

NEUE VORSCHRIFTEN ZUR CYBERSICHERHEIT

Auf die Hersteller von Medizinprodukten kommen neue Vorschriften zur Cybersicherheit zu, über die der Bundesverband Medizintechnologie (BVMed) mit einem neuen Informationsblatt informiert. Grundlage ist die europäische NIS-2-Richtlinie (Netzwerk- und Informationssicherheit) aus dem Jahr 2023, die deutliche Verschärfungen der EU-Vorschriften zur Cybersicherheit enthält. Sie muss bis zum 17. Oktober 2024 in nationales Recht umgesetzt werden. Seit Ende Juni 2024 liegt dazu in Deutschland der vierte Referentenentwurf zu einem NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz (NIS2UmsuCG) vor.



BVMed – Bundesverband Medizintechnologie e.V.
 Georgenstraße 25, 10117 Berlin
 Tel.: +49-(0)40-30 246 255-0
 E-Mail: info@bvmed.de
 www.bvmed.de

CYBERSICHERHEITSRECHT Vorgaben für die Medizintechnik-Branche

Richtlinie (EU) 2022/2555 (NIS-2-RL) & NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz (NIS2UmsuCG) Informationsblatt

Namen der Rechtsakte
 Richtlinie (EU) 2022/2555 vom 14.10.2022 über Maßnahmen für ein höheres gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 952/2014 und der Richtlinie (EU) 2016/1148 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

Verfängerungsstand
 NIS-2-Richtlinie: In Kraft getreten am 16.01.2023, umgesetzt durch die EU-Mitgliedstaaten bis zum 17.10.2024.
 NIS2UmsuCG: Referentenentwurf (24.06.24) veröffentlicht, Verabschiedung ausstehend.

Impressum
 © Bundesverband Medizintechnologie e.V. (BVMed) in Zusammenarbeit mit Reusch Rechtsanwälte (www.reusch.de) (www.bvmed.de). Dieses Übersichtsblatt ist eine Erfindung von Reusch, Juli 2024.

Aktuelles
 Die NIS2UmsuCG dient der Umsetzung der NIS-2-Richtlinie durch den deutschen Gesetzgeber. In nationales Recht. Seit mit der Umsetzung der NIS-2 Richtlinie in deutsches Recht, werden die Vorgaben zur Cybersicherheit für Unternehmen in Deutschland verbindlich. Im Rahmen der Vorlagentextüberprüfung hat das für das NIS2UmsuCG zuständige Bundesministerium des Innern und für Heimat (BMI) angekündigt, auf Grundlage des 4. Referentenentwurfs bis Herbst 2024 einen Kabinettsentwurf vorzulegen und das parlamentarische Verfahren einzuleiten, sodass das NIS2UmsuCG spätestens im Frühjahr 2025 in Kraft treten soll. Hierbei ist zu beachten, dass das NIS2UmsuCG unmittelbar nach Inkrafttreten Anwendung finden wird. Es wird keine zusätzliche nationale Übergangsfrist geben.

Hintergrundinformation
 Hier zur NIS-2-Richtlinie werden die Anforderungen an die Cybersicherheit für die Medizintechnik- und In-vitro-Diagnostik-Branche deutlich verschärft. Insbesondere ab dem 18.10.2024 müssen die neuen Vorgaben durch die EU-Mitgliedstaaten in nationales Recht umgesetzt und angewendet werden.

4 Schritte zur Umsetzung der NIS-2-Richtlinie

1. Prüfung der Betroffenheit
2. Ableitung der konkreten (gesetzlichen) Vorgaben
3. Umsetzung der rechtlichen Vorgaben im Unternehmen und in der Lieferkette (inklusive Dokumentation)
4. Meldung von Verstößen (auch über interne Prozesse) sowie der Prävention in der Lieferkette

Im Bereich der In-vitro-Diagnostik sind Unternehmen regelmäßig betroffen, die die o.g. Schwelmschwerer erfüllen und die ein In-vitro-Diagnostikum (i.v.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika (IVDR) (2017/746/EU) herstellen. Dies umfasst die Medizintechnikherstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Software für die In-vitro-Diagnostik verwendet werden, die menschlichen Körper zum Zwecke der Diagnose, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Im Bereich der In-vitro-Diagnostik sind Unternehmen regelmäßig betroffen, die die o.g. Schwelmschwerer erfüllen und die ein In-vitro-Diagnostikum (i.v.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika (IVDR) (2017/746/EU) herstellen. Dies umfasst die Medizintechnikherstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Software für die In-vitro-Diagnostik verwendet werden, die menschlichen Körper zum Zwecke der Diagnose, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Im Bereich der In-vitro-Diagnostik sind Unternehmen regelmäßig betroffen, die die o.g. Schwelmschwerer erfüllen und die ein In-vitro-Diagnostikum (i.v.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika (IVDR) (2017/746/EU) herstellen. Dies umfasst die Medizintechnikherstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Software für die In-vitro-Diagnostik verwendet werden, die menschlichen Körper zum Zwecke der Diagnose, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Darüber ist es für die betroffenen Unternehmen, dass auch eine Reihe von weiteren Maßnahmen zu ergreifen, die über die Bestimmungen der NIS-2-Richtlinie hinausgehen, wie z.B. die Abstimmung und/oder Verwaltung der gemeinsamen IT-Aufgaben, eine Berichterstattung über die...

CYBERSICHERHEITSRECHT Vorgaben für die Medizintechnik-Branche

Anwendungsbereich
 Die NIS-2-Richtlinie hat einen weiten Anwendungsbereich. Die neuen Cybersicherheitsvorschriften gelten für alle relevanten Unternehmen, die die o.g. Schwelmschwerer erfüllen und die ein Medizintechnikprodukt (i.v.d. Art. 2 Nr. 1 der Medizintechnikverordnung (MTZ) (2022/2269) herstellen. Dies umfasst u.a. die Herstellung von Instrumenten, Apparaten, Geräten, Software, Implantaten oder anderen Gegenständen, die für Menschen bestimmt sind und die einen der folgenden medizinischen Zwecke erfüllen:
 • Diagnose, Vorhersage, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Im Medizintechnik-Bereich betroffen sind damit insbesondere Unternehmen, die die o.g. Schwelmschwerer erfüllen und die ein Medizintechnikprodukt (i.v.d. Art. 2 Nr. 1 der Medizintechnikverordnung (MTZ) (2022/2269) herstellen. Dies umfasst u.a. die Herstellung von Instrumenten, Apparaten, Geräten, Software, Implantaten oder anderen Gegenständen, die für Menschen bestimmt sind und die einen der folgenden medizinischen Zwecke erfüllen:
 • Diagnose, Vorhersage, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Im Bereich der In-vitro-Diagnostik sind Unternehmen regelmäßig betroffen, die die o.g. Schwelmschwerer erfüllen und die ein In-vitro-Diagnostikum (i.v.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika (IVDR) (2017/746/EU) herstellen. Dies umfasst die Medizintechnikherstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Software für die In-vitro-Diagnostik verwendet werden, die menschlichen Körper zum Zwecke der Diagnose, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Im Bereich der In-vitro-Diagnostik sind Unternehmen regelmäßig betroffen, die die o.g. Schwelmschwerer erfüllen und die ein In-vitro-Diagnostikum (i.v.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika (IVDR) (2017/746/EU) herstellen. Dies umfasst die Medizintechnikherstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Software für die In-vitro-Diagnostik verwendet werden, die menschlichen Körper zum Zwecke der Diagnose, Überwachung, Vorhersage, Prognose, Beurteilung, Lenkung von therapeutischen Maßnahmen, Überwachung, Behinderung, Lenkung, Kompensation von Verstößen oder Behinderungen, Untersuchung, Erzielung von Ergebnissen der Analyse oder eines physikalischen oder pathologischen Vorgangs enthalten.

Darüber ist es für die betroffenen Unternehmen, dass auch eine Reihe von weiteren Maßnahmen zu ergreifen, die über die Bestimmungen der NIS-2-Richtlinie hinausgehen, wie z.B. die Abstimmung und/oder Verwaltung der gemeinsamen IT-Aufgaben, eine Berichterstattung über die...

Pflichten in Stichpunkten
 Die Vorgaben der NIS-2-Richtlinie lassen sich grob in drei Gruppen zusammenfassen:
 1. Governance: Die Geschäftsführung muss Maßnahmen zur Cybersicherheit ergreifen und gewährleisten. Sämtliche Mitarbeiter müssen zur Cybersicherheit geschult werden. Die Verbindungen gegen die Governance-Erfüllbarkeit, Geschäftsfortführung, Identifizierung und als kurzfristige Suspendierung durch die Aufsichtsbehörde dienen.
 2. Management: Es ist eine Risikoanalyse durchzuführen und zu dokumentieren. Identifizierte Risiken müssen durch technische und organisatorische Maßnahmen beherrschbar gemacht werden. Die Cybersicherheit muss Teil der Risikoanalyse sein, sondern auch in der Lieferkette gewährleistet werden.
 3. Kommunikation: Erhebliche Cybersicherheitsvorfälle sind in einem gesteuerten Meldesystem an die zuständige Aufsichtsbehörde zu melden. Es nach Bedarf sind bis zu 5 Meldungen erforderlich. Im Falle von erheblichen Cyberbedrohungen sind sofort die Empfänger der Dienste zu unterrichten. Die datenschutzrechtlichen Maßnahmen bleiben unberührt.

Die zuständigen Aufsichtsbehörden ermitteln weitgehend Überwachungs-Überwachungsmaßnahmen und können z.B. präventive Vorbeugungsmaßnahmen und gezielte Überwachungsmaßnahmen durchführen. Bei Verstößen können zudem Anordnungen, Änderungen und öffentliche Warnungen der zuständigen Aufsichtsbehörde auch Maßstäbe von bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes (wobei, welcher Betrag höher ist, Zahlen werden Datenübermittlungsmaßnahmen in der zuständigen Datenverarbeitungsbereichsbehörde.

Die zuständigen Aufsichtsbehörden ermitteln weitgehend Überwachungs-Überwachungsmaßnahmen und können z.B. präventive Vorbeugungsmaßnahmen und gezielte Überwachungsmaßnahmen durchführen. Bei Verstößen können zudem Anordnungen, Änderungen und öffentliche Warnungen der zuständigen Aufsichtsbehörde auch Maßstäbe von bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes (wobei, welcher Betrag höher ist, Zahlen werden Datenübermittlungsmaßnahmen in der zuständigen Datenverarbeitungsbereichsbehörde.

Mit der NIS-2-Richtlinie werden die Anforderungen an die Cybersicherheit in der Medizinprodukte- und In-vitro-Diagnostik-Branche deutlich verschärft. Betroffen sind dabei Unternehmen ab 50 Beschäftigten oder einem Jahresumsatz von über 10 Millionen Euro. Aus den Vorgaben der NIS-2-Richtlinie ergeben sich unter anderem folgende Anforderungen:

- **Governance und Awareness:** Die Geschäftsführung muss Maßnahmen zur Cybersicherheit ergreifen und überwachen sowie sämtliche Mitarbeiter:innen zur Cybersicherheit schulen.
- **Management von Cybersicherheits-Risiken:** Die Unternehmen müssen Risikoanalysen durchführen und dokumentieren. Identifizierte Risiken müssen durch technische und organisatorische Maßnahmen beherrschbar gemacht werden. Die Cybersicherheit muss hierbei nicht nur im Unternehmen selbst, sondern auch in der Lieferkette gewährleistet werden.

- **Berichtspflichten:** Erhebliche Cybersicherheits-Vorfälle müssen in einem gestuften Meldesystem an die zuständige Aufsichtsbehörde gemeldet werden. Je nach Vorfall sind bis zu 5 Meldungen erforderlich. Im Falle von erheblichen Cyberbedrohungen sind zudem die Empfänger:innen der Dienste zu unterrichten. Die datenschutzrechtlichen Meldepflichten bleiben daneben bestehen.

Erst mit der Umsetzung der NIS-2-Richtlinie in deutsches Recht werden die Vorgaben zur Cybersicherheit für Unternehmen in Deutschland verbindlich. Im Rahmen der Verbändanhörung hat das für das NIS2-UmsuCG federführende Bundesinnenministerium angekündigt, bis Herbst 2024 einen Kabinettsentwurf vorzulegen und das parlamentarische Verfahren einzuleiten, sodass das Gesetz

spätestens im Frühjahr 2025 ohne Übergangsfristen in Kraft treten soll.

Das BVMed-Informationsblatt zu den neuen Anforderungen an die Cybersicherheit, das in Zusammenarbeit mit der Kanzlei Reusch Law erarbeitet wurde, kann unter www.bvmed.de/cybersicherheit heruntergeladen werden.

Zu der NIS-2-Richtlinie zur Cybersicherheit bietet die BVMed-Akademie am 9. September 2024 ein Webinar an. Dabei geht es neben einem tiefgreifenden Verständnis der rechtlichen Vorgaben insbesondere um praktische Lösungen, wie die neuen Vorgaben effektiv in Unternehmen umgesetzt werden können.

Programm, Konditionen und Anmeldung unter:
www.bvmed.de/nis2-24