

medizin & technik

05.2026

www.medizin-und-technik.de
EVK 14,70 €

Ingenieurwissen
für die Medizintechnik

TITELTHEMA

Sterilisation

Was nach Gammastrahlen und
Ethylenoxid kommen könnte

Seite 12

Sonderteil Nachhaltigkeit

Warum ein Blick auf den Digitalen
Produktpass jetzt wichtig ist Seite 28

Markt Finnland

Digital, datengetrieben, vernetzt:
ein innovativer Medtech-Hub Seite 48

SPECIAL

Kunststofftechnik: Miniaturisierung,
Mikrospritzguss, Zulieferer Seite 37

Cybersicherheit: Im Spannungsfeld zwischen CRA und MDR

Was gilt wo | Der Cyber Resilience Act gilt zwar nicht für Medizinprodukte gemäß MDR. Bei Komponenten von Medizinprodukten kann es aber schon zu Abgrenzungsschwierigkeiten kommen. Und für Produkte, die im Gesundheitsbereich eingesetzt werden, aber nicht gemäß MDR zertifiziert sind, müssen die CRA-Regeln angewandt werden. Eine Einzelfallprüfung ist daher erforderlich.



(Bild: Frank H./stockadobe.com)

Für Medizinprodukte gemäß MDR soll es keine doppelte Regulierung durch CRA und MDR geben. Im Detail kann die Abgrenzung aber Fragen aufwerfen

Medizinprodukte sind aufgrund ihres steigenden Digitalisierungsgrades zunehmend als eingebettete Bestandteile digitaler Versorgungsumgebungen gestal-

tet. Daraus ergeben sich Innovationspotenziale, die jedoch durch neue Cybersicherheitsrisiken in Frage gestellt werden. Dieser Entwicklung tragen aktuelle Bestrebungen im Digitalrecht Rechnung. Erstmals sollen durch den Cyber Resilience Act (CRA) produktbezogene Cybersicherheitsanforderungen europaweit einheitlich und horizontal ausgestaltet werden. Für die bislang produktregulatorisch weitgehend autonom agierende Medizinprodukteverordnung (Medical Device Regulation, MDR) sieht der Gesetzgeber jedoch Ausnahmen vom Anwendungsbereich des CRA vor.

Im Einzelnen ergeben sich für Wirtschaftsakteure im Medizintechnik-Bereich

jedoch erhebliche Abgrenzungsschwierigkeiten und das Risiko einer Häufung von Compliance-Prozessen. Vor diesem Hintergrund ist es wichtig zu wissen, inwieweit dem europäischen Gesetzgeber der Spagat zwischen Medizinprodukterecht und Cybersicherheitsrecht gelungen ist. Auch stellt sich die Frage, mit welchen weiteren regulatorischen Entwicklungen die betroffenen Wirtschaftsakteure rechnen müssen. Besonderes Augenmerk gilt dabei den Anforderungen an die fristgerechte Umsetzung der Meldepflichten des CRA. Diese gelten bereits ab dem 11.09.2026 und damit deutlich früher als die übrigen Pflichten, die grundsätzlich erst ab dem 11.12.2027 gelten.

IHR STICHWORT

- Vorgaben von CRA und MDR
- Ausnahmeregelung
- Abgrenzungsschwierigkeiten
- Einzelfallprüfung
- Kommende Änderungen

Rechtliche Anforderungen	MDR	CRA
Sichere Konzepte und Entwicklung	Anh. 1 Kap. 1 Sek. 17.2 MDR	Anh.1 Teil 1 Nr. 2 lit. j, k CRA
Schutz vor unbefugtem Zugriff	Anh. 1 Kap. 1 Sek. 18.8 MDR	Anh. 1 Teil 1 Nr. 2 lit. d CRA
Sichere Kombination/Verbindung von Produkten/Systemen	Anh. 1 Kap. 1 Sek. 14.1 MDR	Art. 13 Abs. 3, Anh. 1 Teil 1 Nr. 2 lit. i, j CRA
Risikomanagement und Risikobewertung	Anh. 1 Kap. 1 Sek. 3b, 3c, 3e MDR	Art. 13 Abs. 2, Anh. 1 Teil 1 Nr. 2 CRA
Verfügbarkeit wesentlicher und grundlegender Funktionen	Anh. 1 Kap. 1 Sek. 17.1, 17.2, 17.4 MDR	Anh. 1 Teil 1 Nr. 2 lit. h CRA
Maßnahmen bzgl. bekannten und vorhersehbaren Risiken	Anh. 1 Kap. 1 Sek. 8 MDR	Art. 6 lit. 1, Art. 13 Abs. 3, Anh. 2 Nr. 5 CRA

MDR und CRA weisen in einzelnen Bereichen Parallelen auf. Die MDR bildet die spezifischen Cybersicherheitsanforderungen des CRA jedoch nur punktuell ab. Hersteller dürfen sich daher nicht auf der Einhaltung der MDR-Vorgaben ausruhen

Der CRA gilt für Produkte mit digitalen Elementen, die auf dem Unionsmarkt bereitgestellt werden. Da dieser Begriff entsprechend der Legaldefinition des CRA weit gefasst ist und hierunter grundsätzlich jede Soft- oder Hardware sowie einzelne Komponenten fallen, ist eine Abgrenzung zur MDR entscheidend.

Die zentrale Norm für diese Unterscheidung ist Art. 2 Abs. 2 CRA. Hiernach gilt der CRA nicht für Produkte, auf welche die MDR Anwendung findet. Anknüpfungspunkt ist nicht der Begriff des „Medizinprodukts“, sondern der Anwendungsbereich der MDR. Der Ausschluss des CRA erfasst somit nicht nur Medizinprodukte im engeren Sinne, sondern alle Regelungsobjekte, die zum Anwendungsbereich der MDR gehören.

Bereichsausnahme soll eine Doppelregulierung vermeiden

Hierzu zählt neben Medizinprodukten insbesondere auch deren Zubehör. Die Bereichsausnahme soll eine Doppelregulierung solcher Produkte vermeiden, die bereits einem harmonisierten Produktsicherheitsregime unterliegen.

Die Abgrenzung zwischen MDR und CRA ist – auch wenn es zu Beginn so scheint – aber nicht ganz trennscharf. So gibt es Graubereiche, wonach gewisse Produkte im medizinischen Bereich unter den CRA fallen können.

Beispiele sind die Herstellung und der Einbau von Komponenten. Im Gegensatz zu Ersatzteilen sind Komponenten regelmäßig Bestandteil der ursprünglichen Produktkonzeption. Für die regulatorische Einordnung ist entscheidend, ob die Komponente selbst als Medizinprodukt oder Zubehör im Sinne der MDR zu qualifizieren ist oder lediglich als Zulieferkomponente in ein Gesamtmedizinprodukt integriert wird.

Es ist Aufgabe des Herstellers des Gesamtprodukts, die Konformität des Medizinprodukts insgesamt sicherzustellen. Dabei muss er auch die Sicherheit, Leistungsfähigkeit und Eignung der eingesetzten Komponenten berücksichtigen. Eine Ausnahme hiervon macht Art. 23 Abs. 2 MDR für Gegenstände, die speziell dazu bestimmt sind, Komponenten eines spezifischen Produkts zu ersetzen.

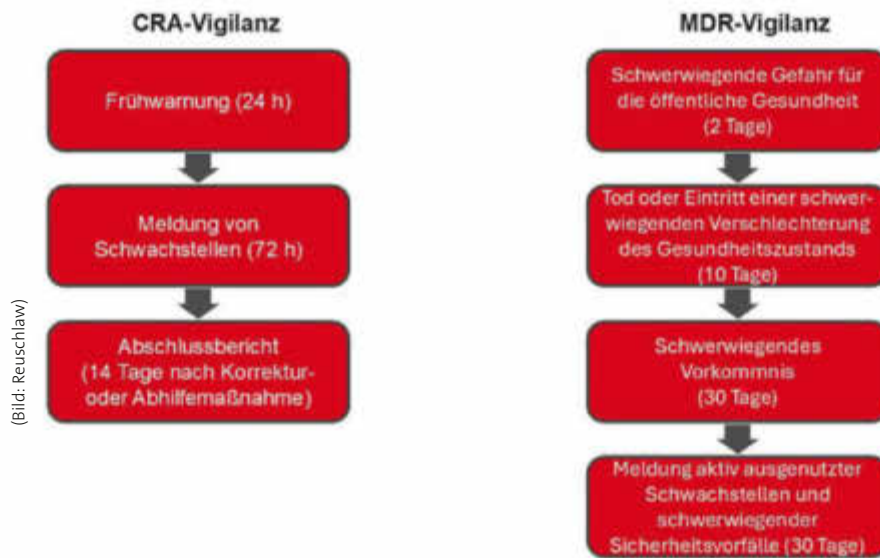
Auch reine Software kann als Medizinprodukt unter die Bereichsausnahme des CRA fallen. Software, die nicht als Medizinprodukt klassifiziert wird (etwa allgemeine Verwaltungs- oder Kommunikationssoftware in Gesundheitseinrichtungen oder Lifestyle- und Fitness-Apps), unterliegt also nicht der MDR und fällt somit regelmäßig in den Anwendungsbereich des CRA. Für am Körper tragbare Gesundheitstracker oder Wearables, die für den Einsatz bei Kindern konzipiert sind und nicht unter die MDR fallen, gelten erhöhte

Cybersicherheitsanforderungen (vgl. Anhang 3 Nr. 19 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. In der Praxis gestaltet sich die Einordnung von Gesundheits- oder Medizin-Apps daher häufig komplex. Apps, die lediglich gesundheitsbezogene Informationen bereitstellen oder Lifestyle-Empfehlungen zu Gesundheit, Ernährung oder Sport ausgeben, gelten regelmäßig nicht als Medizinprodukte.

MDR oder CRA? Zum Teil im Einzelfall prüfen

Ob ein Produkt von den Pflichten des CRA ausgenommen ist, muss für jedes Produkt gesondert geprüft werden. Weder dessen Verwendung im medizinischen Umfeld noch die vorsorgliche Einhaltung medizinprodukterechtlicher Anforderungen bilden eine belastbare Grundlage. Insbesondere in Grenzfällen, in denen das Vorliegen einer medizinischen Zweckbestimmung zweifelhaft ist, kann die Einzelfallprüfung ergeben, dass das Produkt nicht der MDR, sondern dem CRA unterfällt. Darüber hinaus müssen Hersteller digitaler Medizinprodukte in Lieferkettszenarien regelmäßig Komponenten einbeziehen, die eigenständig den Anforderungen des CRA unterliegen.



Die Meldepflichten des CRA sind andere als bei der MDR. Die CRA-Meldepflichten gelten auch bereits ab dem 11.09.2026 und greifen damit über ein Jahr früher als die übrigen im Gesetz festgelegten Pflichten

Einen Orientierungsrahmen für medizinproduktespezifische Cybersicherheitsanforderungen bieten die MDCG-Leitlinien zur Cybersicherheit von Medizinprodukten. Dabei zeigt sich, dass es inhaltliche Schnittmengen zwischen der MDR und dem CRA gibt. So weisen beide Regelungsregime in einzelnen Bereichen Parallelen auf. Die MDR bildet die spezifischen Cybersicherheitsanforderungen des CRA jedoch nur punktuell ab. Dies zeigt, dass sich Hersteller nicht auf der Einhaltung der MDR-Vorgaben ausruhen dürfen. Vielmehr müssen sie den Anwendungsbereich der Regelwerke prüfen und die zwingend die einschlägigen Anforderungen im Einzelfall prüfen.

Reformideen greifen Abgrenzungsfragen auf

Die Abgrenzungsfragen zwischen CRA und MDR werden durch aktuelle Reformbestrebungen aufgegriffen. Sowohl die geplante Revision der MDR und IVDR (Europäische Kommission, COM(2025) 1023) als auch der Digitale Omnibus (Europäische Kommission, COM(2025) 836 final) zielen darauf ab, parallele Pflichten zu synchronisieren, Doppelstrukturen zu vermeiden und Vereinfachungen zu schaffen. Beim Digital Omnibus on AI, der Ende Juli in Kraft trat, stehen der Schutz von Verbraucherrechten angesichts neuer

Technologien und Geschäftsmodelle im Vordergrund.

Für Medizinprodukte ist insbesondere der geplante neue Art. 87a MDR relevant; für In-vitro-Diagnostika enthält Art. 82a IVDR eine entsprechende Regelung. Danach sollen Hersteller aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle im Sinne des CRA künftig unter Rückgriff auf das etablierte Vigilanzsystem der MDR und IVDR über Eu-damed an die zuständigen CSIRTs und die ENISA melden.

Meldepflichten nach MDR und CRA unterscheiden sich

Eine Vereinfachung des Meldesystems für Medizinproduktehersteller ist damit jedoch nicht zwangsläufig verbunden. Die verschiedenen Meldepflichten nach MDR und CRA unterscheiden sich nicht nur hinsichtlich der maßgeblichen Fristen und ihrer Berechnung, sondern auch in Bezug auf das jeweils risikobestimmende Rechtsgut.

In der Praxis bedarf es daher entsprechender Prozesse, die eine einzelfallbezogene Prüfung der einschlägigen Meldetatsachen sowie eine fristgerechte Zuordnung zum jeweiligen Melderegime gewährleisten. Zu beachten ist ferner, dass weitere Meldepflichten, etwa nach der DSGVO, von den Meldepflichten der MDR

und des CRA unberührt bleiben. Diese sind daher ebenfalls in den Meldeprozess einzubeziehen.

Zwar wird der CRA für Produkte, die dem Anwendungsbereich der MDR unterfallen, grundsätzlich ausgeschlossen, doch bestehen zusammenfassend gesagt in der Praxis eine Reihe von Fällen, in denen Produkte aus dem Medizintechnik-Bereich zum Anwendungsbereich des CRA gehören. Hersteller von Produkten sollten stets im Einzelfall prüfen, unter welches Regime das einzelne Produkt fällt. Der einseitige Fokus auf eines der beiden Regelwerke genügt nicht. Vielmehr sind die Wechselwirkungen von MDR und CRA im Hinblick auf das Produktportfolio im Detail zu betrachten. ■

Christina Ziegler-Kiefer, Luka Prgomet, Reuschlaw, Saarbrücken

www.reuschlaw.de

Weitere Informationen

Reuschlaw bietet einen Quick-Check an, der die Einschätzung erleichtern soll, ob das Produkt eines Herstellers von den Vorschriften des Cyber Resilience Acts betroffen ist.

<https://cra-check.de>