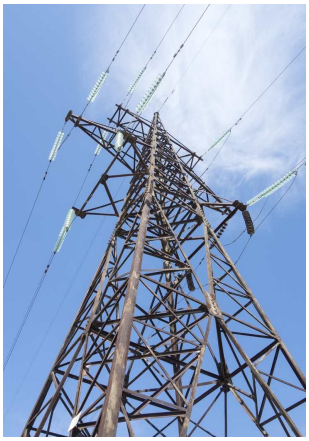
HEUKING

NIS-2 RECHTSKONFORM UMSETZEN

NIS-2-Konformität | Strukturiert verankert.
Cyberrisiken | Frühzeitig erkannt.
Compliance | Mandantenorientiert gestaltet.

Überblick

Die NIS-2-Richtlinie normiert verbindliche Vorgaben zur Cybersicherheit für Unternehmen in kritischen Sektoren – von Energieunternehmen bis zu digitalen Plattformen. Digitale Infrastrukturen sind unverzichtbar für Wirtschaft, Staat und Gesellschaft. NIS-2 verlangt umfassende Schutzmaßnahmen, präzise Meldepflichten und standardisierte Abläufe. Ziel ist ein harmonisierter EU-Rechtsrahmen zur Stärkung der Widerstandsfähigkeit. Die Gefährdungslage steigt, ebenso die regulatorischen Pflichten. Unternehmen haben Risiken frühzeitig zu identifizieren, angemessene technische und organisatorische Vorkehrungen zu treffen und ihre Funktionsfähigkeit bei Sicherheitsvorfällen sicherzustellen.



Betroffene Unternehmen

Wichtige und besonders wichtige Einrichtungen, Betreiber kritischer Anlagen u.a.

Unternehmen in kritischen Sektoren wie Energie, Gesundheit, Verkehr, digitale Infrastruktur, Maschinenbau oder Plattformdienste müssen sicherstellen, dass ihre IT-Systeme den Anforderungen der NIS-2-Richtlinie entsprechen und widerstandsfähig sind.

Dienstleister und Zulieferer

Organisationen, die IT-Leistungen für betroffene Einrichtungen erbringen oder aus Drittstaaten in die EU liefern, sind nicht direkt verpflichtet. Sie werden jedoch von ihren NIS-2-betroffenen Kunden im Regelfall auf Einhaltung der Anforderungen vertraglich verpflichtet und riskieren bei Nichteinhaltung Ihre Zulieferstellung.

Unternehmensgröße

Die NIS-2-Richtlinie gilt innerhalb der betroffenen Sektoren grundsätzlich für Unternehmen mit mindestens 50 Beschäftigten und einem Jahresumsatz oder einer Bilanzsumme von über 10 Mio. €. Ausnahmen gelten für besonders kritische Einrichtungen unabhängig von ihrer Größe.

Geografische Reichweite

Die Richtlinie betrifft alle Unternehmen, die in der EU Dienste erbringen, auch mit Sitz außerhalb der EU.

Ausnahmen

Nicht betroffen sind Unternehmen außerhalb der definierten Sektoren sowie Einrichtungen unterhalb der Schwellenwerte, sofern keine besondere Kritikalität vorliegt.

Sanktionen

Bei Verstößen gegen die nationale Umsetzung der NIS-2-Richtlinie drohen erhebliche Sanktionen bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes. Das deutsche Umsetzungsgesetz wird die Behörden verpflichten, wirksame, verhältnismäßige und abschreckende Maßnahmen zu erlassen. Je nach Schwere des Verstoßes können Bußgelder verhängt werden etwa bei verspäteter Meldung von Sicherheitsvorfällen, unzureichender IT-Sicherheitsorganisation oder fehlender Risikoanalyse. Auch falsche oder irreführende Angaben zur Sicherheitslage oder zur Dienstleistersteuerung können geahndet werden. Die Behörden können zudem öffentliche Bekanntmachungen veranlassen, was zu erheblichen Reputationsrisiken führen kann.

Fristen

Noch nicht verabschiedet: Der Entwurf des NIS-2-Umsetzungsgesetzes wurde am 30. Juli 2025 vom Bundeskabinett beschlossen. Nach Abschluss des parlamentarischen Verfahrens soll das Gesetz Anfang 2026 in Kraft treten. Ab dann gelten die neuen Pflichten für betroffene Einrichtungen.

Registrierungsfrist: Innerhalb von drei Monaten nach Inkrafttreten des Umsetzungsgesetzes müssen sich betroffene Unternehmen registrieren.

Neue Pflichten (Auszug)

Pflichten für wichtige und besonders wichtige Unternehmen

- Risikomanagementsysteme betreiben
- IT-Sicherheitsmaßnahmen regelmäßig prüfen und aktualisieren
- Sicherheitsvorfälle erkennen, bewerten und melden
- Verfügbarkeit, Integrität und Vertraulichkeit der Systeme sicherstellen
- Schutzmaßnahmen für kritische Komponenten umsetzen
- Lieferketten vertraglich und organisatorisch absichern
- Schulungen zur Cybersicherheit durchführen
- Verantwortung der Geschäftsleitung für Umsetzung und Kontrolle

Ergänzende Pflichten für besonders wichtige Unternehmen

- Sicherheitsüberprüfungen durch externe Stellen ermöglichen
- Erweiterte Meldepflichten gegenüber dem BSI beachten
- Nachweise zur Umsetzung der Sicherheitsmaßnahmen regelmäßig vorlegen

---

Unsere Beratung zur NIS-2-Compliance

Initialanalyse und Bestandsaufnahme

- Prüfung, ob und wie Unternehmen unter die NIS-2-Richtlinie fallen (NIS-2-Betroffenheitsanalyse)
- Identifikation von Pflichten, Sicherheitsrisiken und Anpassungsbedarf
- Durchführung von GAP-Analysen

Risikomanagement und Vertragsprüfung

- Unterstützung bei der Einführung eines Risikomanagements und/oder Informationssicherheitsmanagementsystems
- Beratung zur vertraglichen Absicherung technischer und organisatorischer Maßnahmen
- Prüfung und Verhandlung von Dienstleisterverträgen

Governance und technische Umsetzung

- Entwicklung interner Prozesse zur Vorfallbehandlung und Sicherheitsüberwachung
- Begleitung bei der Einführung von Schutzmaßnahmen und Sicherheitsrichtlinien sowie ISMS

Dokumentation und Transparenz

- Erstellung technischer Unterlagen und Sicherheitsnachweise
- Bereitstellung sicherheitsrelevanter Informationen für Behörden und Partner
- Durchführung von Geschäftsleitungs- und Mitarbeiterschulungen

Streitbeilegung und Behördenkommunikation

- Unterstützung bei der Einrichtung von Melde- und Kommunikationsprozessen
- Begleitung bei Anfragen öffentlicher Stellen und behördlichen Verfahren

Kostenstruktur und Fairnesskontrolle

- Prüfung von Sicherheitsinvestitionen auf Angemessenheit und Verhältnismäßigkeit
- Beratung zur Einhaltung gesetzlicher Anforderungen bei interner und externer Kommunikation

HEUKING

Vertrauen Sie auf unsere Expertise – als starker Partner für rechtssichere und praxisnahe Lösungen rund um das Thema Informationssicherheit.

Dr. Hans Markus Wulf
Rechtsanwalt | Partner
Fachanwalt für IT-Recht
ISO/IEC 27001 Auditor (TÜV)
CIPP/E, Datenschutzauditor (TÜV)

m.wulf@heuking.de

Berlin
Chemnitz
Düsseldorf
Frankfurt
Hamburg
Köln
München
Stuttgart

JUVE Handbuch 2024|2025 Wirtschafts Kanzleien

FÜHRENDE KANZLEI Legal500 DEUTSCHLAND 2025

Chambers TOP RANKED Germany 2025 HEUKING

heuking.de