

# NIS-2 Compliance für Labore

*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 Labore deutlich verschärft. In Deutschland wurde die NIS-2 Richtlinie mit dem NIS2-Umsetzungsgesetz ohne weitere Übergangsfrist für die betroffenen Unternehmen zum Dezember 2025 in nationales Recht umgesetzt. Unternehmen sollten daher zeitnah handeln.

## Wer ist betroffen?

Betroffen sind Labore ab 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme von 10 Mio. Euro. Welche Unternehmen konkret betroffen sind, ist Anhang I Nr. 5 und der NIS-2 Richtlinie zu entnehmen. Vom Anwendungsbereich als Sektoren mit hoher Kritikalität erfasst sind insbesondere folgende Labore:

- EU-Referenzlaboratorien, die im Wege eines [Durchführungsrechtsaktes der EU-Kommission](#) als EU-Referenzlaboratorium benannt wurden.
- Labore, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Humanarzneimittel i.S.d. [EU-Richtlinie 2001/83/EG](#) ausüben.
- Labore, die pharmazeutische Erzeugnisse i.S.d. Abschnitts C Abteilung 21 [NACE Rev. 2](#) (pharmazeutische Grundstoffe oder Spezialitäten sowie sonstige pharmazeutische Erzeugnisse) herstellen.
- Labore, die kritische Medizinprodukte i.S.d. [Liste der EU-Arzneimittel-Agentur](#) herstellen.

## 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](mailto:info@reuschlaw.de)