzeugen. Auf der anderen Seite sollte der Hersteller den Mehraufwand zu Datensicherheit und Datenschutz nicht als Hindernis sehen, sondern mehr als Chance zum Wettbewerbsvorteil nutzen. Die Firma Dräger z. B. hat dieses Potenzial erkannt und die Risikobetrachtung von Datensicherheit in ihre gesamte Produktentwicklung miteinfließen lassen. Dabei werden, im Zuge des Risikomanagements, Bedrohungs- und

Sicherheitsanalysen durchgeführt, sowie die Lösungen aus dem Risikomanagement bewertet. Der Hersteller ist auch bereits auf die zukünftig verpflichtend werdenden Software-Penetrationstests vorbereitet, da er sich bereits freiwillig überprüfen lässt. Des Weiteren tragen Schulungen der Mitarbeiter, die Miteinbindung von Sicherheitsexperten, sowie eigene klinische Netzwerk- und Datenmanagement-Systeme zur Marktetablierung bei [36]. Solche Leistungen werden in naher Zukunft stärker durch einheitliche Zertifizierungen, z. B. für den Datenschutz, belohnt werden. Für solch eine Zertifizierung stellt die DSGVO mit Artikel 42 bereits die Rechtsgrundlage für die Überführung in nationales Recht, was 2022, durch die Weiterführung des Digitale-Versorgung-Gesetzes, für Software als Medizinprodukt erfolgen wird. Die EU-Regierung muss weiterhin durch laufend aktualisierte Leitfäden, wie z. B. dem vorgestellten Leitfaden „Guidance on Cybersecurity for Medical Devices“, sicherstellen, dass die Hersteller auch ausreichend Klarheit erhalten, wie sie die gesetzlichen Anforderungen erfüllen können. Das Hauptziel der MDR, die regulatorische Vereinheitlichung innerhalb des europäischen Wirtschaftsraumes für Medizinprodukte, muss konsequent weitergeführt werden. Diese Bemühungen müssen, auch für Datensicherheit und Datenschutz, in harmonisierte Standards münden. Initiativen durch Vereinigungen der Medizinprodukthersteller können den europäischen Gesetzgeber dabei unterstützen. Wie das International Medical Device Regulators Forum, mit ihrer Ausarbeitung einer internationalen Harmonisierung von Sicherheitsaspekten oder der Verein OR.NET, mit der Entwicklung eines internationalen Schnittstellen-Standards zur Lösung des Interoperabilitätsproblems in medizinischen IT-Netzwerken. Die kurzen und frequenten Innovationsintervalle moderner Digitalisierungstechnologien werden auch weiterhin Einzug in das Gesundheitssystem halten. Ungeregelte Zustände, wie z. B. durch das gelöste Problem der regulatorisch nicht erfassten Medizinproduktsoftware im App Store, werden wieder auftreten, wenn die EU-Politik nicht kontinuierlich Hand in Hand mit Herstellern, Betreibern und Experten innerhalb des Gesundheitssektors an praktischen Lösungen arbeitet. Sonst ist die Gefahr der Überregulierung als vorschnelle Reaktion auf unvorbereitete Situationen gegeben. Besonders bei zukünftigen komplexen Herausforderungen, die moderne Technologien bringen. Ein gutes Beispiel ist die Künstliche Intelligenz. KI-unterstützte Software wird immer mehr Anteil an der Diagnostik und Behandlung erlangen. Dafür benötigt sie jedoch sehr viele Gesundheitsdaten, um mit der Zeit selbstständig weiter zu lernen. Der Datenschutz wird hierbei eine große Herausforderung sein. Nicht nur aufgrund der Vielzahl der benötigten Daten, sondern auch aufgrund der Validierbarkeit der daraus entstehenden Informationen durch die KI. Denn die Software von KI ändert sich fortlaufend selbst und kann sich morgen anders verhalten als heute. Die Wiederholbarkeit von Software, die als eine grundlegende

Sicherheits- und Leistungsanforderung in Abschnitt 17.1 der MDR vorgeschrieben ist, könnte daher nicht mehr gegeben sein. Dies könnte Differenzen in der bestimmungsgemäßen Verwendung und damit in der Konformität geben [9]. Dies zeigt, dass sich die MDR und die DSGVO auch fortlaufend anpassen müssen. In Zukunft wahrscheinlich schneller als es zuvor sein musste.

# 5 LITERATURVERZEICHNIS

[1] M. Darms, S. Haßfeld und S. Fedtke, IT-Sicherheit und Datenschutz im Gesundheitswesen, Wiesbaden: Springer Vieweg, 2019.

[2] M. Zauner, „Die Herausforderung, medizinische IT-Netzwerke zu betreiben," in *Dienstleistungsmanagement im Krankenhaus*, Wiesbaden, Springer Gabler, 2016, pp. 311-323.

[3] „Patientendaten: Besonderer Datenschutz bei Gesundheitsdaten," 11 August 2021. [Online]. Available: https://www.datenschutz.org/patientendaten/. [Zugriff am 11 August 2021].

[4] T. Barth, M. Göldner und F. Spitzenberger, „Einfluss von regulatorischen Anforderungen auf Innovationen in der Medizintechnik am Beispiel der europäischen Medical Device Regulation („MDR") und des nationalen Digitale-Versorgung-Gesetzes („DVG").," in *Zukunftsfähigkeit durch Innovation, Digitalisierung und Technologien*, Berlin, Heidelberg, Springer Gabler, 2021, pp. 223-252.

[5] „EU-Medizinprodukte-Verordnungen," 31 Oktober 2019. [Online]. Available: https://www.wko.at/branchen/handel/foto-optik-medizinproduktehandel/EU-Medizinprodukte-Verordnung.html. [Zugriff am 14 Juli 2021].

[6] „VERORDNUNG (EU) 2017/ 745 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 5. April 2017 - über Medizinprodukte, zur Änderung der Richtlinie 2001/ 83/ EG, der Verordnung (EG) Nr. 178/ 2002 und der Verordnung (EG) Nr. 1223/ 2009 und zur Aufhebung der Richtl," [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017R0745&from=DE. [Zugriff am 22 Juli 2021].

[7] L. Salvatore, „EUDAMED: European Databank on Medical Devices," 10 März 2021. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/eudamed/. [Zugriff am 23 Juli 2021].

[8] „EUDAMED-Datenbank," [Online]. Available: https://www.wko.at/branchen/handel/foto-optik-medizinproduktehandel/EUDAMED-Datenbank.html. [Zugriff am 23 Juli 2021].

[9] M. Hastenteufel und S. Renaud, Software als Medizinprodukt, Wiesbaden: Springer Vieweg, 2019.

[10] R. Stender, „Das Ende der Medizinprodukte-Richtlinien rückt näher …," *mt medizintechnik*, p. 2, 22 Oktober 2019.

[11] M. Kindler, „Cybersicherheit im Umfeld der Covid-19-Pandemie," *mt medizintechnik,* pp. 12-15, 24 Juni 2020.

[12] L. Liguori und E. Stefanini, „EU REGULATIONS ON MEDICAL DEVICES AND THE GDPR: FIRST STEP FORWARD A NECESSARY COORDINATION," 7 Juni 2021. [Online]. Available: https://portolano.it/en/blog/life-sciences/eu-regulations-on-medical-devices-and-the-gdpr-first-step-forward-a-necessary-coordination-. [Zugriff am 29 Juli 2021].

[13] C. Schlötelburg, „Cybersecurity von Medizinprodukten als Teil der IT-Sicherheit im Gesundheitswesen," 9 Juni 2020. [Online]. Available: https://meso.vde.com/de/cybersecurity-und-medizinprodukte/. [Zugriff am 12 Juli 2021].

[14] A. Jorzig und F. Sarangi, Digitalisierung im Gesundheitswesen, Berlin, Heidelberg: Springer, 2020.

[15] S. Krenmayr, „Umsetzung der Datenschutz-Grundverordnung im Krankenhaus," 18 Oktober 2017. [Online]. Available: https://epub.jku.at/obvulihs/content/titleinfo/2344951. [Zugriff am 27 Juli 2021].

[16] „Datenschutz-Grundverordnung DSGVO," [Online]. Available: https://dsgvo-gesetz.de/. [Zugriff am 28 Juli 2021].

[17] „DSGVO Privacy by Design," [Online]. Available: https://dsgvo-gesetz.de/themen/privacy-by-design/. [Zugriff am 30 Juli 2021].

[18] C. Johner, „Anonymisierung und Pseudonymisierung," 9 Dezember 2020. [Online]. Available: https://www.johner-institut.de/blog/gesundheitswesen/anonymisierung-und-pseudonymisierung/. [Zugriff am 20 Juli 2021].

[19] „Pflichten von Unternehmen – Datenschutz," 6 April 2021. [Online]. Available: https://www.usp.gv.at/it-geistiges-eigentum/datenschutz/pflichten-von-unternehmen.html. [Zugriff am 16 Juli 2021].

[20] U. Müller, „Gesetze und Normen 2018 – Auswirkungen für die Cyber-Sicherheit von Medizintechnik," [Online]. Available: https://konplan.com/allgemein/gesetze-und-normen-2018-auswirkungen-fuer-die-cyber-sicherheit-von-medizintechnik/#tab-id-2. [Zugriff am 25 Juli 2021].

[21] G. Spyra, „Datenschutz bei vernetzten Medizinprodukten - Teil 1: Verantwortlichkeiten im Bereich des Medizinprodukterechts," *mt medizintechnik,* pp. 90-95, 20 Juni 2014.

[22] G. Spyra, „Über die Sicherheit von Software-Medizinprodukten," *mt medizintechnik,* pp. 9-13, 30 Juni 2019.

[23] J. Schönfeld, „Höherer IT-Sicherheit in Medizinischen IT-Netzwerken mit Next-Generation Threat Protection," *mt medizintechnik,* pp. 10-14, 19 Dezember 2015.

[24] M. Knoll, „Einführung in das IT-Risikomanagement für medizinische Einrichtungen," *mt medizintechnik,* pp. 14-22, 24 Oktober 2017.

[25] „Patch-Management – Definition," [Online]. Available: https://it-service.network/it-lexikon/patch-management. [Zugriff am 19 Juli 2021].

[26] F. Rothe, A. Wirth und K. Kowik, „Kritis-Anforderungen für vernetzte Medizingeräte (Teil 1)," *mt medizintechnik,* pp. 21-25, 26 Februar 2021.

[27] F. Rothe, A. Wirth und K. Kowik, „Kritis-Anforderungen für vernetzte Medizingeräte (Teil 2)," *mt medizintechnik,* pp. 24-29, 23 April 2021.

[28] J. Schönfeld, „Gefährdung von aktiven Medizinprodukten, Medizinprodukten als Software und medizinischen IT-Netzwerken - Schwerwiegender Softwarefehler in der Open-Source Bibliothek OpenSSL," *mt medizintechnik,* pp. 129-133, 22 August 2014.

[29] T. Neumuth, „Herstellerübergreifende Vernetzung von Medizingeräten," *mt medizintechnik,* pp. 14-15, 30 Juni 2019.

[30] F. Grünberg, „Datenvernetzung im Krankenhaus," *mt medizintechnik,* pp. 26-27, 24 Juni 2020.

[31] A. Terhechte, „Medizinische Software/Medical Apps - Aufgaben, Anforderungen und Erfahrungen aus Sicht einer Überwachungsbehörde," *Bundesgesundheitsblatt,* pp. 321-327, 8 Januar 2018.

[32] C. Johner, „Das Digitale-Versorgung-Gesetz (DVG) – als Hersteller damit Geld verdienen?," 20 April 2020. [Online]. Available: https://www.johner-institut.de/blog/gesundheitswesen/digitale-versorgung-gesetz-dvg/. [Zugriff am 17 Juli 2021].

[33] „DiGAV - Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung," 21 April 2020. [Online]. Available: https://www.gesetze-im-internet.de/digav/BJNR076800020.html. [Zugriff am 18 Juli 2021].

[34] C. Johner, „DVPMG – Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz," 6 Juli 2021. [Online]. Available: https://www.johner-institut.de/blog/regulatory-affairs/dvpmg/. [Zugriff am 24 Juli 2021].

[35] A. Koubek, „ISO 27701 (in Kooperation mit CIS GmbH)," [Online]. Available: https://www.qualityaustria.com/produktgruppen/digital-economy/iso-27701-in-kooperation-mit-cis-gmbh/. [Zugriff am 26 Juli 2021].

[36] „IT-Sicherheit im Krankenhaus & Gesundheitswesen,“ Dräger, [Online]. Available: https://www.draeger.com/de_de/Hospital/Cybersecurity. [Zugriff am 1 August 2021].