

NIS-2 Compliance für Hersteller von In-vitro-Diagnostika

Betroffenheit und notwendige Maßnahmen zur Compliance mit der neuen EU-weiten Richtlinie für Cybersicherheit

Mit der neuen Network and Information Security Richtlinie (NIS-2 Richtlinie) werden die Anforderungen an die Cybersicherheit für Hersteller von In-vitro-Diagnostika deutlich verschärft. Spätestens ab dem 18. Oktober 2024 müssen die Vorgaben umgesetzt werden.

Wer ist betroffen?

Betroffen sind Unternehmen ab 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme von 10 Mio. Euro, die ein In-vitro-Diagnostikum im Sinne von Artikel 2 Nr. 2 der EU-Verordnung über In-vitro-Diagnostika herstellen. Dies umfasst die Herstellung von Medizinprodukten, 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 oder pathologische Prozesse oder Zustände;
- kongenitale körperliche oder geistige Beeinträchtigungen;
- Feststellung der Unbedenklichkeit und Verträglichkeit;
- die voraussichtliche Wirkung einer Behandlung oder die voraussichtlichen Reaktionen darauf.

Was ist umzusetzen?

Die Anforderungen der NIS-2 Richtlinie lassen sich in drei Gruppen zusammenfassen. Die erste Gruppe betrifft den Bereich Governance & Awareness. Die Geschäftsführung muss Maßnahmen zur Cybersicherheit ergreifen und überwachen. Bei

Verstößen haften Geschäftsführer persönlich. Die zweite Gruppe umfasst das Management von Cybersicherheitsrisiken. Identifizierte Risiken müssen durch technische und organisatorische Maßnahmen beherrschbar gemacht werden. Cybersicherheit muss auch in der Lieferkette gewährleistet werden. Die dritte Gruppe von Anforderungen beinhaltet Meldepflichten gegenüber den Aufsichtsbehörden.

Was droht bei Verstößen?

Die zuständigen Aufsichtsbehörden können Vor-Ort-Kontrollen und gezielte Sicherheitsüberprüfungen durchführen. Bei Verstößen drohen neben Anordnungen der Aufsichtsbehörde auch hohe Bußgelder und öffentliche Warnungen.

Unsere Unterstützung

Wir unterstützen Sie bei der Umsetzung der Anforderungen der NIS-2 Richtlinie u.a. mit folgenden Leistungen:

- Rechtliche Prüfung der Betroffenheit
- Ableitung der konkreten Vorgaben zur Cybersicherheit und Gap-Analyse
- Rechtliche Unterstützung bei der Umsetzung und Dokumentation
- Einführung eines Cybersecurity Compliance Managements

Next Step: Kontaktaufnahme

Gerne erläutern wir Ihnen unser Vorgehen ausführlich in einem persönlichen Gespräch.

T + 49 30 / 2332 895 0

E info@reuschlaw.de