Gesundheitsrecht.blog

**Beitrag Nr. 22, Jahrgang 2023**

# Digitale Gesundheitsanwendungen und Datenschutz*

## Gesetzliche Rahmenbedingungen und behördliche Spezifikationen

**Dr. Maximilian Wagner und Bernhard Harle**

Veröffentlichung: Bochum, den 22.05.2023

Veröffentlichung auf gesundheitsrecht.blog/digitale-gesundheitsanwendungen-und-datenschutz

Bibliothekslink: https://doi.org/10.13154/294-9896

ISSN: 2940-3170

Empfohlene Zitierweise: *Wagner/Harle*, Gesundheitsrecht.blog Nr. 22, 2023, S.

Kurzzusammenfassung:

Digitale Gesundheitsanwendungen (DiGA) können von Ärzten und Psychotherapeuten verschrieben werden. Dazu müssen eine Reihe von Anforderungen erfüllt sein, insbesondere die Zertifizierung als Medizinprodukt und die Aufnahme in das DiGA-Verzeichnis. Dabei werden auch Anforderungen an den Datenschutz gestellt. Die Erklärung des DiGA-Herstellers, dass die Anforderungen an den Datenschutz erfüllt wurden, wird ab Mitte 2024 auf ein Zertifizierungsverfahren umgestellt. Durch die entsprechenden Prüfkriterien des Bundesinstituts für Arzneimittel und Medizinprodukte erfährt das Prüfverfahren eine detailgenauere Standardisierung.



* Der Beitrag beruht auf einem Vortrag den die Verfasser am 9. Mai 2023 im Rahmen des Health & Law Netzwerks der Rechtsanwaltskanzlei Schürmann Rosenthal Dreyer und der ISiCO Datenschutz GmbH gehalten haben.

Hrsg.: Institut für Sozial- und Gesundheitsrecht | Universitätsstraße 150 | 44801 Bochum | redaktion@gesundheitsrecht.blog
Schriftenleiter u. Verantwortlicher für die redaktionellen Inhalte: Prof. Dr. Stefan Huster | Redaktionsleitung: Paul Bidmon

## I. Herausforderungen und Chancen

Digitale Gesundheitsanwendungen (DiGA) eröffnen neue Möglichkeiten in der medizinischen und psychologischen Patientenversorgung. Die sogenannten Apps auf Rezept unterscheiden sich von herkömmlichen Apps durch ihre Zertifizierung als Medizinprodukt und von anderen Medizinprodukten dadurch, dass sie auf digitalen Technologien beruhen. Ärzte und Psychotherapeuten können DiGA verschreiben. Die Kosten werden grundsätzlich von den Krankenkassen übernommen. Die Erstattungsfähigkeit ist jedoch an die Einhaltung bestimmter Qualitätsvorgaben und den Nachweis „positiver Versorgungseffekte" gekoppelt.[1] Den Chancen, die sich damit für Versicherte und die Hersteller solcher DiGA gleichermaßen bieten, stehen allerdings beträchtliche Risiken gegenüber. Fünf von derzeit 53 verzeichneten DiGA sind in den letzten Wochen durch Negativschlagzeilen aufgefallen: In drei Fällen wurden Patientendaten entgegen den gesetzlichen Vorgaben auf amerikanischen Servern gehostet, in zwei Fällen gelang es Sicherheitsforschern sogar, an sensible Daten heranzukommen, die in der App verarbeitet wurden.[2] Der folgende Beitrag bietet einen ersten Überblick über die rechtlichen Anforderungen, die DiGA erfüllen müssen, und wirft dabei ein Schlaglicht auf die Herausforderungen, vor denen Unternehmen stehen, die eine DiGA anbieten und sich also dem Bewertungsverfahren nach § 139e SGB V unterziehen müssen.

## II. Rechtliche Rahmenbedingungen: DVG, SGB V und DiGAV

### 1. Das DVG als gesundheitspolitischer Ausgangspunkt

Am 19. Dezember 2019 ist das Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (DVG) in Kraft getreten.[3] Das DVG regelt unter anderem die Integration digitaler Gesundheitsanwendungen in die medizinische und psychologische Regelversorgung, räumt gesetzlich Versicherten also einen Anspruch ein auf die „Versorgung mit Medizinprodukten niedriger Risikoklasse, deren Hauptfunktion wesentlich auf digitalen Technologien beruht und die dazu bestimmt sind, bei den Versicherten oder in der Versorgung durch Leistungserbringer die Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder die Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen zu unterstützen", § 33a Abs. 1 S. 1 SGB V. Dieser Anspruch umfasst allerdings nur solche Gesundheitsanwendungen, die ein bestimmtes Verfahren durchlaufen haben und vom Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) in ein besonderes Verzeichnis – das Verzeichnis für digitale Gesundheitsanwendungen nach § 139e SGB V –

---

1 Kritisch zu diesem schillernden Begriff, Techniker Krankenkasse, DiGA-Report 2022, S. 10.

2 Vgl. Eva Wolfangel, Wenn Hacker mit Gesundheits-Apps besonders leichtes Spiel haben, in: Die Zeit vom 9. Mai 2023.

3 Eine konzise Einführung in die Regelungsmaterie bietet Frank Sarangi, Das Digitale-Versorgung-Gesetz (DVG) – ein komprimierter Überblick zum Einstieg, in GuP 2021, 11.

aufgenommen wurden.[4] Damit war bereits vor Inkrafttreten des DVG klar, dass sich die Beratung von DiGA-Herstellern vor allem auf zwei Punkte konzentrieren würde: die Marktzulassung als Medizinprodukt niedriger Risikoklasse und die Eintragung in das DiGA-Verzeichnis.

## 2. Exkurs: Zertifizierung als Medizinprodukt niedriger Risikoklasse

Anders als Arzneimittel werden Medizinprodukte nicht zugelassen, sondern zertifiziert. Die Zertifizierung eines Medizinprodukts erfolgt nach Abschluss eines umfangreichen Verfahrens, in dem eine „Benannte Stelle" prüft, ob das Produkt die jeweils zu erfüllenden Anforderungen erfüllt. Die Bedingungen dieser Prüfung werden insbesondere durch das Medizinprodukterecht-Durchführungsgesetz (MPDG), die Verordnung (EU) 2017/745 (Medical Device Regulation, MDR) und die Verordnung (EU) 2017/746 (In-Vitro Diagnostics Regulation, IVDR) näher bestimmt. Die MDR definiert, bei welchen Produkten es sich um Medizinprodukte handelt, und legt die Risikoklassen fest, die Art und Umfang des Zertifizierungsverfahrens konkretisieren. Ein Medizinprodukt ist nach Art. 2 Nr. 1 MDR ein Gegenstand, der „dem Hersteller zufolge für Menschen bestimmt ist und allein oder in Kombination einen oder mehrere spezifische medizinische Zwecke erfüllen soll und dessen bestimmungsgemäße Hauptwirkung im oder am menschlichen Körper weder durch pharmakologische oder immunologische Mittel noch metabolisch erreicht wird, dessen Wirkungsweise aber durch solche Mittel unterstützt werden kann". Jedes Medizinprodukt wird dabei einer von vier Risikoklassen zugeordnet. Die MDR unterscheidet insofern zwischen geringem, mittlerem, erhöhtem und hohem Risiko (Klasse I, IIa, Iib und III). Als Medizinprodukte mit niedriger Risikoklasse gelten grundsätzlich – es gibt Ausnahmen – Produkte der Risikoklasse I oder Iia, § 33a Abs. 2 SGB V.

Welcher Risikoklasse eine Anwendung zugeordnet wird, hängt maßgeblich von der geplanten Nutzung ab. Software unterfällt nach der Klassifizierungsregel 11 im Anhang VIII zur MDR grundsätzlich Risikoklasse I. Von diesem Grundsatz sieht die Regel jedoch zwei Ausnahmen und zwei Unterausnahmen vor: Soll die Software Informationen bereitstellen, die für eine Diagnose oder Therapie herangezogen werden, so wird sie prinzipiell in Klasse Iia eingestuft. Kann die Diagnose oder Therapie den Tod, eine irreversible oder schwerwiegende Verschlechterung des Gesundheitszustandes oder einen chirurgischen Eingriff zur Folge haben, unterfällt sie sogar den Risikoklassen Iib (schwerwiegende Verschlechterung, chirurgischer Eingriff) oder III (Tod, irreversible Verschlechterung). Soll die Software eingesetzt werden, um physiologische Prozesse zu kontrollieren, so gehört sie grundsätzlich zur Risikoklasse Iia. Kann eine Änderung dieser vitalen physiologischen Parameter aber zu einer unmittelbaren Gefahr für den Patienten führen, so wird sie ausnahmsweise der Risikoklasse Iib zugeordnet.

[4] Das DiGa-Verzeichnis kann online unter https://diga.bfarm.de/de/verzeichnis eingesehen werden.

## 3. Eintragung in das DiGA-Verzeichnis

Die Eintragung in das DiGA-Verzeichnis erfolgt auf elektronischen Antrag des Herstellers beim BfArM, wenn die Anwendung kumulativ

1. den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität einschließlich der Interoperabilität des Medizinproduktes entspricht,
2. den Anforderungen an den Datenschutz entspricht und die Datensicherheit nach dem Stand der Technik gewährleistet und
3. positive Versorgungseffekte aufweist, § 139e Abs. 2 SGB V.

Diese Anforderungen werden durch die – zwischenzeitlich bereits mehrfach geänderte – Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) weiter konkretisiert. Darüber hinaus hat das BfArM im Einvernehmen mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) mittlerweile die Anforderungen an den Datenschutz spezifiziert, die DiGA-Hersteller erfüllen müssen. Bis zum 1. Januar 2024 legt das BSI im Einvernehmen mit dem BfArM und im Benehmen mit dem BfDI fest, welche Anforderungen an die Datensicherheit Hersteller erfüllen müssen. In beiden Fällen muss ab Mitte 2024 anhand eines Zertifikats der Nachweis geführt werden, dass eine DiGA die Anforderungen nach § 139e Abs. 2 Nr. 2 SGB V erfüllt, § 139e Abs. 10 und 11 SGB V.

### a) Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität

Die digitale Gesundheitsanwendung muss den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität einschließlich der Interoperabilität des Medizinproduktes entsprechen.

#### (1) Anforderungen an Sicherheit und Funktionstauglichkeit

Der Nachweis der Sicherheit und Funktionstauglichkeit gilt mit der Zertifizierung als Medizinprodukt und der CE-Konformitätskennzeichnung grundsätzlich als erbracht. Allerdings kann das BfArM aus begründetem Anlass eine zusätzliche Prüfung vornehmen und insbesondere die für das Konformitätsbewertungsverfahren notwendigen Erklärungen und Bescheinigungen, verlangen, § 3 DiGAV.

### (2) Anforderungen an die Qualität

Digitale Gesundheitsanwendungen müssen die in § 5 DiGAV genannten und in Anlage 2 DiGAV spezifizierten Qualitätsmerkmale erfüllen, um in das DiGA-Verzeichnis aufgenommen zu werden. Sie müssen also die Anforderungen der technischen und semantischen Interoperabilität, des Verbraucherschutzes und der Barrierefreiheit umsetzen (§ 5 Abs. 1, 3 und 6), so gestaltet sein, dass sie robust gegen Störungen und Fehlbedienungen sowie frei von Werbung sind (Abs. 2 und 4), außerdem leicht und intuitiv bedienbar sein und Maßnahmen zur Unterstützung der Versicherten und der Patientensicherheit vorsehen (Abs. 5 und 9 DiGAV). Die verwendeten medizinischen Inhalte und (Gesundheits-)Informationen müssen dem allgemein anerkannten Stand der medizinischen Erkenntnisse entsprechen (§ 5 Abs. 8 DiGAV). Die Anforderungen an die Interoperabilität werden durch die §§ 6 und 6a DiGAV näher bestimmt. Weitere Details sind der Anlage 2 DiGAV zu entnehmen, die eine Erklärung enthält, die der Hersteller seinem Antrag auf Eintragung in das DiGA-Verzeichnis nach § 5 Abs. 11 DiGAV beizufügen hat. In dieser Erklärung kann der Hersteller auch begründen, warum seine Anwendung im Einzelfall von den regulativen Vorgaben abweicht, aber die Anforderung an die Qualität gleichermaßen erfüllt, § 5 Abs. 10 S. 2 und 3 DiGAV.

### (3) Nachweis durch Zertifikate

Das BfArM kann von dem Hersteller die Vorlage von Zertifikaten verlangen, die die Erfüllung der Anforderungen nach den §§ 4 bis 6 DiGAV bestätigen, § 7 Abs. 1 S. 1 DiGAV. Es kann außerdem verlangen, dass ihm Berichte über die Durchführung von Penetrationstests, Sicherheitsgutachten über die Komponenten und Dienste der digitalen Gesundheitsanwendung sowie geeignete Zertifikate oder Nachweises über ein Informationssicherheitsmanagement vorgelegt werden, § 7 Abs. 3 S. 1 und 2 DiGAV.

## b) Anforderungen an den Nachweis positiver Versorgungseffekte

Darüber hinaus muss der Hersteller den Nachweis positiver Versorgungseffekte führen. Positive Versorgungseffekte können medizinischer Nutzen oder patientenrelevante Struktur- und Verfahrensverbesserungen in der Versorgung sein, § 8 Abs. 1 DiGAV. Als medizinischer Nutzen gilt jeder patientenrelevante Effekt insbesondere hinsichtlich der Verbesserung des Gesundheitszustands, der Verkürzung der Krankheitsdauer, der Verlängerung des Überlebens oder einer Verbesserung der Lebensqualität, § 8 Abs. 2 DiGAV. Patientenrelevanten Struktur- und Verfahrensverbesserungen in der Versorgung sind im Rahmen der Erkennung, Überwachung, Behandlung oder Linderung von Krankheiten oder der Erkennung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen auf eine Unterstützung des Gesundheitshandelns der Patientinnen und Patienten oder eine Integration der Abläufe zwischen Patientinnen und Patienten und Leistungserbringern ausgerichtet, § 8 Abs. 3 DiGAV.

Zum Nachweis der positiven Versorgungseffekte muss der Hersteller eine Vergleichsstudie vorlegen, die zeigt, dass die Anwendung der digitalen Gesundheitsanwendung besser ist als deren Nichtanwendung (Nichtbehandlung oder Behandlung ohne DiGA) oder vergleichbare DiGA, § 10 Abs. 1 S. 1, Abs. 2 und Abs. 4 S. 1 und 3 DiGAV. Dabei muss es sich nach § 10 Abs. 1 S. 2, Abs. 2 und 3 DiGAV prinzipiell um eine quantitative Studie handeln, die entweder im Inland durchgeführt wurden oder deren Übertragbarkeit auf den deutschen Versorgungskontext ausreichend belegt ist, § 10 Abs. 5 DiGAV. Die Studien müssen im Internet veröffentlicht werden, den rechtlichen Vorgaben genügen und wissenschaftlichen Standards entsprechen, § 10 Abs. 6 S. 1 und Abs. 7 DiGAV. Enthält eine digitale Gesundheitsanwendung ein diagnostisches Instrument, so hat der Hersteller zusätzlich die Sensitivität und Spezifität der digitalen Gesundheitsanwendung im Hinblick auf die angegebene Patientengruppe zu ermitteln, § 12 Abs. 1 DiGAV. Genauere Anforderungen an Studien zum Nachweis positiver Versorgungseffekte finden sich im Leitfaden des BfArM für Hersteller, Leistungserbringer und Anbieter.[5]

Kann der Hersteller den Nachweis des positiven Versorgungseffekts (noch) nicht erbringen, so ist auch eine vorläufige Aufnahme in das DiGA-Verzeichnis möglich. Dann erfolgt die Aufnahme in die Regelversorgung zur Erprobung der Anwendung über einen Zeitraum von zwölf Monaten, der auch bis zu 24 Monaten ausgedehnt werden kann, § 139e Abs. 4 SGB V. In diesem Fall muss der Hersteller allerdings plausibel begründen, dass im Rahmen einer Erprobung ein positiver Versorgungseffekt nachgewiesen werden kann, und mindestens die Ergebnisse einer systematischen Datenauswertung zur Nutzung der digitalen Gesundheitsanwendung vorlegen, § 14 DiGAV.

### c) Anforderungen an den Datenschutz und die Datensicherheit

Dass DiGA die gesetzlichen Anforderungen an den Datenschutz und die Datensicherheit erfüllen müssen, ist selbstverständlich und wird von § 4 Abs. 1 DiGAV daher nur deklaratorisch hervorgehoben. Von diesen Vorgaben abweichende Bestimmungen finden sich insbesondere in den Absätzen 2 und 3, die mögliche Zwecke, mögliche Rechtsgrundlagen und Standorte der Datenverarbeitung engführen. Nach § 4 Abs. 4 S. 1 DiGAV dürfen „personenbezogene Daten“ – bei europarechtskonformer Auslegung müsste es wohl Gesundheitsdaten heißen, vgl. Art. 9 Abs. 4 DSGVO – durch DiGA ausschließlich zu den folgenden Zwecken verarbeitet werden:

1. zu dem bestimmungsgemäßen Gebrauch der digitalen Gesundheitsanwendung durch die Nutzer,
2. zu dem Nachweis positiver Versorgungseffekte im Rahmen einer Erprobung nach § 139e Abs. 4 SGB V,
3. zu der Nachweisführung bei Vereinbarungen nach § 134 Abs. 1 S. 3 SGB V,

[5] BfArM, Das Fast-Track-Verfahren für DiGA nach § 139e SGB V, S. 102ff.

4. zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung, § 4 Abs. 2 S. 1 DiGAV.

Eine Verarbeitung zu Werbezwecken ist explizit ausgeschlossen, § 4 Abs. 4 S. 1 DiGAV.[6] Darüber hinaus dürfen diese Daten nur auf Grundlage einer Einwilligung nach Art. 9 Abs. 2 lit. a DSGVO verarbeitet werden, wobei die Einwilligung in die Datenverarbeitung nach § 4 Abs. 2 S. 1 Nr. 4 getrennt von einer Einwilligung in die Datenverarbeitung für Zwecke nach S. 1 Nr. 1 bis 3 einzuholen ist, § 4 Abs. 2 S. 2 DiGAV. Schließlich darf die Verarbeitung von personenbezogenen Daten durch die Gesundheitsanwendung selbst oder etwaige Auftragsverarbeiter nur im Inland, in einem Mitgliedstaat der Europäischen Union, einem diesen Staaten nach § 35 Abs. 7 SGB I gleichgestellten Staat oder einem Drittstaat erfolgen, für den ein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt.

Weitere Einzelheiten werden einerseits durch eine Erklärung geregelt, die der Hersteller bei Antragsstellung vorlegen muss (Anlage 1 DiGAV), andererseits durch Prüfkriterien für die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an den Datenschutz, die das BfArM im Einvernehmen mit dem BfDI und im Benehmen mit dem BSI erarbeitet und in der Regel jährlich – zum 31. März jeden Jahres – aktualisiert, § 139e Abs. 11 DiGAV.

## III. Im Einzelnen: Erklärung des Herstellers und Prüfkriterien des BfARM

### 1. Die Erklärung nach § 4 Abs. 6 DiGAV

Die Aufnahme in das DiGA-Verzeichnis erfolgt auf elektronischen Antrag des Herstellers, § 139e Abs. 2 S. 1 SGB V. Nach § 4 Abs. 6 S. 2 DiGAV enthält der Antrag zur Aufnahme einer DiGA in das DiGA-Verzeichnis eine Erklärung über die Erfüllung der Anforderungen an den Datenschutz und die Datensicherheit. Gegenwärtig erfolgt diese Erklärung in Form der Anlage 1, § 4 Abs. 6 DiGAV. Dabei handelt es sich um einen Fragebogen mit 40 Fragen zum Datenschutz, 39 Fragen zur Datensicherheit und sechs Zusatzfragen für DiGA mit sehr hohem Schutzbedarf, der vom Hersteller auszufüllen ist. Der Fragebogen enthält Fragen zu unterschiedlichen Themenfeldern beispielsweise zur Einwilligung, zur Zweckbindung oder zur Angemessenheit. Inhaltlich ergeben sich gegenüber den oben skizzierten und allgemeingültigen Anforderungen an den Datenschutz und die Datensicherheit – insbesondere gegenüber der DSGVO – kaum Besonderheiten. Der Fragebogen orientiert sich an den gesetzlichen Vorgaben und lässt dem Hersteller nur wenig Spielraum: Die Antwortmöglichkeiten sind auf „zutreffend“

[6] Dass die Daten nicht zu Werbezwecken verarbeitet werden dürfen und DiGA frei von Werbung sein müssen, §§ 4 Abs. 4 S. 1, 5 Abs. 4 DiGAV, bedeutet nicht, dass sie nicht beworben werden dürfen. Allerdings sind – da es sich um Medizinprodukte handelt – die besonderen Anforderungen des Heilmittelwerbegesetzes (HWG) zu beachten, vgl. Julian Braun, Die Bewerbung von digitalen Gesundheitsanwendungen i. S. d. § 33a Abs. 1 SGB V vor dem Hintergrund des Irreführungsverbots des § 3 S. 2 Nr. 1 HWG, in: PharmR 2021, 1.

und „nicht zutreffend“ beschränkt. In einer dritten Spalte sind zulässige Begründungen für „nicht zutreffend“ aufgeführt. Der Fragebogen trägt daher den Charakter einer Checkliste. Er dient nicht der genauen Erfassung des individuellen Datenschutz- und Datensicherheitsniveaus.

## 2. Prüfkriterien nach § 139e Abs. 11 SGB V

In absehbarer Zeit wird die Erklärung des Herstellers per Fragebogen durch ein Zertifikat nach Art. 42 DSGVO ersetzt. Ab dem 1. August 2024 (für die Anforderungen an die Datensicherheit ab dem 1. Januar 2025) sind daher nicht mehr die Herstellerangaben, sondern die nach § 139e Abs. 10 und 11 SGB V festgelegten Prüfkriterien maßgeblich. Bis es so weit ist, sollen die Prüfkriterien außerdem auch als „Interpretationshilfe für die deutlich grobgranulareren Anforderungen der Anlage 1 DiGAV“ herangezogen werden. Das BfArM gibt daher zu bedenken, dass es „vorrangig eine Auslegung [der Fragen] anerkennen [wird], die im Einklang mit den zukünftig geltenden Prüfkriterien steht“.[7]

Bei den bereits vorliegenden „Prüfkriterien für die von digitalen Gesundheitsanwendungen (DiGA) und digitalen Pflegeanwendungen (DiPA) nachzuweisenden Anforderungen an den Datenschutz“ – die Datensicherheit erhält eigene Prüfkriterien und ein eigenes Zertifikat – handelt es sich um ein knapp 80 Seiten umfassendes Dokument, das mit seinem Spezifikationsstil als Grundlage für die Zertifizierung dient. Damit unterscheidet es sich bereits in Darstellung und Umfang deutlich von dem Fragebogen in Anlage 1 DiGAV. Das Dokument ist in vier Teile gegliedert. In Teil 1 werden die maßgeblichen Definitionen vorangestellt, Teil 2 enthält die eigentlichen Spezifikationen, Teil 3 behandelt Verantwortliche und Auftragsverarbeiter. Im vierten und letzten Teil werden nurmehr die Anlagen gelistet. Jeder Teil enthält ein oder mehrere Kapitel, die – mit Ausnahme der Begriffsbestimmungen und Referenzen – dieselben fünf Unterkapitel enthält: „Regulatorische Grundlagen“, „Gegenstandsbereich und Motivation“, „Kriterien“, „Allgemeine Erläuterungen“ und „Spezifische Erläuterungen“. Als regulatorische Grundlagen wird in erster Linie auf die DSGVO Bezug genommen. Außerdem werden das Bundesdatenschutzgesetz (BDSG) und die DiGAV referenziert. Unter „Gegenstandsbereich und Motivation“ wird der Kontext des Themenfeldes skizziert. Eigentlicher Kern der Prüfkriterien sind demnach die Unterkapitel „Kriterien“, in denen die konkreten Spezifikationen aufgelistet werden.

Auch hier ergeben sich gegenüber den referenzierten Gesetzen und Verordnungen nur wenige Besonderheiten. Die Prüfkriterien geben die Anforderungen der jedem Kapitel vorangestellten regulatorischen Grundlagen wieder. Dabei werden die entsprechenden Anforderungen zum Teil selbstständig weitergedacht und zum Teil angereichert durch die Erwägungsgründe der DSGVO und die Positionen der deutschen und europäischen Aufsichtsbehörden. So werden beispielsweise die Anforderungen an eine wirksame Einwilligung in enger Anlehnung an die

[7] BfArM, Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V, S. 54.

Erwägungsgründe 42 und 43 DSGVO sowie das Kurzpapier Nr. 20 der Datenschutzkonferenz (Einwilligung nach der DSGVO) formuliert.[8] Einige Kapitel beruhen auch explizit auf den sogenannten Gewährleistungszielen des Standard-Datenschutzmodells (SDM) des Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – insbesondere die Grundsätze der Nichtverkettbarkeit und Intervenierbarkeit.[9]

Die Prüfkriterien sind letztlich eine Verquickung eigener Rechtsansichten des BfArM mit den Leitlinien und Interpretationsvorgaben der diversen Aufsichtsbehörden. Dies soll abschließend an einem Beispiel demonstriert werden: Die DSGVO stellt in Art. 5 bestimmte Grundsätze für die Verarbeitung personenbezogener Daten auf. Nach Art. 5 Abs. 1 lit. b DSGVO müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"). Außerdem müssen sie grundsätzlich in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung", Art. 5 Abs. 1 lit. e DSGVO). Beide Grundsätze werden in der DSGVO weiter nicht spezifiziert. Lediglich in Erwägungsgrund 39 DSGVO finden sich einige wenige Hinweise, wie Daten minimiert und Speicher zu begrenzen sind. In den Prüfkriterien des BfArM werden aus diesen Grundsätzen, Erwägungsgrund 39 und den einschlägigen Stellen des SDM dann spezifische Kriterien für Erfordernis und Angemessenheit (DMN_1), Löschen (DMN_2), Datensparsamkeit (DMN_3), Benutzer-Account und Grace-Period (DMN_4). Konkret heißt es beispielsweise: „Der Verantwortliche der digitalen Anwendung MUSS für die Anwendung ein an den Vorgaben der [DIN 66398] ausgerichtetes Löschkonzept erstellen und MUSS nachweisen können, dass die im Löschkonzept festgeschriebenen Löschregeln und Umsetzungsregeln rechtmäßig und wirksam sind." (DMN_2.1)

## IV. Schluss und Ausblick

Bei der Integration digitaler Gesundheitsanwendungen in die medizinische und psychologische Regelversorgung hat sich der deutsche Gesetzgeber zunächst für Geschwindigkeit und gegen Gewissheit entschieden: Fast-Tracks[10] statt langwieriger Verfahren, Vertrauen in Herstellerangaben statt Kontrolle der Dokumentation. Und die Möglichkeit, den Nachweis positiver Versorgungseffekte nachzureichen. Diese Entscheidung ist vielfach als zu herstellerfreundlich kritisiert worden – gerade auch im Hinblick an die sonst strengen Anforderungen an erstattungsfähige Leistungen.[11] Umgekehrt wurde eingewandt, dass das Innovations- und Versorgungspotential der „Apps auf Rezept" durch überzogene

[8] Vgl. BfArM, Prüfkriterien für die Anforderungen an den Datenschutz, S. 11.

[9] Ebd., S. 23 und 32. Das Standard-Datenschutzmodell kann auf der Seite des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (unter https://www.datenschutzzentrum.de/sdm/) eingesehen werden.

[10] Damit ist in erster Linie gemeint, dass das BfArM vollständige Anträge innerhalb von drei Monaten nach Eingang bearbeitet, vgl. BfArM, Das Fast-Track-Verfahren für DiGA nach § 139e SGB V, S. 8.

[11] Vgl. Stefanie Stoff-Ahnis, Digitale Gesundheitsanwendungen – Das erste Jahr aus Sicht der Gesetzlichen Krankenversicherung, in: MedR 2022, 285, 287.

Anforderungen an den Datenschutz und die Datensicherheit erheblich gemindert werde. Auf der einen Seite ist abzusehen, dass der Weg von der Idee zur Erstattungsfähigkeit in Zukunft länger dauern wird. Damit steigt zugleich das Risiko, dass die erstrebte Aufnahme in das DiGA-Verzeichnis letztlich scheitert. Höhere Risiken bedeuten niedrigere Investitionen, niedrigere Investitionen führen – zumal im Start-Up-Bereich – zu weniger Geld für Data Governance und Compliance-Prozesse. Auf der anderen Seite zeigt eine nähere Betrachtung der bislang vorliegenden Prüfkriterien, dass sie einer bestimmten Lesart geltenden (Datenschutz-)Rechts kaum etwas hinzufügen. Die Umstellung von Fragebogen und Erklärung auf Prüfkriterien und Zertifikaten ist daher keine verkappte Revolution, die unbestimmte Herausforderungen mit sich bringt, sondern eine Evolution, die hoffentlich dazu führt, dass die ohnehin zu erfüllenden Anforderungen an den Datenschutz und die Datensicherheit endlich umgesetzt werden.