

DOI 10.52778/MPJ-2025-0037

Der Cyber Resilience Act und Medizinprodukte – Welche Cybersicherheitsanforderungen gelten für Medizinprodukte?

Miriam Schuh / Christina Ziegler-Kiefer

Zusammenfassung: Digitale Gesundheitsprodukte sind aus unserem Alltag nicht mehr wegzudenken – von Smartwatches, die unsere Vitaldaten tracken, über Gesundheits-Apps bis hin zu vernetzten medizinischen Geräten. Der Cyber Resilience Act, Verordnung (EU) 2024/2847 (CRA) soll einen einheitlichen Standard für die Cybersicherheit von Produkten mit digitalen Elementen auf dem europäischen Markt etablieren. Doch für Medizinprodukte gelten bereits strenge Regeln zur Produktsicherheit nach der Medical Device Regulation, Verordnung (EU) 2017/745 (MDR). Wann also greift der CRA – und wann greift er nicht? Der Beitrag beleuchtet die Abgrenzung zwischen beiden Regelwerken, zeigt Graubereiche auf und erklärt, warum Hersteller von Medizinprodukten jetzt besonders genau hinsehen sollten.

© WVG

Schlagwörter: Cyber Resilience Act (CRA), Cybersicherheit von Medizinprodukten, Digitale Gesundheitsprodukte, Software als Medizinprodukt, Wearables und Gesundheits-Apps, EU-Recht und Produktsicherheit, Zweckbestimmung von Medizinprodukten, Regulatorische Abgrenzung CRA-MDR

Der Anwendungsbereich der MDR

Die MDR ist der zentrale europäische Rechtsakt für Medizinprodukte. Die Verordnung gilt für Produkte mit medizinischer Zweckbestimmung. Sie legt Regeln für das Inverkehrbringen, die Bereitstellung auf dem Markt und die Inbetriebnahme von für den menschlichen Gebrauch bestimmten Medizinprodukten und deren Zubehör in der Union fest. Zudem findet die Verordnung nach Art. 2 Abs. 2 MDR auch auf die in Anhang XVI genannten Produktgruppen Anwendung. Es handelt

sich dabei um Produkte ohne medizinische Zweckbestimmung, die aufgrund ihrer inhärenten Risiken und ihrer technologischen Nähe zu Medizinprodukten gleichermaßen reguliert werden, um sicherzustellen, dass sie denselben hohen Sicherheitsstandards unterliegen. In der Verordnung werden sowohl Medizinprodukte und ihr Zubehör sowie die in Anhang XVI aufgeführten Produkte als „Produkt“ bezeichnet.

Art. 2 Nr. 1 MDR definiert ein Medizinprodukt als einen Gegen-

stand, der vom Hersteller für den Menschen bestimmt ist und allein oder in Kombination einen oder mehrere in der MDR festgelegte medizinische Zwecke erfüllen soll. Zu den medizinischen Zwecken gehören unter anderem der Umgang mit Krankheiten, Verletzungen, Behinderungen sowie anderen physiologischen oder pathologischen Prozessen oder Zuständen.¹

Als Zubehör eines Medizinprodukts wird ein Gegenstand bezeichnet, „der zwar an sich kein Medizinprodukt ist, aber vom Hersteller dazu bestimmt ist, zusammen mit einem oder mehreren bestimmten Medizinprodukten verwendet zu werden, und der speziell dessen/deren Verwendung gemäß seiner/ihrer Zweckbestimmung(en) ermöglicht oder mit dem die medizinische Funktion des Medizinprodukts bzw. der Medizinprodukte im Hinblick auf dessen/deren Zweckbestimmung(en) gezielt und unmittelbar unterstützt werden soll“.²

Die MDR erfasst nicht nur klassische physische Produkte, sondern gilt auch für digitale Lösungen. Sie enthält detaillierte Vorgaben zu Risikoklassifizierung, Konformitätsbewertung, klinischer Bewertung, Marktüberwachung und Sicherheitsberichterstattung sowie Anforderungen an die IT-Sicherheit und die technische Dokumentation digitaler Medizinprodukte.³ Hersteller müssen genau prüfen, ob ihr Produkt in den Anwendungsbereich der MDR fällt – insbesondere bei hybriden Systemen oder Softwarelösungen mit medizinischem Bezug. Ob ein Produkt als Medizinprodukt im Sinne der MDR einzustufen ist, kann anhand des

Entscheidungsbaums (o Abb. 1) ermittelt werden.⁴

Der Anwendungsbereich des CRA

Der CRA ist eine neue europäische Verordnung, die darauf abzielt, die Cybersicherheit von Produkten mit digitalen Elementen in der EU zu verbessern. Ziel ist es, klare Rahmenbedingungen für die cybersichere Entwicklung, Herstellung und das Inverkehrbringen solcher Produkte zu schaffen. Dabei soll sichergestellt werden, dass Produkte mit digitalen Elementen über ihren gesamten Lebenszyklus hinweg resilient und widerstandsfähig gegenüber Cyberbedrohungen sind. Der CRA findet als europäische Verordnung in allen Mitgliedstaaten unmittelbar Anwendung und erfasst Hersteller, Einführer und Händler, die Produkte mit digitalen Elementen auf dem europäischen Binnenmarkt bereitstellen. Primärer Adressat sind die Hersteller von Produkten mit digitalen Elementen, die strenge Anforderungen an die Cybersicherheit und das Schwachstellenmanagement erfüllen müssen. Für Importeure und Händler gelten abgestufte Pflichten. Im Falle eines Verstoßes drohen Bußgelder von bis zu 15 Mio. Euro oder 2,5 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Daneben sind die Marktüberwachungsbehörden befugt, einschneidende Maßnahmen – von der Überprüfung bis hin zum Produktrückruf – zu ergreifen. Der CRA ist seit dem 10. Dezember 2024 in Kraft und findet schrittweise bis zum 11. Dezember 2027 Anwendung. Der CRA gilt nach Art. 2 Abs. 1 CRA für alle auf dem Markt bereitgestellten Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder

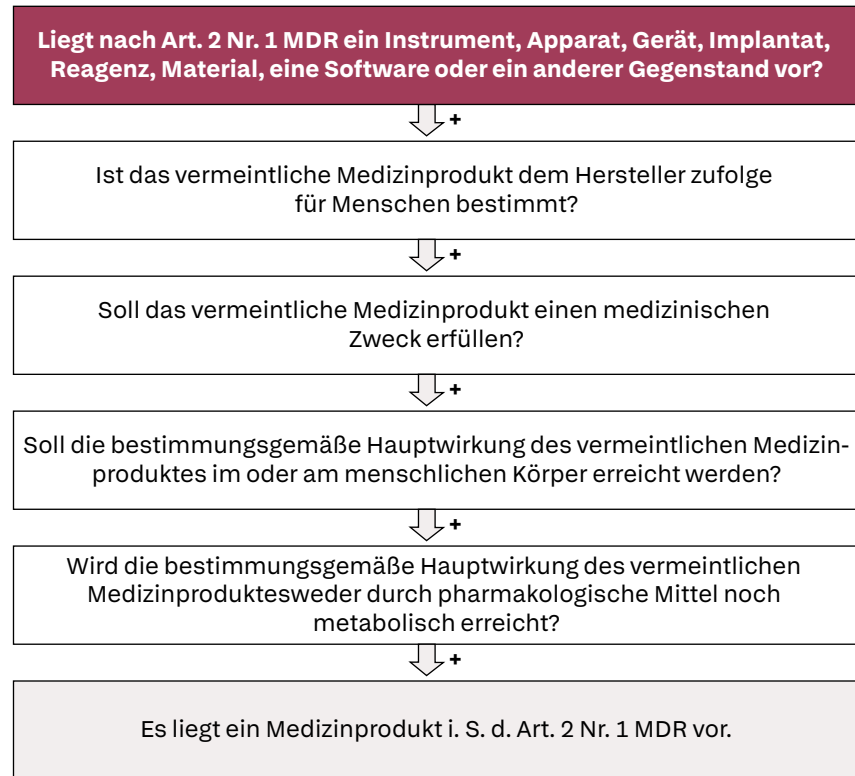


Abb. 1 Medizinprodukt – Entscheidungsbaum nach MDR (+ = Ja)

physische Datenverbindung mit einem Gerät oder Netz einschließt. Der Begriff des Produkts mit digitalen Elementen wird gemäß Art. 3 Nr. 1 CRA definiert, als „ein Software- oder Hardwareprodukt und dessen Datenfernverarbeitungslösungen, einschließlich Software- oder Hardwarekomponenten, die getrennt in den Verkehr gebracht werden“. Der Begriff ist damit weit gefasst. Betroffen ist jegliche Soft- und Hardware, einschließlich einzelner Komponenten, mit einer direkten oder indirekten logischen (mittels Softwareschnittstelle, wie z. B. Netzwerksockets) oder physischen (mittels Hardwareschnittstelle, wie z. B. USB-Anschluss). Der CRA sieht aber auch spezifische Bereichsausnahmen vor. Diese nehmen bestimmte Produkte von den Anforderungen der Verordnung aus. Soweit rechtliche Bestimmungen bereits spezifische Sicherheitsan-

forderungen für Produkte enthalten, soll dadurch eine doppelte Regulierung vermieden werden.⁵ Unter anderem ausgenommen sind nach Art. 2 Abs. 2 lit a CRA Produkte mit digitalen Elementen, auf die die MDR Anwendung findet. Gleichzeitig beansprucht der CRA ausweislich Erwägungsgrund 10 Geltung u. a. für am Körper tragbare medizinische Geräte (Wearables).

Das Spannungsverhältnis zwischen MDR und CRA

Die MDR kennt den Begriff „Cyberresilienz“ nicht. Bezüge zur Sicherheit digitaler Produktkomponenten sind jedoch insbesondere in Anhang I Kap. II Nr. 17 MDR zu finden, der die Grundlegenden Sicherheits- und Leistungsanforderungen beschreibt. Danach sind Produkte mit programmierbaren elektronischen Systemen, einschließlich Software, so zu konzipieren und herzustellen

len, dass Wiederholbarkeit, Zuverlässigkeit und Leistung entsprechend ihrer Zweckbestimmung gewährleistet sind. Die Softwareentwicklung hat nach dem Stand der Technik unter Beachtung des Risikomanagements, der Informationssicherheit sowie von Verifizierung und Validierung zu erfolgen. Produkte müssen gegen unbefugten Zugriff geschützt sein, und Hersteller haben Mindestanforderungen an die IT-Umgebung festzulegen und in der Gebrauchsanweisung anzugeben. Risiken aus Wechselwirkungen mit der IT-Umgebung sind soweit möglich auszuschließen oder zu minimieren.

Die MDR „denkt“ Fragen der Cybersicherheit demnach also bereits mit. Produkte, die in den Anwendungsbereich der MDR fallen, sind damit auch in Bezug auf IT-Sicherheit und den Schutz vor unbefugtem Zugriff reguliert. Als Spezialgesetz gegenüber horizontalen Regelungen geht die MDR dem CRA vor. Dies entspricht auch dem Wortlaut des Art. 2 Abs. 2 CRA, wonach Produkte vom Anwendungsbereich der neuen Verordnung ausgenommen sind, sofern sie durch bestimmte EU-Rechtsvorschriften, wie die MDR, bereits geregelt werden. Somit finden die Vorschriften des CRA keine Anwendung auf Produkte, die dem Anwendungsbereich der MDR unterfallen. Dies soll eine Doppelregulierung verhindern.

Das betrifft zunächst klassische Medizinprodukte wie zertifizierte Operationsroboter, Implantate oder Insulinpumpen. Diese Produkte unterliegen bereits detaillierten Anforderungen an Sicherheit und Leistungsfähigkeit einschließlich Regularien zur IT-Sicherheit.⁶

In der Praxis erscheinen Zusammenspiel und Spannungsverhältnis von MDR und CRA jedoch komplexer: Der CRA kann Produkte be-

treffen, die zwar im Gesundheitsbereich eingesetzt werden, aber nicht unter den Anwendungsbereich der MDR fallen. Diese unterliegen dann dem CRA und müssen dessen Anforderungen eigenständig erfüllen.⁷ Gerade im digitalen Gesundheitsbereich, mit seiner Vielzahl an Schnittstellen und Softwareprodukten, entstehen hier Abgrenzungsfragen mit großer praktischer Relevanz.

Hersteller, Entwickler und Betreiber fragen sich daher zunehmend: Wann genau greift die CRA-Ausnahme – und wann nicht? Welche Komponenten, Zubehörteile oder Softwarelösungen unterliegen weiterhin der MDR und welche müssen zusätzlich oder ausschließlich die neuen Cybersicherheitsanforderungen des CRA erfüllen?

Die Problematik wird dadurch verschärft, dass Software, IT-Module oder Ersatzteile sowohl eigenständig als auch als Teil komplexer Systeme auf den Markt gebracht werden.

Der Teufel im Detail: Zubehör, Ersatzteile, Zulieferkomponenten

Zubehör

Nach Art. 2 Abs. 2 lit. a CRA gilt der CRA nicht für Produkte mit digitalen Elementen, auf welche die MDR Anwendung findet.

Da sich der Wortlaut des Art. 2 CRA nicht auf Medizinprodukte, sondern auf die Anwendbarkeit der MDR bezieht, gilt der Ausschluss des Art. 2 CRA für alle Regelungsobjekte, die von der MDR erfasst werden.⁸

Hierzu zählt somit auch das Zubehör von Medizinprodukten. Art. 1 Abs. 1 MDR bezieht ausdrücklich sowohl Medizinprodukte als auch deren Zubehör in den Anwendungsbereich der MDR ein. Damit findet der CRA sowohl auf Medizinpro-

dukte und auf Zubehör keine Anwendung.

Ersatzteile

Art. 23 MDR trägt den Titel „Teile und Komponenten“ und regelt, unter welchen Bedingungen Gegenstände, die zum Ersatz von Produktbestandteilen bestimmt sind, auf dem Markt bereitgestellt werden dürfen. Gemäß Art. 23 Abs. 2 MDR gilt ein Gegenstand, der speziell dazu bestimmt ist, einen Teil oder eine Komponente eines Produkts zu ersetzen, und durch den sich die Leistungs- oder Sicherheitsmerkmale oder die Zweckbestimmung des Produkts erheblich ändern, als eigenständiges Produkt, das die Anforderungen dieser Verordnung erfüllen muss.⁹ Soweit Ersatzteile somit aufgrund ihrer Zweckbestimmung in den Anwendungsbereich der MDR fallen, ist die Anwendbarkeit des CRA nach Art. 2 Abs. 2 lit. a CRA ausgeschlossen.

Soweit das Ersatzteil aber gerade nicht in den Anwendungsbereich der MDR fällt, bestimmt sich eine mögliche Anwendbarkeit des CRA nach Art. 2 Abs. 1 CRA. Der CRA enthält diesbezüglich eine eigene Bereichsausnahme für Ersatzteile nach Art. 2 Abs. 6 CRA. Danach gilt der CRA nicht für Ersatzteile, die auf dem Markt bereitgestellt werden, um identische Komponenten in Produkten mit digitalen Elementen zu ersetzen, und die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen sollen.¹⁰

Die Intention dieser Regelung besteht darin, die Nutzung langlebiger Produkte durch den CRA nicht zu beeinträchtigen, soweit diese ausschließlich dadurch eintritt, dass für diese Produkte Ersatzteile hergestellt werden.¹¹ Dies ergibt sich auch aus Erwägungsgrund 29 CRA, der bestimmt, dass der CRA eine

Ausnahme für Ersatzteile vorsehen soll, „damit auf dem Markt bereitgestellte Produkte mit digitalen Elementen wirksam repariert werden können und ihre Lebensdauer verlängert wird“. Nach dem Erwägungsgrund gilt die Regelung sowohl für Ersatzteile „die der Reparatur von Altprodukten dienen, die vor dem Geltungsbeginn dieser Verordnung zur Verfügung gestellt wurden, als auch für Ersatzteile, die bereits ein Konformitätsbewertungsverfahren gemäß dieser Verordnung durchlaufen haben“.¹² Sofern also der Einbau eines Ersatzteiles nichts an der Funktionsweise und Art des ursprünglichen Produktes ändert, verändert sich auch nichts an der Cyber-Resilienz des Produktes.¹³

Zulieferkomponenten

Der Einbau eines Ersatzteils in ein Produkt ist von dem originären Einsetzen einer Komponente in das Gesamtmedizinprodukt zu unterscheiden. Die Frage nach der Anwendbarkeit des MDR oder des CRA erfolgt hier maßgeblich nach der Unterscheidung zwischen dem Hersteller- und dem Zuliefererbegriff. Die MDR richtet sich in erster Linie an Hersteller von Medizinprodukten. Nach Art. 2 Nr. 30 MDR ist der Hersteller eine natürliche oder juristische Person, die ein Produkt herstellt oder entwickelt und dieses Produkt unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet.¹⁴ Zulieferer, die Komponenten oder Baugruppen eines Medizinproduktes liefern, gelten in der Regel nicht selbst als Hersteller eines Medizinproduktes - es sei denn, sie vertreiben das Produkt unter eigenem Namen oder geben ihm eine eigenständige Zweckbestimmung.¹⁵ Sie unterliegen daher nicht unmittelbar den Anforderungen des MDR.

Besondere Aufmerksamkeit er-

fordern daher Komponenten oder technische Module. Diese werden in der Regel als Ersatzteile oder optionale Teile verstanden, die separat von dem Produkt geliefert werden, mit dem sie final verwendet werden sollen. Komponenten verfügen für sich genommen über keine medizinische Zweckbestimmung, werden jedoch in einem Gesamtsystem verbaut, das als Medizinprodukt gilt. Komponenten gelten nur dann als Medizinprodukt, wenn sie die Leistungs- oder Sicherheitsmerkmale oder die Zweckbestimmung eines Medizinproduktes erheblich verändern.¹⁶ Sie stellen dagegen gerade keine Medizinprodukte dar, wenn sie nur in Kombination mit anderen Komponenten funktionieren und vom Endhersteller in das medizinische Gesamtsystem integriert werden.¹⁷

Auch hier bleibt wesentlich: über die Zweckbestimmung entscheidet der Hersteller. Demzufolge ist dieser Zweck für jedes Produkt im Einzelfall zu bestimmen. Anschließend lässt sich feststellen, ob die Verwendung des Produktes eine medizinische Maßnahme darstellt oder nicht.¹⁸

Stellt die zu liefernde Komponente ein Produkt mit digitalen Elementen dar, welches keinen medizinischen Zweck aufweist ist der CRA mit seinen Anforderungen an die Cybersicherheit anzuwenden. Dies ist beispielsweise dann der Fall, wenn ein Zulieferer ein Bluetooth- oder WLAN-Kommunikationsmodul entwickelt und vertreibt, das in verschiedene vernetzte Medizinprodukte (z. B. Infusionspumpen, Wearables oder Medizinprodukte mit App-Anbindung) integriert wird. Der entscheidende Faktor: Es geht um die „Zweckbestimmung“

Wearables

Ein Wearable (zu Deutsch: „tragba-

res Gerät“) bezeichnet ein elektronisches Gerät, das direkt am Körper getragen wird, typischerweise als Armband, Uhr, Kleidung oder Implantat. Wearables sind in der Regel mit Sensoren ausgestattet, um physiologische Daten (z. B. Herzfrequenz, Schrittzahl, Schlafmuster) oder Umweltdaten zu erfassen, diese zu analysieren und oft in Verbindung mit mobilen Apps oder Cloud-Diensten darzustellen. Sie können sowohl dem Fitness- und Gesundheitsmonitoring als auch medizinischen Zwecken, z. B. Überwachung chronischer Erkrankungen dienen.

Gemäß Erwägungsgrund 10 findet der CRA u. a. Anwendung auf „am Körper tragbare medizinische Geräte (Wearables). Auf den ersten Blick lässt die Formulierung vermuten, dass in Bezug auf medizinische Geräte, sprich Medizinprodukte in Gestalt von Wearables, die Regeln des CRA gelten. Dies stünde im klaren Widerspruch zur Aussage, dass (alle) Medizinprodukte per se dem Regelungsbereich der MDR unterfallen. Die Formulierung des Erwägungsgrundes 10 gilt es daher im Lichte des Verordnungstextes einzuordnen und zu verstehen. Der CRA findet Anwendung auf Produkte mit digitalen Elementen. Wichtige Produkte mit digitalen Elementen der Klasse I sind nach Anhang III Ziffer 19 CRA „am Körper tragbare Produkte, die zum Zwecke der Gesundheitsüberwachung (z. B. Tracking) bestimmt sind und nicht unter die Verordnungen (EU) 2017/745 (MDR) [...] fallen [...]“. Im eigentlichen Verordnungstext wird somit sehr klar unterschieden zwischen Wearables, die der Definition eines klassischen Medizinproduktes entsprechen und folglich auch von der MDR reguliert werden und solchen, für die dies nicht gilt. Wesentlich ist, ob mit dem Wearable eine diagnostische

oder therapeutische Zweckbestimmung verfolgt wird, so dass die MDR greift,¹⁹ oder ob dies nicht der Fall ist, so dass der CRA anzuwenden ist.

Software

Eine Abgrenzungsfrage bezüglich MDR und CRA betrifft Softwareprodukte. Insbesondere in Bezug auf digitale Gesundheitslösungen stellt sich regelmäßig die Frage, ob Software als Medizinprodukt im Sinne der MDR einzuordnen ist – oder ob sie als Produkt mit digitalen Elementen in den Geltungsbereich des CRA fällt.²⁰

Grundsätzlich kann auch Software ein Medizinprodukt darstellen, wenn und soweit sie vom Hersteller ausdrücklich für medizinische Zwecke vorgesehen ist, etwa zur Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten oder Behinderungen.²¹ Dies wurde von dem Gesetzgeber bereits in den Erwägungsgründen zum MDR festgehalten. Dort heißt es in Erwägungsgrund 19: „Es muss eindeutig festgelegt werden, dass Software als solche, wenn sie vom Hersteller speziell für einen oder mehrere der in der Definition von Medizinprodukten genannten medizinischen Zwecke bestimmt ist, als Medizinprodukt gilt, während Software für allgemeine Zwecke, auch wenn sie in Einrichtungen des Gesundheitswesens eingesetzt wird, sowie Software, die für Zwecke in den Bereichen Lebensstil und Wohlbefinden eingesetzt wird, kein Medizinprodukt ist.“²²

Entscheidend für die Einordnung ist somit in erster Linie die vom Hersteller festgelegte Zweckbestimmung der Software. Ergänzend können objektive Merkmale wie die konkreten Funktionen der Software berücksichtigt werden. Nur wenn die Software dazu bestimmt ist,

spezifisch medizinische Funktionen auszuüben, fällt sie unter den Anwendungsbereich der MDR.²³ Für die Frage, ob der CRA Anwendung findet, ist es daher auch in Bezug auf Software von Bedeutung, zwischen Medizinprodukten und Nichtmedizinprodukten aus regulatorischer Sicht zu unterscheiden. Die MDR erfasst sowohl Software, die in ein physisches Medizinprodukt integriert ist, als auch sogenannte Stand-Alone Software, die unabhängig betrieben wird. Beispiele hierfür sind Diagnostik-Software, Steuerungssoftware für medizinische Geräte oder digitale therapeutische Anwendungen (z. B. Apps zur Verhaltensmodifikation bei psychischen Erkrankungen). Diese Softwaretypen fallen unter die MDR und sind daher vom Anwendungsbereich des CRA ausgenommen (Art. 2 Abs. 2 lit. a CRA).²⁴ Anders stellt sich die Lage bei Software dar, die nicht als Medizinprodukt klassifiziert wird. Hierzu zählen z. B. allgemeine Verwaltungs- oder Kommunikationssoftware in Gesundheitseinrichtungen, digitale Tools zur Patientenverwaltung oder Lifestyle- und Fitness-Apps ohne medizinische Zweckbestimmung.²⁵ Solche Software unterliegt nicht der MDR – und fällt somit regelmäßig in den Anwendungsbereich des CRA. Gleiches gilt für Software, die zwar im medizinischen Umfeld genutzt wird, jedoch keine medizinische Wirkung entfaltet oder nicht direkt an ein Medizinprodukt angebunden ist.²⁶ Ob eine Software als Medizinproduktsoftware im Sinne der MDR einzustufen ist, kann anhand des Entscheidungsbaums (o Abb. 2, s. S. 408) ermittelt werden.²⁷

Medizinische Apps

Ein besonderer Anwendungsfall innerhalb der Kategorie der me-

medizinischen Software sind mobile Anwendungen, sogenannte Medizinische Apps. Diese haben sich in den letzten Jahren zu einem zentralen Bestandteil digitaler Gesundheitsangebote entwickelt – sowohl im klinischen Kontext als auch im Bereich der individuellen Gesundheitsvorsorge. Ihre rechtliche Einordnung bezüglich MDR und CRA erfolgt nach denselben Grundprinzipien wie bei sonstiger Software: Maßgeblich ist auch hier die Zweckbestimmung.²⁸ Wird eine App vom Hersteller gezielt für medizinische Zwecke vorgesehen, beispielsweise zur Diagnoseunterstützung, Therapiebegleitung oder Vitalwertüberwachung, ist sie als Medizinprodukt im Sinne der MDR zu bewerten. Beispiele sind Apps, die auf Basis gemessener Blutzuckerwerte konkrete Dosisempfehlungen für Insulin abgeben, KG-Apps, die Herzrhythmusstörungen erkennen, sowie Anwendungen, die im Rahmen einer psychotherapeutischen Behandlung zur Verhaltensmodifikation beitragen.²⁹ In der Praxis gestaltet sich die Abgrenzung von Gesundheitsapps oder medizinischen Apps als „echte“ Medizinprodukte im Sinne der MDR zu Applikationen, die der Definition eines Medizinprodukts nicht entsprechen, häufig komplex. Apps, die lediglich gesundheitsbezogene Informationen bereitstellen oder Lifestyle-Empfehlungen zu Gesundheit, Ernährung oder Sport ausgeben, gelten regelmäßig nicht als Medizinprodukte.³⁰ Gleiches gilt für reine „Wellness“-Apps wie Achtsamkeits- oder Meditationsapps oder Apps zur Entspannung und Schlafoptimierung. Auch reine Erinnerungsfunktionen, etwa zur Medikamenteneinnahme ohne therapeutische Vorschläge, sowie digitale Nachschlagewerke für medizi-

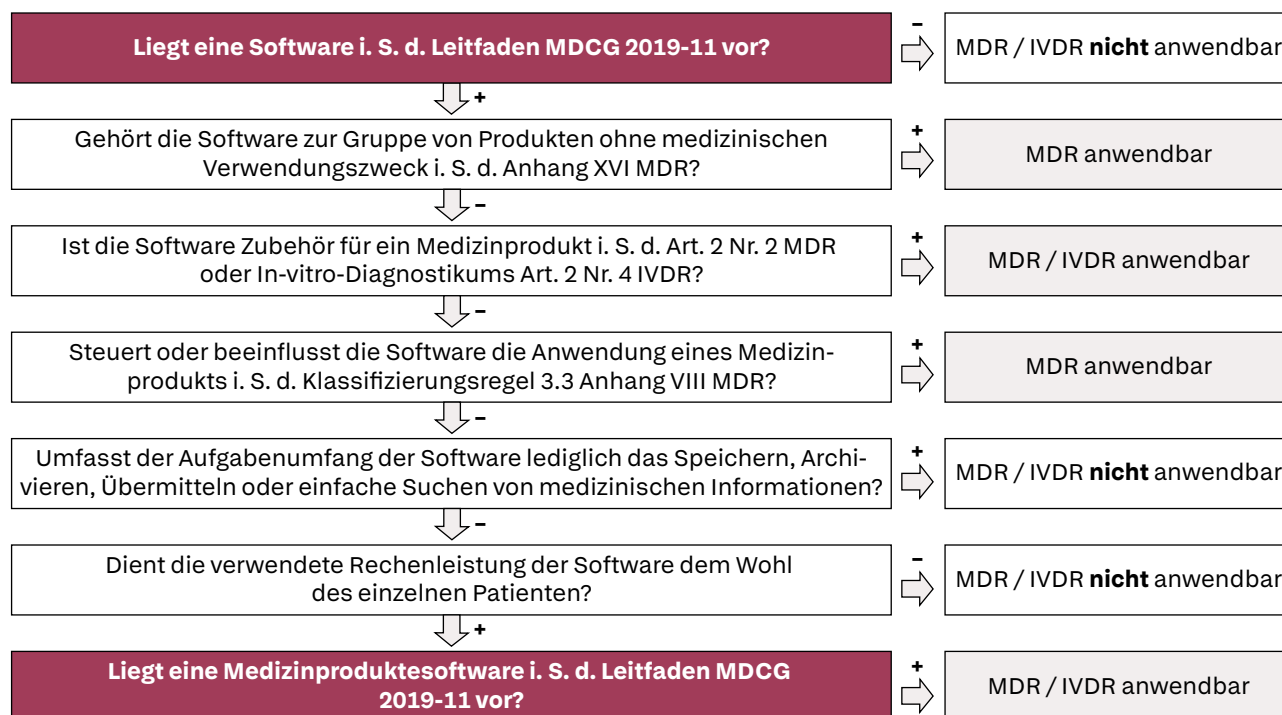


Abb. 2 Software als Medizinprodukt – Entscheidungsbaum nach MDR (+ = Ja, – = Nein)

nisches Wissen gelten in der Regel nicht als Medizinprodukte. Kritisch wird die Abgrenzung zur echten Gesundheitsapp immer dann, wenn eine App Funktionen übernimmt, die aktiv in medizinische Entscheidungsprozesse eingreifen oder eine therapeutische Wirkung beanspruchen.³¹

Medizinische Apps, die nach der MDR als Medizinprodukt klassifiziert werden, sind vom CRA ausgenommen. Alle übrigen gesundheitsbezogenen Apps ohne medizinischen Zweck fallen hingegen in den Anwendungsbereich des CRA, sofern sie ein Produkt mit digitalen Elementen darstellen und keine weitere Ausnahme des CRA einschlägig ist.

Ist der CRA anzuwenden, sind Hersteller insbesondere verpflichtet, die Gestaltung von Produkten mit digitalen Elementen entsprechend den Anforderungen aus Anhang I CRA zu beachten, die neben Cybersicherheitsanforderungen auch Anforderungen an den Umgang

mit Schwachstellen vorsehen. Daneben besteht eine Pflicht zum fortlaufenden Monitoring und einer regelmäßigen Risikobewertung über den gesamten Produktlebenszyklus hinweg. Hersteller müssen zudem sicherstellen, dass kostenlose Sicherheitsupdates über einen bestimmten Supportzeitraum den Nutzern zur Verfügung gestellt werden und während des gesamten Lebenszyklus gegen Cyber Risiken abgesichert sind. Aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle sind zudem der Agentur der Europäischen Union für Cybersicherheit (ENISA) zu melden.

Fazit

Der Cyber Resilience Act (CRA) ergänzt die bestehenden Regelungen der Medical Device Regulation (MDR), ohne diese für klassische Medizinprodukte zu ersetzen. Während die MDR weiterhin alle Produkte mit medizinischer Zweckbestimmung, deren Zubehör und re-

levante Ersatzteile regelt, adressiert der CRA vor allem Produkte mit digitalen Elementen, die nicht als Medizinprodukte klassifiziert sind. Entscheidend für die Abgrenzung ist stets die Zweckbestimmung des Produkts, insbesondere bei Software und mobilen Anwendungen sowie Wearables. Für Hersteller ist eine sorgfältige Zweckbestimmung, Funktionsprüfung und Klassifizierung ihrer App daher essenziell. Medizinprodukte und deren Zubehör sind vom CRA ausgenommen, ebenso bestimmte Ersatzteile, sofern sie keine sicherheitsrelevanten Änderungen bewirken. Software unterliegt nur dann der MDR, wenn sie ausdrücklich für medizinische Zwecke bestimmt ist. Andernfalls fällt sie als Produkt mit digitalen Elementen in den Geltungsbereich des CRA. Eine präzise regulatorische Einordnung ist für Hersteller im Gesundheitsmarkt unerlässlich, um Doppelregulierung zu vermeiden und Cybersicherheitsanforderungen korrekt zu erfüllen.

Verweise

- ¹ Eickbusch, MPR, 2021, 52.
- ² Art. 2 Nr. 2 der Verordnung (EU) 2024/2847 – CRA.
- ³ https://www.bfarm.de/DE/Buergerbereich/Medizinprodukte/_node.html; <https://www.johner-institut.de/blog/tag/klassifizierung/>.
- ⁴ Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, abrufbar unter: <https://ec.europa.eu/docsroom/documents/37581>.
- ⁵ Schöttle, MMR, 2024, 741; https://www.sitra.fi/wp-content/uploads/2025/05/sitra_towards-safer-healthcare-2025.pdf; Dittrich/Heinelt, RDi 2023, 309.
- ⁶ EDPS Opinion 23/2022 on the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, abrufbar unter https://www.edps.europa.eu/system/files/2022-11/2022-0921_d2649_opinion_en.pdf.
- ⁷ <https://medizin-und-technik.industrie.de/recht/regulatorisches/eu-cra-was-der-cyber-resilience-act-fuer-die-medizintechnik-bedeutet/>
- ⁸ Poncza, ZfPC, 2023, 44; Schöttle, MMR, 2024, 741; Art. 2 Abs. 2 lit. a der Verordnung (EU) 2024/2847 – CRA.
- ⁹ Art. 23 Abs. 2 der Verordnung (EU) 2017/745 – MDR.
- ¹⁰ Art. 2 Abs. 6 der Verordnung (EU) 2024/2847 – CRA.
- ¹¹ Schöttle, MMR, 2024, 741; Wolfgang Ecker, Medizinprodukte und IVD, 4. Aufl. 2022, S. 79.
- ¹² Erwägungsgrund 29 der der Verordnung (EU) 2024/2847 – CRA.
- ¹³ https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2023/Februar/Cyber_Resilience_Act/2023-02-09_ZVEI_Position_Paper_Cyber_Resilience_Act_CRA.pdf#:~:text=URL%3A%20https%3A%2F%2Fwww.zvei.org%2Ffileadmin%2Fuser_upload%2FPresse_und_Medien%2FPublikationen%2F2023%2FFebruar%2FCyber_Resilience_Act%2F2023.
- ¹⁴ <https://www.basg.gv.at/fuer-unternehmen/medizinprodukte/hersteller#:~:text=Hersteller%20und%20Bevollm%C3%A4chtigte,Definition,die%20diesen%20Auftrag%20angenommen%20hat.>
- ¹⁵ <https://www.eurocom-info.de/wp-content/uploads/2019/10/Praxisleitfaden-Lieferanten.pdf>.
- ¹⁶ <https://decomplx.com/ist-mein-produkt-ein-medizinprodukt/?lang=de>.
- ¹⁷ Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, abrufbar unter: <https://ec.europa.eu/docsroom/documents/37581?locale=nl>; <https://www.frontiersin.org/journals/drug-safety-and-regulation/articles/10.3389/fdsfr.2022.1089965/full>; https://www.johner-institut.de/blog/iec-62304-medizinische-software/software-als-medizinprodukt-definition/#anchor-section_scroll4.
- ¹⁸ <https://decomplx.com/ist-mein-produkt-ein-medizinprodukt/?lang=de>.
- ¹⁹ <https://www.reuschlaw.de/news/wearables-in-der-medizin/>.
- ²⁰ Dr. Mathias Klümper, MPR, 2024, 240.
- ²¹ Ludvigsen, Nagaraja, Daly, When Is Software a Medical Device? Understanding and Determining the „Intention” and Requirements for Software as a Medical Device in European Union Law’, European Journal of Risk Regulation, Vol. 13, Issue 1, March 2022, S. 78 – 93, abrufbar unter: <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/when-is-software-a-medical-device-understanding-and-determining-the-intention-and-requirements-for-software-as-a-medical-device-in-european-union-law/A3E93F49605216B284554F3FBF1664AE>.
- ²² Erwägungsgrund 19 der Verordnung (EU) 2017/745 – MDR.
- ²³ <https://www.johner-institut.de/blog/iec-62304-medizinische-software/software-als-medizinprodukt-definition/#anchor-section>.
- ²⁴ Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation



Rechtanwältin **Miriam Schuh** ist Head of Healthcare bei reuschlaw in Saarbrücken. Sie berät Akteure der HealthCare Branche im Medizinproduktrecht. Ihre Schwerpunkte liegen in den Bereichen eHealth und mHealth sowie in der Beratung zur Regulierung digitaler Gesundheitsanwendungen (DiGA).

Korrespondenz: Reusch Rechtsanwaltsgesellschaft mbH, Büro Saarbrücken, Stengelstr. 1, 66117 Saarbrücken, 0681 859160-0, Miriam.Schuh@reuschlaw.de

Foto: Urban Zintel, © reuschlaw



Rechtanwältin **Christina Ziegler-Kiefer, LL. M.** (Oslo), ist Senior Associate in der Digital Business Unit bei reuschlaw in Saarbrücken. Sie berät in den Bereichen Datenschutz und Cybersicherheit sowie IT- und Vertragsrecht.

Korrespondenz: Reusch Rechtsanwaltsgesellschaft mbH, Büro Saarbrücken, Stengelstr. 1, 66117 Saarbrücken, 0681 859160-0, christina.kiefer@reuschlaw.de

Foto: Urban Zintel, © reuschlaw

- (EU) 2017/746 – IVDR, abrufbar unter: Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR.
- ²⁵ Hinterreiter, Masterarbeit: Medizinprodukt, 2020, 40, abrufbar unter: <https://epub.jku.at/obvulihs/download/pdf/5459719>.
- ²⁶ <https://www.johner-institut.de/blog/iec-62304-medizinische-software/software-als-medizinprodukt-definition/#anchor-section>.
- ²⁷ https://health.ec.europa.eu/document/download/b865d8e9-081a-4601-a91a-f120321c0491_en?filename=md_mdcg_2021_mdsw_en.pdf; Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR, abrufbar unter: <https://ec.europa.eu/docsroom/documents/37581>.
- ²⁸ https://www.bfarm.de/DE/Medizinprodukte/_FAQ/Klassifizierung-Abgrenzung/faq-liste.html.
- ²⁹ Evers-Wolk, Oertel, Sonk, Gesundheits-Apps, Innovationsanalyse, TAB-Arbeitsbericht Nr. 179, abrufbar unter: <https://edocs.tib.eu/files/e01fn19/1664863419.pdf>.
- ³⁰ Evers-Wolk, Oertel, Sonk, Gesundheits-Apps, Innovationsanalyse, TAB-Arbeitsbericht Nr. 179, 50 ff., abrufbar unter: <https://edocs.tib.eu/files/e01fn19/1664863419.pdf>.
- ³¹ <https://www.johner-institut.de/blog/tag/klassifizierung/>; Pramann, Albrecht, Chancen und Risiken von Gesundheits-Apps, Medizinische Hochschule Hannover, 2016, Kapitel 11, Gesundheits-Apps als Medizinprodukte S. 228-243, abrufbar unter: https://web.archive.org/web/20201212163633id_/https://publikationsserver.tu-braunschweig.de/servlets/MCRFileNodeServlet/dbbs_derivate_00042292/charismha_kapitel_11.pdf; https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/Juli/Checkliste__Medical_Apps_und_digitale_Gesundheitsanwendungen_als_Medizinprodukt/Checkliste-Istmeine-App-ein-Medizinprodukt.PDF.

© WVG

Das bewährte Standardwerk zum Medizinprodukterecht



Herausgegeben von Dr. Volker Lückner und Hans Georg Baumann.
Gesamtwerk inkl. 37. Akt. I. f. g. 2023. 3.358 Seiten. 4 Ringordner.
Loseblatt / Fortsetzung. € 198,- [D]. ISBN 978-3-8047-4467-7

Am 26. Mai 2021 begann eine neue Zeitrechnung im europäischen und nationalen Medizinprodukterecht. Mit diesem Tage traten die Verordnung (EU) 2017/745 über Medizinprodukte (MDR) und das Medizinprodukterecht-Durchführungsgesetz (MPDG) in Kraft. Gleichzeitig traten die wesentlichen Teile des bisher maßgeblichen Medizinproduktegesetzes außer Kraft. Das Standardwerk hat bereits mit den letzten Aktualisierungslieferungen diesen umwälzenden Veränderungen im Recht der Medizinprodukte vor allem durch die Kommentierung wesentlicher Artikel der MDR und den Abdruck des MPDG Rechnung getragen. Nunmehr ist auch die Verordnung (EU) 2017/746 über In-vitro-Produktrechts weitgehend abgeschlossen. Dies berücksichtigt die ausführliche Übersicht über das Medizinprodukterecht, die in weiteren Kapiteln überarbeitet worden ist und einen guten Einstieg in das neue Recht bietet. Wie üblich wird die aktuelle Rechtslage der Vorschriften des MPDG und der Rechtsverordnungen in den Rechtstexten und in den Amtlichen Gesetzes- und Verordnungsgründungen abgebildet. Schließlich werden weitere EU-Durchführungsrechtsakte sowie Dokumente der Medical Device Coordination Group (MDCG), wie immer – als besonderer Service – in deutscher Sprache, aufgenommen.