



TaylorWessing

Digitalisierung im Gesundheitswesen – Chancen und Herausforderungen für Medizinproduktehersteller und Vertreiber

Digitale Woche „Aktuelle Entwicklungen im
Medizinprodukterecht“

11.3.2021

Agenda

- 1 „App auf Rezept“ –Digitale Gesundheitsanwendungen (DiGa)
 - Marktzugangsvoraussetzungen und aktuelle Entwicklungen
 - Datenschutzrechtliche Anforderungen an Digitale Gesundheitsanwendungen
- 2 Intelligente und selbstlernende Medizinprodukte – Marktzutrittsvoraussetzungen und andere Herausforderungen



1

„App auf Rezept“ – Digitale Gesundheitsanwendungen (DiGa)

Dr. Angela Knierim, Thanos Rammos

1a

Marktzugangsvoraussetzungen und aktuelle Entwicklungen

Dr. Angela Knierim

Was ist eine DiGA? (I/II)

- Das Gesetz spricht von **“digitalen Gesundheitsanwendungen”**.
- Mit dem DVG hat der Gesetzgeber in § 33a SGB V einen Leistungsanspruch der Versicherten auf DiGAs geschaffen.
- Auf dieser Grundlage können Ärztinnen und Ärzte DiGAs verschreiben.
- **Die Kosten werden von der GKV erstattet.**



Was ist eine DiGA? (II/II)

Charakteristika der DiGA (vgl. § 33a Abs. 1 Satz 1 SGB V):

- Medizinprodukt
- Hauptsächlich digitale Funktion
- Niedrige Risikoklasse (Klasse I oder IIa nach der Verordnung [EU] 2017/745 [MDR], vgl. § 33a Abs. 2 SGB V)
- Medizinischer Zweck



Wie kommt die DiGA auf den Markt?

Regulatorischer Marktzugang

Erstattung

- Obligatorisch
- Voraussetzung für ein rechtmäßiges Inverkehrbringen
- Anforderungen der Verordnung (EU) 2017/745 (Medical Devices Regulation – „MDR“, gilt ab dem 26. Mai 2021)

- Fakultativ
- Voraussetzung für Kostenübernahme durch die gesetzlichen Krankenversicherungen (GKV)
- Anforderungen des SGB V



Überblick: Erstattungsvoraussetzungen (I/III)

§ 33a Abs. 1 Satz 1 SGB V

Versicherte haben Anspruch auf Versorgung mit

- Medizinprodukten niedriger Risikoklasse,
- deren Hauptfunktion wesentlich auf digitalen Technologien beruht
- 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 (digitale Gesundheitsanwendungen).



Überblick: Erstattungs Voraussetzungen (II/III)

Weitere Voraussetzungen

- Aufnahme in das Verzeichnis für digitale Gesundheitsanwendungen nach § 139e SGB V ("DiGA-Verzeichnis") des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM)

und

- ärztliche/psychotherapeutische Verordnung oder Genehmigung der Krankenkasse

(§ 33a Abs. 1 Satz 2 SGB V)



Überblick: Erstattungs Voraussetzungen (III/III)

Weitere Voraussetzungen

Kein Erstattungsanspruch für DiGAs, die Leistungen enthalten, die

- nach dem 3. Kapitel des SGB V ausgeschlossen sind
- oder
- über die der G-BA bereits eine ablehnende Entscheidung nach den §§ 92, 135 oder 137c SGB V getroffen hat
- (§ 33a Abs. 4 Satz 2 SGB V)



Wie kommt die Health App in das Verzeichnis nach § 139e SGB V? (I/II)

- Antrag des Herstellers beim BfArM (elektronisch)
- Nachweis, dass die Health App
 1. den Anforderungen an Sicherheit, Funktionstauglichkeit und Qualität des Medizinproduktes entspricht,
 2. den Anforderungen an den Datenschutz entspricht und die Datensicherheit nach dem Stand der Technik gewährleistet und
 3. positive Versorgungseffekte aufweist.(vgl. § 139e Abs. 2 SGB V)
- Details zum Aufnahmeverfahren regelt die Verordnung über das Verfahren und die Anforderungen der Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenkasse (Digitale-Gesundheitsanwendungen-Verordnung – „DiGAV“).
- Zudem gibt der Leitfaden „Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 139e SGB V“ des BfArM weitere Hinweise.



Wie kommt die Health App in das Verzeichnis nach § 139e SGB V? (II/II)

- Der Antrag beim BfArM kann auf eine vorläufige oder eine endgültige Aufnahme gerichtet sein.
- Eine endgültige Aufnahme kann beantragt werden, wenn der Hersteller eine vergleichende Studie zum Nachweis eines positiven Versorgungseffekts durchgeführt hat (Vergleich: Mit DiGA besser als ohne?).
- Ansonsten kann ein Antrag auf vorläufige Aufnahme gestellt werden (Erprobung).



Was ist ein positiver Versorgungseffekt?

- Begriff geregelt in § 8 Abs. 1 DiGAV
- Positive Versorgungseffekte sind entweder (alternativ!):

Medizinischer Nutzen

Patientenrelevanter therapeutischer Effekt:

- Verbesserung des Gesundheitszustands
- Verkürzung der Krankheitsdauer
- Verlängerung des Überlebens
- Verbesserung der Lebensqualität

Patientenrelevante Struktur- und Verfahrensverbesserungen in der Versorgung

Erkennung, Überwachung, Behandlung oder Linderung (bzw. Kompensation) von Krankheiten (bzw. Verletzungen / Behinderungen)

Auf eine Unterstützung des Gesundheitshandelns der Patienten oder eine Integration der Abläufe zwischen Patienten und Leistungserbringern ausgerichtet

umfasst insbesondere folgende Bereiche:

- Koordination von Behandlungsabläufen
- Ausrichtung der Behandlung an Leitlinien und anerkannten Standards
- Adhärenz (Therapiecompliance)
- Erleichterung des Zugangs zur Versorgung
- Patientensicherheit
- Gesundheitskompetenz
- Patientensouveränität
- Bewältigung krankheitsbedingter Schwierigkeiten im Alltag
- Reduzierung der therapiebedingten Aufwände und Belastungen der Patienten und ihrer Angehörigen

DiGA-Verzeichnis: Wie ist der aktuelle Stand? (I/II)

Wie viele Anträge wurden seit dem Start des DiGA-Antragsportals zur Prüfung beim BfArM eingereicht?

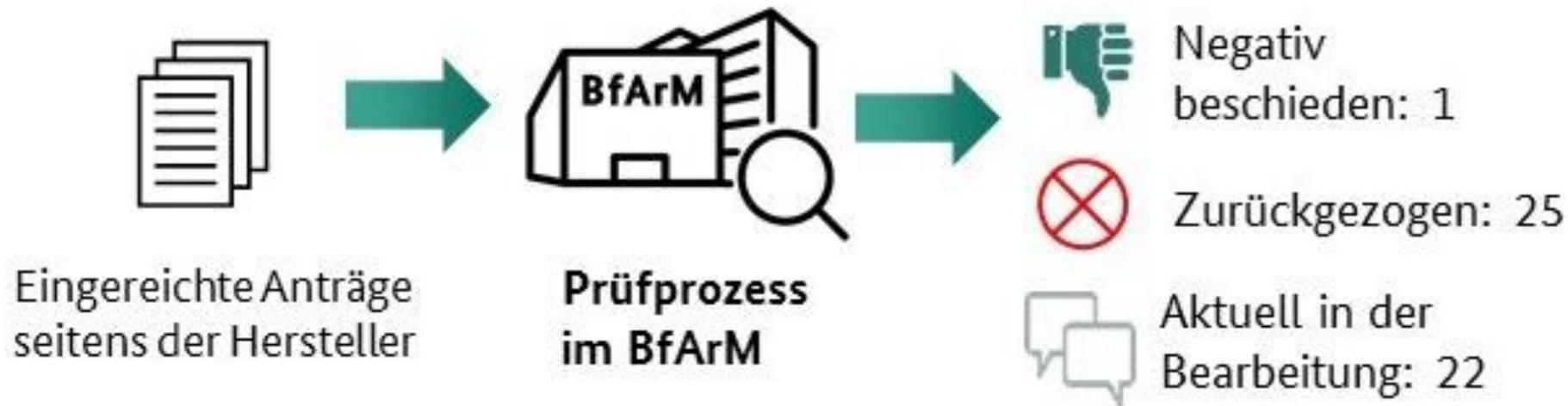


Grafik aktualisiert am:
04.03.2021

Quelle: https://www.bfarm.de/DE/Medizinprodukte/DVG/_node.html;
zuletzt abgerufen am 9. März 2021.

DiGA-Verzeichnis: Wie ist der aktuelle Stand? (II/II)

Was ist das Ergebnis zu den bisherigen Prüfungen der Anträge im BfArM?



Was für DiGAs sind im Verzeichnis gelistet?

Apps für

- Depressionen
- Tinnitus-Beschwerden
- Multiple Sklerose
- Angststörungen
- Schlafstörungen
- Migräne
- Nachsorge von Schlaganfällen
- Gelenkschmerzen
- Adipositas

Abrufbar unter: diga.bfarm.de

Aktuell: Debatte mit Blick auf S3-Leitlinie zu Angsterkrankungen. Bei der in Kürze abgeschlossenen Neufassung werden DiGA wohl nicht berücksichtigt. Als Grund wird die fehlende wissenschaftliche Fundierung genannt – der Nachweis eines positiven Versorgungseffekts sei nicht ausreichend.

Wie ist die Akzeptanz in der Ärzteschaft?

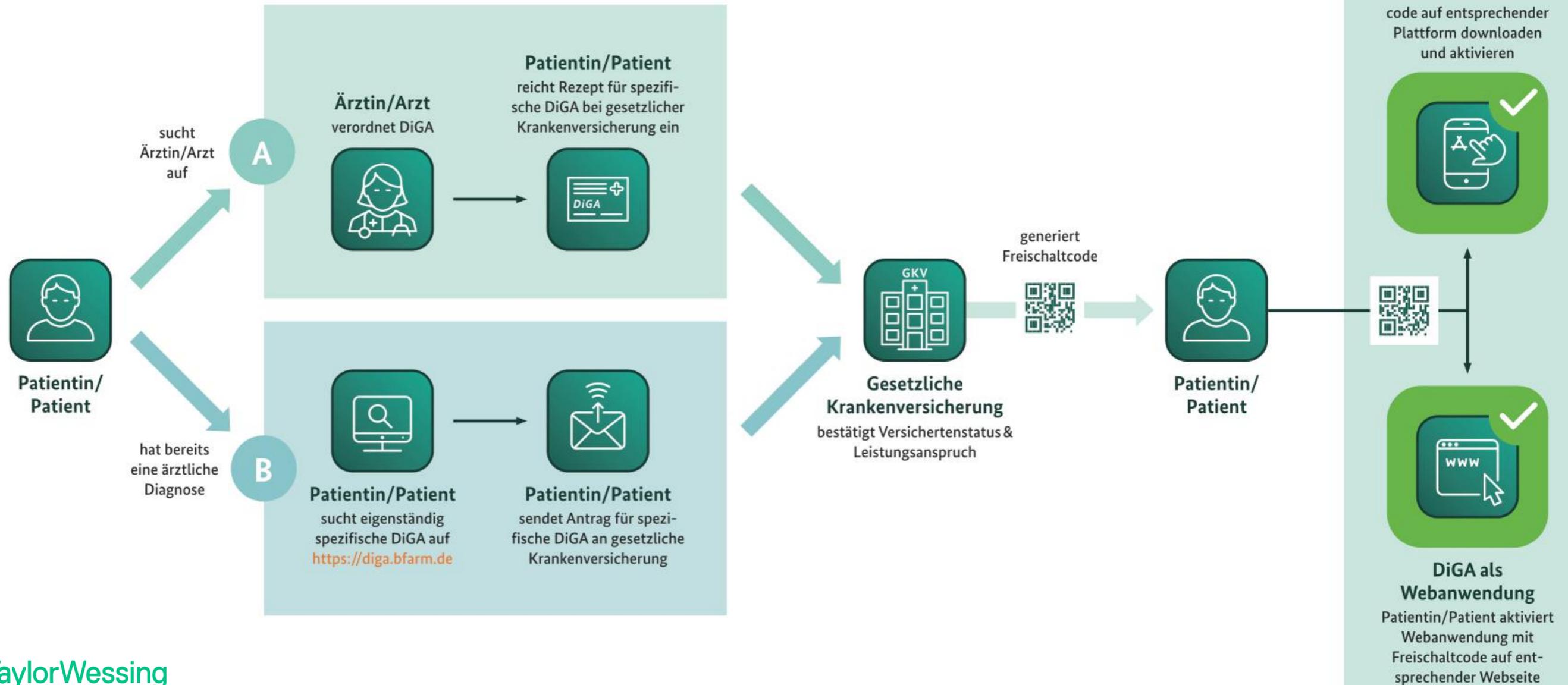
Das Ärzteblatt berichtet von einer Befragung von 51 Allgemeinmedizinerinnen, die unter anderem Folgendes ergab:

- Die Verordnungsbereitschaft liegt bei etwa 63 %.
- Mit Blick auf DiGA, die lediglich zur Erprobung in das DiGA-Verzeichnis aufgenommen worden sind, liegt die Verordnungsbereitschaft nur bei 38 %. Als Grund wird fehlende Evidenz genannt.

<https://www.aerzteblatt.de/archiv/217790/Digitale-Gesundheitsanwendungen-Die-Akzeptanz-steigern>; zuletzt abgerufen am: 10. März 2021



Wie kommt die DiGA zum Patienten?



DiGA-Abrechnungsverfahren

Beschluss der Richtlinie zum DiGA-Abrechnungsverfahren im Juli 2020:

- Die Richtlinie enthält Regelungen über Form und Inhalt des Abrechnungsverfahrens zwischen den Anbietern von DiGAs und den Krankenkassen.
- Der Versicherte erhält einen Freischaltcode/ Rezeptcode von der Krankenkasse, mit dem er die DiGA freischalten kann.
- Über den Code kann der DiGA-Hersteller die Krankenkasse ermitteln.
- Der DiGA-Hersteller sendet die Rechnungsdaten inklusive des Freischaltcodes/ Rezeptcodes elektronisch an die Krankenkasse.



Wie kommen die Vergütungsbeträge zustande?

- Regelung in § 134 SGB V
- Im ersten Jahr nach Aufnahme in das BfArM-Verzeichnis Erstattung der Herstellerpreise
- **Danach:** Vergütungsbetrag nach Vereinbarung der Hersteller und dem GKV-Spitzenverband
- Kommt eine Einigung nicht zustande, werden die Vergütungsbeträge von einer Schiedsstelle festgesetzt
- Derzeit wird zudem eine Rahmenvereinbarung zwischen dem GKV-Spitzenverband und den Herstellerverbänden verhandelt. Nach Pressemeldungen liegt bereits ein vertraulicher Entwurf vor, in dem Höchstbeträge vorgesehen seien (Handelsblatt, Digital Health Newsletter v. 1. Februar 2021)
- Die Geltung von Höchstbeträgen ist zuvor von der Schiedsstelle beschlossen worden

Digitale Gesundheitsanwendungen: Kassen-Belastung durch freie Preiswahl wird eingegrenzt

Handelsblatt Inside liegt die Rahmenvereinbarung für „Apps auf Rezept“ vor. Unter anderem sollen die Möglichkeiten der freien Preiswahl eingeschränkt werden.

Wie sieht die Verordnungs- und Vergütungsrealität aus?

- Nach einer Meldung des Handelsblatts vom 4. Februar 2021 sind bislang rund 3.700 DiGAs verordnet worden
- Die Herstellerpreise betragen demnach bis zu 750 Euro pro Quartal
- Im Durchschnitt haben die Krankenkassen bisher etwa 260 Euro pro Verordnung ausgegeben



Ausblick: Was ändert sich durch das DVPMG?

- Das Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz (DVPMG) soll Mitte 2021 in Kraft treten.
- Ausweislich der Kabinettsvorlage wird die Versorgung mit digitalen Gesundheitsanwendungen (DiGAs) weiterentwickelt.
- Versicherte sollen die Möglichkeit bekommen, Daten aus DiGAs in ihre elektronische Patientenakte einzustellen.
- Leistungen von Heilmittelerbringern und Hebammen, die im Zusammenhang mit DiGAs erbracht werden, werden künftig vergütet.
- Datenschutz und Informationssicherheit von DiGAs werden gestärkt.



1b

Datenschutzrechtliche Anforderungen an Digitale Gesundheitsanwendungen

Thanos Rammos

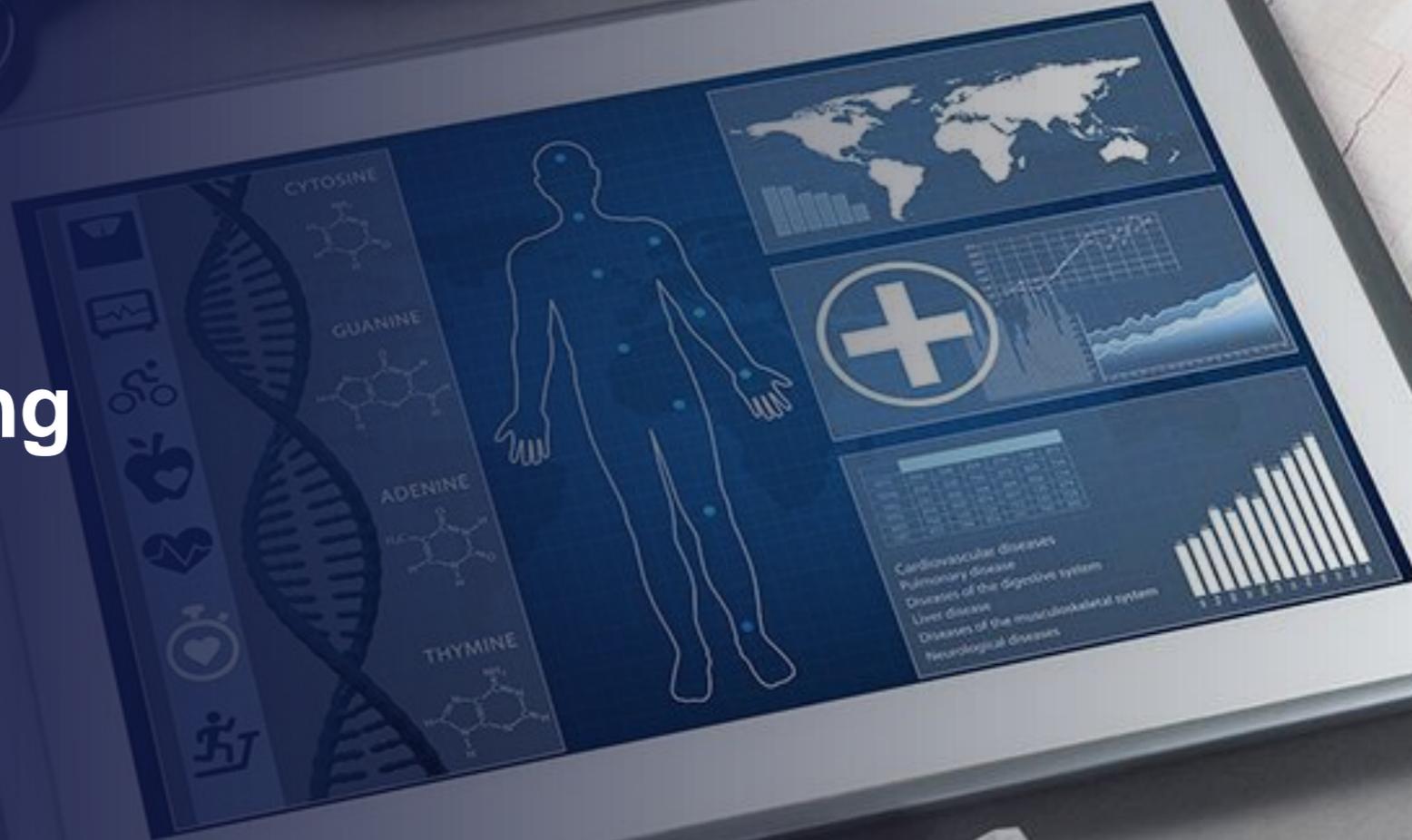
Agenda

- 1 Einleitung
- 2 Anforderungen nach DiGAV
- 3 Einwilligungserfordernisse
- 4 Allgemeine DS-GVO Compliance



1

Einleitung



Einleitung: Hintergrund

Mit dem „Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz – **DVG**)“ wird ein **Leistungsanspruch** der Versicherten auf **digitale Gesundheitsanwendungen** geschaffen. Das bedeutet, dass künftig Ärztinnen und Ärzte Apps verschreiben können. Die Kosten dafür erstattet die gesetzliche Krankenversicherung.

Der Anspruch umfasst nur solche digitalen Gesundheitsanwendungen, die

1. vom Bundesinstitut für Arzneimittel und Medizinprodukte in das Verzeichnis für digitale Gesundheitsanwendungen nach § 139e SGB V aufgenommen wurden und
2. entweder nach Verordnung des behandelnden Arztes oder mit Genehmigung der Krankenkasse angewendet werden.

Details zu dem Verfahren sind in einer Verordnung, der DiGAV, geregelt.

Damit eine App in das **DiGA-Verzeichnis** gemäß § 139e SGB V aufgenommen werden kann, muss diese u.a.

- die Anforderungen an Datenschutz und Datensicherheit nach dem Stand der Technik erfüllen,
- keine Werbung enthalten,
- leicht und intuitiv zu bedienen sein,
- Anforderungen an die Barrierefreiheit erfüllen.

Einleitung: Antragstellung und Nachweispflicht

Hersteller trifft Nachweispflicht für datenschutzrechtliche Compliance

- Nachweis der Umsetzung der datenschutzrechtlichen Anforderungen erfolgt durch Ausfüllen eines Fragebogens gemäß Anlage 1 zur Verordnung

Anlage 1
Fragebogen gemäß § 4 Absatz 6

(Fundstelle: BGBl. I 2020, 779 - 792)

Im nachfolgend aufgeführten Fragenbogen ist durch den Hersteller die Erfüllung der Anforderungen nach § 4 zu erklären. Der Hersteller bestätigt die Erfüllung der Anforderungen durch Kennzeichnung in der Spalte „zutreffend“. Die Vorschriften des Datenschutzes und die Anforderungen an die Datensicherheit – Basisanforderungen sind von allen digitalen Gesundheitsanwendungen zu erfüllen. Die Anforderungen Datensicherheit – Zusatzanforderungen bei digitalen Gesundheitsanwendungen mit sehr hohem Schutzbedarf sind von digitalen Gesundheitsanwendungen zu erfüllen, für die im Rahmen der geforderten Schutzbedarfsanalyse ein sehr hoher Schutzbedarf festgestellt wurde.

Nr.	Themenfeld	Anforderung	zutreffend	nicht zutreffend	zulässige Begründung für „nicht zutreffend“
Datenschutz					
1.	Datenschutz-Grundverordnung als anzuwendendes Recht	Die Verarbeitung personenbezogener Daten durch die digitale Gesundheitsanwendung und deren Hersteller unterfällt der Verordnung (EU) 2016/679 sowie ggf. weiteren Datenschutzregelungen.			

- BfrAM führt keine eigene Prüfung durch
- BfrAM besitzt keine Sanktionsmöglichkeit bei Datenschutzverstößen außer Streichung der DiGA aus dem Verzeichnis



2

Anforderungen nach DiGAV

Anforderungen nach DiGAV: Datenschutz

§ 4 Anforderungen an Datenschutz und Datensicherheit

- (1) Digitale Gesundheitsanwendungen müssen **die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik** unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten.
- (2) Im Rahmen einer digitalen Gesundheitsanwendung dürfen personenbezogene Daten **nur aufgrund einer Einwilligung** der Versicherten (...) und **ausschließlich zu den folgenden Zwecken verarbeitet** werden:

Die **Einwilligung** zu der Datenverarbeitung **nach Satz 1 Nummer 4** ist **getrennt von einer Einwilligung in die Datenverarbeitung für Zwecke nach Satz 1 Nummer 1 bis 3 einzuholen**. Datenverarbeitungsbefugnisse nach anderen Vorschriften bleiben unberührt.

- 1** zu dem bestimmungsgemäßen Gebrauch der digitalen Gesundheitsanwendung durch die Nutzer,
- 2** zu dem Nachweis positiver Versorgungseffekte im Rahmen einer Erprobung nach § 139e Absatz 4 des Fünften Buches Sozialgesetzbuch,
- 3** zu der Nachweisführung bei Vereinbarungen nach § 134 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch,
- 4** zu der dauerhaften Gewährleistung der technischen Funktionsfähigkeit, der Nutzerfreundlichkeit und der Weiterentwicklung der digitalen Gesundheitsanwendung

Anforderungen nach DiGAV: Datensicherheit

Die DiGAV verlangt, dass die DiGA

gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleistet.

Hierzu gibt es einen **40 Datenschutz- und 37 Datensicherheits-Pflichten** umfassenden **Fragebogen**, der u.a. verlangt, dass

- **Umsetzung von Informationssicherheitsmanagementsystemen (ISMS)** gemäß ISO-27000-Reihe oder BSI-Standard 200-2
- Bei einer Datenkommunikation über offene Netze ist eine Transportverschlüsselung gemäß des BSI Mindeststandards zur **Verwendung von Transport Layer Security** nach § 8 (1) S. 1 BSIG zu verwenden
- Falls Passwörter zur Authentisierung des Nutzers verwendet werden, muss die DiGA nur sichere Passwörter akzeptieren (Sonderzeichen, Mindestlänge) und Grenzwert für fehlgeschlagene Anmeldeversuche; Übermittlung von Passwörtern nie im Klartext
- Sitzungen müssen nach maximaler Gültigkeitsdauer deaktiviert werden
- Der **Zugriff durch Mitarbeiter des Herstellers auf die DiGA muss per default restriktiv** eingestellt sein und Berechtigung nur nach Mehraugenprinzip eingeräumt werden
- Protokollierungsdateien müssen automatisiert auf sicherheitsrelevante Ereignisse ausgewertet werden
- Der Zugriff auf Protokollierungsdateien ist durch Berechtigungsmanagement abzusichern
- Information der Nutzer proaktiv über sicherheitsrelevante Updates
- Bei Deinstallation der DiGA müssen alle Daten, einschließlich Caches und temporäre Dateien gelöscht werden

Anforderungen nach DiGAV: Datensicherheit

Bei DiGA mit
„sehr hohem
Schutzbedarf“
zudem u.a.

Problem: Kriterien unklar, um DiGA mit „sehr hohem Schutzbedarf“ zu identifizieren

Aber: 9 weitere Pflichten, u.a.

- pbD, die auf Geräten verarbeitet werden, die nicht in der persönlichen Verfügung der Nutzers stehen, müssen verschlüsselt gespeichert werden
- Durchführung eines Penetrationstest
- Bei der initialen Authentifizierung ist Zwei-Faktor-Authentifizierung durchzuführen
- Maßnahmen gegen DoS und DDoS



Anforderungen nach DiGAV: Ort der Verarbeitung

Die Verarbeitung von der Daten darf **nur**

- im Inland
- in einem Mitgliedsstaat der Europäischen Union
- in einem diesem nach § 35 Absatz 7 des Ersten Buches Sozialgesetzbuch gleichgestellten Staat (EWR und Schweiz)
- in einem Drittstaat, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt

Problem:

- Kein Rückgriff auf Art. 46 und 47 DSGVO, insbesondere BCR, SCC nicht ausreichend
- Einwilligung in Drittstaatenübermittlung nach Art. 49 DSGVO wohl auch nicht möglich

Gilt auch für Auftragsverarbeiter, Art. 28 DSGVO

Aber: Anbieten der App in **App-Stores** bleibt möglich, wobei Anmelde- von Gesundheitsdaten zu trennen sind

Verarbeitung daher **unzulässig**

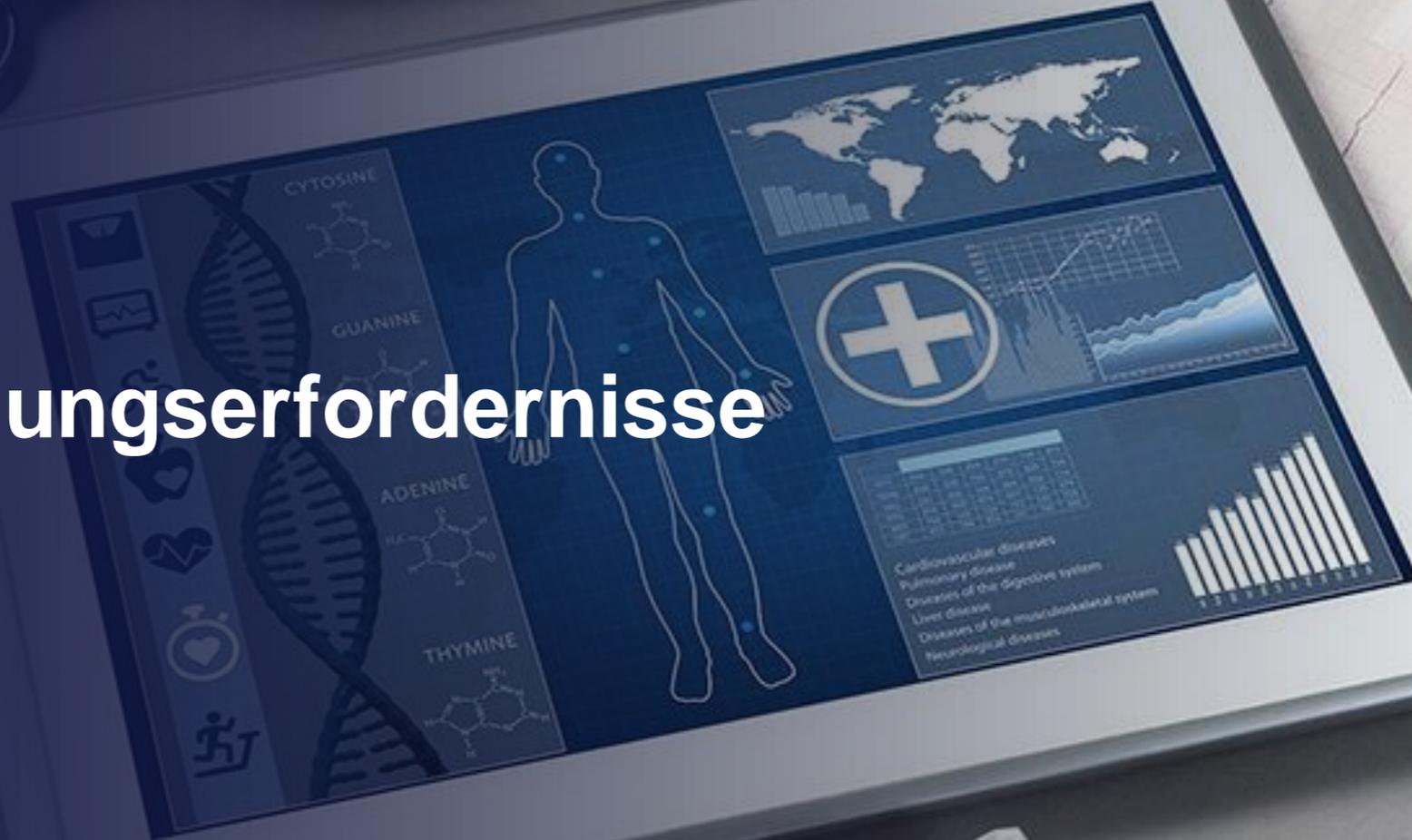
- durch DiGA-Hersteller mit Sitz in Drittstaaten wie z.B. USA, UK, Indien, Russland
- in Clouds, die nicht in der EU sind
- durch Tools innerhalb der App, deren Anbieter nicht in der EU sind

Einsatz von Clouddiensten und sonstigen Dienstleistern aber denkbar, vgl. FAQ des BfArM vom 28. Januar 2021

- **Lösung:**
 - **Verschlüsselung** sofern Schlüssel vom DiGA-Hersteller in der EU selbst verwaltet oder gespeichert werden (beispielsweise Customer-Managed Encryption Keys)
 - **Europäische Tochterunternehmen** und Beauftragte

3

Einwilligungserfordernisse



Voraussetzungen wirksame Einwilligung

Was sind die datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung nach Artt. 7, 9 Abs. 2 lit. a DSGVO?

Einwilligung ist nur wirksam, wenn

- **freiwillig** erteilt
 - keine Freiwilligkeit, wenn Einwilligung nicht getrennt für verschiedene Datenverarbeitungen abgegeben werden kann, obwohl dies im Einzelfall angebracht ist, Erw. 43 (hier: verschiedene Zwecke)
 - keine Freiwilligkeit, wenn Vertragserfüllung von Einwilligung in nicht erforderliche Verarbeitung abhängig gemacht wird
- **Transparenz** (gestalterische und inhaltliche Transparenz, insbes. Falls mit anderen Erklärungen verbunden)

spezifisch und informiert für den bestimmten Fall (alle Zweck benennen)

- **ausdrücklich** unter Bezugnahme auf die Verarbeitung sensibler Daten (aktives “opt-in”, keine konkludente oder stillschweigende Zustimmung, vorgecheckte Boxen oder Inaktivität, sondern klare, bestätigende Handlung (Einwilligungsbewußtsein)
- **in Form** einer Erklärung oder sonstigen eindeutigen bestätigenden Handlung → kein Schriftformerfordernis (mehr)

ABER:
Einwilligungen muss beweisfest dokumentiert sein, Art. 7 Abs. 1 DSGVO

- Bei Verkettung von pbD über zwei oder mehr DiGA gesonderte Einwilligung erforderlich
- **Zeitpunkt** vorherige Zustimmung
- **Mindestalter** 16 Jahre (Einsichtsfähigkeit)
- **Hinweis auf Widerruflichkeit**
 - Jederzeit
 - ohne Begründung
 - mindestens so einfach wie Erteilung
 - barrierefrei
- Jederzeitige **Abrufbarkeit** der erteilten Einwilligung

Voraussetzungen wirksame Einwilligung

- Aufgrund strenger Zweckbindung ist Analyse und Tracking des Nutzerverhaltens zu Zwecken, die nicht der Versorgung des Versicherten dienen, unzulässig
- Eine Verarbeitung für Werbezwecke ist ausgeschlossen – selbst bei Einwilligung
- Eine Nutzung im Rahmen von z.B. medizinischer Versorgungsforschung wäre trotz Einwilligung unzulässig
- Zwecke müssen sich im Einwilligungstext wiederfinden
→ sehr langer Einwilligungstext
- Einwilligung ist jederzeit widerruflich
→ DiGA dann nicht mehr nutzbar
- Es kann auch Verarbeitungen geben, die gemäß Art. 9 Abs. 2 lit. b ff. DSGVO erlaubt wären.
Hier aber Beschränkung auf ausdrückliche Einwilligung, sehr eng

4

Allgemeine DS-GVO Compliance

Allgemeine DS-GVO Compliance

- Strenge **Zweckbindung**; eine Verarbeitung für Werbezwecke ist ausgeschlossen – selbst bei Einwilligung
- Grundsatz der **Datenminimierung**, d.h. Datenverarbeitung ist auf das notwendige Maß beschränkt und die Zwecke der Datenverarbeitung können nicht durch datensparsamere Mittel in gleichem Maße erreicht werden
- **Trennungsgebot**, d.h. gesundheitsbezogene Daten müssen getrennt von den ausschließlich für die Leistungsabrechnung erforderlichen Daten gespeichert werden
- **Need-to-Know-Zugriff**, d.h. Sicherstellung, dass mit administrativen Aufgaben betraute Personen keinen Zugriff auf personenbezogene Daten erhalten
- Etablierung eines **Löschkonzepts**, d.h. Speicherung der pbD nur solange, wie es für die Zwecke erforderlich ist
- Konzept für die **Umsetzung der Betroffenenrechte** nach Artt. 15 ff. DSGVO, insbes. Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Recht auf Datenübertragbarkeit (Datenportabilität)

Allgemeine DS-GVO Compliance

- Erfüllung der Informationspflichten nach Artt. 13, 14 DSGVO, d.h. Bereitstellung einer Datenschutzerklärung
- **Verpflichtung** der Mitarbeiter, die Zugang zu pbD haben, **auf Verschwiegenheit**
- Datenschutzrechtliche **Schulung** von Mitarbeitern
- Durchführung einer dokumentierten **Datenschutz-Folgenabschätzung**
- Konzept für Meldung von Datenschutzverstößen ggü. Aufsichtsbehörde und ggf. Betroffenen

Zusätzlich fordert die DSK in der EntschlieÙung „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen“:

- Anonyme bzw. pseudonyme Datenverarbeitung, soweit möglich
- Nur lokale Speicherung, wenn keine Weitergabe an z.B. Arzt erforderlich ist
- Einwilligungserklärung und Verträge, die unter Ausnutzung von erheblichem Verhandlungsungleichgewicht zustande kommen, sind unwirksam (etwa im Beschäftigungs- oder Versicherungsverhältnis)

2

Intelligente und selbstlernende Medizinprodukte – Marktzutrittsvoraussetzungen und andere Herausforderungen

Dr. Andrea Sautter



Inhalt

- 1 Ein „intelligentes und selbstlernendes Medizinprodukt“ – was ist das?
- 2 Intelligente und selbstlernende Medizinprodukte – Marktzugangsvoraussetzungen
- 3 Intelligente und selbstlernende Medizinprodukte – Haftungsfragen
- 4 Intelligente und selbstlernende Medizinprodukte – offener Regelungsbedarf?



2a

Ein „intelligentes und selbstlernendes Medizinprodukt“ – was ist das?

Was ist ein „intelligentes und selbstlernendes“ Produkt?

Definitionsversuche:

- **Rechtsausschuss des Europäischen Parlaments:** Entwurf eines Berichts mit Empfehlung an die Kommission zu zivilrechtlicher Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL) vom 27.04.2020)
- **EU-Kommission**
 - WEISSBUCH „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“, (19.2.2020, COM(2020) 65 final)
 - „Bericht der über die Auswirkungen künstlicher Intelligenz, des Internets der Dinge und der Robotik in Hinblick auf Sicherheit und Haftung“ (19.2.2020 COM(2020) 64 final)
- **Enquete-Kommission des Deutschen Bundestages** Bericht vom 28.10.2020 „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, Drucksache 19/23700
- **Bitkom/DFKI:** Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) und des Deutschen Forschungszentrums für Künstliche Intelligenz (DFKI)
- **IG-NB („Interessengemeinschaft Benannter Stellen“),** Fragenkatalog „Künstliche Intelligenz bei Medizinprodukten“, Version 2, Stand: 06.11.2020



Ein „intelligentes und selbstlernendes Produkt“ – was ist das?

Datenverarbeitungsprinzip eines intelligenten und selbstlernenden Systems

EVA-Prinzip der Datenverarbeitung

Eingabe

Verarbeitung

Ausgabe

Datenverarbeitungsprinzip eines intelligenten und selbstlernenden Systems

Wahrnehmen

Verstehen

Verarbeiten

Laufendes „maschinelles Lernen“ – begleitendes Analysieren, wie die Umgebung von ihren vorherigen Aktionen beeinflusst wird: „Induktive Schaffung eigener, künstlicher „Wenn-Dann-Regeln“ als numerische Referenzmodelle zur deduktiven Anwendung

Exkurs – wann handelt es sich bei Software um ein Medizinprodukt?

Medizinprodukteverordnung (EU) 2017/745 – Medical Device Regulation (MDR)

Nach Erwägungsgrund (19):

Software als solche gilt als Medizinprodukt, wenn

sie vom Hersteller speziell für einen oder mehrere der in der Definition von Medizinprodukten genannten medizinischen Zwecke bestimmt ist,

Kein Medizinprodukt ist Software

für allgemeine Zwecke, selbst wenn sie in Einrichtungen des Gesundheitswesens eingesetzt wird,

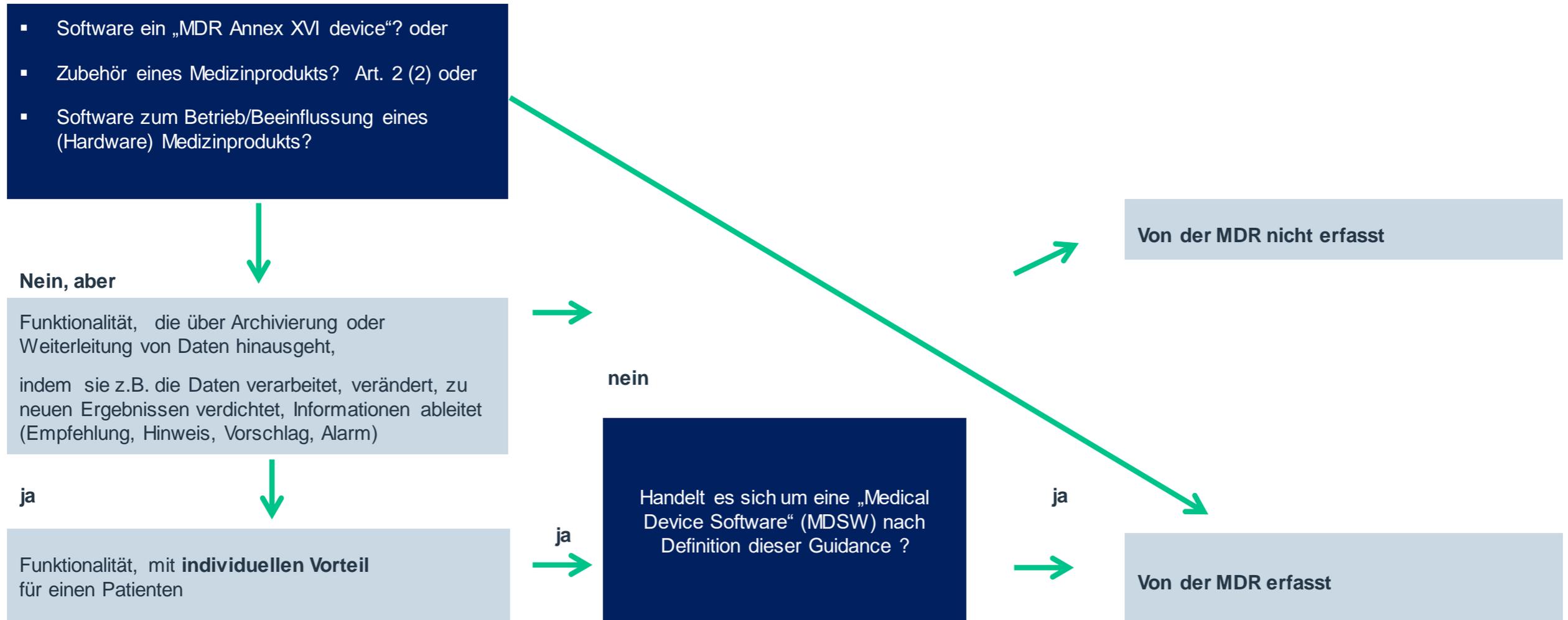
Sowie Software, die für Zwecke in den **Bereichen Lebensstil und Wohlbefinden** eingesetzt wird,

Die Einstufung der Software entweder als Produkt oder als Zubehör ist unabhängig vom Ort der Software und von der Art der Verbindung zwischen der Software und einem Produkt.



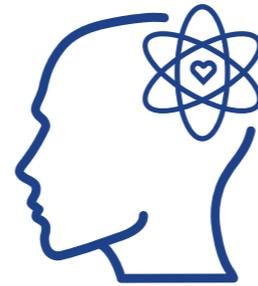
Exkurs – wann handelt es sich bei Software um ein Medizinprodukt?

Entscheidungsbaum MDCG („Medical Device Coordination Group“) Art. 105 MDR – MDCG 2019-11 Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR “ of October 2019



Wann ist ein „intelligentes und selbstlernendes“ Produkt ein Medizinprodukt?

„KI“ – Produkte unter
Einbeziehung künstlicher
Intelligenz



Intelligente und
selbstlernende
Medizinprodukte

Softwareanwendungen
als Medizinprodukt
(MSWD)

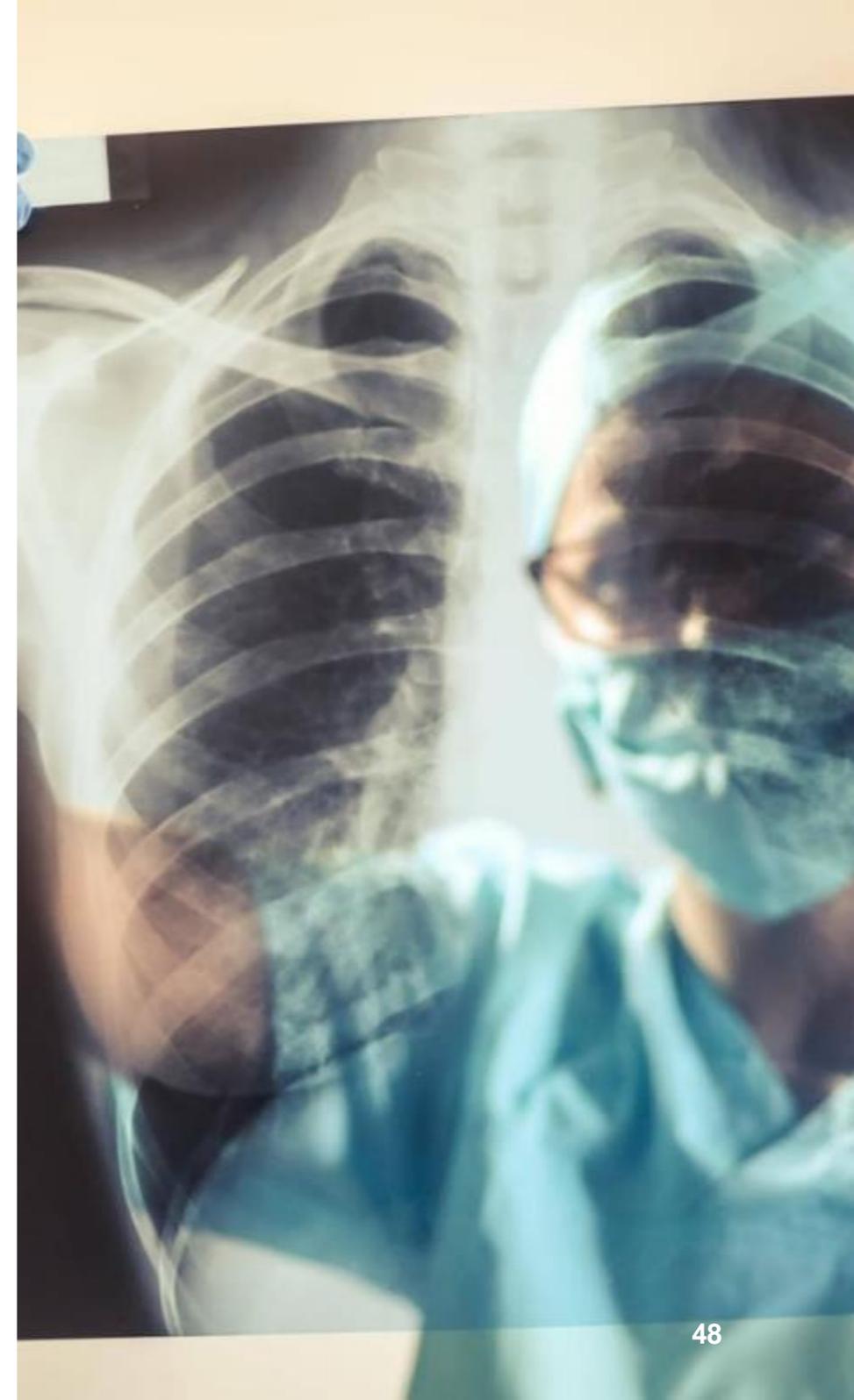
„Intelligentes und selbstlernendes“ Medizinprodukt – Beispiel

Forscherteam der ETH Lausanne (EPFL) um die Ärztin Mary-Anne Hartley:

Entwicklung eines Algorithmus zur Diagnose von Covid-19 samt Vorhersage zur Schwere des Krankheitsverlaufs anhand

„**DeepChest**“: Daten aus tausenden Lungenscans von Patienten des Universitätsspitals Lausanne (CHUV) und

„**DeepBreath**“: mit digitalem Stethoskop erfasste Atemgeräusche

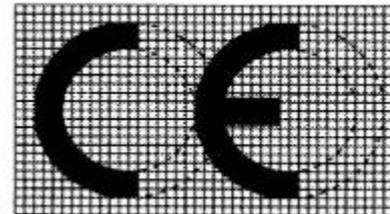


2b

Intelligente und selbstlernende Medizinprodukte – Marktzugangsvoraussetzungen

Marktzugangsvoraussetzungen für Medizinprodukte in der EU

- **Konformitätsbewertungsverfahren** zum Nachweis der Konformität des Produktes mit den grundlegenden Sicherheitsanforderungen
- Abhängig von der Risikoklasse des Medizinprodukts Beteiligung einer **Benannten Stelle**
- Anbringen der **CE-Kennzeichnung** auf dem Medizinprodukt zum Nachweis des durchlaufenen Konformitätsbewertungsverfahrens (Conformité Européenne)

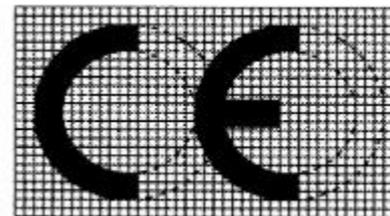


Marktzugangsvoraussetzungen für Medizinprodukte in der EU

Konformitätsnachweis für intelligente und selbstlernende Medizinprodukte

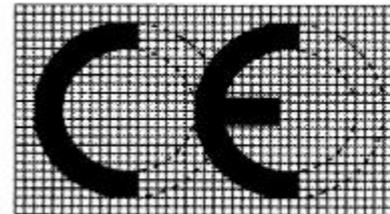
- Konformitätsbewertungsverfahren bezieht sich auf den technischen Stand im Zeitpunkt der Durchführung des Verfahrens – sind “dynamische” Produkte im Vorhinein zertifizierbar?
- Ergänzung der technischen Dokumentation um ein “Algorithmus-Änderungs-Protokoll”; Verlassen des Protokolls löst Notwendigkeit der Neuzertifizierung aus?

(vgl. COCIR (European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry), Artificial Intelligence in EU Medical Device Legislation, September 2020, S. 42)



Marktzugangsvoraussetzungen für Medizinprodukte in der EU

- **Konformitätsnachweis für intelligente und selbstlernende Medizinprodukte**
- **Medizinprodukteverordnung (EU) 2017/745**
- Anhang VIII Abschnitt 7.9 Regel 22
- „Aktive therapeutische Produkte mit integrierter oder eingebauter diagnostischer Funktion, die das Patientenmanagement durch das Produkt erheblich bestimmt, wie etwa geschlossene Regelsysteme oder automatische externe Defibrillatoren, gehören zur Klasse III.“



Marktzugangsvoraussetzungen: Ausnahmen vom Erfordernis der Produktzertifizierung?

Medizinprodukteverordnung (EU) 2017/745

Art. 21 – Produkte für besondere Zwecke

(1) Die Mitgliedstaaten errichten keine Hemmnisse für

[...]

b) **Sonderanfertigungen**, die auf dem Markt bereitgestellt werden, wenn sie Artikel 52 Absatz 8 und Anhang XIII entsprechen.

2c

Intelligente und selbstlernende Medizinprodukte – Haftungsfragen

Bedeutung der Grundsätze zur Produkthaftung für Medizinprodukte

Rechtsgrundlagen der Haftung für Medizinprodukte:

- Produkthaftungsrecht (ProdHG)
- Vertragliche Haftung
- Deliktische Haftung
- **Produkthaftungs-Richtlinie 85/374/EWG**
- Nach den Rechtssystemen der Mitgliedstaaten kann der Geschädigte aufgrund einer vertraglichen Haftung oder aufgrund einer anderen als der in dieser Richtlinie vorgesehenen außervertraglichen Haftung Anspruch auf Schadenersatz haben. Soweit derartige Bestimmungen ebenfalls auf die Verwirklichung des Ziels eines wirksamen Verbraucherschutzes ausgerichtet sind, dürfen sie von dieser Richtlinie nicht beeinträchtigt werden.
- **Art. 13 [Andere Ansprüche]**
- Die Ansprüche, die ein Geschädigter aufgrund der Vorschriften über die vertragliche und außervertragliche Haftung oder aufgrund einer zum Zeitpunkt der Bekanntgabe dieser Richtlinie bestehenden besonderen Haftungsregelung geltend machen kann, werden durch diese Richtlinie nicht berührt.



Bedeutung der Grundsätze zur Produkthaftung für Medizinprodukte

Voraussetzung der verschuldensunabhängigen Haftung nach ProdHG:

- Herstellerposition (§ 4 Abs. 1 ProdHG)
 - Hersteller ist auch, wer einen Grundstoff oder ein Teilprodukt herstellt
- Haftung für
 - **Konstruktionsfehler:** keine Haftung für Fehler, die nach dem Stand von Wissenschaft und Technik in dem Zeitpunkt, in dem das (Vor)Produkt in Verkehr gebracht wurde, nicht erkennbar waren
 - **Fabrikationsfehler:** ggf. haften Zulieferer des Grundstoffs/Teilprodukts und Hersteller des Endprodukts nebeneinander; bei parallelen Sorgfaltspflichten sowohl des Zulieferers und Endherstellers empfehlen sich Qualitätssicherungsvereinbarungen zur Abgrenzung von Verantwortlichkeiten
 - **Instruktionsfehler:** Instruktionspflichten des Zulieferers sind am Endhersteller, nicht am Verbraucher auszurichten



Defekt

Bedeutung der Grundsätze zur Produzentenhaftung für Medizinprodukte

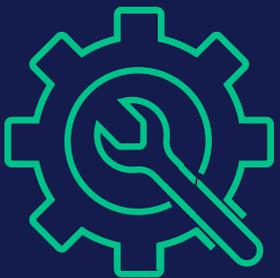
Voraussetzung der verschuldensabhängigen deliktischen Haftung

§ 823 BGB

- Schaden an einem von § 823 Absatz 1 geschützten Rechtsgut
 - (Leben, den Körper, die Gesundheit, Freiheit, Eigentum (nicht Vermögen) oder ein „sonstiges Recht“)
 - Aufgrund Verletzung der Verkehrssicherungspflicht
 - Die jeden Produzenten trifft der mit
 - Inverkehrbringen eines fehlerhaften Produkts
 - eine Gefahrenquelle schafft

§ 823 Abs. 2 BGB: Strafrechtliche Haftung der handelnden natürlichen Personen

- §§ 222- 229 StGB (fahrlässige Körperverletzung/fahrlässige Tötung)
 - §§ 9, 30, 130 Ordnungswidrigkeitengesetz (OWiG)
 - Geldbuße gegen die juristische Person



Defekt

Haftung für selbstlernende Medizinprodukte – besondere Problemstellungen

Haftungsadressat bei selbstlernenden Produkten:

- Hersteller?
- Benannte Stelle?
- Betreiber?
 - § 2 Abs. 2 Medizinprodukte-Betreiberverordnung (MPBetreibV)
„die für den Betrieb von Gesundheitseinrichtungen verantwortlichen Personen“
- Anwender/Arzt?

Beweisführung durch den Geschädigten

„Blackboxeffekt“



2d

Intelligente und selbstlernende Medizinprodukte – offener Regelungsbedarf?

Intelligente und selbstlernende Medizinprodukte – offener Regelungsbedarf?

- **Definition** eines „(künstlich) intelligenten und selbstlernenden“ Medizinproduktes
- Zertifizierungsfragen
- Produkthaftungsfragen
- Aufsichtsstrukturen
- Regelungsebene?



Intelligente und selbstlernende Medizinprodukte – offener Regelungsbedarf?

Ausblick:

- MDCG beabsichtigt eine Leitlinie über „Artificial Intelligence under MDR/IVDR framework – Zeitpunkt offen (vgl. „Ongoing guidance development and other relevant work within MDCG Subgroups – December 2020“)
- EU-Kommission erwägt in ihrem „WEISSBUCH zur Künstlichen Intelligenz“ (19.2.2020) die Evaluation und ggfs. Anpassung des gegenwärtigen Rechtsrahmens



3

BACKUP für anschließende Diskussion:

Rechtsgrundlagen – Zitate zur Definition des Begriffs „KI“

Anhang: Gesundheitssoftware/Apps – Klassifizierung nach MDR

Medizinprodukteverordnung (EU) 2017/745 – Medical Device Regulation (MDR)

Art. 2

4. „**aktives Produkt**“ bezeichnet ein Produkt, dessen **Betrieb von einer Energiequelle** mit Ausnahme der für diesen Zweck durch den menschlichen Körper oder durch die Schwerkraft erzeugten Energie abhängig ist und das mittels Änderung der Dichte oder Umwandlung dieser Energie wirkt. Ein Produkt, das zur Übertragung von Energie, Stoffen oder anderen Elementen zwischen einem aktiven Produkt und dem Patienten eingesetzt wird, ohne dass dabei eine wesentliche Veränderung von Energie, Stoffen oder Parametern eintritt, gilt nicht als aktives Produkt.



Decision Support Software / Apps – Einordnung und Klassifizierung nach MDR (2)

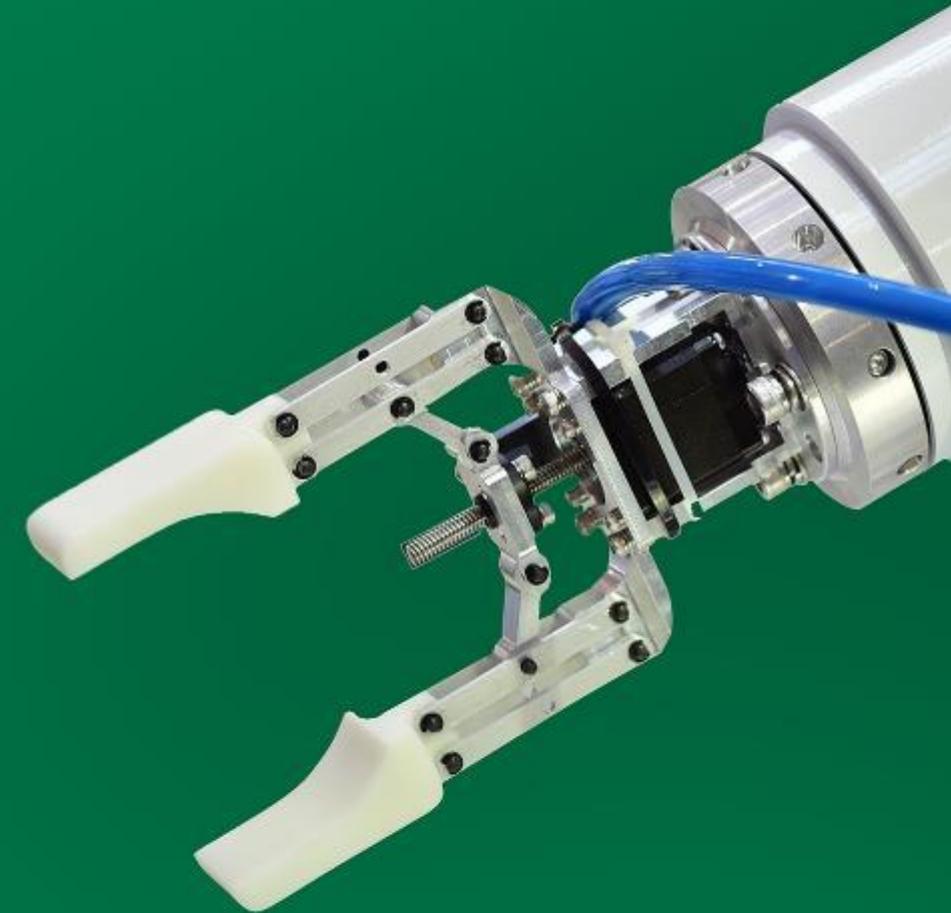
Medizinprodukteverordnung 2017/745/EU – Medical Device Regulation („MDR“)

Anhang VIII Klassifizierungsregeln Kapitel II

3.3. **Software, die ein Produkt steuert oder dessen Anwendung** beeinflusst, wird derselben Klasse zugerechnet wie das Produkt.

Ist die Software von anderen Produkten unabhängig, so wird sie für sich allein klassifiziert.

3.7. Ein Produkt wird als Produkt angesehen, das eine **direkte Diagnose** ermöglicht, wenn es die Diagnose der betreffenden Krankheit oder des betreffenden Gesundheitszustandes selbst liefert oder aber für die Diagnose entscheidende Informationen hervorbringt



Decision Support Software / Apps – Einordnung und Klassifizierung nach MDR (3)

Medizinprodukteverordnung (EU) 2017/745 – Medical Device Regulation (MDR)

Anhang VIII Klassifizierungsregeln Kapitel II

6.2. Regel 10

Aktive Produkte zu **Diagnose- und Überwachungszwecken** gehören zur **Klasse IIa**, wenn [...]

sie dazu bestimmt sind, eine **direkte Diagnose oder Kontrolle von vitalen Körperfunktionen zu ermöglichen**, es sei denn, sie sind speziell für die Kontrolle von vitalen physiologischen Parametern bestimmt und die Art der Änderung dieser Parameter könnte zu einer unmittelbaren Gefahr für den Patienten führen, z.B. Änderung der Herzfunktion, der Atmung oder der Aktivität des zentralen Nervensystems, oder wenn sie für die Diagnose in klinischen Situationen, in denen der Patient in unmittelbarer Gefahr schwebt, bestimmt sind; in diesen Fällen werden sie der Klasse IIb zugeordnet.

Aktive Produkte, die zum Aussenden ionisierender Strahlung sowie für die radiologische Diagnostik oder die radiologische Therapie bestimmt sind, einschließlich Produkte für die interventionelle Radiologie und **Produkte, die solche Produkte steuern oder kontrollieren oder die deren Leistung unmittelbar beeinflussen, werden der Klasse IIb zugeordnet**

Decision Support Software / Apps – Einordnung und Klassifizierung nach MDR (3)

Medizinprodukteverordnung (EU) 2017/745 – Medical Device Regulation (MDR)

Anhang VIII Klassifizierungsregeln Kapitel II

Regel 11

Software, die dazu bestimmt ist, Informationen zu liefern, die zu **Entscheidungen für diagnostische oder therapeutische Zwecke** herangezogen werden, gehört zur Klasse IIa, es sei denn, diese Entscheidungen haben Auswirkungen, die Folgendes verursachen können:

- den Tod oder eine irreversible Verschlechterung des Gesundheitszustands einer Person; in diesem Fall wird sie der Klasse III zugeordnet, oder
- eine schwerwiegende Verschlechterung des Gesundheitszustands einer Person oder einen chirurgischen Eingriff; in diesem Fall wird sie der Klasse II b zugeordnet.

Software, die für die **Kontrolle von physiologischen Prozessen** bestimmt ist, gehört zur Klasse II a, es sei denn, sie ist für die Kontrolle von vitalen physiologischen Parametern bestimmt, wobei die Art der Änderung dieser Parameter zu einer unmittelbaren Gefahr für den Patienten führen könnte; in diesem Fall wird sie der Klasse II b zugeordnet.

Marktzugangsvoraussetzungen: Ausnahmen vom Erfordernis der Produktzertifizierung?

Medizinprodukteverordnung (EU) 2017/745

Art. 22 – Systeme und Behandlungseinheiten

1. Natürliche oder juristische Personen, die Produkte mit einer CE-Kennzeichnung mit folgenden anderen Medizin- oder sonstigen Produkten in einer mit der Zweckbestimmung der Medizin- oder sonstigen Produkte vereinbaren Weise und innerhalb der vom Hersteller vorgesehenen Anwendungsbeschränkungen **kombinieren**, um sie in Form eines Systems oder einer Behandlungseinheit in Verkehr zu bringen, müssen eine Erklärung abgeben:

a) sonstige Produkte mit CE-Kennzeichnung;

b) In-vitro-Diagnostika mit CE-Kennzeichnung gemäß der Verordnung (EU) 2017/746;

c) sonstige Produkte, die den für sie geltenden Rechtsvorschriften entsprechen, nur dann, wenn sie im Rahmen eines medizinischen Verfahrens verwendet werden oder wenn ihr Vorhandensein im System oder in der Behandlungseinheit anderweitig gerechtfertigt ist.

Was ist ein „intelligentes und selbstlernendes“ Produkt?

„Künstliche-Intelligenz-(KI)-Systeme sind vom Menschen entwickelte Software- (und möglicherweise auch Hardware-) Systeme, die in Bezug auf ein komplexes Ziel auf physischer oder digitaler Ebene agieren, indem sie ihre Umgebung durch Datenerfassung wahrnehmen, die gesammelten strukturierten oder unstrukturierten Daten interpretieren, Schlussfolgerungen daraus ziehen oder die aus diesen Daten abgeleiteten Informationen verarbeiten und über die geeignete(n) Maßnahme(n) zur Erreichung des vorgegebenen Ziels entscheiden. KI-Systeme können entweder symbolische Regeln verwenden oder ein numerisches Modell erlernen, und sie können auch ihr Verhalten anpassen, indem sie analysieren, wie die Umgebung von ihren vorherigen Aktionen beeinflusst wird.“

Hochrangige Expertengruppe für Künstliche Intelligenz, Ethikleitlinien für eine Vertrauenswürdige KI, 10.04.2019, S. 47.



Was ist ein „intelligentes und selbstlernendes“ Produkt?

„‘KI-System‘ bezeichnet ein System mit intelligentem Verhalten durch Analysieren bestimmter Eingaben und Treffen von Maßnahmen mit einem gewissen Grad von Autonomie, um spezifische Ziele zu erreichen. KI-Systeme können rein softwaregestützt sein und in der virtuellen Welt arbeiten oder in Hardwarevorrichtungen integriert sein“.

Entwurf eines Berichts mit Empfehlung an die Kommission zu zivilrechtlicher Haftung beim Einsatz künstlicher Intelligenz (2020/2014(INL) des Rechtsausschusses des Europäischen Parlaments vom 27.04.2020, S. 19



Wann ist ein „intelligentes und selbstlernendes“ Produkt ein Medizinprodukt?

Lernende Systeme zeichnet aus „dass ihre initiale Konfiguration durch den Menschen nur die Grundlage für die konkrete Funktionsweise im eigentlichen Betrieb darstellt. Mithilfe von Daten trainieren sie, wie ein Problem zu lösen bzw. eine Aufgabe zu erfüllen ist. Sie passen hierbei ihre Funktionsweise durch einen entsprechenden Lernprozess kontinuierlich an.“

Bericht der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale, Drucksache 19/23700, 28.10.2020, S. 49.



Wann ist ein „intelligentes und selbstlernendes“ Produkt ein Medizinprodukt?

Der Begriff „KI“ beschreibt „Informatik-Anwendungen, deren Ziel es ist, intelligentes Verhalten zu zeigen. Dazu sind in unterschiedlichen Anteilen bestimmte Kernfähigkeiten notwendig: Wahrnehmen, Verstehen, Handeln und Lernen. Diese vier Kernfähigkeiten stellen die größtmögliche Vereinfachung eines Modells zur modernen KI dar: Wahrnehmen – Verstehen – Handeln erweitern das Grundprinzip aller EDV-Systeme: Eingabe – Verarbeitung – Ausgabe. Das wirklich Neue ist das Lernen und Verstehen. Heutigen »echten« KI-Systemen ist gemein, dass sie in der Verarbeitungskomponente auch trainiert werden und damit lernen können und so bessere Ergebnisse erzielen als herkömmliche Verfahren, die nur auf starren, klar definierten und fest programmierten Regelwerken basieren.“

Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, S. 29, abrufbar unter https://www.dfki.de/fileadmin/user_upload/import/9744_171012-KI-Gipfelpapier-online.pdf (zuletzt abgerufen am 16.12.2020).



[Europa](#) > [Mittlerer Osten](#) > [Asien](#)

taylorwessing.com

© Taylor Wessing 2021

Diese Publikation stellt keine Rechtsberatung dar. Die unter der Bezeichnung Taylor Wessing tätigen Einheiten handeln unter einem gemeinsamen Markennamen, sind jedoch rechtlich unabhängig voneinander; sie sind Mitglieder des Taylor Wessing Vereins bzw. mit einem solchen Mitglied verbunden. Der Taylor Wessing Verein selbst erbringt keine rechtlichen Dienstleistungen. Weiterführende Informationen sind in unserem Impressum unter taylorwessing.com/de/legal/regulatory-information zu finden.