BVMed Bundesverband Medizintechnologie e.V.

# CYBERSICHERHEITSRECHT

## Vorgaben für die Medizintechnik-Branche

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

### Namen der Rechtsakte

Richtlinie (EU) 2022/2555 vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG).

### Verkündungsstand

NIS-2-Richtlinie: In Kraft getreten am 16.01.2023, Umsetzung durch die EU-Mitgliedstaaten bis zum 17.10.2024.

NIS2UmsuCG: 4. Referentenentwurf (24.06.24) veröffentlicht, Verkündung ausstehend.

### Impressum


Stand: Juli 2024
**www.bvmed.de**

### Aktuelles

Das NIS2UmsuCG dient der Umsetzung der NIS-2-Richtlinie durch den deutschen Gesetzgeber in nationales Recht. Erst mit der Umsetzung der NIS-2-Richtlinie in deutsches Recht, werden die Vorgaben zur Cybersicherheit für Unternehmen in Deutschland verbindlich. Im Rahmen der Verbändeanhörung hat das für das NIS2UmsuCG federführende 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

Mit der NIS-2-Richtlinie werden die Anforderungen an die Cybersicherheit in der Medizinprodukte- und In-vitro-Diagnostika-Branche deutlich verschärft. Spätestens 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. Monitoring sowohl der Rechtslage als auch der internen Prozesse sowie der Prozesse in der Lieferkette

BVMed Bundesverband Medizintechnologie e.V.

# CYBERSICHERHEITSRECHT

## Vorgaben für die Medizintechnik-Branche

### Anwendungsbereich

Die NIS-2-Richtlinie hat einen weiten Anwendungsbereich. Die neuen Cybersicherheitsvorgaben gelten für alle privaten und öffentlichen Einrichtungen, die die Voraussetzungen des Art. 2 NIS-2-Richtlinie erfüllen. Ob ein Unternehmen betroffen ist, richtet sich in der Regel nach der folgenden 3-Stufen-Prüfung:

1. Schwellenwertanalyse: Ab 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme über 10 Mio. EUR (Empfehlung der EU-Kommission 2003/361/EG) (Ausnahmen nach Art. 2 Abs. 2 möglich)
2. Zugehörigkeit zu einem Sektor aus Anhang I oder II
3. Erbringung von Diensten oder Ausübung von Tätigkeiten in der EU

Im Medizinprodukte-Bereich betroffen sind damit regelmäßig Unternehmen, die die o.g. Schwellenwerte erfüllen und die ein Medizinprodukt i.S.d. Art. 2 Nr. 1 der Medizinprodukteverordnung ((EU) 2017/745) herstellen. Dies umfasst u.a. die Herstellung von Instrumenten, Apparaten, Geräten, Software, Implantaten oder anderen Gegenständen, die für Menschen bestimmt sind und die einem der folgenden medizinischen Zwecke dienen:

- Diagnose, Verhütung, Überwachung, Vorhersage, Prognose, Behandlung, Linderung von Krankheiten;
- Diagnose, Überwachung, Behandlung, Linderung, Kompensierung von Verletzungen oder Behinderungen;
- Untersuchung, Ersatz/Veränderung der Anatomie oder eines physiologischen oder pathologischen Vorgangs/Zustands.

Im Bereich der In-vitro-Diagnostika sind Unternehmen regelmäßig betroffen, die die o.g. Schwellenwerte erfüllen und die ein In-vitro-Diagnostikum i.S.d. Art. 2 Nr. 2 der Verordnung über In-vitro-Diagnostika ((EU) 2017/746) herstellen. Dies umfasst die Medizinprodukte-Herstellung, die u.a. als Reagenzien, Instrumente, Geräte, Software oder Systeme für die In-vitro-Untersuchung von aus dem menschlichen Körper stammenden Proben bestimmt sind und u.a. Informationen zu einem der folgenden Punkte liefern sollen:

- physiologische/pathologische Prozesse/Zustände;
- kongenitale körperliche oder geistige Beeinträchtigungen;
- Feststellung der Unbedenklichkeit und Verträglichkeit;
- die voraussichtliche Wirkung einer Behandlung oder die voraussichtlichen Reaktionen darauf.

Daneben ist stets zu berücksichtigen, dass auch eine bloße Nebentätigkeit eines Unternehmens, die einem der Sektoren der NIS-2-Richtlinie unterfällt, wie z.B. die Bereitstellung und/oder Verwaltung der konzerneigenen IT-Infrastruktur, eine Betroffenheit begründen kann.

### Pflichten in Stichpunkten

Die Vorgaben der NIS-2-Richtlinie lassen sich grob in drei Gruppen zusammenfassen:

1. Governance & Awareness: Die Geschäftsführung muss Maßnahmen zur Cybersicherheit ergreifen und überwachen. Sämtliche Mitarbeiter müssen zur Cybersicherheit geschult werden. Bei Verstößen gegen die Governance-Pflichten haften Geschäftsführer persönlich und es kann eine zeitweilige Suspendierung durch die Aufsichtsbehörde drohen.
2. Management von Cybersicherheitsrisiken: Es ist eine Risikoanalyse durchzuführen und zu 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.
3. Berichtspflichten: Erhebliche Cybersicherheitsvorfälle sind in einem gestuften Meldesystem an die zuständige Aufsichtsbehörde zu melden. Je nach Vorfall sind bis zu 5 Meldungen erforderlich. Im Falle von erheblichen Cyberbedrohungen sind zudem die Empfänger der Dienste zu unterrichten. Die datenschutzrechtlichen Meldepflichten bleiben daneben bestehen.

### Folgen von Verstößen

Die zuständigen Aufsichtsbehörden erhalten weitgehende Überwachungs-/Durchsetzungsbefugnisse und können z.B. präventive Vor-Ort-Kontrollen und gezielte Sicherheitsüberprüfungen durchführen. Bei Verstößen drohen neben Anweisungen, Anordnungen und öffentlichen Warnungen der zuständigen Aufsichtsbehörde auch Bußgelder von bis zu 10 Mio. EUR oder 2 % des gesamten weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Zudem werden Datenschutzverstöße automatisch an die zuständige Datenschutzaufsichtsbehörde gemeldet.