e-beratungsjournal.net
Fachzeitschrift für Onlineberatung und computervermittelte Kommunikation
ISSN 1816 - 7632

15. Jahrgang, Heft 2, Artikel 2
2019

E-Health, Health-Apps & Co. – rechtliche Aspekte

Ulrich M. Gassner & Dominik Strobl

Zusammenfassung
Health-Apps und andere E-Health-Produkte unterliegen verschiedenartigen rechtlichen Bestimmungen. Der Hochschulsektor bildet insofern keine Ausnahme. Gerade auch für Entwickler und Anbieter an Hochschulen sind Grundkenntnisse über die Rahmenbedingungen für digitale Gesundheitsanwendungen von grundlegender Bedeutung. So müssen auch und insbesondere Anforderungen an die Produktkonzeption schon in der Planungs- und Entwicklungsphase bedacht werden. Aus dem Datenschutzrecht ergeben sich beispielsweise Vorgaben zu datenschutzfreundlichem Layout und entsprechenden Voreinstellungen. Auch müssen bereits in der Entwicklungsphase die Weichen dafür gestellt werden, dass Anwender und Anwenderinnen bei Verwendung des Produktes rechtskonform handeln und nicht etwa gegen Berufsrecht verstoßen. Nicht zuletzt ist für den Marktzugang und die Vermarktung entscheidend, ob es sich um ein Medizinprodukt i.S.d. § 3 Nr. 1 Medizinproduktegesetz (MPG) handelt. Auch dies ist grundsätzlich durch Entwickler und Entwicklerinnen bzw. Hersteller und Herstellerinnen steuerbar und daher von Beginn an zu berücksichtigen.

Schlüsselwörter
Health-Apps, DSGVO, Medizinprodukte, Datenverarbeitung, Schweigepflicht, Fernbehandlung, E-Health-Gesetz

Abstract
Health apps and other E-Health products are subject to various legal provisions. The university sector is no exception in this respect. Especially for developers and providers at universities, basic knowledge of the legal framework for digital health applications is of fundamental importance. In particular, the requirements for product design must be taken into account as early as the planning and development phase. The data protection law provides guidelines for data protection-friendly layouts and corresponding default settings. In addition, the course must be set to ensure that users act in accordance with the law when using the product and do not violate professional law. Last but not least, it is decisive for market access and marketing whether the product is a medical device within the meaning of Sect. 3 No. 1 German Medical Device Act. This is basically controllable by the developer or manufacturer and must therefore be taken into account from the outset.

Keywords
Health apps, GDPR, medical devices, data processing, confidentiality, remote treatment, eHealth Law

Autoren
- **Prof. Dr. iur. Ulrich M. Gassner**, Mag. rer. publ., M. Jur. (Oxon.) ist Gründungsdirektor der Forschungsstelle für Medizinprodukterecht (FMPR) und der Forschungsstelle für E-Health-Recht (FEHR) an der Universität Augsburg.
- **Kontakt:** ulrich.gassner@jura.uni-augsburg.de

- **Dominik Strobl**, Jurist (Univ.), ist wissenschaftliche Hilfskraft bei Prof. Dr. Ulrich M. Gassner an der Universität Augsburg

1. E-Health – ein Überblick

Die Digitalisierung ist seit geraumer Zeit dabei, das Gesundheitswesen zu revolutionieren. Die Entwicklung ist rasant: Mittlerweile etabliert sind etwa Fitness-Tracker, Health-Apps oder die elektronische Gesundheitskarte, die Zukunft hält die Videosprechstunde und die Nutzung der Blockchain-Technologie (dazu näher Gassner, 2018) bereit. Die steigende Relevanz in der Versorgungsrealität und das ökonomische Potential sind mittlerweile unübersehbar.

Bekannten wie neuen Einsatzmöglichkeiten ist eine ethische Sensitivität gemein. Schließlich ist mit E-Health immer ein Verlust von menschlicher Macht und Kontrolle verbunden. Auch deshalb bestehen für das einschlägige rechtliche Regelungsumfeld Schwierigkeiten, mit der technischen Entwicklung Schritt zu halten. Dies führt zum vielfach als unbefriedigend empfundenen Zustand, dass gerade für die Forschung an und Entwicklung von konkreten E-Health-Angeboten diverse Unsicherheiten und Grauzonen existieren. Nachfolgend sollen die wesentlichen einschlägigen Regelungen und Vorschriften im Überblick dargestellt werden.

1.1 Facetten

Den Rechtsgrundlagen vorangestellt wird ein kurzer Überblick über die vielfältigen Anwendungsgebiete von E-Health. Diese lassen sich grob in die Kategorien „Digitalisierung der Administration" und „Digitalisierung der Versorgung" einordnen. Zur administrativen Seite sind etwa die Vernetzung von Gesundheitsakteuren und die elektronische Gesundheitskarte zu zählen. Hinsichtlich der Versorgung dominieren Health-Apps die öffentliche Wahrnehmung. Zur Verbesserung der Versorgungsqualität tragen aber auch die verbesserte Vernetzung und Kommunikation innerhalb von Arztpraxen, Kliniken oder OP-Räumen sowie die Entwicklungen im Medtech-Bereich bei. Ebenfalls E-Health zuzuordnen sind die Unterstützung der Ärzte bei der Stellung der Diagnose durch „Big Data" (Clinic Decision Support Systems), die Möglichkeit der Online-Behandlung bzw. Videosprechstunde („Telemedizin"), das „Ambient Assisted Living" (patienteneigene Technologien zur Prävention bzw. Überwachung) sowie die nunmehr endgültig in Deutschland auf den Weg gebrachte elektronische Patientenakte [1]. Im weitesten Sinne sind auch Online-Gesundheitsportale zur Patienteninformation, die Digitalisierung der heilberuflichen Aus- und Weiterbildung sowie sogar Online-Apotheken mit dem Themengebiet zu assoziieren.

Wie diese – notwendig unvollständige – Zusammenschau der Facetten von E-Health verdeutlicht, ist eine allumfassende Darstellung aller einschlägigen Regelungen in diesem Format nicht zu gewährleisten. Es wird sich daher dem Thema dieses Sonderheftes entsprechend vornehmlich auf Health-Apps beschränkt, das dargestellte Regelungsumfeld ist aber mit geringen Abweichungen etwa auch auf die Entwicklung von Technologien für die Videosprechstunde anwendbar. Gerade die Problematik um Rechtskonformität und Qualitätssicherung der den Markt überschwemmenden Health-Apps (dazu schon: Albrecht, 2016) ist eine der Kernfragen des E-Health-Rechts und damit auch für Entwicklerinnen und Entwickler an Hochschulen von großem Interesse.

1.2 Rechtsgrundlagen – ein weites Feld

Das E-Health-Recht ist keine eigenständige, in sich abgeschlossene juristische Materie. Vielmehr sehen sich Interessierte und Betroffene gezwungen, sich die für den jeweils zugrundeliegenden Lebenssachverhalt anwendbaren Vorschriften aus verschiedenen Rechtsquellen zusammenzutragen. Denn E-Health-Recht ist eine Querschnittsmaterie. Überdies befinden sich auch viele dieser Rechtsquellen im Wandel. Insbesondere auf europäischer Ebene sorgt der recht träge Gesetzgebungsprozess mitunter dafür, dass die jeweilige Regulierung nicht oder nicht mehr dem aktuellen Stand des technischen Fortschritts entspricht.

1.2.1 Rechtliche Rahmenbedingungen für E-Health

Die für E-Health zentrale Rechtsmaterie ist das Datenschutzrecht. Denn E-Health-Angebote beruhen entweder in ihrer Funktion darauf, Patientendaten in bestimmter Art und Weise zu erheben bzw. verarbeiten (z. B. wenn eine Health-App den individuellen Gesundheitszustand in Form verschiedener Parameter trackt und darauf basierend Empfehlungen oder Warnungen gibt) oder kommen zumindest notwendigerweise mit den von Gesetzes wegen sensiblen Patientendaten in Berührung (etwa bei der Videosprechstunde). Stets ist daher schon in der Entwicklungs- und Planungsphase eines E-Health-Angebots zu berücksichtigen, ob das geplante Modell datenschutzrechtskonform ist.

Ebenfalls zu beachten sind die sich aus dem Sozialrecht ergebenden regulatorischen Rahmenbedingungen. Der deutsche Gesetzgeber hat unter anderem durch das „E-Health-Gesetz" Vorgaben zur Implementierung von E-Health-Angeboten in das öffentliche Gesundheitswesen gemacht. Ebenfalls für viele Ausprägungen von E-Health determinierend sind die ärztliche Schweigepflicht sowie die berufsrechtlichen Bestimmungen zur ärztlichen Fernbehandlung. Daneben tritt die Produktregulierung. Sie erfordert es, schon bei der Planung und Entwicklung abzuschätzen, ob das Endprodukt ein Medizinprodukt sein wird. In diesem Fall muss ein komplexer Zertifizierungsprozess durchlaufen werden, an dessen Ende die CE-Kennzeichnung des Produktes steht. Medizinprodukte können etwa Health-Apps sein, diskutiert wird derzeit aber etwa auch, ob die Videosprechstunde dem Medizinprodukterecht unterfallen soll [2].

Die einleitend erwähnte stetige Veränderung der rechtlichen Rahmenbedingungen verdeutlicht sich bei einem Blick auf die Neuerungen und Revisionen der jeweiligen Materien: Das Datenschutzrecht sowie das Medizinprodukterecht wurden in den letzten Jahren durch die Datenschutz-Grundverordnung (DSGVO), anzuwenden seit 25.05.2018, die EU-Verordnung über Medizinprodukte (MPVO), in Kraft getreten am 25.05.2017, verpflichtend anzuwenden ab 26.05.2020 und die EU-Verordnung über In-vitro-Diagnostika (IVDVO) in Kraft getreten am 25.05.2017, verpflichtend anzuwenden ab 26.05.2022 weiter harmonisiert. Die Bestimmungen des zum 31.12.2015 in Kraft getretenen E-Health-Gesetzes wurden seitdem vielfach geändert. Erst im Juni 2018 wurde vom deutschen Ärztetag eine liberalisierende Revision zur Fernbehandlung in der ärztlichen Berufsordnung beschlossen. Flankierende Gesetze sind in der parlamentarischen Beratung. Für den verbesserten Zugang innovativer digitaler Gesundheitsanwendungen in die

gesetzliche Krankenversicherung hat das Bundesministerium für Gesundheit (BMG) im Mai 2019 einen Referentenentwurf vorgelegt (Digitale Versorgung-Gesetz). Insgesamt handelt es sich also um einen dynamischen rechtlichen Bereich, dessen Entwicklung analog zum Fortschritt der Digitalisierung keineswegs abgeschlossen ist. Dies erschwert die Konzeption und Entwicklung von E-Health-Angeboten von vornherein, weil nicht verlässlich abgeschätzt werden kann, welche rechtlichen Bedingungen gelten werden, wenn die Marktreife erreicht ist.

1.2.2 E-Health-Entwicklung an der Hochschule

Die soeben vorgestellten Normen sind schon in der Planungs- und Entwicklungsphase von E-Health-Angeboten zu bedenken und berücksichtigen, weil sie spätestens bei Markteintritt des Produkts oder der Dienstleistung durchgreifen und durchgesetzt werden. Das Datenschutzrecht, die ärztliche Schweigepflicht und die Vorgaben zur Fernbehandlung sind auch schon in früheren Entwicklungsstadien zwingend zu beachten, etwa bei Testläufen. Für rein wissenschaftliche Projekte bzw. reine Forschungszwecke sehen die DSGVO und das nationale Bundesdatenschutzgesetz (§ 27 BDSG) sowie Landesdatenschutzgesetze datenschutzrechtliche Privilegierungen vor. Soweit die Entwicklung von E-Health-Angeboten an Hochschulen mit dem Ziel der Entwicklung eines Produkts oder einer Dienstleistung für den Markt erfolgt, liegt kein rein wissenschaftliches Projekt vor, sodass diese datenschutzrechtlichen Erleichterungen nicht greifen.

2. Datenschutzrecht

Die DSGVO hat das Datenschutzrecht stärker als bisher einheitlichen unionsrechtlichen Vorgaben unterworfen. Sie ist direkt in jedem Mitgliedstaat anzuwenden, wobei es den Mitgliedstaaten in bestimmten Bereichen anheimgestellt wird, die DSGVO durch nationale Rechtsvorschriften zu modifizieren und zu konkretisieren. Daher gibt es nach wie vor auf Bundesebene ein Bundesdatenschutzgesetz (BDSG) und weitere bereichsspezifische nationale datenschutzrechtliche Vorschriften. Ebenso verhält es sich auf Landesebene.

2.1 Wann ist das Datenschutzrecht zu beachten?

Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten (Art. 1 Abs. 1 DSGVO). Art. 4 Nr. 1 DSGVO definiert den Begriff der personenbezogenen Daten als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Gesundheits- bzw. Patientendaten sind also personenbezogene Daten im Sinne der DSGVO, sofern hinreichende Zuordnung oder Zuordnungsbarkeit zu einer Person gegeben ist.

Art. 4 Nr. 2 DSGVO definiert die Verarbeitung als „jeden (…) Vorgang (…) im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die

Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung", umfasst also nahezu jede Nutzung personenbezogener Daten.

Die DSGVO kennt außerdem besonders schützenswerte Daten. Eine solche Kategorie bilden „Gesundheitsdaten", welche in § 4 Nr. 15 DSGVO als personenbezogene Daten definiert werden, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Die Grundsätze des Datenschutzes gelten nicht für anonyme Daten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann sind mangels Personenbezug nicht von der DSGVO umfasst. Ob tatsächlich anonyme Daten vorliegen, hängt auch bei Studien an Hochschulen angesichts der heutigen technischen Möglichkeiten vom jeweiligen Einzelfall ab. Auf jeden Fall aber sind die personenbezogenen Daten zu pseudonymisieren, soweit dies der jeweilige Forschungszweck zulässt.

2.2 Rechtmäßigkeit der Datenverarbeitung

Angelpunkt der DSGVO ist die Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. a) DSGVO). Sie ist grundsätzlich unzulässig und nur ausnahmsweise erlaubt (Art. 6 Abs. 1 DSGVO). Man spricht insofern von einem „Verbot mit Erlaubnisvorbehalt". Für die Verarbeitung besonderer Kategorien personenbezogener Daten ist die spezielle Regelung des Art. 9 zu beachten. Art. 9 Abs. 1 DSGVO verbietet ausdrücklich die Verarbeitung von Gesundheitsdaten.

Ausnahmen von diesem Verbot hält Art. 9 Abs. 2 DSGVO bereit. Praktisch bedeutsam für E-Health sind folgende Ausnahmen:

- Erste relevante Ausnahme ist Art. 9 Abs. 2 lit. h) Alt. 2 DSGVO, wonach eine Gesundheitsdatenverarbeitung zulässig ist, wenn sie aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs erfolgt. Für diesen Fall sind zudem die Einschränkungen aus Art. 9 Abs. 3 DSGVO zu beachten, wonach der oder die Angehörige des Gesundheitsberufes zwingend einer Geheimhaltungspflicht unterliegen muss. Ein Beispiel hierfür bildet die Datenverarbeitung durch ärztliches Personal oder Physiotherapeuten und Physiotherapeutinnen (welche jeweils der Schweigepflicht unterliegen) zur Durchführung der aus dem Behandlungsvertrag (§ 630a BGB) geschuldeten Behandlung, etwa in Gestalt einer Dokumentation in der Patientenakte. E-Health-Angebote sind von der Ausnahme des Art. 9 Abs. 2 lit. h) Alt. 2 DSGVO freilich kaum erfasst, weil der Einsatz von Health-Apps oder Telemedizin derzeit regelmäßig kein Teil der geschuldeten Leistung ist. Darunter zu fassen wäre aber etwa die – noch nicht in der Versorgungsrealität anzutreffende – Big-Data-gestützte Unterstützung der Diagnoseentscheidung.

- Die wichtigste Ausnahme ergibt sich aus Art. 9 Abs. 2 lit. a) DSGVO. Danach ist die Gesundheitsdatenverarbeitung zulässig, wenn die betroffene Person in die Verarbeitung für einen oder mehrere festgelegte Zwecke ausdrücklich

eingewilligt hat [3]. Die Anforderungen an eine Einwilligung ergeben sich unter anderem aus Art. 7 DSGVO. Die Einwilligung muss sich konkret auf zuvor konkretisierte Zwecke und in voller Kenntnis der konkreten zu erfolgenden Verarbeitung beziehen. Da die meisten E-Health-Angebote also eine Einwilligung des oder der Betroffenen (d.h. des Patienten oder der Patientin) voraussetzen, ist schon bei deren Entwicklung zu bedenken, wie die Einholung der Einwilligungserklärung strukturiert sein wird und in welche Vorgänge eingewilligt werden muss. Gerade bei Health-Apps ist die Frage nach der Einflechtung einer Einwilligungserklärung technischer Natur.

2.3 Weitere Grundsätze der Verarbeitung personenbezogener Daten

Neben der Rechtmäßigkeit der Datenverarbeitung enthält die DSGVO in Art. 5 DSGVO noch weitere allgemeine Grundsätze für die Datenverarbeitung, welche große Auswirkungen auf die Konzeption eines E-Health-Produktes haben. Nach Art. 5 Abs. 1 lit. a) DSGVO müssen die Daten nicht nur rechtmäßig, sondern nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Daraus folgt, dass der komplette Vorgang für den Betroffenen möglichst transparent zu gestalten ist. Art. 5 Abs. 1 lit. b) DSGVO enthält den Zweckbindungsgrundsatz. Er statuiert, dass Daten nur für „festgelegte, eindeutige und legitime" Zwecke erhoben werden und nicht „in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden" dürfen. Nach Art. 5 Abs. 1 lit. c) DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"). Das in Art. 5 Abs. 1 lit. d) DSGVO normierte Richtigkeitsgebot verlangt, dass die verarbeiteten Daten der Realität entsprechen und nicht falsch bzw. verfälscht sind; das Gebot der Speicherbegrenzung aus Art. 5 Abs. 1 lit. e) DSGVO besagt, dass die Zuordnung eines Betroffenen zu einem Datensatz zeitlich auf die Zeit zu begrenzen ist, die für den Verarbeitungszweck erforderlich ist. Art. 5 Abs. 1 lit. f) DSGVO schreibt schließlich „Integrität und Vertraulichkeit" vor, also letztlich die datensichere Verarbeitung.

Die praktische Umsetzung dieser Grundsätze lässt sich anhand des Beispiels einer Health-App illustrieren, die mithilfe eines externen verknüpften Tools erhobene Daten analysiert und Anwendende warnt, wenn der Blutzuckerspiegel zu niedrig ist bzw. wird: Schon in der Planungsphase ist die Konzeption der App so zu gestalten, dass aus Sicht von Anwendenden zu jeder Zeit Transparenz besteht, also fortwährender Überblick darüber, ob und welche Daten erhoben bzw. verarbeitet werden. Auch ist schon zu diesem Zeitpunkt ein eindeutiger Zweck zu formulieren (etwa: Auswertung der Daten hinsichtlich der Höhe des Blutzuckerspiegels; abgestufter Warnmechanismus), auf dessen Erfüllung sich die Datenverarbeitung zu beschränken hat. Es dürfen auch keinesfalls mehr Daten erhoben werden, als für diese Zwecke nötig sind. Nach dem Grundsatz der Speicherbegrenzung ist schon konzeptionell sicherzustellen, dass solche Daten, die nicht mehr für die Auswertung (oder ggf. Verlaufsanalyse) benötigt werden, gelöscht oder zumindest pseudonymisiert werden.

2.4 Die Verantwortlichen und ihre Pflichten

Für die Anwendungspraxis überaus bedeutsam ist auch, wer für die Einhaltung der erwähnten sowie sonstiger Vorgaben der DSGVO verantwortlich ist. Im medizinischen Bereich kommt dafür eine Vielzahl von Akteuren in Frage. Mit einem E-Health-Produkt- oder Angebot können zahlreiche natürliche oder juristische Personen befasst sein: Entwickler und Entwicklerinnen, Herstellerfirmen, Importeure und Importeurinnen, Vertreiber und Vertreiberinnen, Verkäufer und Verkäuferinnen, Plattform-Betreiber und -Betreiberinnen (z.B. Apple/Google), ärztliches und nichtärztliches Fachpersonal, das solche Produkte empfiehlt, verschreibt oder anwendet, Krankenhäuser und sonstige Einrichtungen, die solche Produkte einsetzen, und nicht zuletzt die Patienten und Patientinnen.

Wesentlicher Normadressat der DSGVO ist der oder die „Verantwortliche", definiert in Art. 4 Nr. 7 DSGVO: „Verantwortlicher bezeichnet die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (…)". Die Verantwortlicheneigenschaft ist je nach Einzelfall zu bestimmen. Zu jedem Stadium der Entwicklung und auch in der Marktphase ist es für die beteiligte natürliche oder juristische Person unerlässlich zu wissen, ob er oder sie DSGVO-Verantwortlicher ist. Verantwortlicher für eine Health-App ist beispielsweise zunächst das Unternehmen, das die App vertreibt. Verantwortlicher für die Videosprechstunde oder die elektronische Patientendatenverarbeitung sind dagegen der Arzt oder die Ärztin. Die DSGVO kennt auch eine geteilte Verantwortlichkeit (Art. 26 DSGVO).

Die Verantwortlichen haften für die Einhaltung der bereits skizzierten Grundprinzipien der Verarbeitung personenbezogener Daten aus Art. 5 DSGVO und müssen deren Einhaltung nachweisen können (Art. 5 Abs. 2 DSGVO). Datenschutzbezogene Vorkehrungen sollten also möglichst umfassend dokumentiert werden. Außerdem sind die Verantwortlichen Adressaten der Betroffenenrechte aus Art. 12 – 23 DSGVO, welche durch die DSGVO enorm gestärkt wurden. Sie können in organisatorischer und damit auch in finanzieller Hinsicht zu nicht unerheblichen Belastungen führen (etwa Informationspflichten, Auskunftsrechte, Recht auf Berichtigung und Recht auf Löschung). In Art. 24 ff. DSGVO werden sodann die bereits in Art. 5 DSGVO verankerten Pflichten des Verantwortlichen weiter konkretisiert.

2.5 Datenschutzmaßnahmen und Datensicherheit

In Art. 24 – 34 DSGVO werden Datenschutzmaßnahmen sowie Vorgaben zur Datensicherheit beschrieben. Art. 24 Abs. 1 DSGVO fordert dazu einleitend:

> „Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (…)."

Art. 25 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) konkretisiert wiederum die allgemeine Pflicht zur DSGVO-Konformität aus Art. 24 DSGVO. In der Fachdiskussion spricht man insofern häufig von „Privacy by design" und „Privacy by default". Diesem Ansatz liegt die Vorstellung zugrunde, dass ein effektiver Datenschutz nicht nur ex post erreicht werden kann, sondern schon ex ante technische Prozesse mit dem Datenschutz in Einklang gebracht werden müssen. Damit gibt die DSGVO Entwicklern und Entwicklerinnen und Herstellerfirmen Werkzeuge an die Hand, mit denen DSGVO-Konformität sichergestellt werden kann (und soll). Datenschutz durch Technikgestaltung meint zum Beispiel, dass eine Health-App schon technisch so beschränkt konzipiert wird, dass gar nicht mehr Daten erhoben werden können, als für die Zweckerreichung notwendig (technische Umsetzung des Grundsatzes der Zweckbindung und der Datenminimierung). Datenschutz durch datenschutzfreundliche Voreinstellungen wird beispielsweise dadurch erreicht, dass schon nicht die invasivste Variante der Datenverarbeitung vorausgewählt ist (etwa durch ein bereits gesetztes „Häkchen" im Layout einer App), sondern die am wenigsten invasivste Variante „ab Werk" geliefert wird und der Anwender eigenständig eine etwaige invasivere Nutzung (etwa durch Setzen entsprechender Häkchen) auswählt. Zur Einhaltung dieser Vorgaben können Verantwortliche auf verschiedene Hilfestellungen zurückgreifen. Anhaltspunkte ergeben sich etwa aus den IT-Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [BSI, Grundschutzkatalog] oder einschlägigen ISO-Normen. Art. 25 Abs. 3 DSGVO sieht zudem zu genehmigende Zertifizierungsverfahren vor, welche Indizwirkung für die Erfüllung der DSGVO-Anforderungen haben. Es ist anzuraten, diese Anforderungen zu jeder Phase der Entwicklung und auch in der Marktphase ernst zu nehmen: Die Verletzung der Anforderungen aus Art. 25 DSGVO kann gem. Art. 83 Abs. 4 DSGVO Geldbußen von bis zu 10 Mio. € oder – falls der Betrag höher ist – bis zu 2 % des Jahresumsatzes eines Unternehmens nach sich ziehen. Für Hochschulen des öffentlichen Sektors gilt dies zwar nicht, wohl aber für Ausgründungen.

Art. 32 DSGVO konkretisiert Maßnahmen des technischen und organisatorischen Schutzes personenbezogener Daten (Datensicherheit). Art. 32 DSGVO enthält keine konkreten technischen Vorgaben, die schnell veralten würden, sondern Zielvorgaben für technische und/oder organisatorische Maßnahmen. Konkretisiert werden (nur) wenige Datensicherheitsmaßnahmen, nämlich Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DSGVO) sowie die Pflicht, Mitarbeiter und Mitarbeiterinnen datenschutzrechtlich zu unterweisen und anzuweisen (Art. 32 Abs. 4 DSGVO). Anhaltspunkte für konkrete Datensicherheits-Maßnahmen finden sich wiederum in den bereits erwähnten IT-Grundschutzkatalogen des BSI [BSI, Grundschutzkatalog]. Die von Art. 32 Abs. 2 lit. b) DGVO geforderte Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme erfordert Maßnahmen wie beispielsweise Zutritts-, Zugangs- und Zugriffskontrolle, die Eingabe- und Weitergabekontrolle, die Auftrags- und Verfügbarkeitskontrolle sowie die Datentrennung. Da wie bei Art. 25 DSGVO empfindliche Geldbußen drohen, sei auch beim Thema Datensicherheit stark zu möglichst weitgehender Compliance angeraten. Wie auch bei allen anderen Fragestellungen zu den datenschutzrechtlichen Implikationen auf das konkrete Projekt ist auch für Datenschutzmaßnahmen und Datensicherheit der Datenschutzbeauftragte der Hochschule der zentrale Ansprechpartner für Entwickler und Entwicklerinnen.

3. Sonstige rechtliche Aspekte

Soll ein E-Health-Projekt entwickelt und in die Praxis umgesetzt werden, sind neben dem Datenschutzrecht noch einige weitere rechtliche Aspekte zu beachten. Dabei ist zu beachten, dass es sich im Gegensatz zum Datenschutzrecht um Aspekte handelt, die nicht zwangsläufig auf jedes Projekt bzw. Produkt anzuwenden sind. Es ist also sorgsam zu prüfen, ob und inwieweit diese Aspekte im konkreten Fall überhaupt beachtet werden müssen.

3.1 Sozialrecht

Das Fünfte Buch des Sozialgesetzbuchs (SGB V) bündelt alle Bestimmungen zur gesetzlichen Krankenversicherung in Deutschland. Vom SGB V erfasst ist zunächst (§ 73 Abs. 1b SGB V) der Datenaustausch zwischen Ärzten bzw. Ärztinnen (Austausch von Behandlungsdaten zwischen Hausarzt bzw. Hausärztin, Facharzt bzw. Fachärztin und sonstigen Leistungserbringern im Rahmen der vertragsärztlichen Versorgung). Nicht erfasst ist von vornherein also der Datenaustausch zwischen Ärzten bzw. Ärztinnen (oder sonstigen Fachkreisen) und Patienten bzw. Patientinnen.

Für E-Health-Produkte von besonderer Bedeutung ist das zehnte Kapitel des SGB V („Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz", §§ 284 – 305b). Dort wird zunächst die Datenerhebung zu bestimmten krankenversicherungstechnischen Zwecken (z. B. Abrechnung von medizinischen Leistungen oder zur Festlegung der Beiträge von Versicherten) erlaubt und u.a. die Kassenärztlichen Vereinigungen werden dazu legitimiert, die zu Abrechnung erforderlichen Daten zu erheben und an die Versicherungsträger weiterzuleiten. Auch für Ärzte und Ärztinnen folgen Legitimationsvorschriften über die Erhebung und Weiterleitung solcher Daten. In diesen Fällen bedarf es zur Legitimation der Datenverarbeitung folglich nicht der Einwilligung von Patienten bzw. Patientinnen. Des Weiteren enthält das zehnte Kapitel des SGB V auch die Festlegung der Krankenversicherungsnummer sowie die Regelungen zur elektronischen Gesundheitskarte (dazu sogleich).

Aus dem Sozialrecht ergeben sich auch faktische Rahmenbedingungen für die Entwicklung von E-Health-Angeboten. Der Gesetzgeber hat in den letzten Jahren durch das „E-Health-Gesetz" und weitere Änderungen des Sozialrechts die Implementierung von E-Health in der Versorgung vorangetrieben. Angelaufene und zum Teil auch schon abgeschlossene Projekte sind das Versichertenstammdaten-Management, der elektronische Arztbrief und das Notfalldatenmanagement. Leuchtturm des E-Health-Gesetzes ist die elektronische Patientenakte, welche nach aktuellem Stand endgültig im Jahr 2021 eingeführt werden soll. Auch Präventionsmaßnahmen und -angebote nach § 20 SGB V können elektronisch bzw. digital sein (z.B. IKT-basierte Selbsthilfeprogramme). Die somit umrissenen Rahmenbedingungen sind Ansatzpunkte für Entwickler und Entwicklerinnen von E-Health-Angeboten. So wurde etwa auch in der Privatwirtschaft an einem Modell für eine elektronische Patientenakte gearbeitet, außerdem werden privatwirtschaftlich zusätzliche (freiwillige) Anwendungen für die elektronische Gesundheitskarte entwickelt. Der Entwurf des Digitale

Versorgung-Gesetzes sieht zudem vor, dass die Krankenkassen digitale Innovationen, etwa im Rahmen fachlicher Kooperationen oder Kapitalbeteiligungen mit bzw. an Forschungseinrichtungen, fördern. Für Entwickler und Entwicklerinnen ergeben sich also aus dem Fortschritt in der Gesetzgebung und aus der Kostenübernahme durch die GKV für bestimmte Produkte (z.B. zur Prävention, § 20 SGB V) konkrete Ansatzpunkte für die Produktoptimierung.

3.2 Ärztliche Schweigepflicht und Restriktionen der Fernbehandlung

Bei der Entwicklung von E-Health-Angeboten wirkt außerdem die ärztliche Schweigepflicht als Determinante. Gem. § 9 Abs. 1 MBO-Ä (Musterberufsordnung Ärzte) müssen Ärzte und Ärztinnen das, was ihnen in ihrer ärztlichen Eigenschaft anvertraut oder bekannt geworden ist, für sich behalten. Die Schweigepflicht ist außerdem Nebenpflicht aus dem Behandlungsvertrag, mithin auch haftungsrelevant. Nach § 203 Abs. 1 StGB wird zudem bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis, offenbart, das ihm als Arzt oder Ärztin anvertraut worden oder sonst bekanntgeworden ist. Ausnahmen davon müssen explizit gesetzlich vorgesehen sein, erlaubt (und auch vorgeschrieben) ist dies etwa bei meldepflichtigen Infektionskrankheiten. Ärzte und Ärztinnen sind außerdem zur Informationsweitergabe berechtigt, wenn der Patient oder die Patientin darin eingewilligt haben. Soweit der Schweigepflicht unterliegende Personen schon in der Entwicklungsphase von E-Health-Angeboten, etwa an Hochschulen, beteiligt sind, müssen diese auch schon in dieser frühen Phase unbedingt die Schweigepflicht beachten. Es gelten grundsätzlich dieselben Normen und Ausnahmen wie bei einem späteren Einsatz des Angebotes im Markt. Dieses Szenario kann beispielsweise aufschlagen, wenn einem kooperierenden Arzt oder einer kooperierenden Ärztin in der Testphase eines Produktes von einer Testperson Krankheiten berichtet werden: die Weitergabe dieser Information (etwa an einen ärztlichen Kollegen oder eine Beratungsstelle) ist grundsätzlich nur mit Einwilligung der Testperson möglich.

Die Einwilligung in die Informationsweitergabe ist streng von der datenschutzrechtlichen Einwilligung in die Datenverarbeitung zu unterscheiden. Es muss sichergestellt und schon in der Entwicklung bedacht sein, dass Ärzte und Ärztinnen durch die Nutzung nicht gegen ihr Berufsrecht verstoßen oder sich haft- oder strafbar machen, weil sie gegen ihre Schweigepflicht verstoßen. Daher sollte schon in der Sicherheits- und Datenschutzkonzeption einer Anwendung gezeigt werden, wie derartige (auch versehentliche) Verstöße konkret verhindert werden sollen. Die praktischen Maßnahmen (etwa Verschlüsselung, dann keine Zuordnung zu einem Patienten mehr möglich) überschneiden sich regelmäßig mit den unter 2. dargestellten Anforderungen an Datenschutz und -sicherheit aus Art. 24 ff. DSGVO.

In der ärztlichen Berufsordnung finden sich auch Regelungen zur ärztlichen Fernbehandlung. Bis 2018 enthielt § 7 MBO-Ä (Behandlungsgrundsätze und Verhaltensregeln) in Absatz 4 ein Verbot der Fernbehandlung. Ärzten und Ärztinnen war es berufsrechtlich untersagt individuelle ärztliche Behandlung, insbesondere auch Beratung, ausschließlich über Print- und Kommunikationsmedien durchführen, die Unmittelbarkeit der Behandlung sollte

stets gewährleistet sein. Demnach waren nur solche telemedizinischen Anwendungen zulässig, die eine Behandlung unterstützen, nicht aber solche, die an die Stelle des persönlichen und unmittelbaren Kontakts zwischen Arzt bzw. Ärztin und Patienten traten. Hintergrund des Verbotes war, dass sich Ärzte und Ärztinnen von Patienten bzw. Patientinnen ein unmittelbares Bild durch eigene Wahrnehmung verschaffen sollen und so eine hohe Behandlungsqualität aufrechterhalten werden kann. Nach jahrelangen Diskussionen um eine Zeitgemäßheit des Fernbehandlungsverbotes wurde vom 121. Deutschen Ärztetag im Mai 2018 schließlich eine liberalisierende Neufassung des § 7 Abs. 4 MBO-Ä beschlossen. Dieser lautet nunmehr:

> „Ärztinnen und Ärzte beraten und behandeln Patientinnen und Patienten im persönlichen Kontakt. Sie können dabei Kommunikationsmedien unterstützend einsetzen. Eine ausschließliche Beratung oder Behandlung über Kommunikationsmedien ist im Einzelfall erlaubt, wenn dies ärztlich vertretbar ist und die erforderliche ärztliche Sorgfalt insbesondere durch die Art und Weise der Befunderhebung, Beratung, Behandlung sowie Dokumentation gewahrt wird und die Patientin oder der Patient auch über die Besonderheiten der ausschließlichen Beratung und Behandlung über Kommunikationsmedien aufgeklärt wird."

Wie eine Betrachtung des Wortlautes zeigt, ist die ärztliche Fernbehandlung damit keineswegs komplett freigegeben. Unter Einhaltung der beschriebenen Voraussetzungen lässt die Berufsordnung nun jedoch die Fernbehandlung zu. Damit ist zumindest in berufsrechtlicher Hinsicht die Tür zur Videosprechstunde geöffnet. Ebenfalls explizit berufsrechtlich ermöglicht sind für Ärzte und Ärztinnen bspw. nunmehr auch „Online-Therapien" zur Behandlung von (z.B.) Depressionen und Angststörungen (E-Mental-Health) unter Ersetzung der Konsultation in der Arztpraxis. Bis dato ist jedoch nur die – unverbindliche – Muster-Berufsordnung geändert, entsprechende Änderungen der für Ärzte und Ärztinnen jeweils geltenden Berufsordnungen der Landesärztekammern stehen noch aus. Dass ärztlicherseits weiterhin Skepsis gegenüber der Fernbehandlung besteht, zeigt sich etwa daran, dass die Delegierten des Ärztetags die Krankschreibung per Telefon oder Videokonferenz bei unbekannten Patienten und Patientinnen sowie Verordnungen ausschließlich im Rahmen von Fernbehandlung ablehnten [4]. Flankierend zur Änderung der Muster-Berufsordnung sieht der Entwurf des Digitale-Versorgung Gesetz vor, dass die Patientenaufklärung (§ 630e BGB) bei telemedizinischer Behandlung über Fernkommunikationsmittel erfolgen kann. Zudem soll das Verbot der Werbung für Fernbehandlungen (§ 9 Heilmittelwerbegesetz) gelockert werden.

3.3 Medizinprodukterecht

Von Beginn der Entwicklung an ist es unabdingbar zu wissen, ob das Endprodukt ein Medizinprodukt im Sinne des Medizinproduktegesetzes (MPG) bzw. der EU-Medizinprodukte-Verordnung (MDR) sein wird bzw. soll. Medizinprodukte dürfen nur in den Verkehr gebracht werden, wenn sie das jeweils kleinteilig vorgeschriebene Konformitätsbewertungsverfahren erfolgreich durchlaufen haben und dies durch CE-Kennzeichnung bestätigt wurde. Auch außerhalb dieses besonderen Marktzugangshindernisses enthält das Medizinprodukterecht, auch für

die Phase der Entwicklung und die Marktphase nach erstmaligem In-Verkehr-Bringen, vielfältige Vorschriften für Herstellerfirmen. Im Ergebnis führt das Label „Medizinprodukt" zu höheren Kosten, größeren Haftungsrisiken, der Gefahr von Verstößen gegen die vielen medizinprodukterechtlichen strafbewehrten und ordnungswidrigkeitsbewehrten Sicherheitsvorschriften und nicht zuletzt zur Verlängerung der Entwicklungsphase bis zum Marktzugang. Diese Nachteile können jedoch oft dadurch aufgewogen werden, dass die Herstellerfirma das Produkt als zertifiziertes Medizinprodukt vermarkten kann.

3.3.1 Definition „Medizinprodukt"

In § 3 Nr. 1 MPG wird legaldefiniert, was unter einem „Medizinprodukt" zu verstehen ist. Zunächst sind Medizinprodukte in Abgrenzung und als Gegenstück zu Arzneimitteln zu sehen. Des Weiteren begrenzt die Definition Medizinprodukte in stofflicher Hinsicht auf Instrumente, Apparate, Vorrichtungen, Stoffe, Zubereitungen aus Stoffen und explizit auch Software. Kern der Definition sind die in lit. a) bis d) genannten medizinischen Zwecke, welche ein Produkt zum „Medizinprodukt" machen. Auf die Zweckbestimmung eines Produktes für die genannten medizinischen Zwecke kann die Herstellerfirma Einfluss nehmen, etwa durch Aufschriften auf der Verpackung bzw. Beipackzetteln oder entsprechender Bewerbung (vgl. den Wortlaut: „die vom Hersteller (…) zum Zwecke (…) zu dienen bestimmt sind"; sog. „subjektive Zweckbestimmung").

Im E-Health-Bereich wurde in den letzten Jahren dahingehend vor allem der regulatorische Status von Health-Apps diskutiert. Doch auch andere E-Health-Produkte und -Angebote können Medizinprodukte sein, etwa durch Digitalisierung vernetzte Produkte in OP-Räumen oder die Videosprechstunde als solche. „Digitale Gesundheitsanwendungen" werden nach dem Entwurf des Digitale Versorgung-Gesetz nunmehr explizit als eigene Kategorie von Medizinprodukten im SGB V erwähnt. Versicherte sollen demnach einen Anspruch auf Versorgung mit digitalen Gesundheitsanwendungen haben, zudem soll am Bundesinstitut für Arzneimittel und Medizinprodukte ein Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen geführt werden.

3.3.2 Konkrete Einstufung als Medizinprodukt am Beispiel Health-App

Health-Apps sind „Software" im Sinne der Definition und damit in stofflicher Hinsicht taugliche Medizinprodukte. Entscheidend für eine Einstufung als solche ist die medizinische Zweckbestimmung (insbesondere: Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten). Bei Health-Apps ergeben sich große Abgrenzungsprobleme zu „lifestyle/wellness"-Apps und „Fitness-Apps", welche ebenfalls mit medizinischen Daten arbeiten und im weitesten Sinne gesundheitlichen Zwecken dienen. Eine „running-App", welche nicht nur die Strecke und Streckenlänge trackt, sondern auch Vitalfunktionen wie den Blutdruck oder die Atemfrequenz, dient rein funktional durchaus der Erkennung von Krankheiten, weil Anwendende durch eine Veränderung der Leistungsfähigkeit und/oder der getrackten Werte gesundheitliche Probleme frühzeitig erkennen können. Gleichwohl ist in diesem Beispiel offensichtlich, dass der Hauptzweck der App nicht in der Krankheitserkennung oder -prävention liegt. Bis dato besteht keine verlässliche Abgrenzung, wann eine App in Grenzfällen ein

Medizinprodukt ist, sondern allenfalls unverbindliche Richt- bzw. Leitlinien. Die Grenze zum Medizinprodukt dürfte jedenfalls dann überschritten sein, wenn die App aufbereitete Vitaldaten an den Arzt oder die Ärztin übermittelt oder selbst eine diagnostische oder therapeutische Entscheidung trifft oder eine solche Empfehlung gibt. Die oben angeführte Running-App wäre demnach kein Medizinprodukt, wohl aber etwa eine App, die die Medikamentendosis oder etwa den Zeitpunkt für eine Insulingabe berechnet. Grundsätzlich Medizinprodukte sind auch alle Apps, welche ein Medizinprodukt steuern. Im Bereich des E-Mental-Health wäre beispielsweise eine App, welche der Bewältigung von chronischem Stress dient und von der Herstellerfirma auch mit dem Zweck der Verbesserung des gesundheitlichen Zustandes vertrieben wird, als Medizinprodukt zu klassifizieren.

Ebenfalls nicht abschließend geklärt sind die Grenzen der subjektiven Zweckbestimmung der Herstellerfirma. Wie in 3.3.1 erläutert, kann diese nach dem Wortlaut der Medizinprodukt-Definition etwa durch eine entsprechende Bewerbung die Zweckbestimmung eines Produktes und damit dessen regulatorischen Status bestimmen. Dies ist jedoch nicht unbegrenzt möglich, der subjektiven Zweckbestimmung sind objektive Grenzen gesetzt. Im Kern geht es dabei um die Frage, inwieweit Herstellerfirmen bei einem Produkt, das objektiv offensichtlich medizinischen Zwecken dient, eine Klassifizierung als Medizinprodukt durch explizite Widmung für nicht-medizinische Zwecke verhindern können, etwa indem die Anwendung für medizinische Zwecke in der Gebrauchsanweisung ausgeschlossen wird. Hier ist zumindest bei vorwerfbaren Verhalten von Herstellerfirmen die Grenze zu ziehen. Handeln diese missbräuchlich, etwa weil Kenntnis über die faktische medizinische Verwendung des Produktes besteht, kann entgegen der expliziten Zweckbestimmung ein Medizinprodukt vorliegen. Der Bundesgerichtshof (BGH) zog die Grenze bei „Willkür" und der wissenschaftlichen Unhaltbarkeit bzw. Widersprüchlichkeit der Zweckbestimmung (BGH, Urt. v. 18.04.2013 - I ZR 53/09). Abgesehen von solchen Extremfällen kann durch Herstellerfirmen aber durchaus auf die regulatorische Einordnung als Medizinprodukt Einfluss genommen werden.

Wie sich gezeigt hat, ist hinsichtlich Zweckbestimmung und Klassifizierung ganz entscheidend, wer im Sinne des Medizinprodukterechts „Hersteller" ist (s. § 3 Nr. 15 MPG, Art. 2 Nr. 30 MPVO). Doch auch die anderen Vorschriften des Medizinprodukterechts adressieren primär den rechtlichen „Hersteller". Daher ist es für Entwickelnde gerade bei der Zusammenarbeit mit Externen unabdingbar, vorab zu klären, ob und wann sie rechtlich „Hersteller" sind.

4. Fazit

Der vorstehende Einblick in die bei der Entwicklung von E-Health-Angeboten wie etwa Health-Apps zu berücksichtigenden Normen und Vorschriften hat gezeigt, dass es diese spezifischen datenschutz- und medizinrechtlichen Vorgaben unbedingt erfordern, schon zu Konzeptionsbeginn die technischen bzw. digitalen Aspekte an ihre rechtlichen Auswirkungen anzupassen. In etwa muss vorab geklärt werden, ob das Endprodukt ein Medizinprodukt sein soll (dazu 3.3). Auch datenschutzrechtliche Vorgaben müssen bei der Entwicklung berücksichtigt werden, um die DSGVO-Konformität zu gewährleisten (dazu 2.). Außerdem setzen die rechtlichen Rahmenbedingungen, etwa im Bereich des Sozialrechts und der

berufsrechtlichen Maßgaben zur ärztlichen Fernbehandlung, für Entwickler und Entwicklerinnen Anregungen zur Entwicklung bestimmter E-Health-Angebote, geben aber auch tatsächliche Grenzen vor, außerhalb derer ein späterer Marktzugang unmöglich ist. Die in diesem Beitrag umrissenen rechtlichen Aspekte sind dabei keineswegs abschließend. Regulatorisches Kernthema der nächsten Jahre wird in etwa die krankenversicherungsrechtliche Erstattungsfähigkeit von E-Health-Angeboten und insbesondere Health-Apps sein, für die der Entwurf des Digitale Versorgung-Gesetzes erstmals spezifische Regelungen vorsieht.

Anmerkungen

[1] § 291a Abs. 5c Satz 2 SGB V.

[2] https://e-health-com.de/details-news/ein-fall-fuer-die-medizinproduktezertifizierung/3e35b34a0c74e668f9153c5b01acf49a/
(Zugriff am 13.06.2019).

[3] Die Einwilligung des Betroffenen ist auch für nicht besonders geschützte Daten, die nicht unter Art. 9 DSGVO fallen, ein Legitimationsgrund für die Verarbeitung personenbezogener Daten, vgl. Art. 6 Abs. 1 lit. a) DSGVO.

[4] https://www.aerztezeitung.de/kongresse/kongresse2018/erfurt2018_aerztetag/article/963610/121-deutscher-aerztetag-fernbehandlungsverbot-gekippt.html
(Zugriff am 13.06.2019).

Literatur

Albrecht, U.-V. (Hrsg.) (2016). *Chancen und Risiken von Gesundheits-Apps (CHARISMHA).* Zugriff am 13.06.2019. Verfügbar unter https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/A/App-Studie/CHARISMHA_gesamt_V.01.3-20160424.pdf

Bundesamt für Sicherheit in der Informationstechnik. *IT-Grundschutz.* Zugriff am 13.06.2019.
Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Gassner, U. M. (2018). Blockchain in EU E-Health – Blocked by the Barrier of Data Protection?, *CEJ 4*(2), 3 – 20. Zugriff am 13.06.2019.
Verfügbar unter http://ul.qucosa.de/api/qucosa%3A32043/attachment/ATT-0/