LIEB. CONSULTANTS

NIS-2-Richtlinie

(EU) 2022/2555

LIEB.Consultants GmbH
Erlangen, Juni 2025

Die NIS-2-Richtlinie (EU) 2022/2555: Neue regulatorische Anforderungen an die Cybersicherheit – Handlungsbedarf für Unternehmen

Mit der Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („NIS-2-Richtlinie“) hat die Europäische Union ihren regulatorischen Rahmen im Bereich der Netz- und Informationssicherheit grundlegend überarbeitet. Die Richtlinie, die am 16. Januar 2023 in Kraft trat und bis zum 17. Oktober 2024 von den Mitgliedstaaten in nationales Recht umzusetzen war, ersetzt die bisherige NIS-Richtlinie aus dem Jahr 2016 und reagiert auf ein verändertes Risikoumfeld, das durch zunehmende Digitalisierung, steigende Interdependenz kritischer Infrastrukturen und eine erhebliche Zunahme komplexer Cyberangriffe geprägt ist.

Ziel ist die Schaffung eines kohärenten, EU-weiten Mindestniveaus für die Sicherheit digitaler Infrastrukturen. Unternehmen mit hoher wirtschaftlicher oder gesellschaftlicher Relevanz stehen im Zentrum dieser neuen Regulierung. Wir sehen erheblichen Informations- und Handlungsbedarf bei einer Vielzahl von Unternehmen, insbesondere im industriellen Mittelstand sowie bei Dienstleistern im IT-, Energie-, Gesundheits- und Transportsektor. Dies geht aus dem Referentenentwurf für das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) hervor, den das Bundesinnenministerium am 23. Juni 2025 vorgelegt hat. Über 30.000 Organisationen müssen künftig IT-Sicherheitsstandards des BSI umsetzen, sich registrieren und Vorfälle melden. Auch konzerninterne IT-Dienstleister sind betroffen, wenn sie groß oder kritisch genug sind. Die Rolle eines zentralen „CISO Bund“ ist noch ungeklärt, gilt aber als notwendig.

I. Hintergrund und Zielsetzung der NIS-2-Richtlinie

Die NIS-2-Richtlinie verfolgt den Ansatz eines risikobasierten, sektorspezifischen Ordnungsrechts, welches sowohl verbindliche Mindeststandards für die Cybersicherheit vorgibt als auch die Kooperation und Meldepflichten zwischen Unternehmen und Behörden intensiviert. Im Gegensatz zur ursprünglichen NIS-Richtlinie, die stark auf kritische Infrastrukturen (KRITIS) beschränkt war, gilt NIS-2 für eine deutlich erweiterte Zahl von Unternehmen, ohne dass es zwingend eines Verwaltungsakts bedarf.

Damit positioniert sich die Richtlinie rechtspolitisch zwischen einem „Sektoransatz“ (KRITIS) und einem „Querschnittsansatz“ (vergleichbar der DSGVO). Insbesondere

sollen „wesentliche“ und „wichtige Einrichtungen“ auf EU-Ebene vergleichbare Mindestanforderungen einhalten, um die Systemresilienz der EU insgesamt zu stärken.

II. Persönlicher und sachlicher Anwendungsbereich

Der persönliche Anwendungsbereich der Richtlinie ergibt sich aus einer Kombination aus sektorspezifischer Tätigkeit und wirtschaftlicher Relevanz. Erstmals wird dabei ein **Größenkriterium** verbindlich in die Systematik aufgenommen.

1. Kategorien von betroffenen Einrichtungen

Die Richtlinie unterscheidet:

- **Wesentliche Einrichtungen (essential entities)** nach Anhang I, z. B. in den Bereichen Energie, Gesundheitswesen, Finanzwesen, Verkehr, öffentliche Verwaltung, Trinkwasserversorgung, Raumfahrt.
- **Wichtige Einrichtungen (important entities)** nach Anhang II, z. B. in den Bereichen Postdienste, Abfallentsorgung, Lebensmittel, verarbeitende Industrie, digitale Dienste, Forschung.

2. Größenschwelle

Einrichtungen gelten grundsätzlich dann als einbezogen, wenn sie:

- **mindestens 50 Mitarbeitende** beschäftigen und
- **mehr als 10 Mio. EUR Jahresumsatz oder Jahresbilanzsumme** aufweisen.

Davon abweichend sind auch kleinere Unternehmen erfasst, sofern sie als besonders kritisch eingestuft werden (z. B. durch Systemrelevanz oder Marktposition).

3. Regelungstechnik: kein Verwaltungsakt erforderlich

Für Unternehmen in den genannten Sektoren erfolgt die Einordnung **per Gesetz**, ohne dass es eines individuellen Verwaltungsakts bedarf. Dies bedeutet, dass Unternehmen **aktiv prüfen und eigenverantwortlich handeln** müssen. Eine unterlassene Umsetzung trotz objektiver Betroffenheit kann sanktioniert werden.

III. Konkrete Pflichten nach der NIS-2-Richtlinie

Die NIS-2-Richtlinie sieht eine detaillierte Pflichtenarchitektur vor, die sich in drei Hauptkategorien gliedern lässt:

1. Pflichten zur Gefahrenabwehr – Risikomanagement und Schutzmaßnahmen

Artikel 21 der Richtlinie nennt explizit umzusetzende Mindestmaßnahmen, darunter:

- Risikobewertungen und Sicherheitskonzepte,
- Regelungen zum Business Continuity Management (BCM) inkl. Backups und Notfallkommunikation,
- Zugriffskontrollen, Verschlüsselung und Authentifizierungsmechanismen,
- Sicherheitsüberprüfungen bei Erwerb, Entwicklung und Wartung von IT-Systemen.

Ein zentraler Bestandteil des Risikomanagements ist die **Berücksichtigung der gesamten Lieferkette**. Unternehmen sind verpflichtet, potenzielle Risiken entlang der **Wertschöpfungskette und von Drittanbietern** zu analysieren, zu dokumentieren und vertraglich abzusichern. Dies betrifft insbesondere Cloud-Anbieter, IT-Outsourcing-Partner und infrastrukturelle Dienstleister.

Hinweis zur Vertragsgestaltung: Die Anforderungen der NIS-2 sollten sich in Einkaufsbedingungen, SLA-Vereinbarungen und Kooperationsverträgen mit Drittanbietern widerspiegeln. Dies umfasst z. B. Auditrechte, Pflichten zur Mitwirkung bei Vorfallmeldungen, vertragliche Sicherheitsstandards und Reaktionszeiten im Ernstfall. In vielen Fällen empfiehlt sich eine Compliance-Klausel zur NIS-2-Umsetzung.

2. Pflichten zur Vorfallmeldung

Art. 23 ff. NIS-2 normieren ein gestuftes Meldeverfahren:

- **Frühwarnung** innerhalb von 24 Stunden nach Kenntnis des Vorfalls,
- **Zwischenmeldung** binnen 72 Stunden mit einer ersten Bewertung,
- **Abschlussbericht** nach spätestens einem Monat mit Ursachenanalyse und Abhilfemaßnahmen.

Adressat in Deutschland ist das **Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Je nach Tragweite ist auch eine EU-weite Weiterleitung über das CSIRTs-Netzwerk vorgesehen.

Die Schwelle für eine Meldepflicht liegt bei erheblichen Störungen der Dienstverfügbarkeit, -authentizität, -integrität oder -vertraulichkeit. Eine falsche Einschätzung oder verspätete Meldung kann bußgeldbewährt sein.

3. Organisationspflichten und persönliche Geschäftsführerverantwortung

Art. 20 NIS-2 betont ausdrücklich die **Verantwortung der Unternehmensleitung**. Dies ist ein wesentlicher Unterschied zur bisherigen Rechtslage: Geschäftsführungen, Vorstände und andere Leitungsorgane werden persönlich verpflichtet, für die Einhaltung der Cybersicherheitsvorgaben zu sorgen.

Konkret bedeutet dies:

- Genehmigung und Überwachung eines angemessenen Risikomanagements,
- aktive Mitwirkung bei Sicherheitsentscheidungen,
- Sicherstellung der finanziellen und organisatorischen Ausstattung,
- regelmäßige Schulungen zum Thema Cybersicherheit auf Leitungsebene.

Ein bloßes „Outsourcing" der Verantwortung an IT-Abteilungen oder externe Anbieter entbindet nicht von der gesetzlichen Verantwortung. Die Pflicht zur persönlichen Steuerung und Kontrolle ist **nicht delegierbar**. Für juristische Personen kann sich daraus ein haftungsrelevantes Organisationsverschulden im Sinne von § 130 OWiG bzw. § 93 AktG ergeben.

IV. Behördenaufsicht und Sanktionen

Das BSI wird künftig nicht nur für KRITIS-Betreiber, sondern auch für wesentliche und wichtige Einrichtungen Aufsichtsbehörde sein. Es erhält weitreichende Eingriffs-, Überwachungs- und Durchsetzungsbefugnisse, darunter:

- Anordnungen zur Mängelbeseitigung,
- Vor-Ort-Kontrollen, auch unangekündigt,
- verpflichtende Sicherheitsprüfungen,
- Veröffentlichungen von Verstößen („Naming and Shaming").

Die Sanktionen wurden im Vergleich zum bisherigen Rechtsrahmen massiv verschärft. Art. 34 NIS-2 sieht Bußgelder vor:

- Für wesentliche Einrichtungen: bis zu **10 Mio. EUR** oder **2 % des weltweiten Jahresumsatzes**,
- Für wichtige Einrichtungen: bis zu **7 Mio. EUR** oder **1,4 % des Jahresumsatzes**.

Die Bemessung erfolgt risikoadäquat und orientiert sich an der Kooperationsbereitschaft sowie dem Reifegrad der IT-Sicherheitsorganisation.

V. Handlungsempfehlungen für Unternehmen – ein Fahrplan zur Umsetzung

Unternehmen sollten den verbleibenden Zeitraum bis zur Geltung der deutschen Umsetzungsregelungen aktiv nutzen, um Compliance herzustellen. Aus Sicht der rechtlichen Beratung ergibt sich folgender priorisierter Handlungsrahmen:

1. **Prüfung der Betroffenheit**
   Analyse anhand von Sektor, Unternehmensgröße, Systemrelevanz. Klare Dokumentation der Prüfungsergebnisse.
2. **Gap-Analyse/ Risikoassessment**
   Erhebung des Ist-Zustands der Cybersicherheit, Identifikation von Lücken und Risikobereichen – einschließlich Bewertung von Risiken in **Lieferketten und Drittbeziehungen**.
3. **Entwicklung und Einführung eines ISMS**
4. Orientierung an **ISO/IEC 27001**, **BSI-Grundschutz**, ggf. branchenspezifische Standards (z. B. KRITIS-Vorgaben, DVGW, TISAX).
5. **Governance-Strukturen schaffen**
   Benennung eines Informationssicherheitsbeauftragten (CISO), Etablierung von Berichtswegen zur Geschäftsleitung. Integration der Geschäftsführung in die Cybersicherheitsgovernance.
6. **Vertragliches Lieferantenmanagement**
   Prüfung bestehender Verträge mit IT- und Cloud-Dienstleistern auf Sicherheitsklauseln. Ergänzung um NIS-2-konforme Verpflichtungen, z. B. Unterstützung bei Meldeverfahren, Sicherheitsüberprüfungen, Kontrollrechte.
7. **Vorfallmanagement und Meldewesen aufbauen**
   Interne Handlungsleitfäden, Schnittstellen zum BSI, Testläufe von Incident Response-Prozessen.
8. **Dokumentation und Nachweisführung**
   Alle Maßnahmen sind revisionsfest zu dokumentieren – sowohl zur internen Steuerung als auch im Hinblick auf behördliche Prüfungen.

VI. Fazit und Ausblick

Die NIS-2-Richtlinie bringt eine neue Qualität der Cybersicherheitsregulierung in Europa – durch Ausweitung des Anwendungsbereichs, Konkretisierung der Maßnahmen und Einführung persönlicher Verantwortung auf Geschäftsführungsebene. Für Unternehmen, insbesondere im industriellen, gesundheitlichen oder technologiegetriebenen Sektor, entsteht dringender Handlungsbedarf.

Die **Lieferkettensicherheit** sowie die **persönliche Geschäftsführungsverantwortung** stehen dabei besonders im Fokus. Der Gesetzgeber setzt auf Eigenverantwortung –

und flankiert diese mit einem scharfen Sanktionsmechanismus. Gleichzeitig bietet die Umsetzung der NIS-2-Pflichten eine Chance: Wer seine digitale Resilienz proaktiv stärkt, sichert nicht nur die Compliance, sondern auch die Wettbewerbsfähigkeit in einem zunehmend digitalen Binnenmarkt.

Wir begleiten unsere Mandanten rechtlich und organisatorisch bei der Umsetzung – von der rechtlichen Erstprüfung über Vertragsgestaltung bis zur Entwicklung rechtssicherer IT-Governance-Strukturen.

Bei Fragen steht das LIEB.Consultants-Teams jederzeit zur Verfügung.