Niebler, Thimo; Zerres, Thomas; Zerres, Christopher

Working Paper

Datenschutzrechtlicher Rahmen von E-Health in Deutschland

Arbeitspapiere für Marketing und Management, No. 54

Provided in Cooperation with:
Fakultät Medien, Hochschule Offenburg

Suggested Citation: Niebler, Thimo; Zerres, Thomas; Zerres, Christopher (2021) : Datenschutzrechtlicher Rahmen von E-Health in Deutschland, Arbeitspapiere für Marketing und Management, No. 54, Hochschule Offenburg, Fakultät Medien, Offenburg, https://doi.org/10.48584/opus-4989

This Version is available at:
https://hdl.handle.net/10419/244671

CHRISTOPHER ZERRES

MARKETING

Schriftenreihe „Arbeitspapiere für Marketing und Management“

Herausgeber:
Prof. Dr. Christopher Zerres

Hochschule Offenburg
Fakultät Medien und Informationswesen

Arbeitspapier Nr. 54

Datenschutzrechtlicher Rahmen von E-Health in Deutschland

Niebler, T., Zerres, T., Zerres, C.

Offenburg, April 2021

ISSN: 2510-4799

Impressum

Prof. Dr. Christopher Zerres
Hochschule Offenburg
Fakultät Medien und Informationswesen
Badstraße 24
77652 Offenburg

ISSN: 2510-4799

INHALT

1 EINLEITUNG

1.1 MOTIVATION

„Was ich in der deutschen Debatte nie verstehen werde, ist, warum am Ende so viel mehr Bereitschaft da ist, Apple, Google, Facebook oder auch Alibaba die eigenen persönlichen Daten jeden Tag zur Verfügung zu stellen, als dann, wenn der eigene Staat einen Rahmen dafür setzt, Daten zum Wohle des Einzelnen - anonymisiert oder pseudonymisiert - zur Forschung und zum Mehrwert für alle Patientinnen und Patienten zu nutzen. Dann gibt es so ein Grundmisstrauen. Solange das so ist und es ein Grundvertrauen in amerikanische Großkonzerne und ein Grundmisstrauen in den eigenen Staat gibt, werden wir in der Digitalisierung nicht vorankommen.“[1]

Mit diesem Appell warnte der Bundesgesundheitsminister Jens Spahn am 3. Juli 2020 vor dem Setzen falscher Prioritäten beim Datenschutz, im Rahmen der von ihm forcierten Digitalisierung im Gesundheitswesen. Diese von ihm kritisierte Inkonsequenz betrifft in Teilen auch den Autor dieser Arbeit. So hat dieser bei seinem letzten Arztbesuch die ausgehändigte „Patienteninformation zum Datenschutz“ erstmals kritisch beäugt und sich Gedanken darüber gemacht, ob der Arzt den alten Praxiscomputer ausreichend vor unberechtigtem Zugriff auf seine Daten schützt. Weniger Bedenken hingegen hat er, während er im Wartezimmer am Smartphone durch die sozialen Netzwerke stöbert und hierbei seine persönlichen Daten in sozialen Netzwerken preisgibt, deren Firmensitze teilweise sogar im Ausland liegen. Dass nicht nur der Autor von der Datenverarbeitung im digitalen Zeitalter betroffen ist, zeigt die „ARD/ZDF-Onlinestudie 2020“, nach der mittlerweile über 90% der deutschen Bevölkerung online sind und ein Viertel der Gesamtbevölkerung regelmäßig soziale Netzwerke nutzt.[2] Doch nicht nur beim Arztbesuch, sondern auch im alltäglichen Leben gewinnt das Thema Datenschutz im E-Health-Bereich eine immer bedeutender werdende Rolle. Im pandemiegeprägten Jahr 2020 wurde zur Einführung der Corona-Warn-App über die digitale Datenverarbeitung im Gesundheitswesen kontrovers diskutiert. Kritiker[3] bemängelten die staatliche Kontrolle, während Befürworter die Effektivität der App zur Pandemiebekämpfung mittels Nachverfolgung sowie die hohen Datenschutzstandards hervorheben.[4,5] Des Weiteren findet sogar das Krankschreiben und die Erstellung von Diagnosen in Pandemiezeiten verstärkt per Videosprechstunde, d.h. digital statt. Bereits im März 2020 sprach der Geschäftsführer des Ärzteportals „jameda“, Dr. Florian Weiß, von einer „1000-prozentigen Steigerung an Anfragen von Medizinern an Videosprechstunden im Vergleich zum Vormonat.“[6]. Diese technische Neuerung zur Fest-

[1] Jens Spahn 2020.
[2] Vgl. ARD/ZDF-Forschungskommission, Pressemitteilung vom 08.10.2020.
[3] Anmerkung des Autors: Im folgenden Text wird aus Gründen der leichteren Lesbarkeit ausschließlich das generische Maskulinum verwendet. Dies soll jedoch keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen und schließt die feminine Form implizit ein.
[4] Vgl. Patrick Beuth et al. 2020.
[5] Vgl. Andreas Noll 2020.
[6] Vgl. Petra Apfel 2020.

stellung der Arbeitsunfähigkeit wird auch über die Coronapandemie hinaus möglich sein und damit der Digitalisierung im Gesundheitswesen weiter Vorschub leisten.[7]

Die öffentliche Datenschutzdiskussion während einer Pandemie zeigt die hohe Relevanz und Aktualität von E-Health und bestärkt den Autor darin, sich ebendiesem Bereich zu widmen. Schon seit dem Inkrafttreten der Anwendbarkeit der DSGVO (Datenschutz-Grundverordnung) im Jahr 2018 verging kaum ein Tag, an dem er nicht zwangsläufig mit Datenschutz konfrontiert wurde. Jedoch war das öffentliche Interesse am Thema Datenschutz nie größer als zum aktuellen Zeitpunkt. Als besonders sensibel gelten die personenbezogenen Gesundheitsdaten der Bevölkerung. Auch diese Daten werden, wie oben dargelegt, immer öfter digital verarbeitet. Neben der Datenverarbeitung durch das staatliche und private Gesundheitswesen findet die Verarbeitung von Gesundheitsdaten auch den Weg in den Alltag vieler Menschen. So ist es für einen wachsenden Teil der Bevölkerung selbstverständlich, auf Smartwatches und in niedrigschwelligen Apps von chinesischen und amerikanischen Anbietern persönliche Gesundheitsdaten wie Alter und Gewicht, aber auch Puls, Laufwege und sogar Schlafzeiten zu hinterlassen. Datenschützer mahnen immer wieder, dass persönliche Daten von internationalen, profitorientierten Unternehmen für Zwecke verarbeitet werden können, die nicht mehr im Interesse der Benutzer sind.[8] Doch wie schützt die aktuelle Rechtslage gerade diese Daten im Rahmen der fortschreitenden Digitalisierung? Welche Produkte und Dienstleistungen sind überhaupt unter dem Begriff E-Health zu subsumieren? Welche Chancen und Risiken bietet E-Health und kann diese Form der Digitalisierung mit den verschiedenen Datenschutzinteressen vereinbart werden? Aus diesen Fragen und Erwägungen heraus möchte der Autor in dieser Arbeit einen datenschutzrechtlichen Überblick über die Datenverarbeitung im E-Health-Bereich erarbeiten.

1.2 Ziel und Aufbau der Studie

Das Ziel dieser Arbeit ist es, unter Einsatz von empirischer Forschung darzulegen, welchen Einfluss das Datenschutzrecht auf die Digitalisierung im hiesigen Gesundheitswesen hat. Mittels einer qualitativen Befragung wird unter anderem untersucht, wie die Umsetzung der Datenschutzgesetze in der Praxis erfolgt und ob ein Spannungsfeld zwischen E-Health und Datenschutz besteht.

Hierbei gliedert sich die Arbeit in sechs Kapitel. Nach der Einleitung werden im zweiten Kapitel, dem konzeptionellen Teil, die für diese Arbeit relevanten Begrifflichkeiten und Grundlagen erläutert. Um Grundlagen der Problematik darzustellen, wird zunächst der Begriff E-Health abgegrenzt. Hierfür werden die Geschichte der Digitalisierung im Gesundheitsbereich aufgearbeitet, der Begriff definiert und die verschiedenen Formen von E-Health dargestellt. Daraufhin werden die rechtlichen Rahmenbedingungen unter Zuhilfenahme juristischer Literatur und mit Berücksichtigung von nationalen und internationalen Gesetzen und Verordnungen vorgestellt. In diesem Zusammenhang werden die DSGVO sowie weitere Rechtsquellen beleuchtet. Hier liegt der Fokus auf der europaweit unmittelbar geltenden DSGVO, welche das Datenschutzrecht seit dem Jahr 2018 maßgeblich prägt. In diesem Teil soll dem Leser ein Überblick über das Datenschutzrecht in Deutschland gegeben werden. Die Forschungsfrage sowie Hypothesen werden im dritten Kapitel

[7] Vgl. G-BA Gemeinsamer Bundesausschuss, Pressemitteilung vom 16.07.2020.
[8] Vgl. Bitkom e.V., Pressemitteilung vom 09.02.2016.

ausgeführt. Das anschließende vierte Kapitel ist Kern dieser Arbeit und beinhaltet den empirischen Teil. Ziel dieses Abschnitts ist es, mit Hilfe einer qualitativen Befragung herauszufinden, inwiefern E-Health vom Datenschutz in der Praxis beeinflusst wird. Mittels Expertenbefragungen soll festgestellt werden, welchen datenschutzrechtlichen Rahmenbedingungen das digitalisierte Gesundheitswesen unterliegt und ob diese zu einem Spannungsfeld zwischen E-Health und Datenschutz führen. Hierbei wird zunächst der Aufbau der Untersuchungsmethode sowie des Fragebogens beschrieben. Nach Durchführung der Interviews werden im Anschluss die ausgewerteten und aufbereiteten Ergebnisse präsentiert. Aus den in Kapitel vier erhobenen Daten werden im fünften Kapitel die Hypothesen geprüft und Handlungsempfehlungen abgeleitet. Die abschließende Schlussbetrachtung fasst die Resultate der durchgeführten Arbeit zusammen und soll Ansatzpunkte für weitere Untersuchungen liefern.

2 KONZEPTIONELLE GRUNDLAGEN

Um einen Überblick über den datenschutzrechtlichen Rahmen im E-Health-Bereich zu geben, ist es zunächst notwendig, den Begriff E-Health zu verdeutlichen und das hierfür relevante Datenschutzrecht in Deutschland darzulegen. Im folgenden Teil wird eine Abgrenzung des E-Health-Begriffs vorgenommen sowie mittels historischer Aspekte und allgemeiner Beispiele dem Leser insofern ein klares Bild von E-Health vermittelt, wie es für den weiteren Verlauf dieser Arbeit relevant ist.

2.1 E-HEALTH

2.1.1 Historische Wurzeln

Der Begriff E-Health wurde erstmals zu Beginn des Internetzeitalters im Jahr 1999 auf medizinischen Kongressen erwähnt und hat sich seither im allgemeinen Sprachgebrauch durchgesetzt. Das Konzept, auf dem E-Health fußt, ist jedoch schon älter und entwickelte sich fortlaufend mit dem jeweils aktuellen Stand der Technik.[9,10] Nachstehende Abbildung stellt diese Entwicklung grafisch dar.

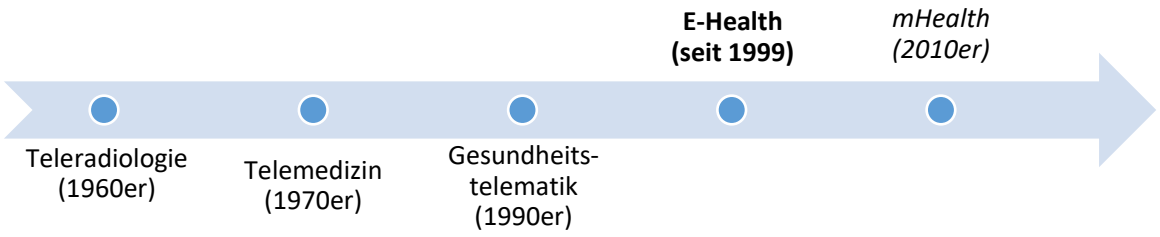

Abbildung 1: Zeitstrahl der medizinischen Errungenschaften auf dem Weg zu E-Health

[Quelle: Eigene Abbildung, basierend auf der Abbildung „From telematics to Digital Health – A brief history“[11] und den zitierten Quellen.]

9 Vgl. Vincenzo Della Mea 2001, S. 1.
10 Vgl. Gunther Eysenbach 2001, S. 1.
11 Vgl. Sven Meister et al. 2016, S. 578.

Im Jahre 1959 wurden erste Röntgenbilder mit Hilfe eines elektronischen TV-Systems zwischen zwei Krankenhäusern übertragen. Diese Form der Datenübertragung ist der Beginn der Teleradiologie, bei der mittels Telekommunikation radiologische Bilder an entfernte Orte übertragen werden können.[12] Medizinische Diagnosen wurden bereits Ende des 19. Jahrhunderts telefonisch kommuniziert, doch erst in den 1970er-Jahren entwickelten sich die Telekommunikationstechniken so weit, dass sich die Telemedizin in verschiedenen medizinischen Disziplinen im Gesundheitswesen etablieren konnte.[13] Schließlich vervielfachten sich in den Neunzigerjahren die technischen Möglichkeiten der Informations- und Kommunikationstechnologien, sodass zunehmend digitale Daten auf elektronischem Wege übermittelt wurden. Die Telematik, die als Technik die Bereiche Telekommunikation und Informatik miteinander verknüpft, verbreitete sich in verschiedene Wirkungsbereiche, so auch in den medizinischen Bereich als Gesundheitstelematik. Hier liegt der Ursprung von E-Health, das in diesem Jahrzehnt schließlich erstmals wissenschaftlich umschrieben wurde. Dass auch E-Health nicht von der fortlaufenden technischen Entwicklung verschont bleibt, zeigt die Etablierung von mHealth (aus dem Englischen für „Mobile Health“). mHealth ist eine Form von E-Health, die mit der zunehmenden Verbreitung von portabler Informations- und Kommunikationstechnologie (IKT), wie etwa Smartphones und Smartwatches, entstanden ist.[14] Im folgenden Kapitel wird der Begriff E-Health weiter abgegrenzt, um anschließend eine einheitliche Definition für diese Arbeit aufzustellen.

2.1.2 Definition

Der Begriff E-Health (aus dem Englischen für „Electronic Health“) ist nicht allgemeingültig definiert und stetig im Wandel.[15] Der Duden versteht unter E-Health generell *„Den Einsatz von Computern und Internet im Gesundheitswesen“*[16]. Das Bundesministerium für Gesundheit (BMG) drückt sich diesbezüglich expliziter aus und subsumiert darunter den *„Oberbegriff für ein breites Spektrum von IKT-gestützten Anwendungen, in denen Informationen elektronisch verarbeitet, über sichere Datenverbindungen ausgetauscht und Behandlungs- und Betreuungsprozesse von Patientinnen und Patienten unterstützt werden können.“*[17]. Das BMG setzt hier den Fokus auf die Unterstützung der Gesundheitsversorgung durch digitalisierte Prozesse, in denen Daten ausgetauscht und verarbeitet werden.[18]

Nach allgemeiner Auffassung werden als E-Health die elektronisch unterstützten Prozesse, Produkte und Dienstleistungen im Gesundheitswesen bezeichnet. Darunter fallen alle Aktivitäten und Systeme, die Informationen und Daten erheben, verarbeiten oder auswerten.[19] Eine verwandte Disziplin ist die Telemedizin, die es ermöglicht, durch Telekommunikationstechniken die räumliche und zeitliche Trennung in der Kommunikation zwischen Ärzten, Patienten und Therapeuten aufzuheben, was im Grunde auch ein wichtiger Bestandteil von E-Health ist. Doch die Telemedizin umfasst neben der Kommunikation über digitale Medien wie E-Mail, Apps und Messenger auch traditionellere Kommunikations-

[12] Vgl. Florian Fischer et al. 2016, S. 297.
[13] Vgl. Florian Fischer et al. 2016, S. 13.
[14] Vgl. David Matusiewicz et al. 2017, S. 4 f.
[15] Vgl. PwC 2016, S. 25.
[16] Dudenredaktion o.J.
[17] Bundesministerium für Gesundheit o.J.
[18] Vgl. Bundesministerium für Gesundheit o.J.
[19] Vgl. David Matusiewicz et al. 2017, S. 3.

formen wie Fax und Telefon und ist daher nicht mit E-Health gleichzusetzen, auch wenn diese beiden Begriffe teilweise synonym verwendet werden.[20,21] Bei der Bezeichnung E-Health liegt der Fokus auf den Möglichkeiten des digitalen Zeitalters, d.h. vor allem dem Zusammentreffen von Internet und Medizin.[22] E-Health impliziert also die Nutzung neuer Technologien. Denn gerade die modernen Informations- und Kommunikationsmöglichkeiten in ihrer heute flächendeckenden Verfügbarkeit ermöglichen die Digitalisierung im Gesundheitswesen, aus der E-Health hervorgeht.[23] Neben der Kommunikation umfasst der Einsatz digitaler Technologien im Gesundheitswesen sehr vielfältige Aspekte dieser Branche. Sowohl Prävention, Diagnose, Behandlung, Überwachung und Forschung, als auch die Verwaltung mit ihren administrativen Prozessen, laufen im 21. Jahrhundert vermehrt digitalisiert ab und lassen sich somit unter dem Begriff E-Health zusammenfassen.[24]

Neben den rein technischen Aspekten weist der Gesundheitsforscher Gunther Eysenbach bereits 2001 auf die damit verbundene innere Einstellung bzw. den Zeitgeist hin, der untrennbar mit E-Health verbunden ist: *„In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology.“*[25] Eysenbach macht deutlich, dass E-Health als globales Themenfeld zu verstehen ist, das zwar auf IKT basiert, aber auch grundlegende Denkweisen beinhaltet, die über die technischen Aspekte hinausgehen. Der Schwerpunkt von E-Health ist mithin die Nutzung moderner Informations- und Kommunikationstechnologien in Bezug auf Gesundheit und Medizin.[26] Da, wie oben dargelegt, auch im deutschsprachigen Raum keine einheitliche Definition von E-Health existiert, wird für diese Arbeit eine Definition festgelegt, die für den Leser und vor allem auch für die interviewten Gesprächspartner leicht nachvollziehbar und mit dem Schwerpunkt Datenschutz vereinbar ist. Die Nachvollziehbarkeit ist im Sinne der wissenschaftlichen Vorgehensweise wichtig, um im empirischen Teil die Fragestellung, die Erhebung der Forschungsdaten und die aufbereiteten Ergebnisse verständlich und reproduzierbar zu erhalten. Aus diesen Gründen wird der Begriff E-Health in dieser Arbeit wie folgt abgegrenzt:

„E-Health meint alle Aktivitäten im Gesundheitswesen, bei denen unter Zuhilfenahme digitaler Technologien Daten verarbeitet werden.“

Für ein tieferes Verständnis der Materie reicht die terminusbezogene Definition jedoch nicht aus. Daher werden nachfolgend die Interessengruppen sowie das Ziel und die Vor- und Nachteile von E-Health aufbereitet.

Interessengruppen

Der E-Health-Sektor schließt unterschiedliche Akteure mit ein. Die nachstehende Abbildung verschafft einen Überblick über die relevanten Interessengruppen.

[20] Vgl. Florian Fischer et al. 2016, S. 13.
[21] Vgl. Jeannette Stark 2018.
[22] Vgl. Manfred Klein 2017.
[23] Vgl. David Matusiewicz et al. 2017, S. 3 f.
[24] Vgl. PwC 2016, S. 27.
[25] Gunther Eysenbach 2001, S. 1.
[26] Vgl. Manfred Klein 2017.

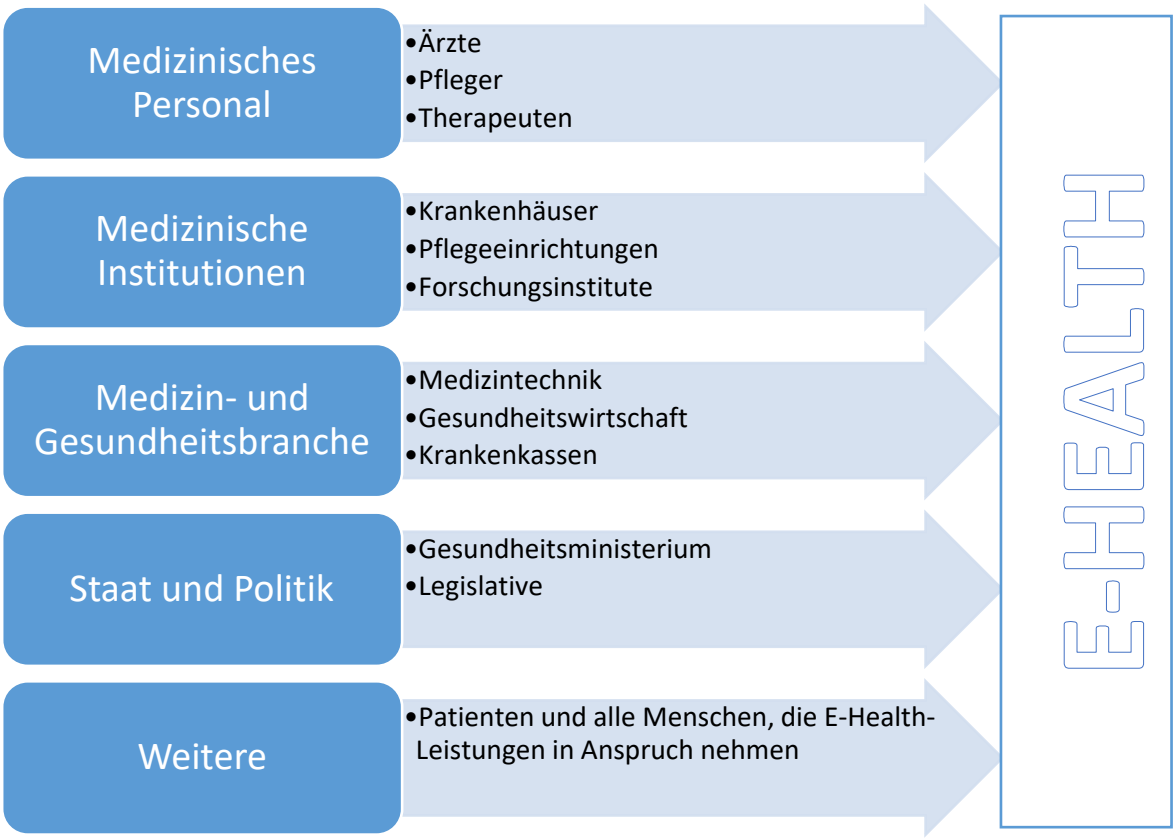

Abbildung 2: Stakeholder von E-Health

[Quelle: Eigene Abbildung, basierend auf den zitierten Quellen.]

Dieses Schaubild zeigt auf, von welchen Interessengruppen und Akteuren der E-Health-Sektor geprägt ist. Hierzu zählen neben den Patienten und dem medizinischen Personal, den Krankenhäusern und Pflegeeinrichtungen, auch die Medizin- und Gesundheitsbranche im Allgemeinen, der Staat und ein jeder Bürger, der eine Smartwatch mit einer vorinstallierten Gesundheitsapp trägt, die seine medizinischen Daten protokolliert.[27,28] Da insbesondere die personenbezogenen Daten der natürlichen Personen wie der Patienten (Leistungsempfänger) und des medizinischen Personals (Leistungserbringer) den datenschutzrechtlichen Regularien unterliegen, werden diese Akteure in dieser Arbeit eine hervorgehobene Rolle spielen.

Ziel

Das Ziel von E-Health ist die Sicherung und Verbesserung der Gesundheitsversorgung.[29] Dies unterscheidet sich zunächst nicht vom Ziel des Gesundheitswesens generell. Die Besonderheit liegt darin, dass dieses Ziel mit digitaler Unterstützung, so etwa durch die Vernetzung der Institutionen und Personen mit Hilfe einer verlässlichen und sicheren digi-

[27] Vgl. Kathrin Schäfer 2019.
[28] Vgl. Margunn Aanestad et al. 2017, S. 11.
[29] Vgl. Florian Fischer et al. 2016, S. 3.

talen Infrastruktur[30] und der effektiveren Analyse von Gesundheitsdaten erreicht werden soll.[31]

2.1.3 Chancen und Risiken

Die Digitalisierung im Gesundheitswesen birgt unterschiedliche Chancen und Risiken. Eine Auswahl der in Fachpublikationen beschriebenen Vor- und Nachteile wird im folgenden Abschnitt dargestellt, ohne jedoch jeden Aspekt vollständig auszuführen, da dies für den weiteren Verlauf dieser Arbeit nicht von entscheidender Relevanz ist.

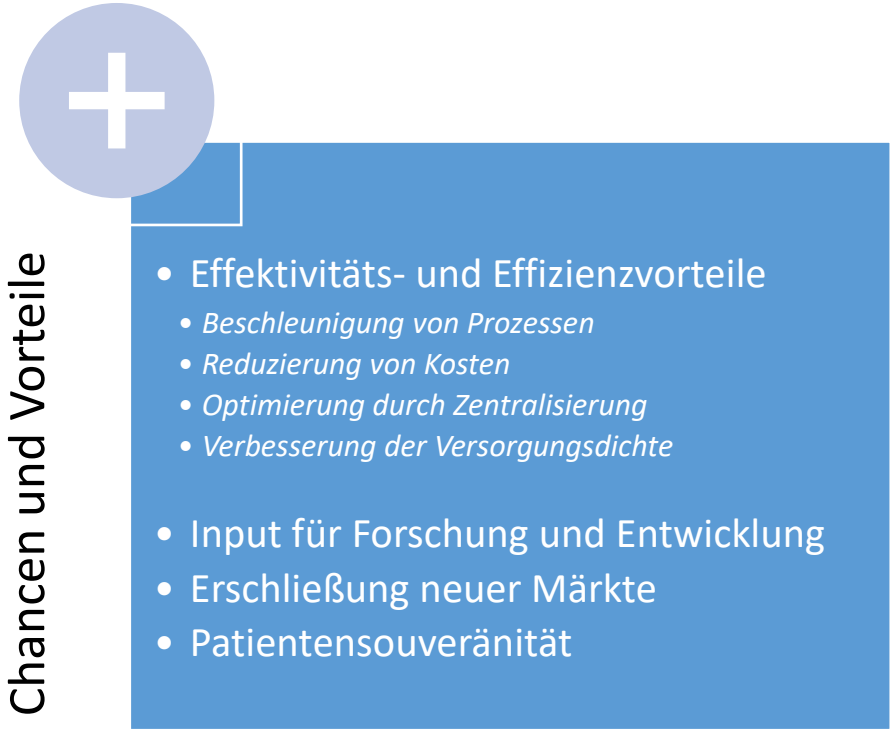

Abbildung 3: Vorteile von E-Health

[Quelle: Eigene Abbildung, basierend auf den zitierten Quellen.]

E-Health ermöglicht den schnelleren Zugang zu medizinischen Informationen, sowohl für die Patienten als auch für die Datenverarbeiter wie Ärzte und Krankenkassen.[32] Durch eine digitale Optimierung der Kommunikation, des Behandlungsablaufs und der Verwaltungsprozesse können Kosten eingespart und Vorgänge beschleunigt werden.[33,34] Einer McKinsey-Studie aus dem Jahr 2018 zufolge liegt das monetäre Einsparpotential im deutschen Gesundheitswesen durch E-Health bei bis zu 34 Milliarden Euro. Zur Einordnung: Der hochgerechnete jährliche Gesamtaufwand der bundesweiten Gesundheits- und Versorgungskosten beläuft sich auf 290 Milliarden Euro. Insbesondere die Digitalisierung der Patientendaten und die internetbasierte Kommunikation zwischen Leistungserbringer und

[30] Vgl. Bundesministerium für Gesundheit 2020.
[31] Vgl. Christoph Bauer et al. 2018, S. 10.
[32] Vgl. Florian Fischer et al. 2016, S. 156 f.
[33] Vgl. Florian Fischer et al. 2016, S. 15 f.
[34] Vgl. PwC 2017, S. 75–78.

Leistungsempfänger bieten der Studie nach sowohl finanziell als auch zeitbezogen das größte Nutzenpotenzial.[35] 70% des erreichbaren Nutzens kommt McKinsey zufolge direkt bei den Leistungserbringern, d.h. bei den Ärzten, Krankenhäusern und Pflegeeinrichtungen, an.[36]

Ein weiterer Vorteil ist die Verbesserung der Versorgungsdichte. Strukturschwache Gebiete sowie bewegungseingeschränkte Menschen profitieren von der Verfügbarkeit einer orts- und zeitunabhängigen Gesundheitsversorgung. E-Health ermöglicht damit auch außerhalb der Großstädte eine flächendeckende und im Idealfall qualitativ hochwertige Gesundheitsversorgung.[37] Eine zentrale Datenerfassung kann Doppeldiagnosen und Fehlmedikationen vermeiden. Der technologische Wandel und eine bessere Vernetzung führen zu einer schnelleren und effektiveren Diagnostik sowie einer mehr individualisierten Gesundheitsversorgung.[38] Nutzern von E-Health-Applikationen wird es ermöglicht, aktiv und eigenverantwortlich am Gesundheitswesen teilzunehmen. Patienten und Dienstleistern wird mithin eine höhere Transparenz über das Leistungs- und Behandlungsgeschehen ermöglicht, wodurch die Patientensouveränität gestärkt wird.[39]

Durch den optimalen, digital unterstützten Einsatz der verfügbaren Ressourcen werden Effektivität und Effizienz der Gesundheitsversorgung gesteigert.[40,41] Die Technologien beschleunigen und erleichtern Routinetätigkeiten für die Leistungserbringer in der Gesundheitsbranche. Die hiermit gewonnenen Ressourcen und Zeitersparnisse können diese nutzen, um sich komplexeren Arbeitsbereichen und der persönlichen Patientenbetreuung zu widmen.[42] Technologische Errungenschaften führen zur Erschließung neuer Märkte und damit zu ökonomischen Vorteilen für die Leistungserbringer.[43]

Die statistische Auswertung von Gesundheitsdaten bringt Input für die Forschung und Entwicklung im Gesundheitswesen. Die Erhebung und der wissenschaftliche Austausch dieser Daten können bspw. dazu führen, dass Gesundheitsrisiken früher erkannt werden.[44] Von dieser umfassenden Datenanalyse profitiert auch der Staat, der so bspw. in Pandemiezeiten gezielt Gegenmaßnahmen (z.B. regionale Lockdowns) ergreifen kann.[45]

Die dargelegten positiven Effekte können im Optimalfall durch die Einbindung von E-Health erreicht werden, jedoch stehen diesen Chancen und Vorteilen auch gewisse Risiken und Nachteile gegenüber. Eine Auswahl ebendieser wird nachfolgend abgebildet.

[35] Vgl. McKinsey & Company 2018, S. 3–8.
[36] Vgl. McKinsey & Company 2018, S. 3.
[37] Vgl. David Matusiewicz et al. 2017, S. 28.
[38] Vgl. PwC 2017, S. 13.
[39] Vgl. Stefan Müller-Mielitz et al. 2017, S. 366 f.
[40] Vgl. Florian Fischer et al. 2016, S. 102.
[41] Vgl. PwC 2016, S. 88 f.
[42] Vgl. David Matusiewicz et al. 2017, S. 57.
[43] Vgl. Florian Fischer et al. 2016, S. 12.
[44] Vgl. David Matusiewicz et al. 2017, S. 28.
[45] Vgl. PwC 2016, S. 90.

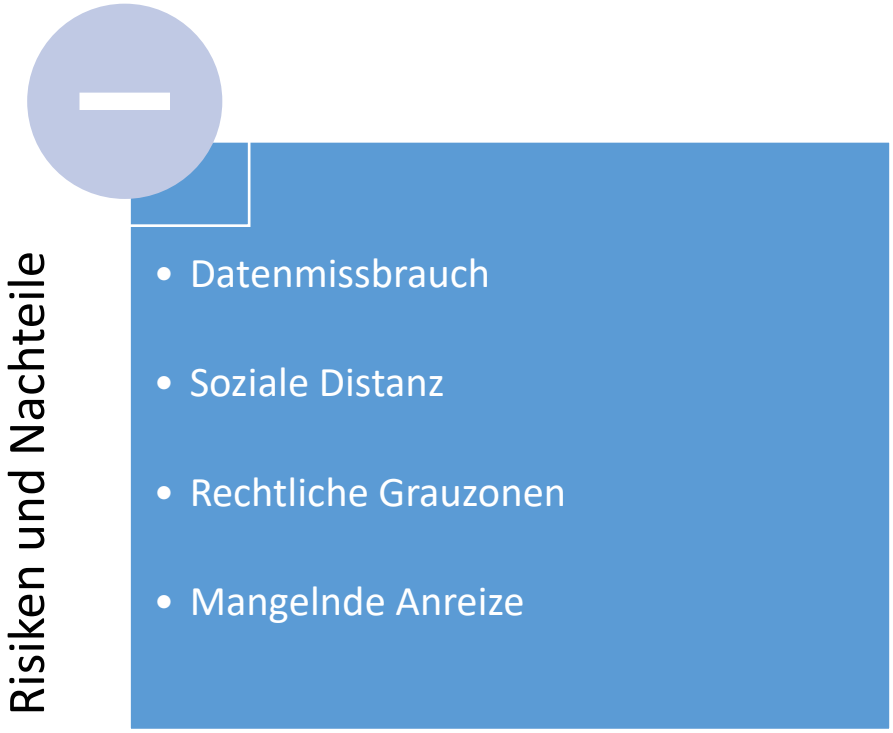

Abbildung 4: Nachteile von E-Health

[Quelle: Eigene Abbildung, basierend auf den zitierten Quellen.]

Kritiker bemängeln eine Störung der persönlichen, nachhaltigen Arzt-Patienten-Beziehung, da im E-Health-Bereich der persönliche Kontakt vermehrt durch den Einsatz von Kommunikationstechnologien, wie bspw. durch Videosprechstunden oder die Erfassung von Patienten- und Behandlungsdaten per Apps, ersetzt wird.[46] Es wird befürchtet, dass die Behandlungsqualität unter der emotionalen Distanz zwischen Leistungserbringer und Leistungsempfänger leidet und bspw. durch fehlende persönliche Beobachtung die Verhaltensweisen des Patienten nicht mehr ausreichend analysiert und gewürdigt werden.[47] Durch die Neuartigkeit von E-Health existieren noch immer rechtliche Grauzonen, die bei den verschiedenen Interessengruppen für juristische Unsicherheiten sorgen. Dazu gehören z.B. ungeklärte Haftungsrisiken[48] und die Auslegung des Fernbehandlungsverbots.[49,50]

Ein weiterer Kritikpunkt sind die mangelnden Anreize für Leistungserbringer, ihre analogen Prozesse in das digitale Zeitalter zu überführen. So sehen bspw. manche Gebührenordnungen eine niedrigere Vergütung für Ärzte bei der Verwendung des elektronischen Arztbriefes vor als bei einer Faxsendung. Diese Rahmenbedingungen setzen finanzielle Fehlreize und erschweren damit die Einführung von E-Health in der Praxis.[51] Dieser Prob-

[46] Vgl. Stefan Müller-Mielitz et al. 2017, S. 145.
[47] Vgl. PwC 2016, S. 91.
[48] Vgl. PwC 2016, S. 92.
[49] Vgl. PwC 2017, S. 53.
[50] Vgl. Florian Fischer et al. 2016, S. 53 f.
[51] Vgl. David Matusiewicz et al. 2017, S. 132.

lematik tritt der Gesetzgeber jedoch zunehmend mit rechtlichen Neuentwicklungen, wie etwa dem im späteren Verlauf dieser Arbeit dargestellten E-Health-Gesetz, entgegen.[52]

Als eine immanente Gefahr von E-Health werden Datenschutzrisiken angesehen. Insbesondere die Beteiligungen von profitorientierten Unternehmen am E-Health-Markt, die typischerweise nicht in der Gesundheitsbranche angesiedelt sind, wie bspw. Apple und Google, wecken Bedenken bei Datenschützern. Doch die latente Gefahr des Datenmissbrauchs geht ebenso von öffentlichen Institutionen bis hin zu Geheimdiensten aus.[53] Thilo Weichert, ehemaliger Datenschutzbeauftragter des Landes Schleswig-Holstein, stellt in einem Beitrag in der Fachzeitschrift Datenschutz und Datensicherheit in diesem Zusammenhang fest: *„Nicht konsentierte, heimliche und/oder zweckwidrige Nutzungen von Daten aus dem höchstpersönlichen Gesundheitsbereich beeinträchtigen generell die persönliche Entfaltung und dies oft in existenziellen Lebensbereichen wie Berufstätigkeit, Familie oder Sexualität. Durch eine Kompromittierung der Vertraulichkeit kann das Vertrauen in die Hilfeleistung beeinträchtigt sein, was sich auf die Inanspruchnahme der medizinischen Hilfe auswirken kann.“*[54].

Die dargestellten Vor- und Nachteile verdeutlichen die kontroverse Debatte um die Digitalisierung im Gesundheitswesen. Vor allem die digitale Datenverarbeitung, die in dieser Arbeit im Vordergrund steht, bringt einerseits Effektivitäts- und Effizienzvorteile, doch andererseits juristische Unklarheiten und Datenschutzrisiken mit sich, deren rechtlicher Rahmen ab Kapitel 2.2 behandelt wird. Die für diese Arbeit relevanten Formen von E-Health werden im nächsten Unterkapitel präsentiert.

2.1.4 Formen

Die Vernetzung der Nutzergruppen miteinander und untereinander ist das zentrale Element von E-Health.[55] Daher werden in der untenstehenden Illustration dessen Formen anhand dieses Kriteriums aufgegliedert. Folgendes Schaubild stellt das „Wer?“ in der Vernetzung dar, also zwischen wem die zu verarbeitenden Daten ausgetauscht werden.

[52] Vgl. Kapitel 2.2.2.4 dieser Arbeit.
[53] Vgl. Thilo Weichert 2014.
[54] Thilo Weichert 2014, S. 834.
[55] Vgl. Florian Fischer et al. 2016, S. 9 f.

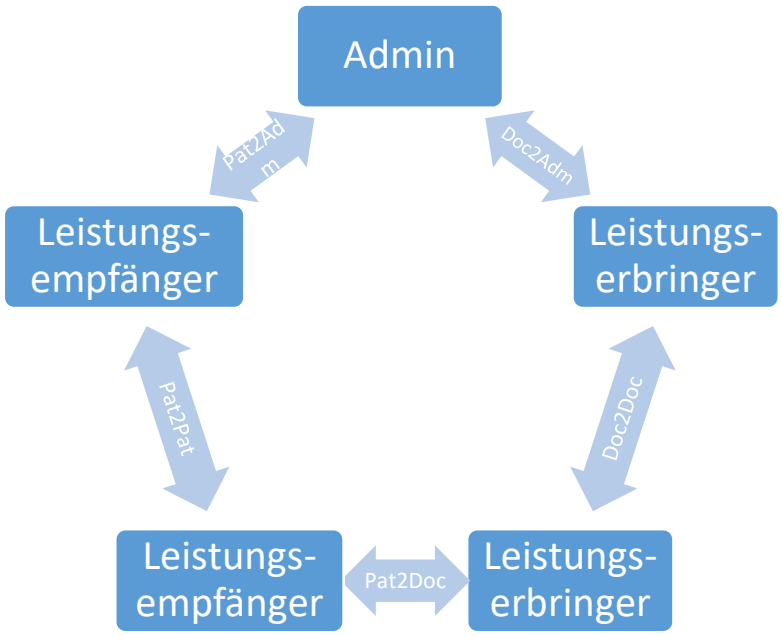

Abbildung 5: Formen von E-Health - Vernetzung (wer)

[Quelle: Eigene Abbildung, vgl. Florian Fischer et al. 2016, S. 9 f.]

Das Schaubild unterscheidet fünf verschiedene Ausprägungen von E-Health. Unter Leistungserbringern sind die ausführenden Berufe wie Ärzte, Therapeuten und Krankenpfleger zu verstehen. Die Leistungsempfänger sind Patienten und andere Menschen, deren Daten aus gesundheitsbezogenen Gründen verarbeitet werden. Die Vernetzung zwischen den Leistungserbringern (Doc2Doc) bedeutet z.B., dass sich zwei Ärzte während einer Telekonsultation miteinander austauschen oder auf Onlineplattformen für die Teleausbildung Informationen ausgetauscht werden. Der Kontakt zwischen Leistungserbringer und Leistungsempfänger (Doc2Pat) findet häufig im Rahmen einer Teletherapie oder in der Telediagnostik statt, bspw. in Videosprechstunden. Zum Datenaustausch zwischen den Patienten untereinander (Pat2Pat) gehören die Selbsthilfeportale im Internet. Unter Doc2Admin sind alle IKT-unterstützten administrativen Prozesse im medizinischen Bereich umfasst, etwa die krankenhausinterne Verwaltung oder die digitalisierte Kommunikation zwischen Ärzten und Krankenkassen oder sonstigen Dienstleistern bzw. Kostenträgern. Pat2Admin stellt unter anderem die Weitergabe personenbezogener Gesundheitsdaten an Dienstleister außerhalb des klassischen Gesundheitswesens dar, bspw. durch die Nutzung von Gesundheitsapps, die von IT-Konzernen angeboten und verwaltet werden.[56]

Nachdem nun die Ausprägungen innerhalb der Kommunikationsstrukturen feststehen, wird nachfolgend eine zweite Untergliederung von E-Health den Hintergrund und die Mittel des Datenaustauschs beleuchten, also das „Wie?“ der Vernetzung. Hierfür wird, wie in der folgenden Abbildung ersichtlich, eine Unterscheidung in der organisatorischen Komplexität vorgenommen, um die verschiedenen Formen von E-Health abbilden zu können.

[56] Vgl. Florian Fischer et al. 2016, S. 10.

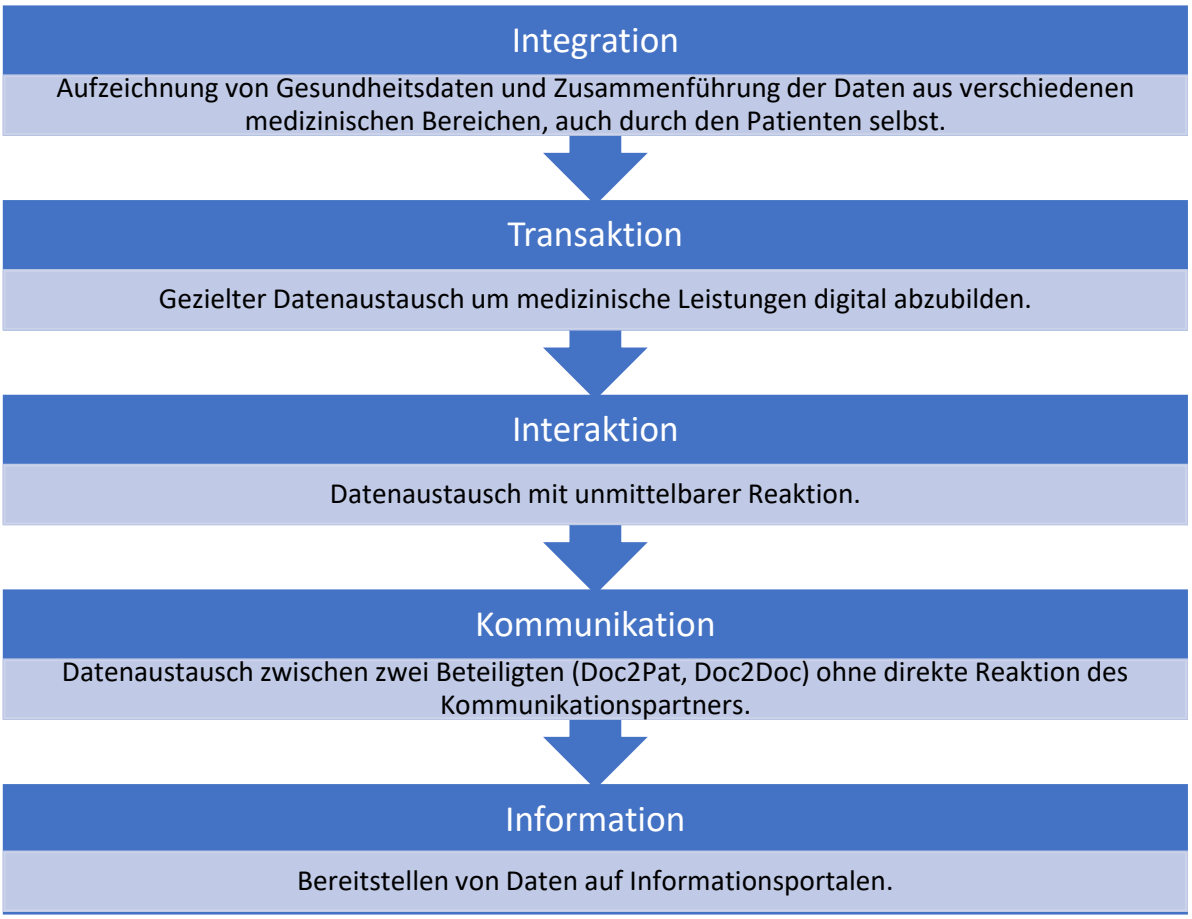

Abbildung 6: Formen von E-Health - Vernetzung (wie)

[Quelle: Eigene Abbildung, vgl. Christian Schmidt et al. 2016.]

Die Reifegrade sind absteigend dargestellt: Integration, Transaktion, Interaktion, Kommunikation und Information. Dieser Aufbau beruht auf dem klassischen Fünf-Stufen-Modell des E-Government von Hiller und Belánger aus dem Jahr 2001.[57]

Ein konkretes Beispiel für die Integration ist etwa die elektronische Patientenakte (ePA). Die ePA stellt eine grundlegende Erneuerung im deutschen Gesundheitswesen dar und hat das Ziel, bundesweit die analoge Aktenführung im Gesundheitswesen durch eine einheitliche digitale Lösung zu ersetzen.[58] Sie wird ab dem Jahr 2021 zunehmend in Deutschland eingeführt und enthält unter anderem die Notfalldaten sowie Diagnose- und Behandlungsdaten des jeweiligen Leistungsempfängers. Außerdem bietet sie auch den Patienten selbst die Möglichkeit, medizinische Informationen in das System einzupflegen und zu löschen.[59] Die ePA wird den Patienten von ihrer Krankenkasse zur Verfügung gestellt und unterstützt deren Leistungsabwicklung mit Arztpraxen, Krankenhäusern und Apotheken.[60] Auch die bereits bestehenden IT-Systeme der Krankenhäuser sind Bestand-

[57] Vgl. Janine Hiller et al. 2001, S. 16.
[58] Vgl. Bundesgesundheitsministerium 2020b.
[59] Vgl. Bundesgesundheitsministerium 2020a.
[60] Vgl. Bundesgesundheitsministerium 2020b.

teil der Integration, wenn hier eine umfassende Datenverarbeitung aus verschiedenen Quellen stattfindet.[61]

Zur Transaktion gehört bspw. die elektronische Gesundheitskarte (eGK), die bereits seit dem 01.01.2015 für alle gesetzlich Versicherten vorgeschrieben ist. Sie stellt die Stammdaten der Versicherten auf einer digitalen Plattform zur Verfügung, erleichtert den Zugriff auf die Administration von Versichertendaten und erschwert durch Sicherheitsmechanismen den Leistungsmissbrauch. Die eGK realisiert als „Europäische Versicherungskarte" die digitale Abwicklung von medizinischen Behandlungen innerhalb der EU.[62] Sie digitalisiert die Verwaltung der Krankenkassen und damit den Datenaustausch zwischen Patienten, Krankenkassen sowie Arztpraxen und ist mithin Zugangsvoraussetzung für andere E-Health-Instrumente wie die ePA und digitale Atteste.[63]

Interaktion wird bspw. mit Home Monitoring und Hausnotrufen erreicht. Home Monitoring, also die medizinische Fernversorgung bzw. -überwachung, wird vor allem bei Patienten mit Herzschrittmachern (Telekardiologie) und implantierten Defibrillatoren angewendet. So kann der Arzt auch außerhalb der stationären Behandlung die Vitalwerte seiner Patienten per Mobilfunk in Echtzeit überwachen. Hierdurch kann die medizinische Diagnostik optimiert und der Arzt zielgerichtet tätig werden, während der Patient weniger Routinebesuche beim Facharzt wahrnehmen muss und dadurch flexibler und freier leben kann.[64,65] Der vor allem für Senioren konzipierte Hausnotruf ermöglicht eine schnelle Intervention bei medizinischen Notfällen und die direkte Kommunikation mit dem Leistungsempfänger und ist daher auch eine Form von Fernüberwachung.[66] Eine andere Form der Interaktion ist die Videosprechstunde. Hier kann der Patient per Videochat mit seinem Arzt kommunizieren und damit von zuhause aus medizinische Sachverhalte abklären. Die Telekonsultation zeigt ihre Vorzüge gegenüber der analogen Sprechstunde nicht nur bei körperlich eingeschränkten Menschen und nach Operationen, sondern ist insbesondere in Pandemiezeiten ein wichtiges Instrument für eine kontaktarme, und daher das Infektionsrisiko verringernde, medizinische Behandlung.[67,68]

Die E-Health-Form der Kommunikation spiegelt sich in Online-Diabetestagebüchern bzw. Diabetes-Apps wider, die der Patient nutzen kann, um sich selbst und dem behandelnden Arzt seine Blutzuckerwerte bzw. seinen Therapiefortschritt aufzubereiten.[69] Andere medizinische Apps dienen der Protokollierung und Kontrolle der Medikamenteneinnahme. Das am 19.12.2020 in Kraft getretenen Digitale-Versorgung-Gesetz (DVG), welches E-Health in Deutschland vereinfachen und regulieren soll, ermöglicht es Ärzten, ihren Patienten auch Apps zu verschreiben.[70] Sogenannte Apps auf Rezept werden einheitlich geprüft und, wenn sie bewiesenermaßen die Gesundheitsversorgung der Patienten verbessern können, von den gesetzlichen Krankenversicherungen (GKV) finanziert.[71] Eine

[61] Vgl. Christian Schmidt et al. 2016, S. 185.
[62] Vgl. Bundesgesundheitsministerium 2020a.
[63] Vgl. Dirk Becker et al. 2020.
[64] Vgl. Bundesverband für Medizintechnologie, Aktion Meditech 2015.
[65] Vgl. Volker P. Andelfinger et al. 2016, S. 14 f.
[66] Vgl. Volker P. Andelfinger et al. 2016, S. 9.
[67] Vgl. Kassenärztliche Bundesvereinigung 2020a.
[68] Vgl. Kassenärztliche Bundesvereinigung 2020b.
[69] Vgl. Volker P. Andelfinger et al. 2016, S. 43.
[70] Vgl. Bundesgesundheitsministerium 2020c.
[71] Vgl. AOK Bundesverband o.J.

weitere Form von Gesundheitsapps sind die Corona-Warn-Apps, die zur Pandemiebekämpfung im Jahr 2020 weltweite Verbreitung gefunden haben. Diese haben das Ziel, den Kontakt mit Infizierten offenzulegen und durch Nachverfolgung als sogenannte Contact-Tracing-App (contact tracing, engl. für „Kontaktrückverfolgung“) die App-Nutzer vor einer möglichen Infektion zu warnen. Hierfür müssen sowohl der Infizierte als auch der zu Warnende die App nutzen. Außerdem ermöglicht die Corona-Warn-App des Robert-Koch-Instituts (RKI) die Übermittlung von Corona-Testergebnissen und trägt somit zu einer unkomplizierten, schnellen und risikoarmen Form der Kommunikation bei. Auf diesem Wege wurden bereits nach wenigen Monaten (Stand Dezember 2020) fünf Millionen Testergebnisse digital übermittelt. Des Weiteren findet eine Harmonisierung der Apps auf EU-Ebene statt, sodass die Informationen und Warnungen europaweit verarbeitet werden können.[72] Die Veröffentlichung der App wurde von einer intensiven datenschutzrechtlichen Debatte begleitet.[73] Durch Einbindung von Datenschützern und IT-Experten in den Entwicklungsprozess der App wurde es bewerkstelligt, dass die Nutzer weder ihren Namen noch ihre E-Mail-Adresse preisgeben müssen und die App der deutschen Öffentlichkeit daher niedrigschwellig und datenminimierend zur Verfügung steht. Nach Angaben des RKI ist der Datenmissbrauch ausgeschlossen, da der Nutzer die volle Kontrolle über seine Daten behält und alle verarbeiteten Daten pseudonymisiert werden.[74]

Formen der Information bzgl. E-Health sind Medizinportale und Datenbanken, auf denen Patienten, Ärzte und interessierte Bürger digital medizinische Informationen abrufen können.[75] Welche Formen von E-Health besonders relevant im Alltagsgeschäft bestimmter medizinischer Institutionen und hinsichtlich der datenschutzrechtlichen Umsetzung besonders hervorzuheben sind, wird im empirischen Teil dieser Arbeit behandelt.

2.2 Rechtlicher Rahmen

2.2.1 DSGVO und BDSG-neu

Seitdem im Mai 2018 nach einer zweijährigen Übergangsphase die DSGVO unmittelbar anzuwendendes Recht in allen EU-Ländern wurde, gilt auch in Deutschland dieses einheitliche, datenschutzrechtliche Mindestniveau. Die DSGVO hat den Rechtscharakter einer europäischen Verordnung und gilt nach Art. 288 II AEUV (Vertrag über die Arbeitsweise der Europäischen Union) unmittelbar und allgemein in jedem Mitgliedsstaat. Als eine solche Verordnung genießt die DSGVO einen Anwendungsvorrang gegenüber den nationalen Gesetzen, wie etwa dem BDSG-neu (Bundesdatenschutzgesetz-neu). Das heißt, bei einer Normenkollision entfaltet allein die DSGVO als ranghöheres Recht ihre Wirkung. Das BDSG-neu als zentrales Datenschutzgesetz in Deutschland, hat seine Aufgabe vor allem in der Konkretisierung und als Erweiterung der DSGVO. Mit sogenannten Öffnungsklauseln in der DSGVO wird es den nationalen Gesetzgebern ermöglicht, in bestimmten datenschutzrechtlichen Bereichen Spezifizierungen vorzunehmen bzw. eigene Rechtsvorschriften zu bestimmen. Das BDSG-neu ist also als eine bundesrechtliche Ergänzung der DSGVO zu betrachten, die nur zur Anwendung kommt, wenn in der DSGVO bestimmte datenschutzrechtliche Aspekte durch Öffnungsklauseln offen- bzw. ausgelas-

[72] Vgl. RKI 2020.
[73] Vgl. GDD e.V. 2020.
[74] Vgl. RKI 2020.
[75] Vgl. Christian Schmidt et al. 2016, S. 185.

sen werden.[76,77] Allerdings ist auch das sonstige nationale Recht gerade im Bereich der Gesundheitsdaten nicht zu vernachlässigen, da wegen der Sensibilität und Vielfältigkeit der diesbezüglichen Datenverarbeitung ein erhöhter Regelungsbedarf besteht. Das Subsidiaritätsprinzip des § 1 I, II BDSG-neu sieht vor, dass spezialgesetzliche Regelungen den Vorschriften des BDSG-neu gegenüber immer vorrangig angewendet werden müssen. So finden etwa die spezifischeren datenschutzrechtlichen Normen aus anderen Bundesgesetzen oder die landesgesetzlichen Datenschutzregelungen, bspw. zum Datenschutz in öffentlichen Krankenhäusern, noch vor den Regelungen des BDSG-neu Anwendung. Jedoch bleiben auch diese Sondervorschriften nachrangig zur DSGVO, die durch ihre priorisierte Stellung in der Normenhierarchie alle hiesigen Rechtsquellen überlagert.[78] Die folgende Abbildung stellt diese Hierarchie grafisch dar.

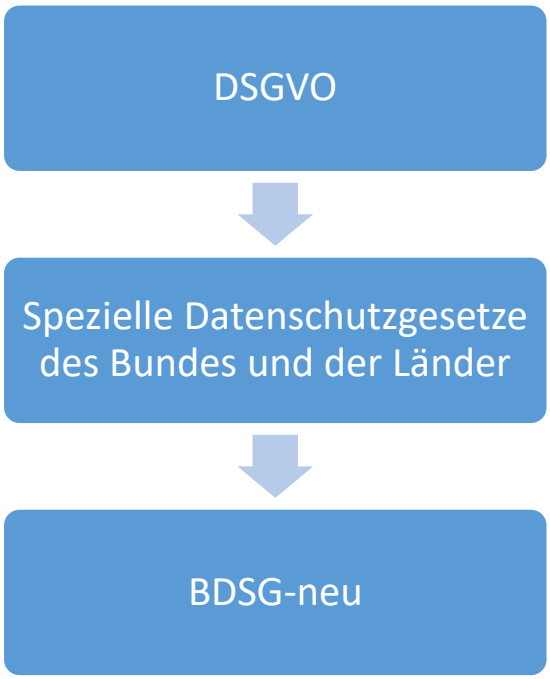

Abbildung 7: Normenhierarchie im Datenschutzrecht

[Quelle: Eigene Abbildung, vereinfacht dargestellt vgl. Bernd Juraschko 2020, Abb. 14.][79]

Durch die dargestellte erhöhte Rangstellung der DSGVO und der Tatsache geschuldet, dass das BDSG-neu rein auf den Öffnungsklauseln der DSGVO basiert, werden zunächst einzelne relevante Aspekte und Normen der DSGVO unter Berücksichtigung der Ergänzungen im BDSG-neu gemeinsam erläutert. Der Fokus bleibt dabei auf den Bestimmungen, die auch die Datenverarbeitung im E-Health-Bereich betreffen.

[76] Vgl. § 1 V BDSG-neu.
[77] Vgl. Thomas Jäschke et al. 2018, S. 27 f.
[78] Vgl. Thomas Jäschke et al. 2018, S. 28–31.
[79] Vgl. Bernd Juraschko 2020.

2.2.1.1 Gegenstand, Ziele und Anwendungsbereich

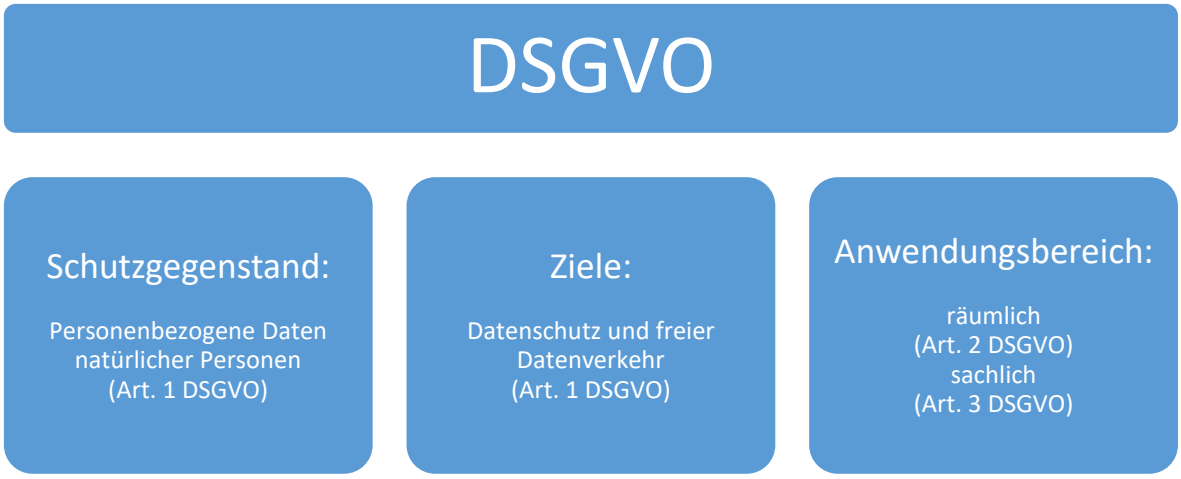

Abbildung 8: Schutzgegenstand, Ziele und Anwendungsbereich der DSGVO

[Quelle: Eigene Abbildung.]

Gegenstand und Ziele der DSGVO sind in Artikel 1 der Verordnung bestimmt. Demnach beziehen sich die Regelungen der DSGVO auf den Schutz natürlicher Personen bei Datenverarbeitungen sowie auf den freien Datenverkehr.[80] Die DSGVO sichert insbesondere das Recht von natürlichen Personen auf den Schutz ihrer personenbezogenen Daten. Diese Schutzfunktion ist abgeleitet aus dem achten Artikel der EU-Grundrechtecharta (GRCh), nach der jede Person „das Recht auf Schutz der sie betreffenden personenbezogenen Daten“[81] hat. Durch die unmittelbare Geltung der DSGVO in allen EU-Ländern als rechtssichere und transparente Rechtsgrundlage sichert die DSGVO auch den freien Verkehr von Daten im EU-Binnenmarkt.[82] Somit sind die personenbezogenen Daten der Schutzgegenstand dieser Verordnung. Die Ziele sind zum einen der Schutz natürlicher Personen bei der Verarbeitung ebendieser und zum anderen der freie Datenverkehr in der EU.[83]

Artikel 2 und 3 der DSGVO legen den sachlichen und räumlichen Anwendungsbereich der DSGVO fest. Der sachliche Anwendungsbereich gem. Art. 2 DSGVO umfasst jede digitale Verarbeitung personenbezogener Daten, die nicht den Ausnahmetatbeständen des Art. 2 II DSGVO entspricht, wie es etwa bei Datenverarbeitungen im Rahmen familiärer Aktivitäten oder zwecks staatlicher Strafverfolgung der Fall ist. Diese Ausnahmetatbestände kommen jedoch bei der Datenverarbeitung im E-Health-Bereich regelmäßig nicht in Betracht und werden daher im Folgenden nicht weiter behandelt. Der räumliche Anwendungsbereich nach Art. 3 I DSGVO legt fest, dass grundsätzlich jede Datenverarbeitung durch Stellen, die innerhalb der EU tätig sind und im Rahmen dieser Tätigkeit personenbezogene Daten verarbeiten, vom Geltungsbereich der DSGVO umfasst ist. Dies gilt unabhängig davon, an welchem Ort die Datenverarbeitung letztendlich stattfindet und

[80] Vgl. Art. 1 I DSGVO.
[81] Art. 8 I GRCh.
[82] Vgl. Erwägungsgrund Nr. 13 der DSGVO.
[83] Vgl. Art. 1 DSGVO.

welche Produkte oder Dienstleistungen angeboten werden (Niederlassungsprinzip[84]).[85] Auch Stellen, die nicht direkt in der EU tätig sind, jedoch nach Art. 3 II DSGVO (Marktortprinzip[86]) ihr Angebot auf den EU-Markt ausrichten oder verhaltensbeobachtende Maßnahmen in der EU durchführen, fallen in den räumlichen Anwendungsbereich der DSGVO. Ein ähnliches Prinzip bringt der § 1 IV S. 2 BDSG-neu zum Ausdruck, nach dem das Bundesdatenschutzgesetz auf öffentliche Stellen generell und darüber hinaus dann anzuwenden ist, wenn die Datenverarbeitung in Deutschland[87] oder im Rahmen der Tätigkeit einer inländischen Niederlassung[88] erfolgt und der ansonsten auf den in der DSGVO definierten Anwendungsbereich verweist[89]. Mithin ist jedes Unternehmen in Deutschland, das in Bezug auf E-Health personenbezogene Daten verarbeitet, vom Anwendungsbereich der DSGVO sowie des BDSG-neu umfasst.

2.2.1.2 Definitionen und Grundsätze

In den Artikeln 4 und 5 der DSGVO werden die Rechtsbegriffe des Datenschutzes definiert und die Grundsätze der Datenverarbeitung ausgeführt. Für ein tiefergehendes Verständnis der Rechtslage werden zunächst anhand des Art. 4 DSGVO die hierfür relevanten Begrifflichkeiten mit Fokus auf die Datenverarbeitung im Gesundheitswesen erläutert.

Datenschutzrechtlicher Schutzgegenstand: Personenbezogene Daten (Art. 4 Nr. 1 DSGVO)

Personenbezogene Daten sind auf eine natürliche Person (nachfolgend "betroffene Person“ oder „Betroffener“) bezogene Informationen, sofern die Person hierdurch identifizierbar ist oder identifiziert werden kann. Daten, die vollkommen anonymisiert worden sind, zählen nicht zu den personenbezogenen Daten und werden daher von der DSGVO nicht umfasst.[90] Ebenso werden Daten von verstorbenen Personen nicht berücksichtigt, diese können jedoch durch landesspezifische Regelungen gesondert geschützt werden.[91] Der Begriff der personenbezogenen Daten umfasst mithin alle Patientendaten, da sich diese regelmäßig auf identifizierbare natürliche Personen beziehen.

Datenschutzrechtlicher Tatbestand: Verarbeitung (Art. 4 Nr. 2 DSGVO)

Eine Verarbeitung ist jeder (teil)automatisierte Vorgang in Zusammenhang mit personenbezogenen Daten. Dies schließt unter anderem die Erhebung, Veränderung, Nutzung, Übermittlung und Löschung personenbezogener Daten mit ein und umfasst sämtliche Aktivitäten in Verbindung mit personenbezogenen Daten. Da bei diesem Rechtsbegriff jeder mögliche Verarbeitungsvorgang mit inbegriffen ist, ist sowohl die Form der Datenerhebung (schriftlich, mündlich, elektronisch) als auch die Quelle der Daten (von der Person selbst oder von Dritten) für das Vorliegen einer datenschutzrelevanten Verarbeitung nicht von Bedeutung.[92]

[84] Vgl. Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.
[85] Vgl. Art. 3 I DSGVO, letzter Halbsatz.
[86] Vgl. Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.
[87] Vgl. § 1 IV S. 2 Nr. 1 BDSG-neu.
[88] Vgl. § 1 IV S. 2 Nr. 2 BDSG-neu.
[89] Vgl. § 1 IV S. 2 Nr. 3 BDSG-neu.
[90] Vgl. Thomas Jäschke et al. 2018, S. 34.
[91] Vgl. Erwägungsgrund Nr. 27 der DSGVO.
[92] Vgl. Art. 4 Nr. 2 DSGVO.

Normadressaten der DSGVO: Verantwortlicher und Auftragsverarbeiter (Art. 4 Nr. 7, 8 DSGVO)

Verantwortliche sind alle juristischen und natürlichen Personen sowie Behörden und alle sonstigen Stellen, die über die Zwecke und Mittel einer Verarbeitung entscheiden.[93] Darunter fallen sowohl freiberufliche Ärzte als auch Krankenkassen oder Therapieeinrichtungen. Auftragsverarbeiter zeichnen sich gem. Art. 4 Nr. 8 DSGVO dadurch aus, dass sie im Auftrag eines Verantwortlichen Datenverarbeitungen durchführen. Dies trifft bspw. zu, wenn ein Arzt bestimmte datenverarbeitende Aufgaben nicht selbst, sondern durch einen Dritten durchführen lässt, z.B. bei Inkassoangelegenheiten. Das Inkassounternehmen handelt als Auftragsverarbeiter, wenn es die Daten unselbständig, d.h. nur im vereinbarten Umfang verarbeitet.[94] Aber auch die Entsorgung und Vernichtung von Patientenakten oder die Wartung der Praxiscomputer durch Dritte werden im Gesundheitsbereich häufig ausgelagert, wodurch der Tatbestand einer Auftragsverarbeitung erfüllt wird.[95] Die Konstellation der Auftragsverarbeitung wird im Kapitel 2.2.1.4 dieser Arbeit vertieft. Insbesondere bei Praxisgemeinschaften kann, wenn die Zwecke und Mittel der Datenverarbeitung gemeinsam festgelegt werden, ein Fall der gemeinsamen Verantwortlichkeit gem. Art. 26 DSGVO vorliegen. Eine gemeinsame Verantwortlichkeit liegt regelmäßig vor, wenn sich die zusammengeschlossenen Ärzte nicht nur die Praxisräume und das Praxispersonal miteinander teilen, sondern auch gemeinsam Daten verarbeiten, etwa durch eine gemeinschaftliche elektronische Verwaltung der Patientendaten.[96]

Besondere Datenkategorie: Gesundheitsdaten (Art. 4 Nr. 15 DSGVO)

Unter dem Begriff der Gesundheitsdaten sind alle personenbezogenen Daten zu verstehen, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen. Dies umfasst sämtliche Daten, die Aufschluss über den gesundheitlichen Zustand einer Person geben oder im Rahmen von Gesundheitsdienstleistungen erhoben werden.[97] Darunter zu subsumieren sind insbesondere Patientendaten, welche im Gesundheitswesen regelmäßig verarbeitet werden.[98] Gesundheitsdaten sind gem. Art. 9 DSGVO als sogenannte besondere Kategorie personenbezogener Daten speziell geschützt und die Verarbeitung nur in besonderen Fällen oder bei ausdrücklicher Einwilligung der betroffenen Person zulässig.[99] E-Health-relevante Rechtsgrundlagen für die Verarbeitung dieser Daten sind etwa ein Behandlungsvertrag, eine gesetzliche Befugnis zur Datenverarbeitung oder die Einwilligung des Patienten.[100]

Daneben existieren im Artikel 4 der DSGVO weitere Begriffsbestimmungen, die jedoch zum Verständnis dieser Arbeit nicht von größerem Belang sind und daher nicht erörtert werden. Nachfolgend werden die Grundsätze der Datenverarbeitung dargestellt. Diese Grundsätze für eine rechtskonforme Datenverarbeitung sind im Artikel 5 der DSGVO festgelegt. Sie müssen bei jeder Verarbeitung umgesetzt und eingehalten werden und sind daher das rechtliche Fundament einer jeden Datenverarbeitung. Nach Art. 5 I lit. a DSG-

[93] Vgl. Art. 4 Nr. 7 DSGVO.
[94] Vgl. Andreas Böhm 2019.
[95] Vgl. Thomas Jäschke et al. 2018, S. 184.
[96] Vgl. Die Landesbeauftragte für den Datenschutz Niedersachsen 2019, Nr. 6.
[97] Vgl. Art. 4 Nr. 15 DSGVO.
[98] Vgl. Erwägungsgrund Nr. 35 der DSGVO.
[99] Vgl. Erwägungsgrund Nr. 51 der DSGVO.
[100] Vgl. Die Landesbeauftragte für den Datenschutz Niedersachsen 2019, Nr. 1.

VO muss die Datenverarbeitung die Prinzipien der „Rechtmäßigkeit“, der „Verarbeitung nach Treu und Glauben“ und der „Transparenz“ einhalten. Während „Treu und Glauben“ ein in der DSGVO nicht weiter bestimmter Begriff ist, werden im Folgenden unter anderem die Grundsätze der „Rechtmäßigkeit“ und der „Transparenz“ anhand ihrer Rechtsnormen erörtert.

Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DSGVO)

Rechtmäßigkeit (Art. 5 I lit. a DSGVO)

Zur Rechtmäßigkeit muss die Verarbeitung die Bedingungen von mindestens einer der Rechtsgrundlagen aus Art. 6 DSGVO „Rechtmäßigkeit der Datenverarbeitung“ erfüllen.[101] In dieser Norm wird deutlich, dass es sich bei der DSGVO um ein generelles Verarbeitungsverbot mit Erlaubnisvorbehalt handelt. Demnach ist jede Datenverarbeitung illegitim, wenn sie nicht explizit per Gesetz erlaubt wird. Im Art. 6 DSGVO wird zwischen sechs Erlaubnistatbeständen unterschieden: Einwilligung[102], Vertragserfüllung und vorvertragliche Maßnahmen[103], rechtliche Verpflichtung[104], lebenswichtige Maßnahmen[105], öffentliches Interesse und öffentliche Gewalt[106] sowie berechtigtes Interesse[107]. Nur, wenn auf die infragestehende Datenverarbeitung mindestens einer dieser Rechtfertigungsgründe mitsamt seiner Voraussetzungen zutrifft, ist die Datenverarbeitung rechtmäßig und das Prinzip der Rechtmäßigkeit erfüllt. Bei der Verarbeitung von Gesundheitsdaten sowie anderer sensibler Daten ist aufgrund der höheren Schutzbedürftigkeit zusätzlich noch das Vorliegen eines besonderen Erlaubnistatbestands aus den Art. 9 II lit. a – i DSGVO notwendig.[108]

Transparenz (Art. 5 I lit. a DSGVO)

Ein weiterer Grundsatz des Art. 5 I lit. a DSGVO ist die Nachvollziehbarkeit der Datenverarbeitung für die betroffene Person. Nur bei Verarbeitungstransparenz kann die Person prüfen, ob die Verarbeitung ihrer Daten rechtmäßig erfolgt und gegebenenfalls von ihren Betroffenenrechten, die im Folgekapitel näher betrachtet werden, Gebrauch machen. Transparenz bedeutet, dass die Informationen zur Datenverarbeitung „präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache“[109] zur Verfügung gestellt werden. Darüber hinaus muss dem Betroffenen ein Überblick über die Verarbeitungsweisen der erhobenen personenbezogenen Daten und den Umfang der Datenverarbeitung ermöglicht werden.[110] Die einzelnen Informationspflichten sind in den Art. 12 – 14 DSGVO kodifiziert und sind sowohl bei Direkterhebung[111] (direkt bei dem Betroffenen) als auch bei Dritterhebung[112] (von bereits durch Dritte erhobenen Daten) sicherzustellen.[113]

---

[101] Vgl. Art. 6 I S. 1 DSGVO.
[102] Vgl. Art. 6 I lit. a DSGVO.
[103] Vgl. Art. 6 I lit. b DSGVO.
[104] Vgl. Art. 6 I lit. c DSGVO.
[105] Vgl. Art. 6 I lit. d DSGVO.
[106] Vgl. Art. 6 I lit. e DSGVO.
[107] Vgl. Art. 6 I lit. f DSGVO.
[108] Vgl. Thomas Jäschke et al. 2018, S. 40.
[109] Erwägungsgrund Nr. 58 der DSGVO, Satz 1.
[110] Vgl. Erwägungsgrund Nr. 39 der DSGVO, Satz 2.
[111] Vgl. Art. 13 DSGVO.
[112] Vgl. Art. 14 DSGVO.
[113] Vgl. Thomas Jäschke et al. 2018, S. 43 f.

Ab der nächsten Seite werden weitere Grundsätze für die Verarbeitung personenbezogener Daten außerhalb des Art. 5 I lit. a DSGVO vorgestellt. Dies sind die Grundsätze der „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“. „Integrität und Vertraulichkeit“[114] sowie der „Rechenschaftspflicht“.[115]

Zweckbindung (Art. 5 I lit. b DSGVO)

Die Datenverarbeitung ist nur zu dem Zweck zulässig, für den eine Einwilligung nach Art. 6 I lit. a DSGVO erteilt wurde oder mit dem ein sonstiger Erlaubnistatbestand gem. Art. 6 I lit. b – f DSGVO begründet werden kann. Der Zweck bzw. die Zwecke müssen im Voraus festgelegt werden, sowie eindeutig und legitim sein. Eine Datenverarbeitung ist mithin nur zulässig, wenn sie in Anbetracht des jeweiligen Zwecks erforderlich und angemessen ist.[116] Eine Lockerung der Zweckbindung kommt unter anderem in Betracht, wenn die über den Zweck hinausgehende Verarbeitung für wissenschaftliche Forschung oder aus statistischen Gründen erfolgt.[117]

Datenminimierung, Speicherbegrenzung (Art. 5 I lit. c, lit. e DSGVO)

Die Datenverarbeitung darf nach Art. 5 I lit. c DSGVO nicht über das für den konkreten Zweck unbedingt notwendige Maß hinausgehen. Es gelten die Grundsätze der Datensparsamkeit und Datenvermeidung. So sollen personenbezogene Daten, wenn dies mit dem Zweck der Datenvereinbarung zu vereinbaren ist, möglichst anonymisiert und bei fehlender Notwendigkeit gelöscht bzw. gar nicht erst erhoben werden. Hier kommen bspw. Löschfristen des Verantwortlichen zum Tragen, die die Zeitspanne festlegen, nach der gespeicherte personenbezogene Daten gelöscht werden müssen.[118,119] Die Speicherbegrenzung gem. Art. 5 I lit. e DSGVO sieht vor, dass der Personenbezug in Daten nur so lange gegeben sein darf, wie er für die zweckgebundene Verarbeitung benötigt wird. Sobald die personenbezogenen Daten für den Zweck nicht mehr erforderlich sind, ist der Datensatz zu anonymisieren bzw. zu vernichten.[120]

Richtigkeit (Art. 5 I lit. d DSGVO)

Die erhobenen Daten müssen bezogen auf ihren Verarbeitungszweck sachlich richtig und möglichst auf dem aktuellsten Stand sein.[121] Der Grundsatz der Richtigkeit ist im Erwägungsgrund Nr. 39 der DSGVO weiter ausgeführt und besagt insbesondere, dass unrichtige bzw. falsche Daten unverzüglich gelöscht oder berichtigt werden müssen.[122]

Integrität und Vertraulichkeit (Art. 5 I lit. f DSGVO)

Das Prinzip der Integrität und Vertraulichkeit bezieht sich auf die Datensicherheit. Die Verarbeiter der Daten müssen stets technische und organisatorische Maßnahmen (TOMs) treffen, die sicherstellen, dass die Daten vor unerlaubter Verarbeitung sowie vor

[114] Vgl. Art. 5 I lit. b – f DSGVO.
[115] Vgl. Art. 5 II DSGVO.
[116] Vgl. Thomas Jäschke et al. 2018, S. 44.
[117] Vgl. Art. 5 I lit. b DSGVO, letzter Halbsatz.
[118] Vgl. Thomas Jäschke et al. 2018, S. 45.
[119] Vgl. Erwägungsgrund Nr. 39 der DSGVO, Satz 7 – 10.
[120] Vgl. Thomas Jäschke et al. 2018, S. 46.
[121] Vgl. Art. 5 I lit. d DSGVO.
[122] Vgl. Erwägungsgrund Nr. 39 der DSGVO, Satz 11.

unbeabsichtigter Vernichtung geschützt sind.[123] Vor unbeabsichtigter Vernichtung der Datensätze schützt bspw. die regelmäßige Erstellung von Sicherungskopien. Zur Integrität und Vertraulichkeit gehört auch, dass mit Hilfe von angemessenen Sicherheitsvorkehrungen auf dem aktuellen Stand der Technik unbefugter Zugriff auf personenbezogene Daten unterbunden wird, etwa durch Verschlüsselung der webbasierten Kommunikation und ein passwortgeschütztes Verwaltungssystem.[124,125]

Rechenschaftspflicht (Art. 5 II DSGVO)

Dieser Grundsatz bestimmt, dass der Verantwortliche die Verantwortung darüber trägt, dass er die zuvor erläuterten Prinzipien (Rechtsmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit) nachweisbar einhält.[126] Dies muss der Verantwortliche durch geeignete und nachprüfbare Maßnahmen sicherstellen können.[127] Die Rechenschaftspflicht schließt mit ein, dass der Verantwortliche bei Verstößen gegen diese Prinzipien grundsätzlich einer Meldepflicht an die zuständige Aufsichtsbehörde unterliegt, außer er kann im Rahmen seiner Rechenschaftspflicht nachweisen, dass die Datenschutzverletzung nicht zu einem Rechts- bzw. Freiheitsrisiko der betroffenen natürlichen Personen führt.[128]

2.2.1.3 Betroffenenrechte

Die DSGVO ist auf den Schutz personenbezogener Daten von betroffenen Personen ausgelegt. Damit die Betroffenen ihre Rechte auch effektiv geltend machen können, sieht die DSGVO in den Art. 15 - 22 DSGVO eine Reihe von Betroffenenrechten vor. Diese enthalten Mitteilungs- und Maßnahmenpflichten, die der Betroffene direkt von dem Verantwortlichen erwirken kann. Bei der Beantwortung von Betroffenenanfragen muss grundsätzlich eine einmonatige Frist zwischen Anfrage und Auskunft gewahrt bleiben.[129] Ihre jeweiligen Betroffenenrechte wahrnehmen können im Gesundheitswesen neben den Patienten auch alle anderen natürlichen Personen, deren personenbezogene Daten verarbeitet werden, wie etwa Ärzte, Pflegepersonal und Verwaltungskräfte.[130] Zu den Betroffenenrechten gehören das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und das Widerspruchsrecht.[131] Nachfolgend werden die eben aufgezählten Betroffenenrechte vertieft behandelt.

Auskunftsrecht des Betroffenen (Art. 15 DSGVO)

Der Verantwortliche ist anfragenden Personen gegenüber verpflichtet mitzuteilen, ob die Person betreffende Daten gespeichert sind bzw. verarbeitet werden. Beim Vorliegen einer Datenverarbeitung hat die betroffene Person ein Recht auf Einsicht in die gespeicherten personenbezogenen Daten sowie das Anrecht auf weitere Informationen. Diese beinhaltet in den Art. 15 I lit. a – h DSGVO unter anderem Auskunft über die Verarbeitungszwecke, Datenkategorien, Datenempfänger, Datenherkunft, Speicherdauer und Herkunft der Daten. Die Form der Datenauskunft kann sowohl schriftlich als auch elektronisch oder münd-

[123] Vgl. Art. 5 I lit. f DSGVO.
[124] Vgl. Erwägungsgrund Nr. 39 der DSGVO, Satz 12.
[125] Vgl. Erwägungsgrund Nr. 83 der DSGVO.
[126] Vgl. Art. 5 II DSGVO.
[127] Vgl. Thomas Jäschke et al. 2018, S. 47.
[128] Vgl. Erwägungsgrund Nr. 85 der DSGVO, Satz 2.
[129] Vgl. Art. 12 III DSGVO.
[130] Vgl. Thomas Jäschke et al. 2018, S. 116.
[131] Vgl. Art. 15 - 22 DSGVO.

lich erfolgen. [132] Jedoch sollte, damit keine Daten an unbefugte Dritte ausgehändigt werden, vor der Auskunftserteilung seitens des Verantwortlichen eine Identitätsprüfung stattfinden.[133,134] Die Auskunft darf gem. Art. 15 IV DSGVO abgelehnt werden, falls durch sie die Rechte und Freiheiten anderer Personen tangiert werden. Dies ist etwa der Fall, wenn die beantragte Auskunft Betriebs- und Geschäftsgeheimnisse oder personenbezogene Daten Dritter enthält.[135] Weitere Ausnahmen sind im § 34 BDSG-neu kodifiziert, wonach etwa bei Gefährdung der öffentlichen Sicherheit[136] oder unangemessenem Aufwand der Auskunftserteilung[137] die Auskunft verweigert werden darf. Der Anspruch auf Auskunft erstreckt sich explizit auch auf gesundheitsbezogene Daten wie Diagnosen, Behandlungsdaten und sonstige Befunde.[138] Das Auskunftsrecht der DSGVO ist von dem im § 630g BGB geregelten Recht zur Einsichtnahme in die Patientenakte zu unterscheiden, welches vom Leistungserbringer nur verweigert werden kann, wenn der vollständigen Einsichtnahme in die Patientenakte erhebliche therapeutische Gründe oder andere Rechte Dritter entgegenstehen.[139]

Die Grenzen des Auskunftsrechts sind gem. Art. 12 V DSGVO, wie bei der missbräuchlichen Inanspruchnahme aller anderen Rechte auch, bei exzessiven und offenkundig unbegründeten Auskunftsanträgen zu finden. Der Missbrauch eines Betroffenenrechts kann zu Ablehnung des Antrags[140] sowie Kostenerstattungsforderungen[141] des Verantwortlichen gegenüber der betroffenen Person führen. Bei einem solchen Fall liegt die Beweispflicht beim Verantwortlichen der Datenverarbeitung.[142]

Recht auf Berichtigung, Löschung und Einschränkung der Verarbeitung (Art. 16 - 18 DSGVO)

Die betroffene Person hat bei Unrichtigkeit sowie bei Unvollständigkeit der sie betreffenden Daten das Recht auf unverzügliche Korrektur bzw. Ergänzung des Datensatzes.[143] Das Recht auf Löschung ist unter den Voraussetzungen des Art. 17 I lit. a – f DSGVO gegeben. Insbesondere bei Zweckerfüllung der Datenverarbeitung sowie Widerruf einer Einwilligung und sonstiger Unrechtmäßigkeit der Verarbeitung ist der Verantwortliche verpflichtet, die diesbezüglichen personenbezogenen Daten zu löschen.[144] Sowohl für das Recht auf Berichtigung als auch für das Recht auf Löschung sieht der Gesetzgeber eine Unverzüglichkeit des Handelns durch den Verantwortlichen vor. Im Recht auf Löschung enthalten ist bei Öffentlichkeitmachung von Daten, etwa durch die Verbreitung im Internet, das Recht auf Vergessenwerden gem. Art. 17 II DSGVO. Beim Recht auf Vergessenwerden ist der Verantwortliche dazu verpflichtet, Anstrengungen zu unternehmen, die zur Entfernung der Daten aus der öffentlichen Sphäre (bspw. Internet-Such-

[132] Vgl. Art. 12 I S. 2 DSGVO.
[133] Vgl. Art. 12 I S. 3 DSGVO.
[134] Vgl. Art. 12 VI DSGVO.
[135] Vgl. Erwägungsgrund Nr. 63 der DSGVO, Satz 5.
[136] Vgl. §§ 34 I Nr. 1, 33 I Nr. 2 lit. b BDSG-neu.
[137] Vgl. § 34 I Nr. 2 BDSG-neu.
[138] Vgl. Erwägungsgrund Nr. 63 der DSGVO, Satz 2.
[139] Vgl. Bundesärztekammer 2018, S. 10, 18.
[140] Vgl. Art. 12 V lit. b DSGVO.
[141] Vgl. Art. 12 V lit. a DSGVO.
[142] Vgl. Art. 12 V S. 3 DSGVO.
[143] Vgl. Art. 16 DSGVO.
[144] Vgl. Art. 17 I DSGVO.

maschinen[145]) führen. Die Schranken des Löschungsrechts sind im Art. 17 III DSGVO bestimmt. Demnach gilt das Recht auf Löschung nicht wenn die Verarbeitung gemäß den Art. 17 III lit. a – e DSGVO notwendig ist. Gründe hierfür sind das Recht auf Meinungs- und Informationsfreiheit, der Löschung entgegenstehende rechtliche Verpflichtungen und Ansprüche sowie das öffentliche Interesse an der Datenverarbeitung. Diese Schranken sind im § 35 BDSG-neu weiter spezifiziert, wonach in bestimmten Fällen eine Interessenabwägung zwischen Betroffenem und Verantwortlichem unternommen werden muss. Diese Interessenabwägung kann dazu führen, dass der Betroffene sein Recht auf Löschung nicht in dem von ihm beantragten Umfang durchsetzen kann.[146] Des Weiteren können auch rechtliche Aufbewahrungsfristen dem Recht auf Löschung entgegenstehen.[147]

Eine abgeschwächte Form des Rechts auf Löschung ist das Recht auf Einschränkung der Verarbeitung. Es kommt zum Tragen, wenn eine unverzügliche Löschung aufgrund schutzwürdiger Interessen des Betroffenen oder des Verantwortlichen nicht möglich ist.[148] Hier ist dem Verantwortlichen der Besitz bzw. die Speicherung der Daten weiterhin erlaubt, jedoch wird er in seinen Verwendungsmöglichkeiten eingeschränkt.[149] Treffen die rechtlichen Voraussetzungen zu, und wird dieses Recht in Anspruch genommen, benötigt jede Verarbeitung die individuelle Einwilligung des Betroffenen. Außerhalb dieser genehmigten Datenverarbeitung ist nur noch eine aus Rechtsansprüchen oder aus einem wichtigen öffentlichen Interesse erwachsene Verarbeitung, sowie die Verarbeitung zum Schutz der Rechte von natürlichen oder juristischen Personen, erlaubt.[150] Der Betroffene hat einen Anspruch auf Einschränkung der Verarbeitung, wenn eine der Bedingungen des Art. 18 I lit. a – d DSGVO zutrifft. Dies ist der Fall, wenn der Betroffene die Richtigkeit der ihn betreffenden Daten bestreitet[151] oder gegen die Datenverarbeitung Widerspruch erhebt[152]. In diesen Fällen muss der Verantwortliche die Datenverarbeitung so lange einschränken, bis der Sachverhalt geklärt ist. Außerdem muss der Verantwortliche die Datenverarbeitung einschränken, wenn der Betroffene die Einschränkung der Verarbeitung einer Löschung vorzieht oder seine Daten zur Wahrung von Rechtsansprüchen benötigt[153]. Der Verantwortliche ist verpflichtet, dem Betroffenen das Ende der eingeschränkten Verarbeitung mitzuteilen, noch bevor er die Einschränkung beendet.[154] Bei der Inanspruchnahme dieser Rechte im Gesundheitsbereich ist jedoch zu beachten, dass bei Diagnosen und Patientenakten die ärztliche Dokumentationspflicht überwiegt. Da gemäß dieser Pflicht der Behandlungsverlauf transparent und nachweisbar dokumentiert werden muss, kommt auch bei vom Patienten bestrittener Richtigkeit der Daten nur eine Aktualisierung des Datensatzes in Betracht, jedoch keine absolute Berichtigung oder Löschung von behandlungsrelevanten Daten.[155]

Sowohl bei der Berichtigung und Löschung als auch bei der Einschränkung der Verarbeitung ist der Verantwortliche gem. Art. 19 DSGVO grundsätzlich verpflichtet, etwaige Emp-

[145] Vgl. Thomas Jäschke et al. 2018, S. 51.
[146] Vgl. § 35 I, II BDSG.
[147] Vgl. § 35 III BDSG.
[148] Vgl. Thomas Jäschke et al. 2018, S. 52.
[149] Vgl. Erwägungsgrund Nr. 67 der DSGVO.
[150] Vgl. Art. 18 II DSGVO.
[151] Vgl. Art. 18 I lit. a DSGVO.
[152] Vgl. Art. 18 I lit. d DSGVO.
[153] Vgl. Art. 18 I lit. b, lit. c DSGVO.
[154] Vgl. Art. 18 III DSGVO.
[155] Vgl. Thomas Jäschke et al. 2018, S. 308 f.

fänger der betreffenden Daten über die Inanspruchnahme des jeweiligen Rechtes zu informieren.[156]

Recht auf Datenübertragbarkeit (Art. 20 DSGVO)

Der Verantwortliche hat dem Betroffenen bei automatisierter Datenverarbeitung die Möglichkeit einzuräumen, seine eigenen personenbezogenen Daten in einem geläufigen und maschinenlesbaren Format zu erhalten.[157] Der Datensatz muss alle Daten enthalten, die der Betroffene selbst bereitgestellt hat und in einer Form vorliegen, die zur Übermittlung an Dritte geeignet ist. Des Weiteren muss der Verantwortliche auf Verlangen des Betroffenen die personenbezogenen Daten auch direkt an Dritte übermitteln.[158] Hintergrund ist, dass der Betroffene so die Kontrolle über seine Daten behält und in die Lage versetzt wird, sich seinen Datenverarbeiter selbst auszusuchen (Stärkung der Datensouveränität).[159] Mit diesem Recht kann ein Patient etwa die Übertragung seiner Behandlungsdaten von einem Arzt zu einem nachbehandelnden Arzt erwirken oder einen Auszug von den in Gesundheitsapps über ihn gespeicherten Daten verlangen.[160] Zur Geltendmachung dieses Rechtes muss die Datenverarbeitung entweder aufgrund einer Einwilligung oder eines Vertragsverhältnisses erfolgt sein.[161] Bei allen anderen Erlaubnistatbeständen und insbesondere bei der Datenverarbeitung aus öffentlichem Interesse sowie bei der Tangierung von Rechten Dritter besteht dieses Recht nicht.[162]

Widerspruchsrecht (Art. 21 DSGVO)

Einer Datenverarbeitung, die ohne Einwilligung des Betroffenen, aber aufgrund eines öffentlichen oder berechtigten Interesse durch den Verantwortlichen erfolgt, kann der Betroffene jederzeit widersprechen.[163] Der Betroffene hat das Widerspruchsrecht nicht, wenn der Verantwortliche die Daten zur Geltendmachung oder Verteidigung von Rechtsansprüchen benötigt oder eine Interessenabwägung zugunsten des Verantwortlichen erfolgt.[164] Gegeben ist das Widerspruchsrecht also nur, wenn die Patienteninteressen überwiegen, nicht aber bei Datenverarbeitungen die auf einer medizinischen Behandlung oder einer expliziten Einwilligung basieren.[165] Bei Datenverarbeitungen zum Zweck des Direktmarketings hat der Betroffene ein uneingeschränktes Widerspruchsrecht, dem der Verantwortliche jederzeit nachkommen muss.[166] Der Betroffene muss bereits beim ersten Kontakt mit dem Verantwortlichen transparent über das ihm zustehende Widerspruchsrecht informiert werden.[167]

2.2.1.4 Verantwortliche und Auftragsverarbeiter

Die in Kapitel 2.2.1.2 dieser Arbeit definierten Normadressaten der DSGVO unterliegen weiteren datenschutzrechtlichen Pflichten, die über die Grundsätze der Datenverarbeitung

[156] Vgl. Art. 19 S. 1 DSGVO.
[157] Vgl. Art. 20 I DSGVO.
[158] Vgl. Erwägungsgrund Nr. 68 der DSGVO.
[159] Vgl. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2016, S. 14 f.
[160] Vgl. Bundesärztekammer 2018, S. 11.
[161] Vgl. Art. 20 I lit. a DSGVO.
[162] Vgl. Art. 20 II S. 2, IV DSGVO.
[163] Vgl. Erwägungsgrund Nr. 69 der DSGVO, Satz 1.
[164] Vgl. Art. 21 I DSGVO.
[165] Vgl. Thomas Jäschke et al. 2018, S. 309.
[166] Vgl. Art. 21 II, III DSGVO.
[167] Vgl. Art. 21 IV DSGVO.

und die Verpflichtungen der Betroffenenrechte hinausgehen. So sind sowohl Verantwortliche als auch Auftragsverarbeiter regelmäßig dazu verpflichtet, eine Datenschutz-Folgenabschätzung[168] (DSFA) durchzuführen, einen Datenschutzbeauftragten[169] (DSB) zu bestellen und ein Verzeichnis von Verarbeitungstätigkeiten[170] (VVT) anzulegen. Aufgrund der Praxisrelevanz einer solchen Konstellation (Verantwortlicher und Auftragsverarbeiter) werden zunächst die rechtlichen und praktischen Rahmenbedingungen einer Auftragsverarbeitung erörtert. Anschließend werden die einzelnen Rechtsinstrumente und -bestandteile (TOMs, VVT, DSFA, DSB) dargestellt.

Auftragsverarbeitung (Art. 28 ff. DSGVO)

Bei einer Auftragsverarbeitung findet eine Auslagerung der Datenverarbeitung durch den Verantwortlichen an Dritte statt (siehe Kapitel 2.2.1.2 „Normadressaten der DSGVO“). Die primäre Verantwortlichkeit zur Einhaltung der datenschutzrechtlichen Vorgaben liegt hier beim Verantwortlichen als Auftraggeber. Der Auftragsverarbeiter trägt als Auftragnehmer eine Mitverantwortung und unterliegt eigenen datenschutzrechtlichen Pflichten. Der Hintergrund einer solchen Datenübermittlung ist, dass der Verantwortliche nicht in jedem Fall eine Datenverarbeitung durchführen kann oder will. Die Durchführung einer Auftragsverarbeitung ist regelmäßig wirtschaftlich sinnvoll, da hierdurch Kosten gespart und datenverarbeitende Prozesse effektiver durchgeführt werden können.[171] Jedoch unterliegt gerade die Datenverarbeitung im Gesundheitsbereich sehr strengen Legitimierungsvoraussetzungen. Bei der Übermittlung von Gesundheitsdaten müssen nicht nur die Voraussetzungen eines Erlaubnistatbestandes gem. Art. 6 DSGVO erfüllt, sondern auch eine Ausnahme des Verarbeitungsverbots nach Art. 9 II DSGVO gegeben sein. In der Praxis bedeutet dies, dass ein Arzt, der veraltete Patientenakten durch ein Entsorgungsunternehmen vernichten lassen möchte[172] oder mit ärztlichen Verrechnungsstellen seine Verwaltung entlastet[173], hierfür auf die Einwilligung der Betroffenen oder eben eine andere gesetzliche Grundlage angewiesen ist. Bei dieser Problematik entfaltet die Auftragsverarbeitung nach Art. 28 ff. DSGVO ihre Wirkung. Sie vereinfacht das datenschutzrechtliche Prozedere insoweit, dass als gesetzliche Legitimationsgrundlage für die Datenübermittlung sowie das Tätigwerden des Dritten ein schriftlicher Auftragsverarbeitungsvertrag (AV-Vertrag) datenschutzrechtlich ausreichend ist. Der Vertragsinhalt muss sich an den im Art. 28 III DSGVO vorgesehenen Mindestanforderungen orientieren und von beiden Vertragspartnern strikt eingehalten werden.[174] Sobald eine begründete Auftragsverarbeitung vorliegt, ist zur Datenweitergabe kein Erlaubnistatbestand der Art. 6, 9 DSGVO mehr notwendig, da der auftragsverarbeitende Datenempfänger im Sinne des Gesetzes nicht als befugter Dritter[175], sondern vielmehr als der „verlängerte Arm“[176] des Verantwortlichen tätig wird. Die Zusammenarbeit zwischen Verantwortlichen und Auftragsverarbeitern wird insofern von der DSGVO privilegiert, dass sie bezüglich der Datenverarbeitung als rechtliche Einheit gewertet werden.[177] Doch nicht jede Datenübermittlung ist eine Auftragsverar-

[168] Vgl. Art. 35 DSGVO.
[169] Vgl. Art. 37 DSGVO.
[170] Vgl. Art. 30 DSGVO.
[171] Vgl. Thomas Jäschke et al. 2018, S. 182.
[172] Vgl. Thomas Jäschke et al. 2018, S. 194.
[173] Vgl. Bayerisches Landesamt für Datenschutzaufsicht 2018, S. 1.
[174] Vgl. Thomas Jäschke et al. 2018, S. 182–188.
[175] Vgl. Art. 4 Nr. 10 DSGVO.
[176] Vgl. Axel von Walter et al. 2018, S. 188.
[177] Vgl. Der Bayerische Landesbeauftragte für den Datenschutz 2019, S. 7.

beitung. Eine Auftragsverarbeitung liegt nur vor, wenn die Verarbeitung personenbezogener Daten der Schwerpunkt des Auftrags ist und der Verantwortliche allein über die Zwecke und Mittel der Datenverarbeitung bestimmt. Außerdem darf der Beauftragte außerhalb der ihm aufgetragenen Aufgaben kein eigenes Interesse an den übermittelten Daten haben und ausschließlich eine (technische) Hilfs- oder Unterstützungsfunktion für den Verantwortlichen ausführen.[178] Die Auftragsverarbeitung ist zu anderen Konstellationen der Datenübermittlung abzugrenzen, bei denen es regelmäßig zu einer eigenen Verantwortlichkeit des Dritten kommt. Beispielhaft für eine eigene Verantwortlichkeit ist bspw. die Tätigkeit von Steuerberatern und Rechtsanwälten.[179] Außerdem liegt keine Auftragsverarbeitung nach Art. 28 DSGVO vor, wenn die Verarbeitung personenbezogener Daten nicht Kern des Auftrags ist, sondern nur beiläufig geschieht, wie etwa bei der Beauftragung von Handwerkern oder bei Reinigungsdienstleistungen.[180] Der Auftragsverarbeiter ist mithin weisungsgebundener[181] Vertragspartner des Verantwortlichen, der Duldungs- und Mitwirkungspflichten bei Kontrollen durch den Auftraggeber unterliegt[182] und bei Beendigung des Vertragsverhältnisses die Daten zurückzugeben bzw. zu vernichten hat[183]. Der Verantwortliche prüft nachweisbar die Rechtmäßigkeit der Datenverarbeitung[184], ist Ansprechpartner für die Betroffenenrechte[185], trägt primär das Haftungsrisiko[186] und bleibt alleiniger „Herr der Daten“[187].

Technische und organisatorische Maßnahmen (Art. 25, 32 DSGVO)

Die DSGVO greift das rechtliche Konstrukt der TOMs mehrmals auf.[188] Sie dienen vor allem der Umsetzung der Datenschutzgrundsätze, der Durchsetzung der Betroffenenrechte[189] und der Gewährleistung der Verarbeitungssicherheit[190]. Hierbei müssen die gesetzlich bestimmten Parameter berücksichtigt werden. Diese sind der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die Risiken für die die Rechte und Freiheiten natürlicher Personen. Wie die meisten Auflagen der DSGVO richten sich auch die TOMs in erster Linie an den Verantwortlichen der Datenverarbeitung.[191] So sollte dieser gemäß dem Erwägungsgrund Nr. 78 der DSGVO *„interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun.“*[192]. Dennoch ist bei der Implementierung von TOMs auch der Auftragsverarbeiter Normadressat, wie die nachstehende Tabelle aufzeigt.

[178] Vgl. Bitkom e.V. et al. 2017, S. 17 f.
[179] Vgl. Bayerisches Landesamt für Datenschutzaufsicht 2018, S. 2.
[180] Vgl. Bayerisches Landesamt für Datenschutzaufsicht 2018, S. 3.
[181] Vgl. Art. 28 III lit. a DSGVO.
[182] Vgl. Art. 28 III lit. h DSGVO.
[183] Vgl. Art. 28 III lit. g DSGVO.
[184] Vgl. Der Bayerische Landesbeauftragte für den Datenschutz 2019, S. 11.
[185] Vgl. Der Bayerische Landesbeauftragte für den Datenschutz 2019, S. 11.
[186] Vgl. Der Bayerische Landesbeauftragte für den Datenschutz 2019, S. 23.
[187] Axel von Walter et al. 2018, S. 188.
[188] Vgl. Art. 5 I it. f, 24, 25, 32 DSGVO.
[189] Vgl. Art. 25 I DSGVO.
[190] Vgl. Art. 32 I DSGVO.
[191] Vgl. Art. 25 I, 32 I DSGVO.
[192] Erwägungsgrund Nr. 78 der DSGVO, Satz 2.

Implementierung von TOMs	Verantwortlicher	Verarbeiter
Nach Art. 24 DSGVO *„um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“*	X	
Nach Art. 25 DSGVO *„um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“*	X	
Nach Art. 32 DSGVO *„um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“*	X	X
Nach § 64 BDSG-neu *„um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten“*	X	X

Sowohl der Verantwortliche als auch der Auftragsverarbeiter haben die Sicherheit jeder Datenverarbeitung zu gewährleisten, indem sie risikoabhängig und unter Beachtung der Empfehlungen und Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), technische und organisatorische Maßnahmen implementieren.[193] Im § 64 BDSG-neu, der dem Anhang I dieser Arbeit zu entnehmen ist, sind die zu unternehmenden Maßnahmen spezifiziert und erläutert. Der Verantwortliche darf nur mit Auftragsverarbeitern zusammenarbeiten, die hinreichende Garantien dafür bieten, dass sie rechtskonforme TOMs in ihrer Datenverarbeitung etabliert haben.[194] Hierfür sieht der AV-Mustervertrag der Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ eine vertragliche Garantie zur Umsetzung der TOMs und einen gesonderten Vertragsanhang vor, in dem der Auftragsverarbeiter die von ihm umgesetzten TOMs beschreibt und bestätigt.[195,196]

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

Auftragsverarbeiter und Verantwortliche sind dazu verpflichtet, ein VVT zu führen.[197] Dieses Verzeichnis dient dem Nachweis der DSGVO-Compliance und ist bei Verlangen der zuständigen Aufsichtsbehörde vorzulegen.[198],[199] Der Inhalt besteht zum einen aus allgemeinen Informationen, wie den Kontaktdaten des Verantwortlichen bzw. des Auftragsverarbeiters sowie von deren Vertreter und des zuständigen Datenschutzbeauftragten.[200] Zum anderen müssen für jede Verarbeitungstätigkeit individuelle Informationen bereitgestellt werden. Der Verantwortliche hat in seinem Verfahrungsverzeichnis den Zweck der Verarbeitung, die Kategorien der betroffenen Personen, personenbezogenen Daten sowie

[193] Vgl. § 64 I, II BDSG-neu.
[194] Vgl. Art. 28 I DSGVO.
[195] Vgl. Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie et al. 2018, S. 52.
[196] Vgl. Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie et al. 2018, S. 55.
[197] Vgl. Art. 30 I, II DSGVO.
[198] Vgl. Erwägungsgrund Nr. 82 der DSSGVO.
[199] Vgl. Art. 30 IV DSGVO.
[200] Vgl. Art. 30 I lit. a DSGVO.

den Empfänger, etwaige Datenübermittlungen an Drittländer oder internationale Organisationen, Löschfristen und eine Beschreibung der ergriffenen TOMs darzulegen.[201] Der Auftragsverarbeiter führt ein VVT mit reduzierten individuellen Inhaltsvorgaben, in dem die Kategorien der beauftragten Datenverarbeitungen, etwaige Datenübermittlungen an Drittländer oder internationale Organisationen sowie eine Beschreibung der ergriffenen TOMs enthalten sind.[202] Das VVT ist nach Maßgabe des Art. 30 III DSGVO schriftlich zu führen. Diese schriftliche Führung ist auch unter der Verwendung elektronischer Medien möglich.[203] Von der Pflicht zum Führen eines VVT ausgenommen sind, bei nur gelegentlicher Datenverarbeitung und nach einer Risikoabwägung, Organisationen mit weniger als 250 Mitarbeitern, die keine sensiblen Daten verarbeiten.[204] Diese Ausnahme betrifft Unternehmen und Institutionen in der Gesundheitsbranche nicht, da schon die dort verarbeiteten Gesundheitsdaten als besondere Datenkategorie besonders schützenswert sind.[205] Mithin sind Unternehmen im E-Health-Bereich zur Führung eines VVT verpflichtet, da diese regelmäßig sensible Daten (Gesundheitsdaten bzw. Patientendaten) verarbeiten.[206]

Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Verantwortliche haben gem. Art. 35 I DSGVO i.V.m. § 67 BDSG-neu bei bestimmten, besonders sensiblen Datenverarbeitungsvorgängen eine DSFA vorzunehmen. Dieses Rechenschaftsinstrument kommt zum Einsatz, wenn die Wahrscheinlichkeit gegeben ist, dass die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“[207] mit sich bringt.[208] Grundlage für eine DSFA ist zunächst die Identifizierung und Katalogisierung der einzelnen Verarbeitungsvorgänge. Hierfür dient im Idealfall das bereits in dieser Arbeit behandelte VVT.[209] Mit den dort beschriebenen Datenverarbeitungsvorgängen kann der Verantwortliche prüfen, ob die in Frage stehende Verarbeitungstätigkeit in einer der gem. Art. 35 IV DSGVO von Aufsichtsbehörden veröffentlichten Blacklists behandelt wird. Kommt der Verarbeitungsvorgang auf einer solchen Blacklist vor, ist der Verantwortliche verpflichtet eine DSFA durchzuführen. Hilfreich können auch die Whitelists der Aufsichtsbehörden gem. Art. 35 V DSGVO sein, die die Verarbeitungsvorgänge auflisten, für die keine DSFA erforderlich ist.[210] Falls diese Listenkontrolle nicht den erhofften Aufschluss bringt, hat der Verantwortliche die Erforderlichkeit einer DSFA anhand der Kriterien des Art. 35 III lit. a – c DSGVO zu prüfen. Unter diese Kriterien fallen bspw. die Videoüberwachung öffentlich zugänglicher Bereiche oder eine umfangreiche Verarbeitung von Gesundheitsdaten sowie die Nutzung neuartiger Technologien, aber auch andere Verarbeitungsvorgänge mit einem ähnlichen Risikopotential.[211] Von einer Relevanz der DSFA im E-Health-Bereich ist aufgrund der dort immanenten Datensensibilität grundsätzlich auszugehen.[212] Die Datenschutzkonferenz[213] benennt den Einsatz von

[201] Vgl. Art. 30 I lit. b – g DSGVO.
[202] Vgl. Art. 30 II lit. a – d DSGVO.
[203] Vgl. Art. 30 III DSGVO.
[204] Vgl. Art. 30 V DSGVO.
[205] Vgl. Art. 9 I DSGVO.
[206] Vgl. Thomas Jäschke et al. 2018, S. 320 f.
[207] Art. 35 I S. 1 DSGVO.
[208] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017b, S. 4.
[209] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017b, S. 14.
[210] Vgl. Thomas Jäschke et al. 2018, S. 312 f.
[211] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017b, S. 8 - 12.
[212] Vgl. Thomas Jäschke et al. 2018, S. 98.

Telemedizin als konkretes Beispiel für die Verpflichtung zu einer DSFA.[214] Bei der Durchführung einer DSFA wird das Verarbeitungsrisiko analysiert und die Folgen anhand der Eintrittswahrscheinlichkeiten und Schwere bewertet. Hierfür werden unter anderem die Verarbeitungsinteressen des Verantwortlichen sowie die Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung betrachtet.[215] Nachdem die Risikoquellen feststehen, werden Gegenmaßnahmen zur Risikominimierung festgelegt.[216] Diese Maßnahmen müssen als Unternehmensprozesse implementiert, sichergestellt und dokumentiert werden.[217] Kommt die DSFA zum Ergebnis, dass die Verarbeitung zwar notwendig, jedoch mit einem hohen Restrisiko behaftet ist, das nicht durch die Implementierung von Gegenmaßnahmen beherrscht werden kann, hat der Verantwortliche die zuständige Aufsichtsbehörde zu konsultieren.[218,219]

Datenschutzbeauftragter (Art. 37 DSGVO)

Die DSGVO sieht die Benennung eines DSB sowohl durch Verantwortliche und Auftragsverarbeiter dann vor, wenn eine der Voraussetzungen des Art. 37 I lit. a - h DSGVO gegeben ist. Außerdem hat der deutsche Gesetzgeber im § 38 BDSG-neu die Pflicht einen DSB zu bestellen insoweit ergänzt, dass alle verarbeitenden Stellen, die mehr als 20 Mitarbeiter mit der automatisierten Datenverarbeitung betraut haben oder deren Verarbeitungen einer DSFA nach Art. 35 DSGVO bedürfen, dieser Pflicht unterliegen. Da die computergestützte Datenverarbeitung generell und auch Excel-Listen bereits als automatisierte Datenverarbeitung zu werten sind, besteht die DSB-Benennungspflicht praktisch für alle Unternehmen und Institutionen des Gesundheitswesens mit mehr als 20 Mitarbeitern. Als Mitarbeiter sind hier alle Personen zu verstehen, die mit der Datenverarbeitung befasst sind, unabhängig des jeweiligen Angestelltenverhältnisses oder der Position im Unternehmen.[220] Doch auch ungeachtet dieser Spezifizierung im BDSG-neu sieht der Art. 37 I lit. c DSGVO vor, dass alle Stellen, die als Kerntätigkeit eine umfangreiche Verarbeitung von sensiblen Daten gem. Art. 9 DSGVO vornehmen, zur Benennung eines DSB verpflichtet sind. Die Verarbeitung sensibler Daten findet im Gesundheitsbereich ständig statt. Bezüglich des Begriffes der „Kerntätigkeit“ und der „umfangreichen Verarbeitung“ stellt der europäische Datenschutzausschuss in seiner Leitlinie zum DSB klar, dass eine solche datenverarbeitende Kerntätigkeit vorliegt, wenn ein Krankenhaus zur medizinischen Versorgung auf die Verwendung von Patientenakten angewiesen ist[221] und eine umfangreiche Verarbeitung bereits im gewöhnlichen Krankenhausbetrieb stattfindet.[222] Mithin liegt bei größeren Institutionen des Gesundheitswesens wie Krankenhäusern und Pflegeeinrichtungen die Pflicht zur Bestellung eines DSB zweifelsfrei vor. Keine umfangreiche Datenverarbeitung ist hingegen bei der Tätigkeit eines einzelnen Arztes bzw. einer anderen in der Gesundheitsbranche tätigen Einzelperson

---

[213] Anmerkung des Autors: Die Datenschutzkonferenz ist das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder.
[214] Vgl. Datenschutzkonferenz 2018, S. 4.
[215] Vgl. Art. 35 VII lit. a, b DSGVO.
[216] Vgl. Erwägungsgrund Nr. 84 der DSGVO, Satz 2.
[217] Vgl. Thomas Jäschke et al. 2018, S. 314 f.
[218] Vgl. Art. 36 DSGVO.
[219] Vgl. Erwägungsgrund Nr. 84 der DSGVO, Satz 3.
[220] Vgl. Thomas Jäschke et al. 2018, S. 88.
[221] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017a, S. 8.
[222] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017a, S. 9.

gegeben.[223] Solange in der Arztpraxis eines selbständigen Arztes also weniger als 20 Mitarbeiter tätig sind, ist er von der DSB-Benennungspflicht grundsätzlich befreit.[224] Der DSB muss für seine Aufgabe beruflich qualifiziert sein und dementsprechendes Fachwissen vorweisen können.[225] Die Mindestaufgaben des DSB sind im Art. 39 DSGVO bestimmt. Demnach ist er sowohl für die Überwachung der DSGVO-Compliance[226], als auch für die datenschutzrechtliche Unterrichtung und Beratung im Unternehmen allgemein[227] und als Ansprechpartner für Aufsichtsbehörden[228] und Betroffene[229] zuständig. Zu seinem Aufgabenbereich gehört neben der innerbetrieblichen Selbstkontrolle auch die Beratung bezüglich der Umsetzung von einzelnen Instrumenten der DSGVO, wie bspw. der oben beschriebenen DSFA.[230] Der DSB ist im Rahmen seiner Tätigkeit nicht weisungsgebunden[231] und kann entweder Mitarbeiter oder externer Dienstleister des Unternehmens sein.[232] Sofern keine Interessenkonflikte seine Arbeit als DSB behindern, spielt es keine Rolle, ob er auch in anderen Abteilungen arbeitet oder für dritte Unternehmen tätig ist.[233] Aufgrund der gesetzlich auferlegten Vermeidung von Interessenkonflikten können aber weder der Vorstand noch hohe Managementpositionen wie die Leiter von Personal-, Rechts- oder IT-Abteilung oder der geschäftsleitende Arzt die Stellung des DSB im jeweiligen Unternehmen einnehmen. Hier wäre ein Konflikt zwischen den persönlichen bzw. wirtschaftlichen Zielen und den Datenschutzzielen der DSGVO unvermeidbar.[234] Zusätzlich sollte ein DSB im Gesundheitsbereich, aufgrund der Sensibilität der Daten und der Variation der Rechtsquellen, dem Aufgabenbereich angemessene datenschutzrechtliche, technische und medizinische Vorkenntnisse besitzen.[235]

[223] Vgl. Erwägungsgrund Nr. 91 der DSGVO, Satz 4.
[224] Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE 2017a, S. 9 f.
[225] Vgl. Art. 37 V DSGVO.
[226] Vgl. Art. 39 I lit. b DSGVO.
[227] Vgl. Art. 39 I lit. a, c DSGVO.
[228] Vgl. Art. 39 I lit. d - e DSGVO.
[229] Vgl. Art. 38 IV DSGVO.
[230] Vgl. Art. 35 II DSGVO.
[231] Vgl. Art. 38 III DSGVO.
[232] Vgl. Art. 37 VI DSGVO.
[233] Vgl. Art. 38 VI DSGVO.
[234] Vgl. Thomas Jäschke et al. 2018, S. 93.
[235] Vgl. Thomas Jäschke et al. 2018, S. 90 f.

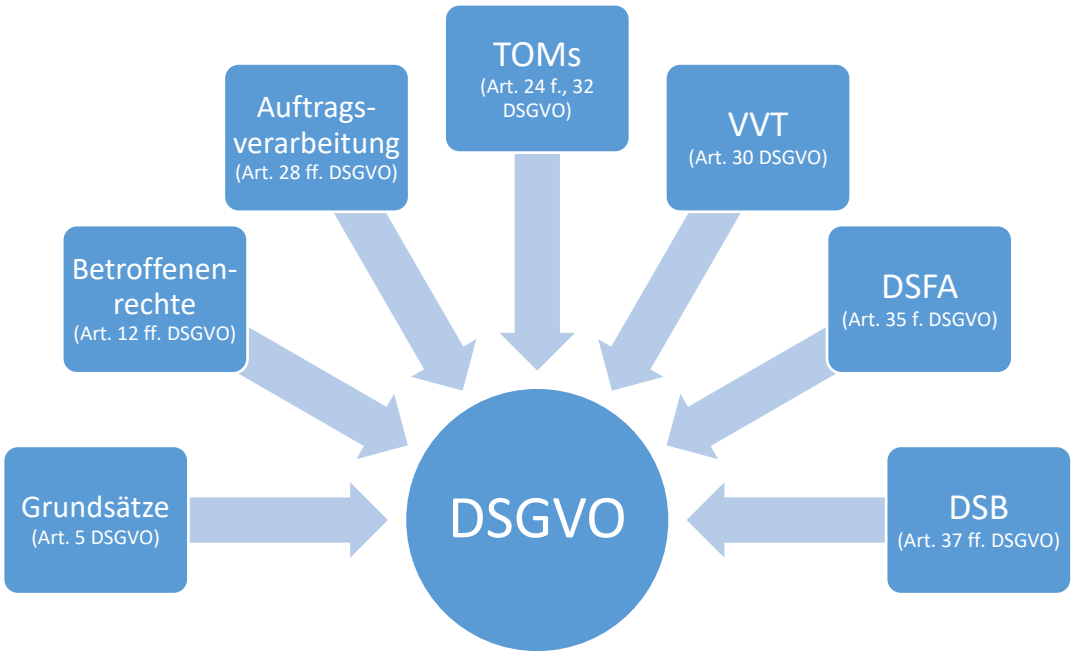

Abbildung 9: Bestandteile und Instrumente der DSGVO

[Quelle: Eigene Abbildung.]

Zur Veranschaulichung der Rechtsbestandteile und -instrumente werden in dieser Abbildung die in den vorangegangenen Unterkapiteln präsentierten Aspekte der DSGVO mitsamt den dazugehörigen Rechtsnormen zusammenfassend dargestellt.

2.2.1.5 Haftung und Sanktionen

Die rechtliche Belangbarkeit bei Nichtbeachtung der gesetzlichen Vorgaben ist im achten Kapitel der DSGVO geregelt. Es drohen erhebliche Bußgelder und Schadenersatzforderungen, die existenzgefährdende Auswirkungen auf die für den Datenschutzverstoß verantwortliche Person bzw. Institution haben können. So ist nach Art. 83 DSGVO die Verhängung eines Bußgeldes in Höhe von bis zu 20 Millionen Euro respektive vier Prozent des weltweiten Jahresumsatzes möglich.[236] Diese Sanktionsmöglichkeit ist für Fälle vorgesehen, in denen Anweisungen von Aufsichtsbehörden missachtet werden[237] oder gegen die Grundsätze der Datenverarbeitung[238], die Betroffenenrechte[239] oder andere Bestandteile[240] der DSGVO verstoßen wird. Ein Bußgeld von maximal 10 Millionen Euro bzw. 2 % des Jahresumsatzes ist fällig, wenn bestimmte gesetzliche Pflichten von Verantwortlichen und Auftragsverarbeitern oder Zertifizierungs- und Überwachungsstellen missachtet werden.[241] Im BDSG-neu sind bei Datenmissbrauch sogar Haftstrafen mit bis zu drei Jahren Freiheitsentzug vorgesehen.[242] Die Geldbußen sollen gemäß der DSGVO

[236] Vgl. Art. 83 V, VI DSGVO.
[237] Vgl. Art. 83 V lit. e, VI DSGVO.
[238] Vgl. Art. 83 V lit. a DSGVO.
[239] Vgl. Art. 83 V lit. b DSGVO.
[240] Vgl. Art. 83 V lit. c – e DSGVO.
[241] Vgl. Art. 83 IV DSGVO.
[242] Vgl. § 42 I, II BDSG-neu.

„wirksam, verhältnismäßig und abschreckend“[243] sein. Sie bemessen sich in einer Einzelfallabwägung anhand verschiedener Kriterien wie Schwere des Verstoßes, betroffene Datenkategorien, Vorsatz bzw. Fahrlässigkeit, etwaige Meldung des Verstoßes an die Aufsichtsbehörde sowie alle anderen erschwerenden oder schuldmildernden Aspekte des Einzelfalls.[244] Da die DSGVO keine Regelungen für das formelle Straf- und Bußgeldverfahren beinhaltet, wird dies national im BDSG-neu geregelt. Demnach gelten bei Verfahren wegen Datenschutzverstößen die allgemeinen Gesetze über Strafverfahren (Strafprozessordnung und Gerichtsverfassungsgesetz).[245] Des Weiteren ist bei Verstößen das Gesetz über Ordnungswidrigkeiten (OWiG) mit den Maßgaben des § 41 BDSG-neu anzuwenden.[246] Daher kann bspw. die Staatsanwaltschaft nur mit Zustimmung der zuständigen Aufsichtsbehörde das Verfahren einstellen.[247] Dass die Verhängung von Bußgeldern auch in der Gesundheitsbranche eine reelle Gefahr ist, hat sich durch mehrere Verfahren in der Vergangenheit bestätigt. Ein deutsches Universitätsklinikum wurde wegen defizitärer TOMs, die zu Patientenverwechslungen und Falschabrechnungen geführt haben, zur Zahlung eines Bußgelds im sechsstelligen Eurobereich verurteilt. Der zuständige Landesdatenschutzbeauftragte begründete das Urteil auch als pädagogische Maßnahme für andere Institutionen des Gesundheitswesens.[248] Neben den Sanktionierungsmöglichkeiten gegen Verantwortliche und Auftragsverarbeiter mit Bußgeldern nach Art. 83 DSGVO und den Geld- und Haftstrafen der § 42 f. BDSG-neu beinhaltet die DSGVO im Art. 82 DSGVO noch eine eigene und unmittelbare Anspruchsgrundlage für Schadenersatz bei Datenschutzverstößen. Anspruchsberechtigt ist jede Person „der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“[249]. Da die DSGVO sich auf den Datenschutz natürlicher Personen bezieht, sind hier nur natürliche Personen aktivlegitimiert. Für einen Schadenersatzanspruch muss eine Kausalität zwischen Rechtsverletzung und Schaden vorliegen.[250] Als Rechtsverletzung kommt jede Nichtbeachtung einer DSGVO-Vorschrift in Betracht. Dazu zählen z.B. die hier bereits behandelnden Verarbeitungsgrundsätze, Betroffenenrechte und TOMs.[251] Ein datenschutzrelevanter Schaden kann aufgrund der in der DSGVO vorgesehenen weiten Auslegung des Begriffs sowohl immateriell als auch materiell sein.[252] Als Beispiele für immaterielle und materielle Schäden werden im Erwägungsgrund 85 folgende Szenarien aufgezählt: *„Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.“*[253]. Da die DSGVO mit Ausnahme der Öffnungsklauseln europaweit einheitlich durchgesetzt wird, ist damit zu rechnen, dass sich die Höhe des Schadenersatzes von der diesbezüglich eher zurückhal-

[243] Art. 83 I DSGVO.
[244] Vgl. Art. 83 II lit. a – k DSGVO.
[245] Vgl. § 41 II S. 1 BDSG-neu.
[246] Vgl. § 41 I, II BDSG-neu.
[247] Vgl. § 41 II S. 3 BDSG-neu.
[248] Vgl. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz 2019.
[249] Art. 82 I DSGVO.
[250] Vgl. Art. 82 I, II DSGVO.
[251] Vgl. Kapitel 2.2.1.2 - 2.2.1.4 dieser Arbeit.
[252] Vgl. Erwägungsgrund Nr. 146 der DSGVO, Satz 3.
[253] Erwägungsgrund Nr. 85 der DSGVO, Satz 1 am Ende.

tenden deutschen Rechtspraxis abhebt und somit für hiesige Verhältnisse hohe Forderungen entstehen können. Mithin ist eine Kausalität zwischen Rechtsverletzung und Schaden notwendig für den Schadenersatzanspruch, nicht aber, dass der Schutzzweck der Norm betroffen ist.[254] Die DSGVO ermöglicht also einen Schadenersatzanspruch für jeden etwaigen Schaden, der dem Anspruchsteller aufgrund einer Datenschutzrechtsverletzung entsteht. Jedoch kann sich der Verantwortliche bzw. der Auftragsverarbeiter nach Art. 82 III DSGVO exkulpieren, wenn ihn nachweislich kein Verschulden trifft.[255] Auftragsverarbeiter und Verantwortliche haften gesamtschuldnerisch für Schäden, die aufgrund der zusammen durchgeführten Datenverarbeitung entstehen.[256] Formell ist für die prozessuale Verfolgung von Schadenersatzansprüchen die nationale Gerichtbarkeit verantwortlich.[257] Als Beispiel für einen erfolgreichen Schadenersatzanspruch gem. Art. 82 I DSGVO sei das Urteil des Arbeitsgerichts Düsseldorf vom 05.03.2020 genannt, wonach dem Kläger 5000€ Schadenersatz aufgrund der verspäteten und unvollständigen Beantwortung eines Auskunftsantrags zugesprochen wurde. Den hierfür auschlaggebenden immateriellen Schaden sahen die Richter darin begründet, dass der Anspruchsteller um seine Rechte und Freiheiten, namentlich dem Auskunftsrecht des Art. 15 I DSGVO, gebracht wurde.[258] Dieses Urteil bestätigt die oben dargelegte weite Auslegung des Schadenbegriffs sowie die auch für Unternehmen spürbare Höhe des Schadenersatzes.

2.2.2 Weitere relevante Rechtsquellen

Nachdem nun die Grundlagen des in Deutschland geltendes Datenschutzrechts anhand der Rechtsquellen DSGVO und BDSG-neu ausführlich erläutert wurden, werden aufgrund der vielschichtigen Strukturen, Interdisziplinarität und Datensensibilität beim Thema E-Health nachfolgend weitere Rechtsquellen beleuchtet, die ebenso Einfluss auf den Datenschutz im E-Health-Bereich haben. Wie der geschäftsführende Direktor am Institut für Informations-, Gesundheits- und Medizinrecht der Universität Bremen, Benedikt Buchner, in einem in der Fachzeitschrift Medizinrecht veröffentlichten Beitrag zu Datenschutz und Datensicherheit in der digitalisierten Medizin treffend feststellt *„beruht [der Gesundheitsdatenschutz] im Wesentlichen auf drei Eckpfeilern: dem klassischen Datenschutzrecht mit seinen allgemeinen und bereichsspezifischen Vorgaben, dem Sozialdatenschutzrecht und den Regelungen zur ärztlichen Schweigepflicht.“*[259]. Daher werden im Folgenden vorwiegend die Regelungen aus Strafgesetzbuch und Musterberufsordnung zur Schweigepflicht sowie die Sozialgesetzbücher und andere, bereichsspezifische Gesetze im E-Health-Bereich betrachtet.

2.2.2.1 StGB

Im deutschen Strafgesetzbuch (StGB) muss in Bezug auf E-Health- und datenschutzrelevante Normen die ärztliche Schweigepflicht betrachtet werden. Für Ärzte und andere Angehörige des Gesundheitswesens gilt als Berufsgeheimnisträger die Schweigepflicht des § 203 StGB. Diese schützt insbesondere das Patientengeheimnis, wie dem Wortlaut des Gesetzes zu entnehmen ist:

§ 203 StGB Verletzung von Privatgeheimnissen

[254] Vgl. Jens Eckhardt 2020.
[255] Vgl. Erwägungsgrund Nr. 146 der DSGVO, Satz 2.
[256] Vgl. Erwägungsgrund Nr. 146 der DSGVO, Satz 7.
[257] Vgl. Art. 82 VI DSGVO.
[258] Vgl. ArbG Düsseldorf, Urteil vom 05.03.2020 - 9 Ca 6557/18, Rn. 111.
[259] Vgl. Benedikt Buchner, S. 661.

„(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, […] anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."

Als „fremdes Geheimnis" sind im medizinischen Bereich sämtliche Daten zu verstehen, die im Kontakt zwischen Leistungserbringer und Leistungsempfänger erhoben werden. Dazu gehört insbesondere auch das reine Vorliegen des Behandlungsverhältnisses und alle auf diesem Verhältnis basierenden Informationen.[260] Die Offenbarung von Gesundheitsdaten der Patienten ist demnach grundsätzlich strafbar, es sei denn der Patient hat in die Weitergabe eingewilligt (sogenannte Entbindung von der Schweigepflicht) oder die Weitergabe fußt auf einer gesetzlichen Offenbarungspflicht (etwa aufgrund des Infektionsschutzgesetzes) bzw. auf einer Güterabwägung (die einen rechtfertigenden Notstand gem. § 24 StGB begründet).[261] Keine strafrechtlich relevante Offenbarung liegt vor, wenn die Weitergabe der Daten zur Ausübung der beruflichen Tätigkeit notwendig ist. Dies schließt mit ein, dass bspw. Angestellte in einer Arztpraxis Zugriff auf Daten haben, die der ärztlichen Schweigepflicht unterfallen.[262]

Die ärztliche Schweigepflicht wurde in der Vergangenheit von Experten in Bezug auf E-Health kontrovers diskutiert. So stellt die 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2015 fest, dass der Bund *„klare Rahmenbedingungen für die Einschaltung externer Dienstleister durch Berufsgeheimnisträger schaffen und den Vertraulichkeitsschutz bei den Dienstleistern sicherstellen [muss]. Die Einschaltung von externen Dienstleistern ist für Berufsgeheimnisträger oft ohne Alternative, wenn sie – wie auch vom Gesetzgeber beispielsweise mit dem eHealth-Gesetz gewünscht – moderne Informationstechnik nutzen wollen. Jedoch ist damit regelmäßig die Gefahr eines Verstoßes gegen die Schweigepflicht verbunden."*[263]. Hiermit appelliert sie an den Gesetzgeber, dass er darüber Rechtssicherheit schaffen muss, inwieweit und unter welchen Voraussetzungen Gesundheitsdaten an externe Dienstleister weitergeleitet werden können, ohne dass der Berufsgeheimnisträger Gefahr läuft, sich strafbar zu machen. Die Konferenz fordert, dass die Grundsätze der Datenminimierung (nur so viele Daten übermitteln wie nötig) und Transparenz sowie Weisungsrechte des Verantwortlichen und die Datensicherheit durch TOMs gewährleistet werden sollen.[264] Mit diesen Anforderungen könnten aus einer DSGVO-konformen Auftragsverarbeitung grundsätzlich keine strafgesetzlichen Verstöße gegen die ärztliche Schweigepflicht resultieren, da diese Anforderungen, wie in den obigen Kapiteln aufgezeigt wurde, in der DSGVO bereits ausführlich geregelt sind. Diesem Wunsch der Datenschutzkonferenz ist der Gesetzgeber in einer Novellierung des § 203 III StGB im Juni 2017 nachgekommen, mit der die Schweigepflicht auf externe Dienstleister erweitert wurde. Seit dem ist die Datenweitergabe im Rahmen von (Unter-)Auftragsverhältnissen von der Schweigepflicht abgedeckt, solange dem Dritten nur das für die Dienstleistung erforderliche Wissen offenbart wird und mitwirkende Personen zur

[260] Bernd Schütze, S. 10.
[261] Vgl. Christoph Bauer et al. 2018, S. 153 f.
[262] Vgl. § 203 III StGB.
[263] 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2015, S. 2.
[264] Vgl. 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder 2015.

Geheimhaltung verpflichtet werden.[265] Die Vereinfachung der Datenweitergabe an Dienstleister begründet der Gesetzgeber ausdrücklich mit der „Digitalisierung der letzten Jahrzehnte“[266], die dazu geführt hat, dass nicht alle datenverarbeitenden Tätigkeiten selbst ausgeführt werden können, unter anderem weil es zur IT-Administration spezieller Kenntnisse bedarf und oftmals „die Einstellung von informationstechnisch spezialisiertem Personal nicht wirtschaftlich wäre.“[267,268]

2.2.2.2 Musterberufsordnung für Ärzte

Die (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte (MBO-Ä) ist das Standesrecht dieses Berufszweigs und enthält die ärztlichen Berufspflichten und Grundsätze der Berufsausübung. Sie wird vom deutschen Ärztetag beschlossen und gewährleistet ein weitgehend einheitliches Berufsrecht. Die MBO-Ä stellt an sich kein anwendbares Recht dar, ist jedoch die Basis für die Berufsordnungen der Länder, welche von Vertreterversammlungen im Rahmen des Selbstverwaltungsrecht bestimmt werden und mithin unmittelbar anwendbares und sanktionierbares Satzungsrecht sind. Die jeweilige Berufsordnung ist für jeden approbierten Arzt gültig, unabhängig davon, ob er im Ruhestand ist und wie er seinen Beruf ausübt.[269] Die MBO-Ä enthält weitere Ausführungen zur ärztlichen Schweigepflicht. Demnach haben Ärzte *„über das, was ihnen in ihrer Eigenschaft als Ärztin oder Arzt anvertraut oder bekannt geworden ist – auch über den Tod der Patientin oder des Patienten hinaus – zu schweigen. Dazu gehören auch schriftliche Mitteilungen der Patientin oder des Patienten, Aufzeichnungen über Patientinnen und Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.“*[270] Weiterhin gelten im Grunde die gleichen Ausnahmetatbestände zur Datenweitergabe, die bereits oben in Bezug auf den § 303 StGB dargelegt wurden.[271] Im § 10 MBO-Ä werden Dokumentations- und Transparenzpflichten bestimmt. Demnach haben Patienten ein Recht auf Einsicht in die sie betreffende Dokumentation, soweit dem keine erheblichen Rechte Dritter oder therapeutischen Gründe entgegenstehen. Ärzte müssen ihre Aufzeichnungen bzw. Daten für mindestens 10 Jahre nach Behandlungsabschluss aufbewahren und die Daten müssen unter Beachtung der Empfehlungen der Ärztekammer besonders technisch geschützt werden.[272]

2.2.2.3 SGB

Das SGB stellt das formelle Sozialrecht in Deutschland dar und wird in 13 Bücher (SGB I – XIV) gegliedert.[273] Bezüglich des Datenschutzrechts sind vor allem die Gesetze SGB I und X relevant. Das SGB I enthält, vergleichbar mit dem Allgemeinen Teil des BGB, die allgemeinen Regelungen des Sozialrechts, welche gem. § 37 SGB I gemeinsam mit dem

[265] Vgl. Bernd Schütze, S. 15–19.
[266] Deutscher Bundestag 2017.
[267] Deutscher Bundestag 2017, S. 17.
[268] Vgl. Deutscher Bundestag 2017, S. 17.
[269] Vgl. Ärztekammer Berlin o.J.
[270] § 9 I MBO-Ä.
[271] Vgl. § 9 II – V MBO-Ä.
[272] Vgl. § 10 I – V MBO-Ä.
[273] Anmerkung des Autors: Die römische Ziffer XIV steht zwar für die Zahl 14, jedoch wurde aus Rücksicht auf die durch Aberglauben bedingte negative Konnotation der Zahl 13 auf ein SGB XIII verzichtet. Quelle: www.augsburger-allgemeine.de/politik/Aberglaeubisch-Bundesminister-Heil-will-auf-die-Zahl-13-verzichten-id53137981.html (zuletzt abgerufen am 09.02.2021).

SGB X, vorbehaltlich abweichender Regelungen, für das ganze Sozialrecht gelten.[274] Das SGB regelt unter anderem die Organisation und Zusammenarbeit der Sozialleistungsträger und hat in diesem Sinne auch Auswirkungen auf den Datenschutz im E-Health-Bereich. Sowohl SGB I als auch SGB X wurden in Bezug auf die DSGVO aktualisiert und enthalten spezifizierte Normen für den Datenschutz im Sozialrecht. Das SGB hat hierbei das Ziel, unter Beachtung des Unionsrechts das Sozialdatenschutzrecht in Deutschland zu ergänzen. Dies wird insbesondere in § 35 I SGB I deutlich:

§ 35 SGB I Sozialgeheimnis

„(2) Die Vorschriften des Zweiten Kapitels des Zehnten Buches und der übrigen Bücher des Sozialgesetzbuches regeln die Verarbeitung von Sozialdaten abschließend, soweit nicht die Verordnung (EU) 2016/679 des Europäischen Parlaments […] (Datenschutz-Grundverordnung) […] in der jeweils geltenden Fassung unmittelbar gilt. Für die Verarbeitungen von Sozialdaten im Rahmen von nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fallenden Tätigkeiten finden die Verordnung (EU) 2016/679 und dieses Gesetz entsprechende Anwendung, soweit nicht in diesem oder einem anderen Gesetz Abweichendes geregelt ist.“

Das SGB regelt sozialdatenschutzrechtliche Sachverhalte, die in der DSGVO nicht abschließend behandelt werden. So wird etwa im § 35 V SGB I die Verarbeitung personenbezogener Daten von Verstorbenen für zulässig erklärt. Weitere Konkretisierungen des Datenschutzrechts finden sich im zweiten Kapitel des SGB X, welches den „Schutz der Sozialdaten“ im Titel trägt und die §§ 67 – 85 a SGB X umfasst. Die DSGVO ergänzende Begriffsbestimmungen werden im § 67 SGB X kodifiziert. Hier wird z.B. die Datenkategorie „Sozialdaten“ definiert, die demnach alle personenbezogenen Daten gem. Art. 4 Nr. 1 DSGVO sind, welche von einer im § 35 SGB I genannten Stelle verarbeitet werden. Darauf folgen in den §§ 67a – 78 SGB X grundsätzliche Regelungen zur Erhebung, Übermittlung und Verarbeitung von Sozialdaten. Im § 78 I S. 3 SGB X werden auch Dritte, d.h. nicht im § 35 SGB genannte Personen oder Stellen, verpflichtet, übermittelte Daten mit den Maßgaben des Sozialdatenschutzrechts geheim zu halten. Der dritte Abschnitt des zweiten Kapitels hat besondere Datenverarbeitungsarten zum Inhalt. In den §§ 81 ff. SGB X werden Betroffenenrechte, Informationspflichten und die Stellung der Datenschutzbeauftragten spezifiziert. Außerdem sind dort Normen zum Rechts- und Klageweg im Sozialdatenschutzrecht enthalten. Außerhalb des zweiten Kapitels umfasst das zehnte SGB in den §§ 98 ff. SGB X noch Spezialvorschriften zu Datenauskunftspflichten zwischen den Sozialleistungsträgern und Ärzten bzw. Krankenhäusern. Darüberhinausgehend beinhalten andere Sozialgesetzbücher, die bereichsspezifisch die verschiedenen Leistungsträger abdecken, weitere datenschutzrechtliche Regelungen. So kodifiziert das fünfte SGB in den §§ 284 – 305 SGB V weitere datenschutzrechtliche Normen, die an die gesetzlichen Krankenversicherungsträger adressiert sind. Besondere datenschutzrechtliche Relevanz des SGB im E-Health-Bereich entfaltet sich mithin durch die Digitalisierung bei den gesetzlichen Krankenkassen, welche als Sozialleistungsträger an die Regelungen der SGB gebunden sind, sowie deren Zusammenarbeit mit Kassenärzten und anderen medizinischen Leistungserbringern.

[274] Vgl. Bundesrechtsanwaltskammer 2020.

2.2.2.4 E-Health-Gesetz

Das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen sowie zur Änderung weiterer Gesetze, kurz E-Health-Gesetz, befasst sich mit der elektronischen Gesundheitskarte und medizinischen Telematikinfrastruktur im Allgemeinen sowie mit der Einführung von elektronischen Arztbriefen, modernem Versichertenstammdatenmanagement, Videosprechstunden und der elektronischen Patientenakte. Damit dient es der Umsetzung von bereits hier in der Arbeit erläuterten E-Health-Anwendungen. Hierfür enthalten die Artikel 1 und 1a des E-Health-Gesetzes Anpassungen von verschiedenen Rechtsnormen des SGB V. Ex-Bundesgesundheitsminister Hermann Gröhe, unter dessen Schirmherrschaft das E-Health-Gesetzes verabschiedet wurde, fasst die Ziele des E-Health-Gesetzes zu dessen Einführung wie folgt zusammen: *„Mit dem E-Health-Gesetz treiben wir den Fortschritt im Gesundheitswesen voran. Dabei stehen Patientennutzen und Datenschutz im Mittelpunkt. Eine sichere digitale Infrastruktur verbessert die Gesundheitsversorgung und stärkt die Selbstbestimmung der Patienten – das bringt echten Nutzen für die Versicherten. Ärzte, Kassen und Industrie stehen jetzt gleichermaßen in der Pflicht, die gesetzlichen Vorgaben im Sinne der Patienten zügig umzusetzen.“*[275]. Das Gesetz enthält finanzielle Anreize für die Digitalisierung der ärztlichen Verwaltungsprozesse. Durch das E-Health-Gesetz wird die Vergütung von Arztbriefen im § 291f I SGB V um eine Pauschale in Höhe von je 55 Cent erhöht, wenn diese elektronisch und durch geeignete technische Maßnahmen gesichert versendet werden. Im Gesetz enthalten sind, neben datenschutzrechtlichen Regelungen und Vergütungen für E-Health, auch klare Vorgaben und Fristen zur einheitlichen Digitalisierung im Gesundheitswesen sowie Sanktionierungsmöglichkeiten. Während die Kassenärztliche Bundesvereinigung die Bemühungen zur Digitalisierung im Gesundheitswesen grundsätzlich begrüßte, sorgten dort die Terminvorgaben und Vergütungsminderungen bei Nichteinhaltung für Unverständnis.[276]

2.2.2.5 Neue Entwicklungen: Patientendaten-Schutz-Gesetz und andere

Die fortschreitende Digitalisierung im Gesundheitswesen wird begleitet von ständigen Gesetzesentwürfen und -beschlüssen. Beispielhaft seien hier das Patientendaten-Schutz-Gesetz (PDSG), das bereits in Kapitel 2.1.4 erwähnte DVG und das sich noch in der Entwicklung befindliche Tracing-App-Freiwilligkeits- und Zweckbindungs-Gesetz (TrAppFZG) genannt. Letzteres wurde am 16.06.2020 von der Bundestagsfraktion BÜNDNIS 90/DIE GRÜNEN als Entwurf veröffentlicht und bezieht sich auf die aktuell in Diskussion stehenden Corona-Warn-Apps. Mit dem Gesetzesentwurf sollen rechtliche Unklarheiten bzgl. eines etwaigen faktischen Nutzungszwangs von Contact-Tracing-Apps, etwa im Rahmen von Arbeitsverhältnissen oder dem Zutritt zu Einkaufszentren und anderen Institutionen dadurch gelöst werden, in dem ein allgemeines Benachteiligungsverbot für die Nichtbenutzung dieser Apps kodifiziert wird. Außerdem werden in Bezug auf die erhobenen und verarbeiteten Daten eine strenge Zweckbindung sowie ein Beschlagnahmeverbot festgelegt.[277] Das PDSG, eigentlich „Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur“, ist am 20.10.2020 in Kraft getreten[278] und hat Änderungen von verschiedenen bereichsspezifischen Gesetzen wie der SGB V und XI, dem Apothekenge-

[275] Bundesgesundheitsministerium 2015.
[276] Vgl. Kassenärztliche Bundesvereinigung 2015, S. 2.
[277] Vgl. § 6 TrAppFZG.
[278] Vgl. Art. 9 PDSG.

setz und dem Krankenhausfinanzierungsgesetz zum Inhalt. Es enthält Regelungen zu Förderung digitaler Innovationen, der elektronischen Gesundheitskarte und Patientenakte, dem Zugriff auf elektronische Rezepte mit Hilfe von Gesundheitsapps und dem Datenschutz in der Telematikinfrastruktur. Patienten haben mit dem PDSG einen Anspruch auf die Datenübertragung in die ePA.[279] Das Bundesgesundheitsministerium verkündet, dass mit Einführung des PDSG *„allein der Patient [entscheidet], was mit seinen Daten geschieht. […], welche Daten in der ePA gespeichert und welche wieder gelöscht werden. Er entscheidet auch in jedem Einzelfall, wer auf die ePA zugreifen darf.“*[280]. Der § 307 SGB V wird durch das PDSG in Bezug auf die datenschutzrechtlichen Verantwortlichkeiten aktualisiert. Mit dem Inkrafttreten des Gesetzes ist jede patientendatenverarbeitende Stelle (Ärzte, Krankenhäuser, Apotheken, etc.) explizit für den Schutz der verarbeiteten Patientendaten verantwortlich. Ebenso kodifiziert werden Fristen zur Umsetzung bestimmter digitaler Innovationen, wie bspw. dem Zugriff auf die ePA per Smartphone ab 2022.[281]

Die Vielzahl an weiteren, potenziell relevanten Rechtsquellen, welche datenschutzrechtliche Normen mit Einfluss auf das Gesundheitswesen beinhalten, wie bspw. die einzelnen Landeskrankenhausgesetze oder allgemeine formelle Gesetze wie das IT-Sicherheitsgesetz und weitere Verordnungen erschweren die intensive, theoretische Auseinandersetzung mit ebendiesen.[282] Eine detaillierte Darstellung all dieser Rechtsvorschriften würde den Umfang dieser Arbeit bei Weitem überschreiten. Daher soll der nachstehende empirische Teil durch die Erarbeitung von Hypothesen und Handlungsempfehlungen mit Hilfe von Expertenwissen einen abschließenden Überblick über die datenschutzrechtlichen Rahmenbedingungen von E-Health liefern, der dem Zweck dieser Arbeit gerecht wird.

3 Empirische Analyse

3.1 Forschungsfrage

Aus der im konzeptionellen Teil beschriebenen Digitalisierung im Gesundheitswesen und den dazugehörigen datenschutzrechtlichen Aspekten lässt sich für den empirischen Teil die nachstehende Fragestellung herleiten:

„Welche Auswirkungen hat das Datenschutzrecht auf die Digitalisierung im deutschen Gesundheitswesen?“

Aus dieser Forschungsfrage lassen sich die folgenden Hypothesen ableiten:

Hypothese 1:

Nullhypothese: Die E-Health-Umsetzung in Deutschland ist weit vorangeschritten und ein wichtiger Bestandteil in der beruflichen Praxis.

[279] Vgl. aktualisierte Fassung des § 347 SGB V.
[280] Bundesgesundheitsministerium 2020d.
[281] Vgl. aktualisierte Fassung des § 341 II SGB V
[282] Vgl. Thomas Jäschke et al. 2018, S. 28–31.

Alternativhypothese: Die E-Health-Umsetzung in Deutschland ist nicht weit vorangeschritten und kein wichtiger Bestandteil in der beruflichen Praxis.

Hypothese 2:

Nullhypothese: Es gibt ein Spannungsfeld zwischen Datenschutz und E-Health.

Alternativhypothese: Es gibt kein Spannungsfeld zwischen Datenschutz und E-Health.

Hypothese 3:

Nullhypothese: Außer der DSGVO haben auch andere Rechtsquellen einen erheblichen Einfluss auf die datenschutzrechtliche Umsetzung im E-Health-Bereich.

Alternativhypothese: Außer der DSGVO haben andere Rechtsquellen keinen erheblichen Einfluss auf die datenschutzrechtliche Umsetzung im E-Health-Bereich.

Hypothese 4:

Nullhypothese: Die verschiedenen Bestandteile und Instrumente der DSGVO überfordern Unternehmen in der Praxis.

Alternativhypothese: Die verschiedenen Bestandteile und Instrumente der DSGVO überfordern Unternehmen in der Praxis nicht.

Mittels einer qualitativen Forschungsmethode werden nachfolgend die hier aufgestellten Hypothesen geprüft, um anschließend aus den erhobenen Informationen Handlungsempfehlungen abzuleiten. Die hierfür angewendete Methode wird im nächsten Kapitel erörtert.

Der folgende Abschnitt definiert, wie die Forschungsfrage beantwortet werden soll. Hierfür wurde dieser in vier Teile gegliedert. Im ersten Teil werden die Rahmenbedingungen (Untersuchungsmethode und Zielgruppe) erörtert. Daraufhin folgen die Darstellung des Fragebogens und die Umsetzung der qualitativen Befragung inklusive einer fünftstufigen Inhaltsanalyse. Zuletzt werden die Ergebnisse abgebildet.

3.2 Untersuchungsmethode und Zielgruppe

Untersuchungsmethode

Der empirische Teil dieser Arbeit beruht auf der Durchführung und Analyse von Experteninterviews und hat das Ziel, weitere Erkenntnisse bezüglich der Umsetzung von E-Health und Datenschutz in der Praxis zu gewinnen. Des Weiteren dienen die Experteninterviews zur Beantwortung der formulierten Forschungsfrage und der Hypothesen. Durch die zunehmende Verbreitung von E-Health und der damit einhergehenden Datenschutzproblematiken ist einschlägiges Expertenwissen in Bezug auf Authentizität und Umfang der erfragten Informationen besonders wertvoll. Die qualitative Forschungsmethode der systematisierenden Experteninterviews, welche im Folgenden angewendet wird, wird gegenüber einer quantitativen Forschungsmethode in dieser Studie bevorzugt, da mit dieser Art von Expertenbefragung präzisiertes Spezialwissen von direkt mit E-Health und Datenschutz involvierten Personen generiert werden kann.[283] Das Erkenntnisziel bei systematisierenden Experteninterviews liegt in der Erhebung eines weitgehenden und umfassenden Expertenwissens bezüglich des Forschungsthemas. Zur Informationsgewin-

[283] Vgl. Bernd Blöbaum et al. 2014, S. 1.

nung wurde ein ausdifferenzierter Fragebogen erstellt, der das hierfür relevante Fachwissen weitgehend lückenlos erschließen soll.[284]

Zielgruppe
Zur Durchführung der Befragung erfolgte zunächst ein sogenanntes Sampling von Interviewpartnern, also die qualitative Auswahl der zu interviewenden Experten.[285] Die Digitalisierung im Gesundheitswesen beruht darauf, dass sowohl kleine als auch große Institutionen hierfür einen Beitrag leisten. Daher wurden vor allem Experten aus mittelständischen Unternehmen interviewt, die durch die Größe ihres Unternehmens intensiv und persönlich in die E-Health- und Datenschutzumsetzung mit eingebunden sind, da sie keine großen Kapazitäten für eigene Datenschutz- bzw. Rechtsabteilungen haben. Auch im Hinblick auf die Zugangsbarrieren, die ein Hindernis für den direkten Zugang zu Experten sind, wurden im Rahmen dieser Befragung mittelständische Unternehmen präferiert. Zugangsbarrieren äußern sich etwa in der sozialen und unternehmerischen Stellung, die dazu führt, dass der direkte Zugang zu den Experten durch PR-Abteilungen oder unterstellte Assistenten blockiert ist.[286] Es wurden vorrangig Ansprechpartner im höheren Management von mittelständischen Gesundheitsdienstleistern mit dem Ziel befragt, durch ähnliche Kompetenz und Stellung der Interviewpartner eine Vergleichbarkeit der Antworten herzustellen. Auch Blöbaum empfiehlt bei Experteninterviews mit dem primären Ziel, die Funktionsweise gesellschaftlicher Teilbereiche zu ergründen, den Fokus auf „Rollenträger in diesen Teilbereichen“[287], also Personen mit Leitungsfunktion, zu legen.[288] Als Ansprechpartner im höheren Management sind die interviewten Personen sogenannte Entscheider, die als „Experten für ihre jeweilige Organisation und genaue Beobachter von Entscheidungsprozessen, Strukturen und Veränderungen“[289] besonders geeignete Interviewpartner sind.[290]

3.3 Aufbau des Fragebogens

Der Fragebogen (Anhang) ist in drei Themenblöcke gegliedert und besteht aus zehn Hauptfragen. Die im Fragenkatalog vorgenommene Gruppierung in verschiedene Themenblöcke hat die Strukturierung der Interviewfragen zum Ziel und trägt somit zu einer besseren Übersicht für die Befragten bei. Jeder Themenblock trägt einen Oberbegriff (individuelle Attribute, E-Health, Datenschutz). Die dazugehörigen Interviewfragen behandeln die jeweilige Thematik. Einzelne Hauptfragen werden zur weiteren Vertiefung durch Teilfragen konkretisiert. Die Interviewfragen sind nicht mit den Forschungsfragen bzw. -hypothesen identisch, da sie auf den Wissens- und Erfahrungshorizont der Interviewpartner ausgerichtet sind.[291] Das Wissen und die Erfahrung der Experten sollen mit Hilfe der Interviewfragen, in Bezug auf die im konzeptionellen Teil behandelten Themen, offengelegt werden. Die nachstehende Abbildung gibt einen Überblick über den Aufbau des Fragenkatalogs.

[284] Vgl. Alexander Bogner et al. 2014, S. 24.
[285] Vgl. Alexander Bogner et al. 2014, S. 34 f.
[286] Vgl. Alexander Bogner et al. 2014, S. 37.
[287] Bernd Blöbaum et al. 2014, S. 9.
[288] Vgl. Bernd Blöbaum et al. 2014, S. 9.
[289] Andreas Scheu et al. 2014, S. 76.
[290] Vgl. Bernd Blöbaum et al. 2014, S. 9 f.
[291] Vgl. Alexander Bogner et al. 2014, 33 f.

Abbildung 10: Aufbau des Fragenkatalogs

[Quelle: Eigene Abbildung, vgl. Anhang]

Themenblock 1

Im ersten Themenblock werden mit den Interviewfragen 1 und 2[292] die individuellen Attribute des Interviewpartners (Unternehmensvorstellung und unternehmensinterne Stellung) erfragt. Dies dient der Einordnung der gewonnenen Informationen und als Einstieg in den thematischen Teil des Fragebogens. Themenblöcke 2 „E-Health“ und 3 „Rechtlicher Rahmen“ hingegen orientieren sich am konzeptionellen Teil dieser Arbeit, der die Basis für die im Folgenden durchgeführte qualitative Forschung darstellt. Die relevanten Sachbereiche, die sich im konzeptionellen Teil herauskristallisiert haben, werden hierbei tiefergehend untersucht.

Themenblock 2

Im zweiten Themenblock, der die Interviewfragen 3, 3*, 4 und 5 enthält, geht es daher zunächst um die Umsetzung von E-Health im Unternehmen, unabhängig von den rechtlichen Rahmenbedingungen. Hierfür werden die im Unternehmen präsenten und priorisierten Formen von E-Health erfragt. Bei dieser Frage stehen dem Interviewpartner die zwei Formenmodelle aus Abbildung 5 und 6 dieser Arbeit zur Verfügung.[293] Dies soll die Einheitlichkeit der Antworten fördern, ohne den Interviewpartner in seinen Antwortmöglichkeiten einzuengen. Darauffolgend werden Fragen zu den Chancen und Risiken von E-Health gestellt. Hier soll der jeweilige Experte einen tieferen Einblick bezüglich der Vor- und Nachteile der ihm obliegenden E-Health-Umsetzung vermitteln und so die aus der einschlägigen Fachliteratur entnommenen, im Kapitel 2.1.3 dargelegten Vor- und Nachteile, validieren bzw. ergänzen. Die im zweiten Themenblock gestellten Fragen dienen der Untersuchung von Hypothese 1.

Themenblock 3

Der dritte Themenblock ist Kern des Fragebogens und zielt auf eine strukturierte Informationsgewinnung bezüglich der rechtlichen Rahmenbedingungen von E-Health. Wie auch im konzeptionellen Teil liegt hier der Fokus auf der DSGVO. Die erste Frage des dritten Themenblocks, mithin die sechste Interviewfrage, beginnt mit einem einleitenden Satz, der den Interviewpartner einen kurzen Einstieg in die folgenden rechtlichen Fragen bieten soll: *„Das E-Health-Geschäft wird neben den technischen Möglichkeiten auch von rechtli-*

[292] Anmerkung des Autors: Die Interviewfragen 1-11 sind dem Anhang „Fragenkatalog“ zu entnehmen.
[293] Vgl. Kapitel 2.1.4 dieser Arbeit.

chen Rahmenbedingungen beeinflusst. Das rechtliche Grundgerüst einer jeden personenbezogenen Datenverarbeitung in Deutschland ist die DSGVO bzw. das BDSG-neu. Doch welche Rechtsquellen beeinflussen Ihre E-Health-Umsetzung noch?"[294] Diese Frage zielt darauf ab, den rechtlichen Rahmen von E-Health außerhalb der DSGVO abzudecken. Wie im konzeptionellen Teil beschrieben, existiert eine Vielzahl an Rechtsquellen mit Normen, welche unter das Datenschutzrecht im Gesundheitswesen subsumiert werden können, sodass auch im Kapitel 2.2.2 nur beispielhaft einzelne Gesetze präsentiert wurden. Mit dieser Frage soll ermittelt werden, ob die anderen Rechtsquellen trotz dessen im beruflichen Alltag zur Geltung kommen, oder die datenschutzrechtliche Thematik regelmäßig von der DSGVO dominiert wird. Die hier gewonnenen Informationen dienen der Untersuchung von Hypothese 3.

Interviewfrage 7 dient dem Einstieg in den DSGVO-Teil des Fragebogens und stellt dem Interviewpartner in einem einleitenden Satz die Relevanz der DSGVO im Gesundheitswesen vor: *„Gesundheitsdaten sind besonders schützenswerte Daten. Die DSGVO hat sie als sensible Daten bzw. besondere Datenkategorie besonders geschützt. Wie wirkt sich die DSGVO seit 2018 auf Ihr Alltagsgeschäft aus?"*[295]. Diese Frage hat die Wissensgenerierung zu Hypothese 2 zum Ziel. Durch die hier vom Experten preisgegebenen Informationen soll festgestellt werden, ob die DSGVO die E-Health-Umsetzung in seinem Unternehmen eher gefördert oder zurückgeworfen hat und ob mithin ein Spannungsfeld zwischen E-Health und Datenschutz besteht. Des Weiteren liefert die siebte Interviewfrage Ansatzpunkte für Hypothese 4, die sich mit einer etwaigen Überforderung durch die verschiedenen Bestandteile und Instrumente der DSGVO befasst. Interviewfrage 8 ist die ausführlichste Frage des Interviews und besteht aus verschiedenen Teilfragen. In seiner Antwort soll der Interviewpartner darlegen, welche konkreten Maßnahmen bezüglich der einzelnen Rechtsinstrumente der DSGVO (vgl. Kapitel 2.2.1.1 bis 2.2.1.4 dieser Arbeit) im Unternehmen ergriffen werden und wie er diese Rechtsbestandteile bzgl. Wichtigkeit und Relevanz gewichtet. Anschließend folgen die Interviewfragen, mit denen festgestellt werden soll, ob ein DSB vorhanden ist, welche Stellung er innehat und wie dieser agiert. Mit Hilfe dieser Fragen soll Hypothese 4 ausführlich beleuchtet werden.

Die elfte und letzte Frage soll einen Ausblick in die Zukunft liefern und befasst sich mit den Herausforderungen, die der Experte in Bezug auf den Datenschutz im E-Health-Bereich sieht und was er sich von der zukünftigen Rechtsentwicklung erhofft. Dies dient der weiteren Informationserhebung zu den Hypothesen 2, 3 und 4.

3.4 Durchführung der Befragung

Vorbereitung und Abwicklung

Sowohl die Vorbereitung als auch die Durchführung der Experteninterviews erfolgte digital. Der Fragebogen wurde per E-Mail an die Befragten versendet. Dieser Vorgehensweise liegt die Überlegung zugrunde, dass die Experten ohne Zeitdruck und Flüchtigkeitsfehler durchdachte Antworten auf die konkreten Antworten geben können. Auch möglichen Transkriptions- und Verständnisfehlern, mit etwaigem negativem Einfluss auf die Validität der Antworten, wird so vorgebeugt. Eine Befragung in digitaler Form ist thematisch stimmig mit dem hier behandelten Forschungsthema. Ebenso ist aus datenschutzrechtlicher

[294] Anhang, Frage 3.
[295] Anhang, Frage 7.

Sicht die Befragung per E-Mail gegenüber dem Mitschnitt eines Videointerviews bzw. Telefonats unter Einholung von expliziten Einwilligungserklärungen zu bevorzugen und für alle Beteiligten weniger kompliziert. Der Fragenkatalog hing der E-Mail als PDF- sowie als bearbeitungsfähige DOCX-Datei an. Mit den E-Mails wurde der folgende Einstiegstext versendet und bzgl. der Anrede individuell angepasst:

> „Sehr geehrte/r Herr/Frau […],
>
> mein Name ist Thimo Niebler und ich studiere Wirtschaftsrecht an der Hochschule Konstanz. Im Rahmen meiner Bachelor-Thesis zum Thema „Datenschutzrechtlicher Rahmen von E-Health in Deutschland“ befrage ich verschiedene Institutionen und mittelständische Unternehmen der Gesundheitsbranche zum Thema Datenschutz und E-Health für eine empirische Untersuchung.
>
> Für den Begriff "E-Health" gibt es keine standardisierte Definition. Daher sind in meiner Arbeit unter E-Health alle Aktivitäten im Gesundheitswesen zu verstehen, bei denen unter Zuhilfenahme digitaler Technologien Daten verarbeitet werden.
>
> Im Anhang finden Sie den Fragenkatalog, der in drei Themenbereiche gegliedert ist, als PDF-Datei. Ich freue mich sehr, wenn Sie sich die Zeit nehmen und mich bei meiner Abschlussarbeit unterstützen. Sie können die Fragen entweder per E-Mail oder in der beigefügten Word-Datei beantworten. Bei Rückfragen stehe ich Ihnen jederzeit zur Verfügung.
>
> Viele Grüße
>
> Thimo Niebler“

Dieser Text dient der Rekrutierung von Interviewpartnern und soll diese motivieren, an der Befragung teilzunehmen. Hierfür weist der Text auf das Forschungsinteresse hin und beinhaltet eine grobe Themenübersicht.[296] Um bezüglich des Verständnisses von „E-Health“ eine Einheitlichkeit herzustellen, wird im obenstehenden Text, die im konzeptionellen Teil erarbeitete Definition von E-Health verwendet.

Befragte

Im Rahmen der Probandenfindung wurden zehn potenzielle Ansprechpartner angeschrieben. Daraufhin haben sich drei der angefragten Experten bereit erklärt, den Fragebogen zu beantworten. Diese werden nachstehend vorgestellt.

Interviewpartner 1: Juniormanagerin auf Geschäftsführungsebene

Unternehmen 1: Reha-Zentrum in Baden-Württemberg

Mitarbeiteranzahl: ca. 160 Mitarbeiter

Beschreibung:
Tagesklinik für orthopädische und neurologische Rehabilitation. Neben ambulanter Rehabilitation nach Operationen oder im Rahmen von klassischen Heilverfahren, werden auch Patienten nach Arbeitsunfällen und mit einem Heilmittelrezept betreut.

[296] Vgl. Bernd Blöbaum et al. 2014, 9 f.

Interviewpartner 2: Verwaltungsleiter und Assistent der Geschäftsführung eines Pflegedienstes (ehemalig), jetzt: Wirtschaftsprüfer im Gesundheitsbereich.

Unternehmen 2: aus Sicht eines ambulanten Pflegedienstes

Mitarbeiteranzahl: ca. 50 Mitarbeiter

Beschreibung:
Dienstleistungsunternehmen, das Leistungen nach SGB V und XI erbringt. Als ambulanter Pflegedienst ist das Unternehmen Mitglied im „Bundesverband privater Anbieter sozialer Dienste e.V.“.

Interviewpartner 3: Bereichsleiterin Mobile Soziale Dienste, zweite Hierarchieebene

Unternehmen 3: Wohlfahrtsorganisation in Nordrhein-Westfalen

Mitarbeiteranzahl: ca.1100 Mitarbeiter (500 hauptamtlich, 600 ehrenamtlich)

Beschreibung:
Wohlfahrtsorganisation die hauptsächlich im ambulanten Bereich tätig ist (ambulante Pflege- und hauswirtschaftliche Versorgung). Außerdem: Betreuung von Suchterkrankten und Menschen mit psychischer Erkrankung, Katastrophenschutz, Notfallausbildung, Integrationsassistenz an Schulen, Tagespflege.

Bei etwaigen Unklarheiten und Rückfragen bezüglich der Interviewfragen und -antworten folgte eine weitere Kommunikation per E-Mail, um möglichst aussagekräftige und valide Antworten zu erhalten. Die finalisierten Versionen der erhaltenen Antworten liegen dem Anhang III dieser Arbeit bei.

3.5 Auswertung der Interviews

3.5.1 Inhaltsanalyse nach Bogner

Als Analyseinstrument zur Informationsgewinnung bei systematisierenden Experteninterviews empfiehlt Bogner die qualitative Inhaltsanalyse. Diese folgt einem fünfstufigen Auswertungskonzept, welches in einer Kurzdarstellung nachstehend beschrieben wird.[297]

1. Fragestellung und Materialauswahl

Hierbei geht es um die Bestimmung von Fragestellung und -perspektive sowie der Definition des zu analysierenden Materials. Die Frageperspektive richtet sich, da die hier vorgenommene Expertenbefragung der Informationsgewinnung dient, ausschließlich auf den informativen Inhalt der Expertenantworten, d.h. etwaige emotionale Aspekte werden nicht betrachtet. Die relevanten inhaltlichen Aspekte der Expertenbefragung wurden im Kapitel „Forschungsfragen und Hypothesen“ dargelegt. Diese werden im Fragenkatalog in mehrere Fragestellungen übersetzt. Da die Antworten per E-Mail in Textform vom Experten selbst verfasst werden und auf dem ex ante strukturierten und formulierten Fragenkatalog basieren, ist davon auszugehen, dass das Interview ausschließlich stichhaltige Informationen enthält. Die Materialauswahl erfolgt also ohne Transkription eines mündlichen Ge-

[297] Vgl. Alexander Bogner et al. 2014, S. 73–75.

sprächs. Mithin liegt das zu untersuchende Forschungsmaterial in Form der E-Mail-Antwort des jeweiligen Experten zur tiefergehenden Analyse unmittelbar vor.[298]

2. Aufbau eines Kategoriensystems

Das Kategoriensystem setzt sich aus vorher bestimmten Kategorien und deren Beziehung zueinander zusammen. Es dient der Einordnung der in den Expertenantworten erhaltenen Informationen anhand der im Kategoriensystem vordefinierten Variablen. Die Grundlage des für die Informationseinordnung verwendeten Kategoriensystems ergibt sich aus der im konzeptionellen Teil vorgenommenen Auseinandersetzung mit der Fachliteratur und ähnelt den im Fragenkatalog vorgegebenen Themenblöcken, die in Kapitel 3.3 „Aufbau des Fragebogens“ präsentiert wurden.[299]

3. Extraktion

Im Extraktionsteil erfolgt die systematische Untersuchung der Expertenantworten. Hierbei werden die, für den Forschungszweck unmaßgeblichen Informationen, aus den in den E-Mails erhaltenen Rohdaten herausgefiltert und die relevanten Informationen anschließend dem Kategoriensystem zugeordnet. Ziel ist die Schaffung einer forschungsrelevanten und thematisch geordneten Informationsbasis.[300]

4. Aufbereitung der Daten

Die Datenaufbereitung dient der Qualitätskontrolle und -optimierung der geschaffenen Informationsbasis. Die Expertenantworten werden auf offensichtliche Fehler und redundante Informationen geprüft und dahingehend korrigiert. Vom Experten empfohlene, die jeweilige Antwort ergänzende Informationen aus externen Quellen werden recherchiert und hinzugefügt. Inhaltliche Überschneidungen in den Antworten der Experten untereinander werden analysiert und zusammengefasst.[301]

5. Auswertung

Im fünften und letzten Schritt werden die Hypothesen und die Forschungsfrage auf Basis der aufbereiteten Informationen wissenschaftlich untersucht und beantwortet. Hierfür werden die Kausalzusammenhänge aufgedeckt, indem analysiert wird, welche Faktoren zu welchem Ergebnis führen.

3.5.2 Auswertung und Interpretation der Interviews

Die qualitative Inhaltsanalyse der Experteninterviews wurde gemäß dieser fünf Schritte durchgeführt. Die Expertenantworten zu den einzelnen Interviewfragen werden anhand der jeweiligen Datenkategorie nachfolgend ausgeführt.

3.5.2.1 Datenkategorie K1

Die erste Datenkategorie (K1) behandelt E-Health im Allgemeinen. Hierbei wird auf Formen, Vor- und Nachteile und Vision bei der Digitalisierung im Gesundheitswesen eingegangen, um auch außerhalb der theoretischen Fachliteratur einen Einblick in die prakti-

[298] Vgl. Alexander Bogner et al. 2014, S. 73.
[299] Vgl. Alexander Bogner et al. 2014, S. 73 f.
[300] Vgl. Alexander Bogner et al. 2014, S. 74.
[301] Vgl. Alexander Bogner et al. 2014, S. 74.

sche Umsetzung von E-Health im Jahr 2021 zu gewinnen und die Hypothese 1 zu beantworten. Zunächst beschreiben die Interviewpartner die in ihrem Unternehmen relevanten Formen von E-Health. Bei allen drei Interviewpartnern findet auf Kommunikationsebene ein Datenaustausch mit Kostenträgern (Renten-, Kranken- und Pflegeversicherungen), Leistungserbringern (Ärzten, Krankenhäusern) und den Leistungsempfängern (Patienten) sowie Mitarbeitern und Angehörigen der Patienten statt.

Interviewpartner 1, Managerin einer Tagesklinik, führt aus, dass die Digitalisierung des Alltagsgeschäfts sich grundsätzlich noch in der Anfangsphase befindet. Patienten müssen die sie betreffenden Dokumente (Aufzeichnung der Krankenhistorie, Entlassbriefe) in Papierform mitbringen, damit diese im Unternehmen 1 zur weiteren Verarbeitung zunächst eingescannt und damit digitalisiert werden können. Die Entlassberichte der eigenen Rehabilitation werden digital an den Kostenträger Deutsche Rentenversicherung (DRV) übermittelt, andere Kostenträger sind jedoch erst ab Mitte 2021 dementsprechend digitalisiert. Trotz der digitalen Übertragungswege zu den Kostenträgern werden die Entlassberichte den Patienten weiterhin in Papierform ausgehändigt. Auch für die Patientenzuweisungen bietet die DRV ein digitales Portal an. Dieses Portal ist für die Kostendeckung bereits enorm relevant, da die Hälfte aller in der Klinik betreuten Patienten auf diesem Weg zugewiesen und per Kostenzusage vom Kostenträger finanziert werden. Diese Datenübermittlung erfolgt hier gem. § 301 SGB V, der die Datenfernübertragung für Reha-Einrichtungen kodifiziert. Je nach Geschäftsbereich findet die Kommunikation mit den Ärzten noch ausschließlich per Fax statt. Unternehmen 1 bietet App-gestützte Therapien für seine Patienten an.

Auch bei Interviewpartner 2, der die Fragen aus Sicht eines ambulanten Pflegedienstes beantwortet hat, erfolgt die externe Kommunikation mit Ärzten, Krankenhäusern und Sozialarbeitern in der Regel per Telefon und Fax. Im internen Arbeitsablauf ist die Digitalisierung im Gesundheitswesen jedoch schon deutlich vorangeschritten. So werden bei der Patientenaufnahme die Patientendaten per App auf einem Tablet erfasst. Die hierbei verwendete App ist mit der Verwaltungs- und Abrechnungssoftware des Unternehmens verbunden, sodass die relevanten Daten in Echtzeit auf die firmeninternen Server übertragen werden. Auch die Leistungserbringung, Tourenpläne und Arbeitszeiterfassung werden über eine Software gesteuert und dokumentiert. Die Leistungsabrechnung mit den Kranken- und Pflegekassen erfolgt ausschließlich digital per elektronischem Datenaustausch gem. § 302 SGB V. Jedoch werden auch bei der Kommunikation mit den Krankenkassen bestimmte Daten derzeit ausschließlich per Fax übertragen. Außerdem bietet Unternehmen 2 digitale Fernüberwachungsdienstleistungen in Form von Hausnotrufsystemen für seine Kunden an.

Wie die anderen beiden Unternehmen digitalisiert auch Unternehmen 3, eine Wohlfahrtsorganisation, alle für die Behandlung notwendigen Unterlagen zur weiteren Datenverarbeitung. Zur Arbeitsabwicklung werden verschiedene Softwares und Apps genutzt. Die in den Arbeitsalltag integrierten Apps ermöglichen auch unterwegs den Zugriff auf und die Erfassung von Patientendaten per App, auf den von den Mitarbeitern genutzten Geschäftshandys. Des Weiteren werden auch in diesem Unternehmen die Versichertendaten elektronisch übermittelt, sodass die erbrachten Leistungen mit den Kostenträgern digital abgerechnet werden können. Zur Organisation der Mitarbeiter und Leistungen werden softwaregestützt Kunden-, Mitarbeiter- und Patientendaten verarbeitet. So werden die Mitarbeiter digital ihren Touren und Aufgaben zugewiesen, Kundendaten können jederzeit erfasst und abgerufen und Schulungen verwaltet werden. Interviewpartner 3 betont, dass

der Einsatz von E-Health mittlerweile unverzichtbarer Bestandteil für die tägliche Arbeitsabwicklung in allen Geschäftsbereichen ist.

Aus diesen Aussagen der interviewten Experten lässt sich ableiten, dass die Digitalisierung im mittelständischen Gesundheitsbereich erst teilweise stattgefunden hat. Zwar erfolgt die Zusammenarbeit mit den Kostenträgern zumeist digital und auch bei der internen Arbeitsgestaltung spielt E-Health bereits eine große Rolle. Doch die Kommunikation und der Datenaustausch von den interviewten mittelständischen Gesundheitsdienstleistern mit anderen Akteuren des Gesundheitswesens, etwa Ärzten, Krankenhäusern und Patienten, findet meist auf traditionellen Wegen wie über das Telefon, per Fax und analog in Papierform statt. Hervorzuheben ist der in allen befragten Unternehmen etablierte Einsatz von Apps, der gerade im ambulanten Bereich zu einer Erleichterung und Optimierung der Datenerfassung und Patientenbetreuung beigetragen hat. Dies liefert Ansatzpunkte für eine besondere Relevanz von mHealth.

Zu den Vor- und Nachteilen von E-Health äußern sich die Experten wie folgt: Interviewpartner 1 kritisiert vor allem die Uneinheitlichkeit bei der E-Health Umsetzung: Wenn jeder Akteur ein eigenes System verwendet, erschwere dies die digitale Zusammenarbeit. Hier fehlt es nach Meinung des Experten nicht am Willen zu investieren, vielmehr ist die Ursache im fragmentierten Aufbau des Gesundheitswesens zu finden. Chancen der Digitalisierung sieht der Experte in der Vereinfachung von Prozessen, einem schnellerem Datenzugriff mit mehr Kontrollmöglichkeiten und in potenziellen Kosteneinsparungen.

Experte 2 sieht mehrere Chancen und Vorteile bei E-Health. Diese reichen von einer allgemeinen Prozessoptimierung bei der Datenerfassung über die schnelleren Datenauswertung in der Arbeitszeiterfassung und Leistungsabrechnung bis hin zu einer flexibleren Tourenplangestaltung im ambulanten Dienst. Auch eine vereinfachte Datenverarbeitung und Dokumentation wirkt sich demnach positiv aus, da so bspw. die analoge, doppelte Buchführung entfällt. Als Risiko der Digitalisierung im Gesundheitswesen wird die Gefahr von Cyberangriffen gesehen. Hier nennt der Experte als Beispiel den Hackerangriff auf das IT-System des Universitätsklinikums in Düsseldorf vom 10.09.2020. Hier starb eine Patientin, nachdem diese wegen einem fremdverschuldeten Ausfall der IT-Systeme vom Krankenhaus abgewiesen werden musste und die Behandlung im nächstgelegenen Klinikum zu spät erfolgte.[302] Der Krankenhausbetrieb war durch einen Hackerangriff über mehrere Tage hinweg so eingeschränkt, dass die meisten Operationen nicht stattfinden und im stationären Betrieb keine neuen Patienten aufgenommen werden konnten.[303] Doch auch ohne einen Cyberangriff von außen, kann es zu einem Ausfall der Elektronik, bspw. bei Stromausfall, kommen. In einem solchen Fall warnt der interviewte Experte bei fortschreitender Digitalisierung, trotz möglicher Notstromversorgung, vor erheblichen Problemen bei der Arbeitsabwicklung. Ein weiterer Nachteil sei das Haftungsrisiko, etwa bei unbeabsichtigten Verstößen gegen die DSGVO.

Auch Experte 3 sieht ein großes Risiko bei den Folgen, die ein Totalausfall von Internet oder Software mit sich bringen würde. Der Experte stellt fest, dass zur Risikoprävention weiterhin analoge Akten geführt werden müssen, um im Notfall Zugriff auf relevante Daten haben zu können. Ein weiterer genannter Nachteil ist der potenzielle Datenverlust. Dem liegt die Befürchtung zugrunde, dass trotz regelmäßiger Backups ein Verlust von Datens-

[302] Vgl. Christof Kerkmann et al. 2020.
[303] Vgl. Handelsblatt 2020.

ätzen vorkommen kann, etwa bei sehr aktuellen Daten, die außerhalb der Backupintervalle erfasst wurden. Positive Effekte von E-Health sind dem Interviewpartner zufolge die schnellere Erreichbarkeit der Mitarbeiter und eine optimierte Kommunikation mit Ärzten, Kostenträgern und Angehörigen, der flexible Zugriff auf tagesaktuelle Daten, die Möglichkeit, Änderungen schnell umsetzen zu können und eine bessere Datenkontrolle, bspw. über die Einsatzzeiten.

Im Vergleich zu den im konzeptionellen Teil erarbeiteten Vor- und Nachteilen[304] lässt sich hier feststellen, dass die interviewten Experten den großen Vorteil von E-Health vor allem in den Optimierungen im kommunikativen und organisatorischen Bereich sehen. Diese wurden als Effektivitäts- und Effizienzvorteile bereits in Abbildung 3 dargestellt. Bei den Nachteilen hingegen dominiert die Angst vor Systemausfällen, Hackerangriffen und Datenverlust. Das Risiko einer sozialen Distanzierung zwischen Leistungserbringer und Leistungsempfänger wird nicht geteilt, vielmehr wird die Chance von E-Health in einer Verbesserung des Versorgungsumfelds gesehen. Weitere Kritikpunkte sind das Haftungsrisiko durch eine unklare Rechtslage und die fehlende Harmonisierung der E-Health-Systeme bei den verschiedenen Akteuren im Gesundheitswesen untereinander, die die digitale Expansion und Zusammenarbeit erschwert.

Für die Zukunft von E-Health schweben den Experten unterschiedliche Visionen vor: Experte 1, der die immer noch vorherrschende Kommunikation per Fax und Telefon kritisiert, sieht die Zukunft für eine zukünftige, digitalisierte Kommunikation im Gesundheitswesen in einer zentralen Plattform, auf die alle Akteure Zugriff haben. Als Beispiel für eine optimierte Kommunikation auf digitaler Basis nennt der Experte zwei bereits bestehende E-Health-Dienstleister. Zum einen das Startup „Recare“[305], welches die Kommunikation zwischen den Leistungserbringern, bspw. von Krankenhaus zu Rehaklinik, digitalisieren soll. Dies entspricht der E-Health-Form „Doc2Doc“[306]. Mit Hilfe dieses Anbieters findet, der Firmenwebseite zufolge, die Suche und Zuweisung von Versorgungsplätzen für Patienten auf einer digitalen Plattform statt und ersetzt damit langwierige Telefonate. Für jeden Patienten wird demnach ein Versorgungsprofil erstellt und anhand diesem können zum gewünschten Behandlungszeitpunkt Patientenanfragen an die Versorger gesendet werden, welche diese wiederum per Mausklick annehmen bzw. ablehnen können. Bei Annahme werden medizinische Dokumente mit den relevanten Patientendaten, bspw. die Überleitungsbögen, digital und verschlüsselt vom Sender zum Versorger übermittelt. Durch die Teilnahme an einer solchen Kommunikationsplattform wäre das Unternehmen 1 nicht mehr davon abhängig, dass der Patient die ihn betreffenden medizinischen Dokumente vor Behandlungsbeginn vollständig und in Papierform selbst mitbringt. Dies würde, wenn alle Akteure an dieser Plattform teilnehmen würden, neben der Verwaltung der Leistungserbringer, auch den Patienten selbst entlasten. Das zweite vom Experten genannte Beispiel ist der für das Jahr 2021 angekündigte „Rehamanager“[307], der speziell die Suche nach freien Rehaplätzen optimieren soll und auf dem bereits existierenden „Pflegeplatzmanager“ aufbaut. Auch hier findet die Patientenzuweisung digital statt, sodass zeitintensive Telefonate und Faxe auf ein Minimum reduziert und Medienbrüche verhindert werden können. Patientendaten, die für die Aufnahmeentscheidung benötigt werden, werden pseudonymisiert übermittelt. Durch Einbindung der Kostenträger in dieses System sollen

[304] Vgl. Kapitel 2.1.3 dieser Arbeit.
[305] Vgl. www.recaresolutions.com.
[306] Vgl. Kapitel 2.1.4 dieser Arbeit, Abbildung 5.
[307] Vgl. www.pflegeplatzmanager.de/reha-vorteile.

alle Beteiligten von einem schnellen, ressourcenschonenden und transparenten Patientenverwaltungsprozess profitieren. Darüber hinaus möchte Experte 1 eine unternehmensinterne Patientenapp einführen, die neben der Kommunikation mit dem Patienten auch den digitalen Zugriff auf Trainingspläne, Entlassberichte und andere relevante medizinische Dokumente ermöglicht. Hier fehlt es laut dem Experten aber an Schnittstellen zum bestehenden IT-System. Experte 1 fordert, bzgl. der fehlenden Harmonisierung bei der E-Health-Umsetzung in Deutschland, die Einführung einer elektronischen Patientenakte nach dänischem Vorbild. Diese soll eine zentrale Plattform für die verschiedenen Akteure im Gesundheitswesen bieten, welche die Speicherung, Zugriff und Verwaltung aller relevanten Daten und Unterlagen ermöglicht. Eine solche Plattform sieht Experte 2 in der im konzeptionellen Teil vorgestellten eGK und ePA, die mit einer digitalisierten, zentralen Informationsbasis über Vorerkrankungen, Allergien und Medikationspläne der Patienten ein verbessertes Versorgungsumfeld schaffen soll.

3.5.2.2 Datenkategorie K2

In der zweiten Datenkategorie (K2) geht es um den Einfluss und die Umsetzung von DSGVO und BDSG-neu im E-Health-Geschäft. Hierbei sollen Anhaltspunkte zu den Hypothesen 2, 3 und 4 geliefert werden. Der Einfluss der DSGVO auf das medizinische Alltagsgeschäft wird von den interviewten Experten eher kritisch gesehen. Besonders der zusätzliche Aufwand, wie die von allen Patienten obligatorisch auszufüllenden Datenschutzerklärungen, etwaige Anpassungen von Verträgen und Prozessen beim Inkrafttreten der DSGVO, zusätzliche Mitarbeiterschulungen und eine ausufernde Meldepflicht wird kritisiert. Dieser finanzielle und personelle Mehraufwand amortisiert sich Interviewpartner 2 zufolge nur durch nicht eintretende Strafen. Beispielhaft für einen vermeidbaren Aufwand nennt Experte 1, dass nicht auffindbare Patientenakten innerhalb von 24 Stunden gemeldet werden müssen, auch wenn diese kurze Zeit später wiederauftauchen und nie das Risiko eines Datenmissbrauchs bestanden hat. Ebenso kritisiert der Experte die stark variierenden Aufbewahrungs- und damit Löschfristen, denen man als Datenverarbeiter im Gesundheitswesen aus verschiedenen Rechtsvorschriften unterworfen ist: *„Die Daten in unserem IT-System müssen datenschutzkonform unter penibler Beachtung der Mindestaufbewahrungsfristen archiviert werden. Je nach Archivierungszweck variiert die Dauer dieser Fristen im Gesundheitswesen zwischen 5 und 30 Jahren, was auch einen organisatorischen Aufwand bedeutet.“* Diese Aufbewahrungsfristen sind insbesondere bei dem im konzeptionellen Teil dieser Arbeit dargestellten Betroffenenrecht auf Löschung zu beachten, dem ebendiese rechtlichen Aufbewahrungsfristen entgegenstehen können.

Allgemein herrscht eine Unsicherheit unter den Experten wegen der in Teilen unklaren Rechtslage und der latenten Gefahr von Sanktionen, die auch bei unbewussten bzw. unbeabsichtigten Verstößen gegen die DSGVO verhängt werden können. Die Vorgaben der DSGVO erscheinen den Experten häufig schwer umsetzbar und erschweren gemäß der Erfahrung von Experte 3, den Zugang zu den Kunden sowie die Kommunikation mit den verschiedenen Akteuren des Gesundheitswesens. Die Bestandteile und Instrumente der DSGVO (Abbildung 9) sind den Experten bekannt und werden weitgehend umgesetzt. In den Interviews konnte hier besonders zur praktischen Umsetzung der TOMs Praxiswissen generiert werden. Getroffene Maßnahmen zum Datenschutz im E-Health-Bereich sind der Schutz durch möglichst sichere Passwörter, Alarmanlagen, externe Serverräume, Datenzugriff nur mit Berechtigung und personenbezogenen Kennungen, Datenverschlüsselung, Firewall, Antivirusprogramm und regelmäßige Backups auf Servern. Zur Wahrung der Betroffenenrechte wurde ein Verzeichnis über die erhobenen Daten erstellt, in dem auch

Datenübermittlungen, etwa die Weitergabe von Gesundheitsdaten im akuten Notfall an Notärzte, festgehalten werden. Eine relevante Konstellation bei der Inanspruchnahme von Betroffenenrechten im Gesundheitsbereich, die sich im Rahmen der Befragungen herauskristallisiert hat, ist, dass neben dem Patienten selbst auch der gesetzliche Vertreter, etwa der rechtliche Betreuer von Demenzkranken oder nahe Angehörige hierzu aktivlegitimiert sein können. Für die DSFA wird bei den befragten Experten entweder spezielle Software in Form von Analysetools verwendet oder diese Aufgabe an eine externe Kanzlei ausgegliedert. Zusätzlich zu den im konzeptionellen Teil genannten Konstellationen einer Auftragsverarbeitung sind laut Experte 3 die Übermittlung von Daten an die Kostenträger oder der Datenaustausch mit dem medizinischen Dienst der Krankenversicherung (MDK). Alle drei Unternehmen greifen auf externe Dienstleister als DSB zurück. Die Ursache hierfür liegt entweder am besonderen Kündigungsschutz, den ein interner DSB mit sich bringen würde, oder an den gestiegenen rechtlichen Anforderungen der DSGVO, die in der mittelständischen Gesundheitsbranche intern nicht vollumfänglich bewältigt werden könnten. Die Aufgaben des DSB sind die Erarbeitung von DSGVO-relevanten Prozessen, die Beantwortung von datenschutzrechtlichen Fragen, die Datenschutzorganisation, -beratung, -prüfung, -kommunikation und -schulung sowie die Aktualisierung und Prüfung von datenschutzrechtlichen Klauseln in Verträgen und Datenschutzerklärungen. Externe DSB sind demzufolge vor allem für die Kontrolle und Information über Sachverhalte in der DSGVO-Compliance zuständig. Aus der im Fragebogen erbetenen Prioritätensetzung bzgl. der Wichtigkeit und Relevanz von DSGVO-Bestandteilen konnte kein einheitliches Bild gewonnen werden: Während Experte 1 an erster Stelle die DSFA sieht, ordnet Experte 3 die DSFA an letzter Stelle ein.

Anschließend wurden die Experten gebeten, auch bezüglich der datenschutzrechtlichen Rahmenbedingungen einen praxisrelevanten Ausblick in die Zukunft zu geben. Sie äußern sich wie folgt: Experte 1 wünscht sich vor allem eine Vereinfachung der datenschutzrechtlichen Vorgaben, um so die flächendeckende Vernetzung im E-Health-Bereich zu erleichtern. Experte 2 sieht in der immer tiefergehenden Rechtslage, die mit mehr datenschutzrechtlichen Auflagen verbunden ist, eine Herausforderung, die gesellschaftliche Teilbereiche verunsichert. Er wünscht sich, dass der Gesetzgeber bei der Rechtsentwicklung den Fokus mehr auf den Nutzen einer Datenverarbeitung als auf etwaige Risiken setzt. Experte 3 sieht die Wichtigkeit von Datenschutz in einer Zeit, die durch eine Pandemie geprägt ist, in den Hintergrund gerückt. Zum Schutz von Kunden und zum Erhalt von Unternehmen wären in solchen Ausnahmesituationen Lockerungen des Datenschutzes wünschenswert, die eine schnelle und angepasste Reaktion ermöglichen.

3.5.2.3 Datenkategorie K3

Die in Datenkategorie 3 (K3) erfragten Rechtsquellen zum Datenschutz abseits der DSGVO sind den Experten nur teilweise bekannt, bzw. werden nicht mit dem klassischen Datenschutz in Verbindung gebracht. So nennt auf Nachfrage nur ein Experte weitere Rechtsquellen, die Einfluss auf die datenschutzrechtliche Umsetzung im E-Health-Bereich haben, wie etwa das im konzeptionellen Teil behandelte E-Health-Gesetz und das DVG. Des Weiteren nennt dieser Experte das Fernbehandlungsverbot im § 7 MBO-Ä, welches bereits im Kapitel 2.1.3 als Nachteil von E-Health genannt wurde. Darüber hinaus verweist der Experte auf das Medizinproduktegesetz und das Krankenhauszukunftsgesetz, deren rechtliche Relevanz im konzeptionellen Teil nicht erarbeitet wurde.

Diese Aussage bestätigt wiederum die Vielfältigkeit von potenziellen Rechtsquellen bei dieser Thematik. Ein anderer Experte nennt als rechtlichen Einfluss die Vorgaben der Kostenträger bzgl. zugelassener Software. Demnach wird der Leistungserbringer durch externe Vorgaben in der Wahl seiner Softwaresysteme eingeschränkt. Da die reibungslose Zusammenarbeit mit den Kostenträgern für die Gesundheitsdienstleister existenziell ist, lässt sich daraus schließen, dass neben den Gesetzen und Verordnungen des Gesetzgebers auch die Vorgaben der anderen Akteure im Gesundheitswesen die E-Health-Umsetzung in der Praxis beeinflusst.

Abschließend lassen sich mit der Auswertung und Interpretation der Expertenantworten folgende Überschneidungen erkennen:

- E-Health ist bei der internen Arbeitsabwicklung und in der Leistungsabrechnung mit den Kostenträgern bereits etabliert. Ausbaubedarf besteht bei der Kommunikation mit Patienten und anderen Leistungserbringern.
- E-Health bringt Effizienz- und Effektivitätsvorteile mit sich. Datenschutzrechtliche Vorgaben verursachen einen Mehraufwand und eine Unsicherheit bei den jeweiligen Akteuren im Gesundheitswesen.

3.6 Hypothesenprüfung und Handlungsempfehlungen

3.6.1 Prüfung der Hypothesen

Die gewonnenen Erkenntnisse werden nachstehend in Verbindung mit den im konzeptionellen Teil erarbeiteten Grundlagen analysiert, um die aufgestellten Hypothesen zu belegen bzw. widerlegen und anschließend die Forschungsfrage zu beantworten.

Hypothese 1:

Nullhypothese: Die E-Health-Umsetzung in Deutschland ist weit vorangeschritten und ein wichtiger Bestandteil in der beruflichen Praxis.

Alternativhypothese: Die E-Health-Umsetzung in Deutschland ist nicht weit vorangeschritten und kein wichtiger Bestandteil in der beruflichen Praxis.

Die Analyse der ausgewerteten Experteninterviews zeigt, dass im mittelständischen Gesundheitsbereich die Informationsübermittlung zu anderen Akteuren im Medizinwesen (Doc2Doc, Doc2Pat) auch im Jahr 2021 überwiegend mit Hilfe von traditionellen Kommunikationsmitteln wie Fax, Telefon und Brief stattfindet. Hier fehlt es bislang an einer digitalen Plattform, an der sich alle externen Stakeholder beteiligen. Ob sich diese mit der zunehmenden Einführung der ePA in Deutschland etabliert, werden die kommenden Jahre zeigen. Eine Ausnahme ist die Datenübermittlung an Kostenträger zur Leistungsabrechnung, die bereits weitestgehend digital stattfindet. Diese Digitalisierung der Leistungsabrechnung wird vom Gesetzgeber forciert und ist im SGB V gesetzlich festgeschrieben. In der internen Arbeitsabwicklung spielt E-Health, etwa in Form von Apps auf Tablets und Smartphones, bereits eine bedeutende Rolle. Apps werden sowohl zur Unterstützung von Patienten in der Therapie als auch zur flexiblen Datenerfassung und den schnellen Zugriff auf Informationen für das Management und die Mitarbeiter verwendet. Daraus lässt sich schlussfolgern, dass, obwohl das Potential von E-Health als externes Kommunikationsmittel noch nicht vollumfänglich ausgeschöpft wird, die Nullhypothese belegt werden kann,

da die Nutzung von Software und Apps im internen Arbeitsalltag bereits als essentieller Geschäftsbestandteil gesehen wird und mithin weit vorangeschritten ist, auch wenn hier, gerade im Vergleich zu anderen EU-Ländern, in Deutschland noch Ausbaubedarf besteht.

Hypothese 2:

Nullhypothese: Es gibt ein Spannungsfeld zwischen Datenschutz und E-Health.

Alternativhypothese: Es gibt kein Spannungsfeld zwischen Datenschutz und E-Health

Der aus den datenschutzrechtlichen Vorgaben resultierende Mehraufwand wird von den Experten durchweg kritisch betrachtet. Prozesse und Instrumente, die speziell zur DSGVO-Compliance eingerichtet, angepasst und umgesetzt werden müssen, lenken die Gesundheitsdienstleister von ihrem Alltagsgeschäft ab. Ein Experte, der im Vergleich zu den anderen Experten relativ wenige E-Health-Anwendungen in seinem Arbeitsalltag integriert hat, sieht die Ursache hierfür beim Datenschutz: „*Für mich ist es schwierig, diese Frage [bzgl. der Vor- und Nachteile von E-Health, Anm. des Autors] zu beantworten, da wir im Gesamten betrachtet noch recht wenig im Bereich E-Health haben - da spielt der Datenschutz wirklich eine große Rolle.* Das verbesserte Versorgungsumfeld durch E-Health wird begleitet von einer latenten Angst vor datenschutzgesetzlichen Sanktionierungen. Dieses Spannungsfeld wird durch eine aus Sicht der Experten komplizierten und immer tiefergehenden Rechtslage und den vermeintlichen Fokus des Gesetzgebers auf die Risiken von Datenverarbeitungen verstärkt. Ausgehend von den durchgeführten qualitativen Befragungen lässt sich belegen, dass zumindest in der mittelständischen Medizinbranche die Nullhypothese zutreffend ist.

Hypothese 3:

Nullhypothese: Außer der DSGVO haben auch andere Rechtsquellen einen erheblichen Einfluss auf die datenschutzrechtliche Umsetzung im E-Health-Bereich.

Alternativhypothese: Außer der DSGVO haben andere Rechtsquellen keinen erheblichen Einfluss auf die datenschutzrechtliche Umsetzung im E-Health-Bereich.

Die Expertenbefragungen haben bezüglich des Einflusses anderer Rechtsquellen ein geteiltes Bild ergeben. Die Vorgaben der DSGVO dominieren die Umsetzung des Datenschutzes in den Unternehmen, so wird bspw. die gesetzlich kodifizierte ärztliche Schweigepflicht, welche im konzeptionellen Teil dieser Arbeit erläutert wird, mit dem allgemeinen Datenschutz bei der E-Health-Umsetzung gar nicht erst in Verbindung gebracht. Außer den bereits in Kapitel 2.2.2 erarbeiteten Rechtsquellen werden das Medizinproduktegesetz und das Krankenhauszukunftsgesetz genannt, welche einen Einfluss auf die Umsetzung im E-Health-Bereich haben. Mithin lassen sich weder Null- noch Alternativhypothese eindeutig widerlegen, tendenziell beherrscht jedoch die DSGVO die Datenschutzumsetzung in der Praxis.

Hypothese 4:

Nullhypothese: Die verschiedenen Bestandteile und Instrumente der DSGVO überfordern Unternehmen in der Praxis.

Alternativhypothese: Die verschiedenen Bestandteile und Instrumente der DSGVO überfordern Unternehmen in der Praxis nicht.

In den befragten Unternehmen werden externe Dienstleister und/oder Kanzleien zur DSGVO-Compliance beauftragt: *„Anfangs wurde ein Mitarbeiter intern zum Datenschutzbeauftragten ausgebildet. Im Zuge der Weiterbildung wurde schnell klar, dass die Erfüllung aller Anforderungen in einem mittelständischen Unternehmen nicht intern umsetzbar ist. Zeitnah wurde ein externer Dienstleister hinzugezogen.“* So wie dieser Experte geben alle drei Experten an, dass spätestens seit Einführung der DSGVO auf externe DSB zurückgegriffen wird. Auch die Kritik am zusätzlichen Aufwand und bezüglich einer schweren Umsetzbarkeit der datenschutzrechtlichen Vorgaben lassen eine Überforderung erkennen. Demnach liegt eine interne Überforderung zumindest bei mittelständischen Unternehmen im Gesundheitsbereich vor, womit sich die Nullhypothese verifizieren lässt.

Forschungsfrage:
Welche Auswirkungen hat das Datenschutzrecht auf die Digitalisierung im deutschen Gesundheitswesen?

Die Auswertung der Experteninterviews hat ergeben, dass E-Health von Gesundheitsdienstleistern als unverzichtbarer Geschäftsbestandteil betrachtet wird und mit vielen Vorteilen im Arbeitsablauf verbunden ist. Die aus den rechtlichen Rahmenbedingungen hervorgehenden Vorgaben zum Datenschutz bei E-Health verunsichern die Leistungserbringer jedoch und bringen einen Mehraufwand mit sich, was zu einem Spannungsfeld zwischen E-Health und Datenschutz führt. Grundsätzlich lässt die Analyse der Experteninterviews darauf schließen, dass die verschiedenen Bestandteile und Instrumente der DSGVO die Leistungserbringer überfordern, da diese bspw. regelmäßig auf das Knowhow von externen Datenschutzexperten zugreifen müssen. Der datenschutzrechtliche Rahmen von E-Health wird von der DSGVO dominiert. Doch auch andere Gesetze und Vorschriften, wie etwa die im Kapitel 2.2.2 präsentierten Rechtsquellen, haben einen Einfluss auf die Digitalisierung im Gesundheitswesen, was die Rechtslage für die Leistungserbringer intransparent macht. Zur besseren Umsetzbarkeit von E-Health und um diesbezüglich mehr Transparenz und Klarheit zu schaffen, wäre aus Sicht der Experten eine Vereinfachung des Datenschutzrechts in Deutschland wünschenswert.

3.6.2 Handlungsempfehlungen

Im Folgenden werden drei prägnante Handlungsempfehlungen formuliert. Aufgrund der unterschiedlichen Ansprüche und Aufgabengebiete der jeweiligen Akteure im E-Health-Bereich wird für Leistungsempfänger, Leistungserbringer und Staat bzw. Politik jeweils eine eigene, differenzierte Handlungsempfehlung verfasst.

Für Leistungserbringer:

Unternehmen und im Gesundheitsbereich Tätige, die in Zukunft mehr E-Health-Leistungen anbieten wollen, sollten sich von den datenschutzrechtlichen Vorgaben nicht entmutigen lassen. Die Umsetzung der TOMs und des Grundsatzes der Integrität und Vertraulichkeit, also die Optimierung der IT-Sicherheit, dient nicht nur der Erfüllung von datenschutzrechtlichen Vorgaben, sondern minimiert auch etwaige von den Experten genannte Risiken von E-Health in Form von Systemausfällen und Hackerangriffen. Bspw. helfen Firewalls präventiv vor Angriffen von außen auf das eigene IT-System und kurze Backup-Intervalle, also regelmäßige Datensicherungen in kurzen zeitlichen Abständen, beugen etwaigem Datenverlust vor. So können durch die DSGVO-Compliance Synergien realisiert werden, die den Aufwand aus unternehmerischer Sicht rechtfertigen und das in

Hypothese 2 festgestellte Spannungsfeld zwischen Datenschutz und E-Health entkräftigen.

Für Leistungsempfänger:

Die DSGVO bietet wirksame Instrumente zur Durchsetzung der datenschutzrechtlichen Interessen von Patienten. Betroffenenrechte ermöglichen es Patienten jederzeit, einen Einblick in ihre von den Leistungserbringern verarbeiteten Gesundheitsdaten zu bekommen. Die Geltendmachung dieser Rechte bedeuten einen großen Schritt in Richtung Patienten- und Datensouveränität und sind in Anbetracht der Sensibilität der von den Patienten erhobenen Daten richtig und wichtig. Gerade Patienten- und Gesundheitsdaten unterliegen als besondere Datenkategorie einem ausgeprägten gesetzlichen Schutz. Bürger und Patienten sollten sich aufgrund der für sie vorteilhaften Rechtslage nicht scheuen, digitale Technologien im Gesundheitswesen in Anspruch zu nehmen und bspw. auch Apps, die eine effizientere Behandlung und Prävention ermöglichen, nutzen.

Für Staat und Politik:

Die Leistungserbringer im Gesundheitswesen fühlen sich durch die ständig wandelnde, immer tiefergehende und sanktionsbewehrte Gesetzgebung verunsichert. Der Gesetzgeber sollte die Bedürfnisse und Sorgen der Gesundheitsdienstleister ernstnehmen und eine mit dem Datenschutz vereinbare Digitalisierung im Gesundheitswesen mit Anreizen statt mit Strafen und einer klaren, transparenten Rechtslage vorantreiben. Dahingehend sollte der Fokus mehr auf den Zweck und Nutzen als auf die Risiken einer Datenverarbeitung gelegt werden. Hierbei könnte die Umsetzung datenschutzrechtlicher Maßnahmen von medizinischen Unternehmen, zu deren Kerngeschäft regelmäßig nicht die Datenschutzcompliance gehört, vom Staat finanziell und fachlich unterstützt werden. Dies könnte z.B. in Form von Subventionierung digitaler Schutzmaßnahmen und aktiver Hilfe von Experten in den Datenschutzbehörden geschehen.

4 Fazit

Die abschließende Betrachtung wird die gewonnenen Erkenntnisse wiedergeben und diese Arbeit kritisch würdigen sowie Ansatzpunkte für weitere Untersuchungen liefern. Ziel der Arbeit war es, die datenschutzrechtlichen Rahmenbedingungen von E-Health in Deutschland zu analysieren und dem Leser einen datenschutzrechtlichen Überblick über die Digitalisierung im Gesundheitswesen zu verschaffen. Die rechtlichen Rahmenbedingungen von E-Health in Bezug auf Datenschutz werden im konzeptionellen Teil beleuchtet und im empirischen Teil mit Hilfe von drei Experteninterviews verifiziert und auf ihre praktische Umsetzung hin weiter ausgeführt. In dieser Arbeit wird nicht nur ein Einblick in den datenschutzrechtlichen Rahmen von E-Health gewährt, indem die Bestandteile und Instrumente der DSGVO ausführlich dargestellt werden, sondern auch aufgezeigt, welche Vor- und Nachteile mit E-Health verbunden sind und wie die Umsetzung theoretisch und in der Praxis erfolgt. Es ist festzustellen, dass unabhängig davon, ob die Datenverarbeitung im Gesundheitswesen analog oder digital stattfindet, im Grunde die gleichen datenschutzrechtlichen Vorgaben beachtet werden müssen. Der Gesetzgeber zielt nicht auf die Form der Datenverarbeitung, sondern auf die Kategorie der verarbeiteten Daten. Gesundheits- bzw. Patientendaten werden mit einem besonderen Schutzniveau privilegiert. Mithin ist der Komplex „Datenschutz und E-Health“ schwer von Datenschutz im Gesund-

heitswesen allgemein abzugrenzen. Die enorme Relevanz des Datenschutzes für Leistungserbringer ergibt sich aus den existenzbedrohenden Sanktionen bei Non-Compliance in diesem Bereich, die von Geldbußen in Millionenhöhe (DSGVO) bis hin zu Haftstrafen (StGB, BDSG-neu) reichen. Doch auch die Leistungsempfänger haben an den Verarbeitungsumständen ihrer sensibelsten Daten naturgemäß ein Eigeninteresse. Die Vielzahl an Rechtsquellen (DSGVO/BDSG-neu, SGB, gesetzlich kodifizierte Schweigepflicht, etc.), die im zweiten Kapitel dieser Arbeit dargestellt werden, erschwert nicht nur den Akteuren im Gesundheitswesen, sondern auch dem Autor dieser Arbeit die intensive und detaillierte Auseinandersetzung mit der juristischen Thematik. Die in den letzten Jahren verabschiedeten (E-Health-Gesetz, PDSG) und zum jetzigen Zeitpunkt noch diskutierten (TrApp-FZG) Gesetze, sorgen für eine Unbeständigkeit der Rechtslage im E-Health-Bereich.

Während diese Arbeit als Leitfaden für die Akteure im Gesundheitswesen zum Thema Datenschutz und E-Health allgemein dienen kann, könnten folgende Forschungsarbeiten den ständigen Wandel der hiesigen Rechtslage und die hieraus resultierenden Auswirkungen auf E-Health betrachten. Überdies könnte eine empirische Untersuchung darüber stattfinden, welchen Stellenwert die Patienten selbst dem Datenschutz bei der Inanspruchnahme von E-Health-Dienstleistungen beimessen, um so die Vereinbarkeit von E-Health und Datenschutz weiter zu vertiefen und für beide Seiten akzeptable Lösungen zu finden. Darüber hinaus könnte unter Anwendung einer quantitativen Forschungsmethode festgestellt werden, ob die Erkenntnisse aus den Experteninterviews auch für die breite Masse der Leistungserbringer im E-Health-Bereich repräsentativ sind.

5 LITERATURVERZEICHNIS

Konferenz der Datenschutzbeauftragten des Bundes und der Länder (2015): Entschließung: Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich. Online verfügbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/ 2015/2015-DSK-eHealth.pdf, zuletzt geprüft am 11.12.2020.

Aanestad, Margunn; Grisot, Miria; Hanseth, Ole; Vassilakopoulou, Polyxeni (2017): Information Infrastructures within European Health Care. Working with the Installed Base. Cham, Switzerland: Springer (Health Informatics, ISSN: 1431-1917).

Andelfinger, Volker P.; Hanisch, Till (2016): eHealth. Wie Smartphones, Apps und Wearables die Gesundheitsversorgung verändern werden. 1. Aufl. Wiesbaden: Springer Gabler.

AOK Bundesverband (o.J.): Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation. Digitale-Versorgung-Gesetz (DVG). Online verfügbar unter https://www.aok-bv.de/hintergrund/gesetze/index_22127.html, zuletzt geprüft am 29.12.2020.

Apfel, Petra (2020): Jameda-CEO: „Das Interesse an Videosprechstunden ist durch Corona explodiert“, 25.03.2020. Online verfügbar unter https://www.focus.de/gesundheit/news/ krise-als-katalysator-fuer-telemedizin-jameda-ceo-das-interesse-an-videosprechstunden-ist-durch-corona-explodiert_id_11810914.html, zuletzt geprüft am 03.11.2020.

ARD/ZDF-Forschungskommission (Pressemitteilung vom 08.10.2020): ARD/ZDF-Onlinestudie 2020. Zahl der Internetnutzer wächst um 3,5 Millionen. Frankfurt am Main. Online verfügbar unter https://www.ard-zdf-onlinestudie.de/files/2020/ Pressemitteilung_ARD_ZDF_Onlinestudie_2020.pdf, zuletzt geprüft am 03.11.2020.

ARTIKEL-29-DATENSCHUTZGRUPPE (2017a): WP 243 Rev. 01 - 16/DE. Leitlinien in Bezug auf Datenschutzbeauftragte ("DSB"). Unter Mitarbeit von Isabelle Falque-Pierrotin. Online verfügbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/ Dokumente-Art29Gruppe_EDSA/Guidelines/WP243_DPO_DE.html.

ARTIKEL-29-DATENSCHUTZGRUPPE (2017b): WP 248 Rev. 01 - 17/DE. Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“. Unter Mitarbeit von Isabelle Falque-Pierrotin. Online verfügbar unter https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP248_LeitlinienZurDatenschutzFolgenabschaetzung.html.

Ärztekammer Berlin (o.J.): Die Berufsordnung und ihre Durchsetzung. Online verfügbar unter https://www.aerztekammer-berlin.de/10arzt/30_Berufsrecht/ 08_Berufsrechtliches/ 02_Berufsordnung_und_Durchsetzung/05_BODurchs.html, zuletzt geprüft am 11.12.2020.

Bauer, Christoph; Eickmeier, Frank; Eckard, Michael; Kafke, Kerstin; Klette, Daniela; Schwaner, Astrid (2018): E-Health: Datenschutz und Datensicherheit. Herausforderungen und Lösungen im IoT-Zeitalter. 1. Aufl. Wiesbaden: Springer Gabler.

Bayerisches Landesamt für Datenschutzaufsicht (2018): FAQ zur DS-GVO. Was ist Auftragsverarbeitung und was nicht? Online verfügbar unter https://www.lda.bayern.de/media/ FAQ_Abgrenzung_Auftragsverarbeitung.pdf, zuletzt geprüft am 26.11.2020.

Becker, Dirk; Eschenbach, Jessica (2020): Ein Chip, viele Funktionen: Das kann die elektronische Gesundheitskarte. In: *Presseportal.de*, 2020. Online verfügbar unter https://www.presseportal.de/pm/53836/4494493, zuletzt geprüft am 29.12.2020.

Beuth, Patrick; Höflinger, Laura; Knobbe, Martin; Rojkov, Alexandra; Rosenbach, Marcel; Schindler, Jörg (2020): Überwachung per Corona-App. Die dunkle Seite der Wunderwaffe. In: *DER SPIEGEL (online)*, 24.04.2020. Online verfügbar unter https://www.spiegel.de/netzwelt/netzpolitik/corona-app-die-dunkle-seite-der-wunderwaffe-a-00000000-0002-0001-0000-000170604442, zuletzt geprüft am 03.11.2020.

Bitkom e.V. (Pressemitteilung vom 09.02.2016): Fast ein Drittel nutzt Fitness-Tracker. Konferenz von BMJV und Bitkom zum Thema „Am Puls der Zeit? – Wearables und Gesundheits-Apps“. Berlin. Online verfügbar unter https://www.bitkom.org/Presse/Presseinformation/Gemeinsame-Presseinfo-von-Bitkom-und-BMJV-Fast-ein-Drittel-nutzt-Fitness-Tracker.html, zuletzt geprüft am 03.11.2020.

Bitkom e.V.; Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2017): Begleitende Hinweise zu der Anlage Auftragsverarbeitung. Leitfaden. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/170515-LF-Auftragsverarbeitung-online.pdf, zuletzt geprüft am 29.11.2020.

Blöbaum, Bernd; Nölleke, Daniel; Scheu, Andreas M. (2014): Handbuch nicht standardisierte Methoden in der Kommunikationswissenschaft. Das Experteninterview in der Kommunikationswissenschaft: Springer Fachmedien Wiesbaden. Online verfügbar unter https://link.springer.com/content/pdf/10.1007%2F978-3-658-05723-7_11-1.pdf.

Bogner, Alexander; Littig, Beate; Menz, Wolfgang (2014): Interviews mit Experten. Eine praxisorientierte Einführung. 1. Aufl. Wiesbaden: Springer Fachmedien Wiesbaden.

Böhm, Andreas (2019): Auftragsverarbeitung, Art. 28 DSGVO. Online verfügbar unter https://boehmanwaltskanzlei.de/auftragsverarbeitung, zuletzt geprüft am 22.11.2020.

Buchner, Benedikt: Datenschutz und Datensicherheit in der digitalisierten Medizin. In: MedR (Medizinrecht), Bd. 34, S. 660–664.

Bundesärztekammer (2018): Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis. In: *Deutsches Ärzteblatt*. Online verfügbar unter https://www.bpm-ev.de/images/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf, zuletzt geprüft am 06.02.2021.

Bundesgesundheitsministerium (2020c): Ärzte sollen Apps verschreiben können. Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz - DVG). Online verfügbar unter https://www.bundesgesundheitsministerium.de/digitale-versorgung-gesetz.html, zuletzt geprüft am 29.12.2020.

Bundesgesundheitsministerium (2020a): Elektronische Gesundheitskarte (eGK). Die elektronische Gesundheitskarte. Online verfügbar unter https://www.bundesgesundheits-

ministerium.de/themen/krankenversicherung/egk.html#c1063, zuletzt geprüft am 09.12.2020.

Bundesgesundheitsministerium (2020b): Fragen und Antworten zur elektronischen Patientenakte. Online verfügbar unter https://www.bundesgesundheitsministerium.de/elektronische-patientenakte.html, zuletzt geprüft am 18.12.2020.

Bundesgesundheitsministerium (2020d): Patientendaten-Schutz-Gesetz. Online verfügbar unter https://www.bundesgesundheitsministerium.de/patientendaten-schutz-gesetz.html, zuletzt geprüft am 02.01.2021.

Bundesgesundheitsministerium (2015): Pressemitteilung Nr. 45. Hermann Gröhe: „Patientennutzen und Datenschutz im Mittelpunkt". 2./3. Lesung des E-Health-Gesetzes im Bundestag. Online verfügbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/4_Pressemitteilungen/2015/2015_4/151203-45_PM_E-Health-Gesetz.pdf, zuletzt geprüft am 02.01.2021.

Bundesministerium für Gesundheit (o.J.): Glossar. E-Health. Online verfügbar unter https://www.bundesgesundheitsministerium.de/service/begriffe-von-a-z/e/e-health.html, zuletzt geprüft am 03.11.2020.

Bundesministerium für Gesundheit (2020): E-Health – Digitalisierung im Gesundheitswesen. Online verfügbar unter https://www.bundesgesundheitsministerium.de/e-health-initiative.html, zuletzt geprüft am 08.11.2020.

Bundesrechtsanwaltskammer (2020): Sozialgesetzbuch – Erstes Buch (SGB I) – Allgemeiner Teil. Online verfügbar unter https://brak.de/die-brak/organisation/ausschuesse-und-gremien-der-brak/ausschuss-sozialrecht/sgb-i-bis-xii/sgb-i-allgemeiner-teil/, zuletzt geprüft am 02.01.2021.

Bundesverband für Medizintechnologie, Aktion Meditech (2015): Telekardiologie: Home Monitoring rettet Leben und verbessert die Patientenversorgung. Online verfügbar unter https://www.aktion-meditech.de/presse/pressemeldungen/pm-2015-03-01.html, zuletzt geprüft am 29.12.2020.

Datenschutzkonferenz (2018): Offizielles Kurzpapier der DSK. Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist. Version 1.1. Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf, zuletzt geprüft am 07.12.2020.

Della Mea, Vincenzo (2001): What is e-health (2): the death of telemedicine? In: *Journal of Medical Internet Research* 3 (2), E22. DOI: 10.2196/jmir.3.2.e22.

Der Bayerische Landesbeauftragte für den Datenschutz (2019): Auftragsverarbeitung. Orientierungshilfe. Online verfügbar unter https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf, zuletzt geprüft am 26.11.2020.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2016): Datenschutz-Grundverordnung. BfDI-Info 6. Online verfügbar unter https://www.uni-paderborn.de/fileadmin/datenschutz/INFO6.pdf, zuletzt geprüft am 26.11.2020.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (2019): Geldbuße gegen Krankenhaus aufgrund von Datenschutz-Defiziten beim Patien-

tenmanagement. Online verfügbar unter https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/, zuletzt geprüft am 07.12.2020.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie; Berufsverband der Datenschutzbeauftragten Deutschlands e. V.; Bundesverband Gesundheits-IT e. V.; Deutsche Krankenhausgesellschaft e. V.; Gesellschaft für Datenschutz und Datensicherheit e. V. (2018): Muster-Auftragsverarbeitungs-Vertrag für das Gesundheitswesen. Online verfügbar unter https://www.gesundheitsdatenschutz.org/download/Muster-AV-Vertrag_2018.pdf, zuletzt geprüft am 29.11.2020.

Deutscher Bundestag (2017): Drucksache 18/11936. Gesetzentwurf der Bundesregierung: Entwurf eines Gesetzes zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen 18. Wahlperiode. Online verfügbar unter https://dip21.bundestag.de/dip21/btd/18/119/1811936.pdf, zuletzt geprüft am 06.02.2021.

Die Landesbeauftragte für den Datenschutz Niedersachsen (2019): DS-GVO im Gesundheitsbereich. Häufige Fragen und Antworten. Online verfügbar unter https://lfd.niedersachsen.de/startseite/infothek/faqs_zur_ds_gvo/ds-gvo-im-gesundheitsbereich-166950.html, zuletzt geprüft am 22.11.2020.

Dudenredaktion (o.J.): "E-Health" auf Duden online. Online verfügbar unter https://www.duden.de/rechtschreibung/E_Health, zuletzt geprüft am 03.11.2020.

Eckhardt, Jens (2020): Schadenersatzansprüche: Das unterschätzte Risiko der DSGVO. Online verfügbar unter https://www.datenschutz-praxis.de/fachartikel/schadenersatzansprueche-das-unterschaetzte-risiko-der-dsgvo/, zuletzt geprüft am 09.12.2020.

Eysenbach, Gunther (2001): What is e-health? In: *Journal of Medical Internet Research* 3 (2), E20. DOI: 10.2196/jmir.3.2.e20.

Fischer, Florian; Krämer, Alexander (2016): eHealth in Deutschland. Anforderungen und Potenziale innovativer Versorgungsstrukturen. Berlin: Springer Vieweg.

G-BA Gemeinsamer Bundesausschuss (Pressemitteilung vom 16.07.2020): Arbeitsunfähigkeits-Richtlinie: Krankschreibung künftig per Videosprechstunde möglich. Pressemitteilung Nr. 35 / 2020. Online verfügbar unter https://www.g-ba.de/downloads/34-215-879/35_2020-07-16_AU-RL_Fernbehandlung.pdf, zuletzt geprüft am 03.11.2020.

GDD e.V. (2020): Corona-Warn-App (CWA) - Expertenbeiträge und Ansichten der Aufsichtsbehörden. Online verfügbar unter https://www.gdd.de/datenschutz-und-corona/Datenspende%20Apps%20und%20Corona%20Tracing, zuletzt geprüft am 29.12.2020.

Handelsblatt (2020): Mutmaßlicher Hackerangriff: IT-Ausfall an Uniklinik Düsseldorf betrifft immer mehr Patienten. Der IT-Ausfall an der Uniklinik Düsseldorf hat gravierende Folgen. Für immer mehr Patienten fallen Termine aus, die oft im Voraus vergeben wurden. In: *Handelsblatt*, 15.09.2020. Online verfügbar unter https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-mutmasslicher-hackerangriff-it-ausfall-an-uniklinik-duesseldorf-betrifft-immer-mehr-patienten/26190142.html, zuletzt geprüft am 17.01.2021.

Hiller, Janine; Bélanger, France (2001): Privacy Strategies for Electronic Government. Online verfügbar unter http://www.businessofgovernment.org/sites/default/files/ PrivacyStrategies.pdf, zuletzt geprüft am 17.11.2020.

Jäschke, Thomas; et al. (2018): Datenschutz und Informationssicherheit Gesundheitswesen. Grundlagen, Konzepte, Umsetzung. 2., aktualisierte und erweiterte Auflage. Berlin: MWV Medizinisch Wissenschaftliche Verlagsgesellschaft.

Juraschko, Bernd (2020): Praxishandbuch Recht für Bibliotheken und Informationseinrichtungen. 2. Aufl. Berlin: De Gruyter Saur.

Kassenärztliche Bundesvereinigung (2020b): KBV PraxisInfo. Coronavirus: Hinweise zur Videosprechstunde. Online verfügbar unter https://www.kbv.de/media/sp/PraxisInfo_ Coronavirus_Videosprechstunde.pdf, zuletzt geprüft am 29.12.2020.

Kassenärztliche Bundesvereinigung (2020a): Videosprechstunde. Kassenärztliche Bundesvereinigung (KBV). Online verfügbar unter https://www.kbv.de/html/videosprechstunde.php, zuletzt geprüft am 29.12.2020.

Kassenärztliche Bundesvereinigung (2015): Stellungnahme der Kassenärztlichen Bundesvereinigung vom 28. Oktober 2015. zum Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen. Online verfügbar unter https://www.kbv.de/media/sp/Stellungnahme_KBV_eHealth.pdf, zuletzt geprüft am 02.01.2021.

Kerkmann, Christof; Nagel, Lars-Marten (2020): Cyberkriminalität: Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf. Eine Patientin stirbt, nachdem ihr Rettungswagen wegen einer Cyberattacke umgeleitet werden musste. Der Fall illustriert die wachsenden IT-Risiken. In: *Handelsblatt*, 18.09.2020. Online verfügbar unter https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html, zuletzt geprüft am 16.02.2021.

Klein, Manfred (2017): Was ist eHealth? In: *eGovernment Computing*, 11.01.2017. Online verfügbar unter https://www.egovernment-computing.de/was-ist-ehealth-a-570980/, zuletzt geprüft am 03.01.2021.

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Was ist der räumliche Anwendungsbereich? Düsseldorf. Online verfügbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/EU-Datenschutzreform__FAQ_/Was_ist_der_r__umliche_Anwendungsbereich_.php, zuletzt geprüft am 22.01.2021.

Matusiewicz, David; Thielscher, Christian (2017): Die digitale Transformation im Gesundheitswesen. Transformation, Innovation, Disruption. Berlin: Medizinisch Wissenschaftliche Verlagsgesellschaft.

McKinsey & Company (2018): Digitalisierung im Gesundheitswesen: die Chancen für Deutschland. Online verfügbar unter https://www.mckinsey.de/~/media/mckinsey/ locations/europe%20and%20middle%20east/deutschland/news/presse/2018/2018-09-25-digitalisierung%20im%20gesundheitswesen/langfassung%20digitalisierung%20im%20gesundheitswesen__neu.pdf, zuletzt geprüft am 15.11.2020.

Meister, Sven; Deiters, Wolfgang; Becker, Stefan (2016): Digital health and digital biomarkers – enabling value chains on health data. In: *Current Directions in Biomedical Engineering* 2 (1), S. 577–581. DOI: 10.1515/cdbme-2016-0128.

Müller-Mielitz, Stefan; Lux, Thomas (2017): E-Health-Ökonomie. 1. Aufl. Wiesbaden: Springer Gabler.

Noll, Andreas (2020): Zwei Wochen Corona-Warn-App: Läuft! In: *Deutschlandfunk-Nova*, 02.07.2020. Online verfügbar unter https://www.deutschlandfunknova.de/beitrag/zwei-wochen-corona-warn-app-ueber-datenschutz-downloads-und-fehlermeldungen, zuletzt geprüft am 03.11.2020.

PwC (2016): Weiterentwicklung der eHealth-Strategie. Studie im Auftrag des Bundesministeriums für Gesundheit. Unter Mitarbeit von Dr. Rainer Bernnat, Frederik Blachetta, Marcus Bauer, Dr. Nicolai Bieber, Karl Poerschke, Dr. Thomas Solbach. PwC Strategy&. Berlin. Online verfügbar unter https://www.bundesgesundheitsministerium.de/ fileadmin/Dateien/3_Downloads/E/eHealth/BMG-Weiterentwicklung_der_eHealth-Strategie-Abschlussfassung.pdf, zuletzt geprüft am 05.11.2020.

PwC (2017): Effizienzpotentiale durch eHealth. Studie im Auftrag des Bundesverbands Gesundheits-IT – bvitg e.V. und der CompuGroup Medical SE. Online verfügbar unter https://www.strategyand.pwc.com/de/de/studien/2017/potentiale-ehealth/effizienzpotentiale-durch-ehealth.pdf, zuletzt geprüft am 10.11.2020.

RKI (2020): Coronavirus SARS-CoV-2. Infektionsketten digital unterbrechen mit der Corona-Warn-App. Online verfügbar unter https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html;jsessionid=B0242E60DC8CC253947C D68711280430.internet061?nn=13490888#doc14201188bodyText7, zuletzt geprüft am 29.12.2020.

Schäfer, Kathrin (2019): E-Health betrifft alle. In: *devicemed.de*, 07.11.2019. Online verfügbar unter https://www.devicemed.de/e-health-betrifft-alle-a-880857/, zuletzt geprüft am 08.11.2020.

Scheu, Andreas; Volpers, Anna-Maria; Summ, Annika; Blöbaum, Bernd (2014): Von der Gutenberg-Galaxis zur Google-Galaxis. Medialisierung von Forschungspolitik. Wahrnehmung von und Anpassung an Medienlogik. Konstanz, München: UVK-Verl.-Ges (Schriftenreihe der Deutschen Gesellschaft für Publizistik- und Kommunikationswissenschaft, Bd. 41).

Schmidt, Christian; Hillebrandt, Berndt (2016): Patientenversorgung im digitalen Zeitalter. In: *Arzt und Krankenhaus* 89 (5), S. 184–188. Online verfügbar unter https://docplayer.org/156519354-Arzt-und-krankenhaus-digital-health-eine-chance-fuer-die-medizin-planungsrelevante-qualitaetsindikatoren-das-iqtig-macht-ernst.html.

Schütze, Bernd: Änderung der Schweigepflicht: § 203 StGB und ein bisschen mehr. Informationen zur Anpassung des § 203 StGB 2017-10. Online verfügbar unter https://gesundheitsdatenschutz.org/download/201901_14_Paragraph-203-StGB.pdf, zuletzt geprüft am 06.02.2021.

Spahn, Jens (2020): BULLETIN DER BUNDESREGIERUNG Nr. 74-2. Rede des Bundesministers für Gesundheit, Jens Spahn, zum Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG). Bundes-

regierung. Deutscher Bundestag. Berlin, 03.07.2020. Online verfügbar unter https://www.bundesregierung.de/breg-de/service/bulletin/rede-des-bundesministers-fuer-gesundheit-jens-spahn--1768966, zuletzt geprüft am 03.11.2020.

Stark, Jeannette (2018): Wir schaffen Begriffsklarheit in der eHealth-Domäne. Hg. v. Fakultät Wirtschaftswissenschaften. TU Dresden. Online verfügbar unter https://tu-dresden.de/bu/wirtschaft/winf/sysent/die-professur/news/wir-schaffen-begriffsklarheit-in-der-ehealth-domaene, zuletzt geprüft am 15.11.2020.

Walter, Axel von; Klein (Hg.) (2018): Datenschutz im Betrieb. Die DSGVO in der Personalarbeit. Datenschutz im Betrieb. 1. Auflage. Freiburg: Haufe Group.

Weichert, Thilo (2014): Big Data, Gesundheit und der Datenschutz. In: *Datenschutz und Datensicherheit - DuD* 38 (12), S. 831–838. DOI: 10.1007/s11623-014-0328-x.

6 ANHANG: FRAGEBOGEN

Themenblock 1: Individuelle Attribute des Interviewpartners

1. Könnten Sie zu Beginn kurz Ihr Unternehmen systematisieren? Insbesondere auf welchen Märkten bzw. Geschäftsfeldern des Gesundheitswesens das Unternehmen aktiv ist und wie viele Mitarbeiter beschäftigt sind.
2. Welche Position nehmen Sie im Unternehmen ein? (Hierarchieebene, Verantwortungsbereich)

Themenblock 2: E-Health

3. Wie wird E-Health in Ihrem Unternehmen umgesetzt?

   3* Welche Formen von E-Health sind hervorzuheben und besonders relevant für das Alltagsgeschäft?

4. Welche Chancen und Vorteile ergeben sich durch E-Health in Ihrem Unternehmen?

5. Mit welchen Risiken und Nachteilen sehen Sie sich konfrontiert?

Themenblock 3: Rechtlicher Rahmen

6. Das E-Health-Geschäft wird neben den technischen Möglichkeiten auch von rechtlichen Rahmenbedingungen beeinflusst. Das rechtliche Grundgerüst einer jeden personenbezogenen Datenverarbeitung in Deutschland ist die DSGVO bzw. das BDSG-neu. Doch welche Rechtsquellen beeinflussen Ihre E-Health-Umsetzung noch?

7. Gesundheitsdaten sind besonders schützenswerte Daten. Die DSGVO hat sie als sensible Daten bzw. besondere Datenkategorie besonders geschützt. Wie wirkt sich die DSGVO seit 2018 auf Ihr Alltagsgeschäft aus?

8. Welche Maßnahmen haben Sie ergriffen, um die verschiedenen Bestandteile der DSGVO im E-Health-Bereich umzusetzen?

   a. Grundsätze für die Verarbeitung personenbezogener Daten (Rechtmäßigkeit, Transparenz, etc.)

b. Betroffenenrechte (Auskunftsrecht, Recht auf Löschung, etc.)
c. Auftragsverarbeitung (Auftragsverarbeitungsvertrag bei Auslagerung der Datenverarbeitung an weisungsgebundene Dritte)
d. Technische und organisatorische Maßnahmen (TOMs)
e. Verarbeitungsverzeichnis (VVT)
f. Datenschutz-Folgenabschätzung (DSFA)
Welche Reihenfolge wäre angebracht, wenn Sie diese Bestandteile nach Wichtigkeit und Relevanz gewichten müssten?

9. Mit welchen Aufgaben ist der für Ihr Unternehmen zuständige Datenschutzbeauftragte hauptsächlich befasst (falls vorhanden)?

10. Ist der Datenschutzbeauftragte interner Mitarbeiter oder externer Dienstleister und aus welchen Gründen haben Sie sich für diesen entschieden?

11. Welche Herausforderungen sehen Sie in Bezug auf den Datenschutz im E-Health-Bereich? Was erhoffen Sie sich von der zukünftigen Rechtsentwicklung?

7 AUTORENINFORMATION

Thimo Niebler ist Absolvent des Bachelorstudienganges Wirtschaftsrecht (LL.B.) an der Hochschule Konstanz.

Dr. Thomas Zerres ist Professor für Zivil- und Wirtschaftsrecht an der Hochschule Konstanz. Vor seinem Ruf an die Hochschule Konstanz lehrte Prof. Dr. Thomas Zerres 15 Jahre an der Hochschule Erfurt, nachdem er mehrere Jahre als Rechtsanwalt und als Bundesgeschäftsführer eines großen Wirtschaftsverbandes der Dienstleistungsbranche tätig war. Seine Lehr- und Forschungsschwerpunkte sind das Marketingrecht sowie das Europäische Privatrecht.

Dr. Christopher Zerres ist Professor für Marketing an der Hochschule Offenburg. Seine Schwerpunkte in Lehre und Forschung liegen auf dem Online-Marketing und dem Marketing-Controlling. Christopher Zerres ist Autor zahlreicher Publikationen zu den Bereichen Management und Marketing.