# Was ist die NIS2-Richtlinie?

**Im heutigen digitalen Zeitalter ist Cybersicherheit aufgrund der zunehmenden Häufigkeit von Cyberangriffen ein wichtiges Anliegen für Einzelpersonen und Organisationen. Angesichts dessen hat die Europäische Kommission 2016 die EU-Richtlinie für Netz- und Informationssicherheit (NIS) eingeführt, um die Cybersicherheit in der Europäischen Union zu stärken. Die Richtlinie wies jedoch Schwächen auf, was die Kommission dazu veranlasste, ihre Ersetzung durch die zuverlässigere NIS2-Richtlinie zu planen.**

NIS2 verpflichtet Unternehmen, wichtige Cybersicherheitsmaßnahmen umzusetzen, darunter Sicherheit in der Lieferkette, Kryptographie und Verschlüsselung (Artikel 18). Artikel 89 hebt die Einführung grundlegender Cybersicherheitspraktiken wie Zero-Trust-Prinzipien, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung sowie Identitäts- und Zugriffsverwaltung für wesentliche und wichtige Einrichtungen hervor.

### NIS vs. NIS2 - Was hat sich geändert?

Es gibt einige wichtige Unterschiede zwischen der alten und der neuen Richtlinie:

- Der neue Vorschlag verzichtet auf die Unterscheidung zwischen Betreibern wesentlicher Dienste (OES) und Anbietern digitaler Dienste (DSP). Stattdessen wird in Zukunft zwischen sogenannten Essential Entities und Important Entities unterschieden.
- Der Anwendungsbereich der Richtlinie wurde um neue Sektoren erweitert, die für Wirtschaft und Gesellschaft von entscheidender Bedeutung sind, einschließlich aller mittleren und großen Unternehmen in diesen Sektoren. Mitgliedstaaten können ebenso kleinere Einrichtungen mit einem hohen Risikoprofil identifizieren.
- Die Einrichtung eines Europäischen Netzwerks für die Krisenkoordination in der Cybersicherheit (EU-CyCLONe) vorgeschlagen, um gemeinsam an der Vorbereitung und Umsetzung schneller Notfallpläne zu arbeiten, beispielsweise im Falle einer groß angelegten Cyberattacke oder einer Krise.
- Verstärkte Koordination bei der Offenlegung neuer Schwachstellen, die in der gesamten EU entdeckt werden. Es wird eine Liste von Sanktionen (ähnlich denen der DSGVO) erstellt, einschließlich Geldstrafen für Verstöße gegen Melde- und Verwaltungspflichten im Bereich Cybersicherheitsrisiken.
- NIS2 nimmt die Geschäftsleitung direkt in die Pflicht, die Umsetzung und Überwachung der Einhaltung der Gesetzgebung in ihrer Organisation sicherzustellen. Verstöße können zu Geldstrafen und einem vorübergehenden Verbot der Ausübung von Leitungsfunktionen, auch auf Vorstandsebene führen.

Darüber hinaus führt die Richtline genauere Bestimmungen zum Meldeprozess von Vorfällen, zum Inhalt der Berichte und zum Zeitpunkt (innerhalb von 24 Stunden nach Entdeckung des Vorfalls) ein. Auf europäischer Ebene stärkt der Vorschlag die Cybersicherheit für wichtige Informations- und Kommunikationstechnologien. Die Mitgliedstaaten müssen in Zusammenarbeit mit der Kommission und ENISA, der Agentur der Europäischen Union für Cybersicherheit, koordinierte Risikobewertungen kritischer Lieferketten durchführen.

**Für wen gilt die NIS2-Richtlinie?**

Während unter der alten NIS-Richtlinie die Mitgliedstaaten dafür verantwortlich waren, zu bestimmen, welche Einrichtungen die Kriterien erfüllen, um als Betreiber wesentlicher Dienste zu gelten, führt die neue NIS2-Richtlinie eine Größendeckelung ein. Dies bedeutet, **dass alle mittleren und großen Einrichtungen, die innerhalb der von der Richtlinie erfassten Sektoren tätig sind oder Dienstleistungen erbringen, in ihren Anwendungsbereich fallen werden**. Die Anzahl der von der NIS2-Richtlinie erfassten Sektoren steigt von 19 auf 35.

Nachfolgend finden Sie eine Klassifizierung nach der Größendeckelung:

| **Wesentliche Einrichtungen**<br><br>Größenkriterien: variiert je nach Sektor, aber in der Regel 250 Mitarbeiter, Jahresumsatz von 50 Millionen Euro oder Bilanzsumme von 43 Millionen Euro | **Wichtige Einrichtungen**<br><br>Größenkriterien: variiert je nach Sektor, aber in der Regel 50 Mitarbeiter, Jahresumsatz von 10 Millionen Euro oder Bilanzsumme von 10 Millionen Euro |
|---|---|
| Energie | Postdienste |
| Transport | Abfallwirtschaft |
| Finanzen | Chemikalien |
| Öffentliche Verwaltung | Forschung |
| Gesundheit | Lebensmittel |
| Weltraum | Herstellung |
| Wasserversorgung (Trink- und Abwasser) | Digitale Anbieter (z. B. soziale Netzwerke, Suchmaschinen, Online-Marktplätze) |
| Digitale Infrastruktur (z. B. Cloud-Computing-Dienstleister und ICT-Management) | |

NIS2 umfasst auch öffentliche Verwaltungseinrichtungen auf zentraler und regionaler Ebene, schließt jedoch Parlamente und Zentralbanken aus.

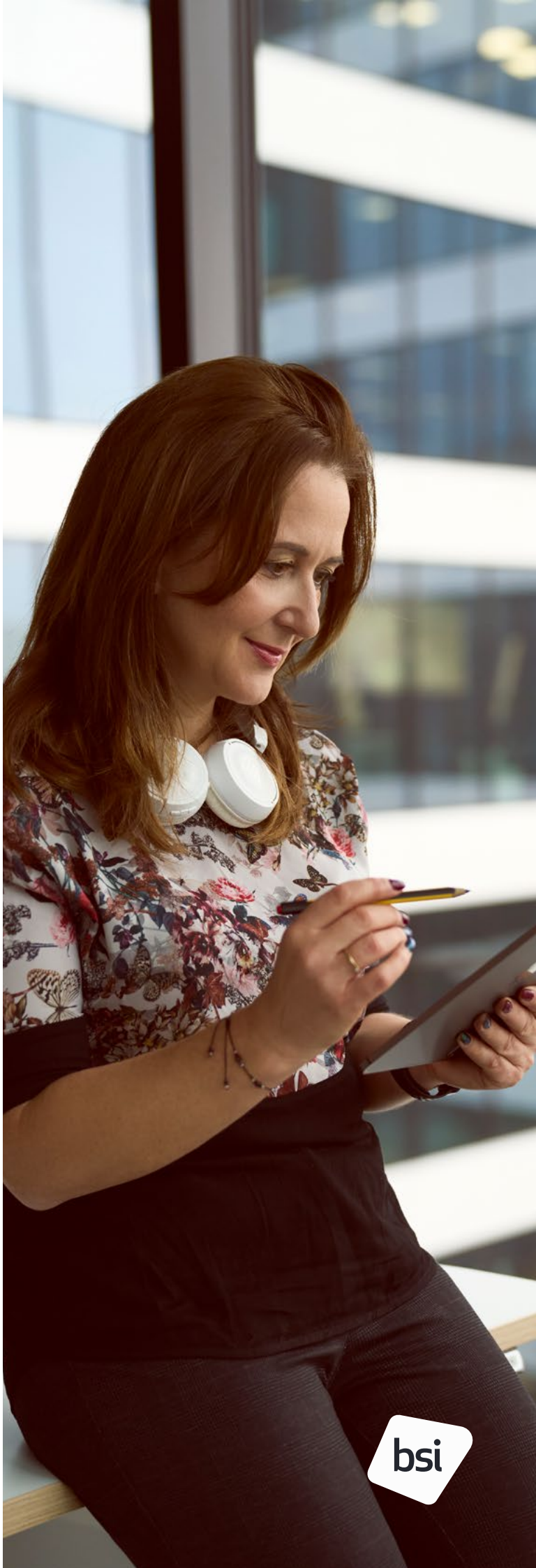
## Wann tritt sie in Kraft?

Alle EU-Mitgliedstaaten müssen diese neuen Verpflichtungen bis September 2024 in ihre nationalen Gesetze übernehmen. Nach endgültiger Genehmigung haben die betroffenen Einrichtungen einen 21-monatigen Compliance-Zeitraum, sobald die Richtlinie in Kraft tritt. Die folgende Liste zeigt den NIS-Entwicklungsplan:

- **6. Juli 2016:** NIS verabschiedet
- **9. Mai 2018:** Frist für die Mitgliedstaaten zur Umsetzung von NIS in nationales Recht
- **7. Juli 2020:** Die Europäische Kommission startet eine Konsultation zur NIS-Reform
- **16. Dezember 2021:** Die Europäische Kommission veröffentlicht den Vorschlag für NIS2
- **22. November 2021:** Das Europäische Parlament verabschiedet seine Verhandlungsposition
- **3. Dezember 2021:** Der Europäische Rat verabschiedet seine Verhandlungsposition
- **13. Januar 2022:** Erste Runde der Trilog-Verhandlungen
- **16. Februar 2022:** Zweite Runde der Trilog-Verhandlungen
- **13. Mai 2022:** Politische Einigung erzielt
- **10. November 2022:** Das Europäische Parlament stimmt für die Annahme von NIS2
- **28. November 2022:** NIS2 wird vom Rat der EU genehmigt
- **27. Dezember 2022:** NIS2 wird im Amtsblatt veröffentlicht und wird 20 Tage später am 16. Januar 2023 eingeführt
- **17. Oktober 2024:** Frist für die Mitgliedstaaten, NIS2 in nationales Recht umzusetzen.

## Wie können wir Ihrem Unternehmen helfen, die NIS2-Richtlinie einzuhalten?

Bei BSI verfügen wir über ein großes Team hoch erfahrener, branchenführender Experten, die sicherstellen, dass Sie und Ihr Unternehmen alle Sicherheitsanforderungen erfüllen, die Sie benötigen, um der NIS2-Richtlinie voraus zu sein. Mit unserer Hilfe können Organisationen potenzielle finanzielle Strafen vermeiden und das Vertrauen ihrer Kunden stärken.  Von der initialen OES-Identifizierung bis hin zur Selbstbewertung, Risikobewertung und Risikobehandlung - unsere Erfahrung in der Zusammenarbeit mit Organisationen in allen Sektoren kann Ihnen auf dem Weg zur Einhaltung der NIS2-Richtlinie helfen.



**BSI bietet derzeit folgende Dienstleistungen bezüglich der NIS2 Anforderungen an:**

- Cyberstrategie/Governance
- Bewertung der Cybersicherheitsposition/Reifeprüfung anhand von Branchenstandards
- Entwicklung von Informationssicherheits-/Cyberstrategien/Vorstandspresentationen- Gap-Analyse und Umsetzungsunterstützung (ISO 27001, SOC 2, NIST CSF/800-53)
- Schulungen zur Informationssicherheit und Cybersecurity
- Business Continuity Management (ISO 22301)

**Krisenmanagement und Maßnahmen bei Sicherheitsvorfällen**

- Business Continuity (ISO 22301)
  - Geschäftsauswirkungsanalyse (BIA)/ Richtlinienentwicklung/ Business Continuity Planning
- Unterstützung bei der Wiederherstellung im Schadensfall, Implementierung und regelmäßiges Testen
- Bedrohungsbasiertes Penetrationstesten (TLPT)
- Open-Source-Intelligence (OSINT)
- Bewertung der physischen Sicherheit Angriffssimulation (Red/Blue/Purple Team)
- Reaktionsplanung auf Sicherheitsvorfälle und Implementierung (ISO 27035)
- Bedrohungsmodellierung/Bedrohungsbeurteilungen
- Bewertung der aktuellen Sicherheitsvorfallreaktionsplanung und Berichtsfähigkeit
- Tests der Sicherheitsvorfallreaktion/Mitarbeiterschulung

**Risikomanagement und Berichterstattung**

- Entwicklung und Implementierung eines IT-Risikomanagement-Frameworks (ISO 27005)
  - Risikomanagement für Dritte (ISO 27036-2)
  - Aktuelle Zustandsbewertung des Lebenszyklusmanagements für Dritte
  - Entwicklung eines ganzheitlichen Lieferantenmanagement-Frameworks
  - Implementierung des Risikomanagement-Frameworks für Dritte sowie fortlaufende Unterstützung beim Risikomanagement
- BSI arbeitet mit Technologiepartnern zusammen, die Tools zur Unterstützung des gesamten Managements des Lieferantenlebenszyklus bereitstellen
  - Zertifizierung für Threat Intelligence/Computer Emergency Response Team (CERT)
  - Bewertung der aktuellen Lage und Bestimmung des künftigen Zustands
  - Aufbau eines Reporting-Rahmens

## Warum sind ISO/IEC 27001 und ISO 22301 entscheidend für die NIS2-Konformität?

Die NIS-Vorschriften empfehlen Unternehmen in ihren Compliance-Bemühungen, „die Einhaltung internationaler Standards“ zu priorisieren. Darüber hinaus stimmen die technischen Leitlinien der Europäischen Agentur für Cybersicherheit (ENISA) jedes Sicherheitsziel mit bewährten Praxisstandards wie ISO 27001 ab.

Von allen Dienstleistungen, die BSI Ihrem Unternehmen im Zusammenhang mit NIS2 bieten kann, spielen zwei Standards eine entscheidende Rolle: ISO/IEC 27001 und ISO 22301.

- Die Implementierung eines ISO-27001-konformen Informationssicherheitsmanagementsystems (ISMS) befähigt Organisationen, Risiken und Anfälligkeit gegenüber Sicherheitsbedrohungen zu minimieren. Dazu gehört die Identifizierung erforderlicher Richtlinien, die Nutzung geeigneter Technologien und die Schulung des Personals zur Vermeidung von Fehlern. Da ISO 27001 jährliche Risikobewertungen vorschreibt, können Organisationen proaktiv auf die sich entwickelnde Risikolandschaft reagieren.
- ISO 27001 erleichtert nicht nur die Erfüllung der NIS2-Anforderungen, sondern ermöglicht es Organisationen auch, eine unabhängig geprüfte Zertifizierung zu erlangen. Diese Zertifizierung dient als greifbarer Nachweis für Lieferanten, Stakeholder und Regulierungsbehörden und zeigt die Umsetzung “angemessener und verhältnismäßiger” technischer und organisatorischer Maßnahmen sowie einen Wettbewerbsvorteil auf dem Markt.
- Organisationen, die einen erweiterten Ansatz anstreben, wird empfohlen, die ISO 22301 für das Business Continuity Management hinzuzufügen. ISO 22301 unterstützt bei der Implementierung, Aufrechterhaltung und kontinuierlichen Verbesserung von Geschäftskontinuitätspraktiken. Während ISO 27001 Aspekte des Business Continuity Managements (BCM) enthält, bietet ISO 22301 einen definierten Prozess für die Implementierung eines BCMS. Die Zertifizierung nach ISO 22301 stärkt die NIS2-Konformität zusätzlich.

Die Synergie zwischen ISO 27001 und ISO 22301 ermöglicht es Organisationen, ein integriertes Managementsystem zu entwickeln, das sowohl ein ISMS als auch ein BCMS umfasst. Dieser ganzheitliche Ansatz erleichtert nicht nur die Compliance, sondern fördert auch die Entwicklung robuster Cybersicherheit.

## Warum BSI?

BSI verfügt über erstklassige Fähigkeiten, die den Kunden in den Bereichen Cybersicherheit und Cyberhygiene Vertrauen schaffen. Wir bieten fundiertes Fachwissen in den Bereichen Cybersicherheit, Risikomanagement und Informationsresilienz mit einer globalen, sektorübergreifenden Perspektive. Unser Fachwissen umfasst Themen, die den öffentlichen Sektor betreffen, neu auftretende Bedrohungen und praktische Branchenerfahrung bei der Verwaltung von Cyber-Risiken und -Resilienz.

## Was sollten Sie als nächstes tun?

- Prüfen Sie, ob Ihre Organisation in den Regelungsbereich fällt.
- Informieren Sie Ihr Management/ Ihren Vorstand über die bevorstehenden Vorschriften.
- Kontaktieren Sie uns, um Unterstützung bei der NIS2-Konformität zu erhalten **sales.de@bsigroup.com**