HEUKING

NIS-2
IT-SICHERHEIT RECHTSKONFORM UMSETZEN

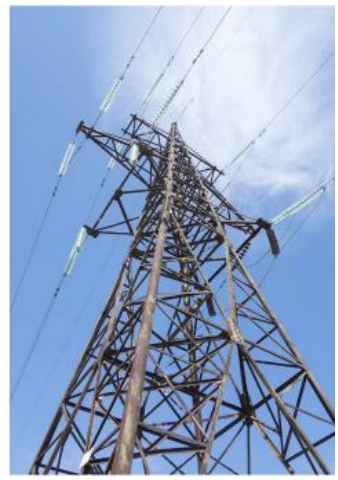
NIS-2-Konformität | Strukturiert verankert.

Cyberrisiken | Frühzeitig erkannt.

Compliance | Mandantenorientiert gestaltet.

Überblick

Die NIS2-Richtlinie ist ein zentraler Baustein der europäischen Cybersicherheitsstrategie und dient dazu, in zahlreichen Sektoren das Cybersicherheitsniveau zu erhöhen. Entsprechend zielt das deutsche NIS2-Umsetzungsgesetz darauf ab, dass die betroffenen Unternehmen und Organisationen umfangreiche Vorgaben zum Schutz ihrer Netzwerk- und IT-Infrastruktur umsetzen. Dazu gehört insbesondere die Umsetzung von Maßnahmen im Bereich des IT-Risikomanagements sowie die Einhaltung von gesetzlichen Meldepflichten.



Betroffene Unternehmen

Wichtige und besonders wichtige Einrichtungen

Unternehmen in bedeutenden Sektoren, wie Energie, Wasser, Gesundheit, Verkehr, digitale Infrastruktur, aber auch Lebensmittelherstellung, Maschinenbau oder Plattformdienste müssen sicherstellen, dass ihre IT-Systeme den Anforderungen des NIS-2-Umsetzungsgesetzes entsprechen.

Dienstleister und Zulieferer

Unternehmen, die IT-bezogene Leistungen für betroffene Einrichtungen erbringen, müssen, auch wenn sie selbst nicht betroffen sind, dafür sorgen, ihnen vertraglich auferlegte IT-Sicherheitspflichten umsetzen zu können. Lieferkettensicherheit ist ein zentrales Element der NIS2-Anforderungen.

Unternehmensgröße

Das NIS2-Umsetzungsgesetz gilt abhängig von der Tätigkeit der Einrichtung größenabhängig oder größenunabhängig. Soweit die Anwendbarkeit größenabhängig ist, gelten die Vorgaben idR für Einrichtungen mit mindestens 50 Beschäftigten oder einem Jahresumsatz und einer Jahresbilanzsumme von jeweils mindestens EUR 10 Mio.

Ausnahmen

Nicht betroffen sind Unternehmen, die nicht in einem regulierten Sektor tätig sind, sowie Einrichtungen, welche die Schwellenwerte nicht überschreiten.

Sanktionen

Bei Verstößen drohen erhebliche Sanktionen bis zu 10 Mio. € oder 2% des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres.
Das NIS2-Umsetzungsgesetz verpflichtet die zuständigen Behörden, wirksame, verhältnismäßige und abschreckende Maßnahmen zu erlassen.
Je nach Schwere des Verstoßes können Bußgelder verhängt werden, etwa bei unzureichender Umsetzung der IT-Sicherheitsmaßnahmen oder verspäteter Meldung von Sicherheitsvorfällen.

Fristen

NIS2-Umsetzungsgesetz noch nicht verabschiedet: Der Entwurf des NIS2-Umsetzungsgesetzes wurde am 30. Juli 2025 vom Bundeskabinett beschlossen.
Nach Abschluss des parlamentarischen Gesetzgebungsverfahrens soll das Gesetz Ende 2025 bzw. Anfang 2026 in Kraft treten. Ab dann gelten die neuen Pflichten **ohne Übergangsfrist** für **alle regulierten Einrichtungen**.

Registrierungsfrist: Innerhalb von drei Monaten nach Inkrafttreten des NIS2-Umsetzungsgesetzes müssen sich betroffene Unternehmen registrieren.

Neue Pflichten (Auszug)

Pflichten für wichtige und besonders wichtige Einrichtungen

- Einführung eines Informationssicherheits-Risikomanagementsysteme
- Prozesse zur Bewältigung von Sicherheitsvorfällen
- Business Continuity Management, Desaster Recovery, Krisenkommunikation
- Gewährleistung der Sicherheit der Lieferkette
- Einführung von Prozessen zur Sicherstellung der Sicherheit von IT-Systemen bei Erwerb, Entwicklung und Wartung
- Schulungen von Mitarbeitern und Geschäftsleitung
- Einsatz von Kryptografie und Verschlüsselung

Ergänzende Pflichten für besonders wichtige Einrichtungen

- Sicherheitsüberprüfungen durch externe Stellen ermöglichen
- Erweiterte Meldepflichten bei Sicherheitsvorfällen
- Regelmäßige Nachweispflicht betreffend die Umsetzung der IT-Sicherheitsmaßnahmen

Unsere Beratung zur NIS-2-Compliance

Initialanalyse und Bestandsaufnahme

- Durchführung von NIS-2-Betroffenheitsanalysen für Unternehmen und Unternehmensgruppen
- Identifikation einschlägiger regulatorischer Pflichten und Compliance-Vorgaben
- Durchführung von GAP-Analysen

Risikomanagement und Vertragsprüfung

- Unterstützung bei der Einführung eines Informationssicherheits-Managementsystems
- Begleitung bei der Durchführung von Überprüfungs- und Zertifizierungsaudits
- Beratung zur vertraglichen Absicherung technischer und organisatorischer Maßnahmen
- Prüfung und Verhandlung von Dienstleisterverträgen

Governance und technische Umsetzung

- Unterstützung bei der Definition und Implementierung interner Prozesse zur Umsetzung der festgelegten IT-Sicherheitsmaßnahmen
- Unterstützung bei der Definition und Implementierung interner Prozesse zur Vorfallbehandlung und Sicherheitsüberwachung

Dokumentation und Kommunikation

- Erstellung von Informationssicherheits-Richtlinien und -konzepten
- Durchführung von Workshops mit Mitarbeitern, Betriebsräten, Geschäftsleitungen
- Durchführung von Geschäftsleitungs- und Mitarbeiterschulungen

Behördenkommunikation und Streitbeilegung

- Unterstützung bei der Einrichtung von Melde- und Kommunikationsprozessen
- Begleitung und Übernahme der Kommunikation IT-sicherheitsrelevanter Informationen an Behörden und Partner
- Vertretung in zivil- und verwaltungsrechtlichen Verfahren und Prozessen

Lieferkette und Verantwortung

- Prüfung und Verhandlung vertraglicher Vereinbarungen zur Gewährleistung der Cybersicherheitsanforderungen in der Lieferkette

HEUKING

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

Berlin
Chemnitz
Düsseldorf
Frankfurt
Hamburg
Köln
München
Stuttgart