

NIS2- Umsetzungsgesetz: Aktueller Stand und Pflichten für Unternehmen



Warum gibt es die NIS2-Richtlinie?



- Zunehmende Cyberbedrohungen in Europa
- Harmonisierung der Sicherheitsstandards
- Schutz kritischer Dienste & Versorgungsketten
- Ziel: **Erhöhte Resilienz und robuste Sicherheitsanforderungen**

NIS2UmsuCG – NIS2-Umsetzungs- und Cybersicherheitsstärkungs-Gesetz



- Bundestag hat das Gesetz am **13.11.2025** beschlossen
 - Abschließende Schritte: Bundesrat + Verkündung
 - **EU-Frist: 17.10.2024** – verpasst
 - Rückstand führt zu keiner Übergangsfrist
 - Anforderungen gelten **sofort** mit Inkrafttreten des Gesetzes
 - Anzahl der betroffenen Einrichtungen steigt auf ca. 29.000 (vorher 4.500)
- **Unternehmen müssen jetzt handeln**

KRITIS	Sektoren hoher Kritikalität ANLAGE 1	Sonstige kritische Sektoren ANLAGE 2
Energie	Energie Stromversorgung, Fernwärme/-kälte, Kraftstoff/Heizöl, Gas	
Transport/Verkehr	Transport/Verkehr Luftverkehr Schienenverkehr, Schifffahrt, Straßenverkehr	Transport/Verkehr Post und Kurier
Finanz/Versicherung	Finanz/Versicherung Banken, Finanzmarkt-Infrastruktur	
Gesundheit	Gesundheit Dienstleistungen, Referenzlabore, F&E, Pharma (NACE C Abt. 21), Medizinprodukte,	
Wasser/Abwasser	Wasser/Abwasser Trinkwasser, Abwasser	
IT und TK	IT und TK IXPs, DNS, TLD, Cloud Provider, RZ-Dienste, CDNs, TSP, elektronische Kommunikation/Dienste, Managed Services und Security Services	Digitale Dienste Marktplätze, Suchmaschinen, soziale Netzwerke
Weltraum	Weltraum Bodeninfrastrukturen	
Ernährung		Lebensmittel Großhandel, Produktion, Verarbeitung
Entsorgung		Entsorgung Abfallbewirtschaftung
		Forschung Forschungseinrichtungen
		Verarbeitendes Gewerbe Medizin/Diagnostika; DV, Elektro, Optik (NACE C Abt. 26 und 27); Maschinenbau (NACE C 28), Kfz/Teile (NACE C 29), Fahrzeugbau (NACE C 30)
		Chemie Herstellung, Handel, Produktion

Wer ist betroffen?

Sektoren

Die Sektoren weichen von früheren Definitionen und auch EU NIS2 leicht ab.

KRITIS-Sektoren sind separat in §28 (6) definiert.

Unternehmensgröße

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>

Wer ist betroffen?

KATEGORIE	GRÖßE	SEKTOREN
Besonders wichtige Einrichtungen (bwE)	Großunternehmen Unternehmen ≥ 250 MA oder > 50 Mio. € Umsatz / > 43 Mio. € Bilanzsumme	Energie, Transport/Verkehr, Finanzwesen, Gesundheit, Wasser, Digitale Infrastruktur, Weltraum
	Größenunabhängig	Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste
	Mittlere Unternehmen	Öffentliche TK-Netze und TK-Dienste
	KRITIS-Anlagen	Betreiber kritischer Anlagen
Wichtige Einrichtungen (wE)	Mittlere Unternehmen Unternehmen ≥ 50 MA oder > 10 Mio. € Umsatz / > 10 Mio. € Bilanz	Energie, Transport/Verkehr, Finanzenwesen, Gesundheit, Wasser, Digitale Infrastruktur, Weltraum
	Großunternehmen Mittlere Unternehmen	Post/Kurier, Abfallbewirtschaftung, Chemie, Lebensmittel, Verarbeitendes Gewerbe, Digitale Dienste, Forschung
	Größenunabhängig	Vertrauensdienste, Öffentliche TK-Netze und TK-Dienste
Betreiber Kritischer Anlagen (NIS2 und Kritis-DachG)	KRITIS-Anlagen Einstufung nach Anlagen-Schwellenwerten (z. B. 500.000 versorgte Personen)	Energie, Transport und Verkehr, Finanzen und Versicherungen, Gesundheit, Trinkwasser und Abwasser, Ernährung, IT und TK, Weltraum, Entsorgung
Bundeseinrichtungen Ausnahme: Bereiche der nationalen Sicherheit		

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>

NIS2UmsuCG

Pflichten von Betreibern und Einrichtungen

PFLICHT	BETREIBER KRITISCHER ANLAGEN	BESONDERS WICHTIGE EINRICHTUNG	WICHTIGE EINRICHTUNG
Geltungsbereich	Anlage(n)	Unternehmen	Unternehmen
Risikomanagement	✓	✓	✓
Höhere Maßstäbe für KRITIS	✓		
Besondere Maßnahmen z.B. Einsatz von Systemen zur Angriffserkennung	✓		
Registrierung	✓	✓	✓
Meldepflichten	✓	✓	✓
Nachweise	✓		
Informationsaustausch	✓	✓	
Unterrichtungspflichtigen Kunden	✓	✓	✓
Geschäftsleitung	✓	✓	✓

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Registrierungspflicht beim BSI (§33, §34)

- **Besonders wichtige Einrichtungen**
 - Registrierung innerhalb von drei Monaten nach Identifizierung §33 (1)
 - Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten §30 (7)
- **Wichtige Einrichtungen**
 - Registrierung innerhalb von drei Monaten nach Identifizierung
- **Betreiber kritischer Anlagen**
 - Registrierung innerhalb von drei Monaten nach Identifizierung §33 (2)
 - Erstmaliger Nachweis über Maßnahmenumsetzung spätestens zu einem vom BSI und BBK bei der Registrierung festgelegten Zeitpunkt: frühestens drei Jahre nach Inkrafttreten des Gesetzes, d.h. ab 2027.
 - Fortlaufende Nachweise über Maßnahmenumsetzung anschließend alle drei Jahre §39 (1)
 - Teilnahme am Informationsaustausch innerhalb eines Jahres nach Inkrafttreten §30

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Kernelement: Risikomanagement (§ 30)

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung und Wiederherstellung, Backup-Management, Krisen-Management
- Sicherheit der Lieferkette, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, Beschaffung und Wartung
- Management von Schwachstellen
- Bewertung der Effektivität von Cybersicherheit und Risiko-Management
- Schulungen Cybersicherheit und Cyberhygiene
- Kryptografie und Verschlüsselung
- Personalsicherheit, Zugriffskontrolle und Anlagen-Management
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Sicherheit in der Lieferkette (§ 30)

- Unternehmen haften auch für IT-Sicherheitsrisiken ihrer Dienstleister und Lieferanten.
- Pflicht zur Überprüfung und vertraglichen Absicherung von Partnern:
 - Sicherheitsstandards (z. B. ISO 27001, TISAX)
 - Auditrechte, Nachweise, Sicherheitsklauseln
- Empfehlung: Aufbau eines Lieferantenbewertungssystems mit Risikoanalyse.
- **Ziel:** Stärkung der gesamten Lieferkette gegen Cyberangriffe.



Geschäftsleitungshaftung (§ 38)

- Geschäftsführung ist persönlich verantwortlich für Umsetzung der Sicherheitsmaßnahmen.
- Bei Verstößen drohen:
 - Bußgelder bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes
 - Persönliche Haftung bei grober Fahrlässigkeit oder Untätigkeit nach gesellschaftsrechtlichen Grundsätzen
- Pflicht zur regelmäßigen Berichterstattung über IT-Sicherheitslage
- Verpflichtende Sicherheits-Schulungen (mind. alle 3 Jahre)
- **Empfehlung:** Einbindung von ISMS-Verantwortlichen und internen Audits

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Zertifizierte Produkte (Cybersecurity Act / Art. 49 EU 2019/881)

➤ **Neue Pflicht** für bwE und wE

Wenn besonders wichtige oder wichtige Einrichtungen bestimmte – noch festzulegende – IKT-Produkte, Dienste oder Prozesse einsetzen, müssen diese künftig eine EU - Cybersicherheitszertifizierung besitzen.

Grundlage: §30 (6) NIS2UmsuCG

Rechtsrahmen: EU-Verordnung 2019/881 (Cybersecurity Act)

Wichtig: Welche Produkte, Dienste oder Prozesse betroffen sind, legt das BMI später per Rechtsverordnung nach §56 (4) fest.

Beispiele (vermutlich betroffen, sobald benannt):

- Netzwerkkomponenten
- Betriebssysteme / IT-Management-Software
- Firewalls, VPN, IDS/IPS
- Sicherheitsrelevante SaaS- oder Cloud-Dienste



Zertifizierte Produkte (Cybersecurity Act / Art. 49 EU 2019/881)

➤ Bedeutung für Unternehmen:

- Anschaffung nur noch von zertifizierten Produkten möglich
- Lieferantenmanagement wird deutlich strenger
- Hersteller müssen Zertifizierungen vorweisen



Kritische Komponenten (§41 NIS2UmsuCG)

- **Betraff bisher v. a. Telekommunikation – jetzt deutlich vereinfacht und neu geregelt**
- **Meldepflicht vor Einsatz**
 - Betreiber kritischer Anlagen müssen den Einsatz einer kritischen Komponente **vorab beim Innenministerium anzeigen** (§41 Abs. 1).
- **Garantieerklärung des Herstellers**
 - Der Betrieb ist nur zulässig, wenn eine **Vertrauenswürdigkeits-Garantieerklärung** des Herstellers vorliegt (§41 Abs. 3).
 - Diese garantiert u. a.:
 - keine Manipulationen
 - keine versteckten Zugänge
 - geprüfte Lieferkette
 - Transparenz über Schwachstellen und Updates
- **Wann darf das Innenministerium den Einsatz untersagen?**
 - Das BMI kann kritische Komponenten verbieten, wenn:
 - Sicherheits- oder außenpolitische Gründe vorliegen (§41 Abs. 2)
 - Fehlende Vertrauenswürdigkeit des Herstellers (§41 Abs. 4–5):

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Nachweispflichten (§ 39)

	Betreiber kritischer Anlagen		Einrichtungen	
			Besonders wichtig	Wichtig
Gesetz	NIS2UmsuCG	KRITIS-DachG	NIS2UmsuCG	NIS2UmsuCG
Zeitraum	ab 2026	ab 2027	ab 2025	ab 2025
Pflicht	§39 (1)	§16	§61	§62
Prüfungen	Alle drei Jahre	Teil von Audits	Stichproben durch BSI	
Inhalt	Risiko-Management	Risiko-Management	Risiko-Management	Risiko-Management
	IT-Sicherheit	Resilienz	IT-Sicherheit	IT-Sicherheit
	Meldepflicht		Meldepflicht	Meldepflicht
	SzA			
	KRITIS			
Scope	Anlage	Anlage	Unternehmen	Unternehmen
Empfänger	BSI	BBK	BSI	BSI
Behörden	Tiefenprüfung	Nachweise	Risikobasiert	bei Anlass

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



NIS2UmsuCG - Ausschlüsse

EU-Vorrang: Ausschlüsse durch „Implementing Acts“

Für bestimmte digitale Dienste gelten EU-einheitliche technische Sicherheitsstandards, nicht die deutschen Detailregeln. §30 (2)

Betroffene Dienste (Auswahl):

- DNS-Dienste
- Top-Level-Domain-Registries
- Cloud-Computing
- Rechenzentren / Hosting
- Content Delivery Networks
- Managed Services / Managed Security Services
- Marktplätze, Suchmaschinen, soziale Netzwerke
- Vertrauensdienste / Zertifizierungsdienste

→ Diese Dienste fallen nicht unter die nationalen technischen Detailpflichten, aber unter die allgemeinen NIS2-Pflichten (Registrierung, Meldewesen, Leitungshaftung).



NIS2UmsuCG - Ausschlüsse

- In vielen Sektoren werden Unternehmen ausgenommen, **wenn die kritische Tätigkeit nur einen unwesentlichen Teil ihrer Gesamtaktivität ausmacht.**
- Beispiele:
 - Trinkwasser / Wasser
 - Ausgenommen sind Unternehmen, für die die Lieferung von Wasser nur ein nicht wesentlicher Teil der Tätigkeit ist.
 - Abwasser
 - Ausgenommen sind Unternehmen, für die das Sammeln/Behandeln von Abwasser kein wesentlicher Teil der Tätigkeit ist.
- Diese Ausnahmen verhindern Überregulierung, z. B. bei Betrieben, die nur nebenbei Energie erzeugen oder Wasser handeln.
- Finanzunternehmen, die unter die EU-Verordnung **DORA (Digital Operational Resilience Act)** fallen, werden **nicht als NIS2-Einrichtungen eingestuft** und unterliegen daher **keinen Pflichten aus dem NIS2-Umsetzungsgesetz.**
- Stattdessen gelten für sie ausschließlich die Anforderungen der DORA-Verordnung, die ab Januar 2025 verbindlich anzuwenden ist. DORA enthält vergleichbare, jedoch in vielen Bereichen deutlich **umfangreichere und stärker standardisierte** Vorgaben zur digitalen Resilienz und zum ICT-Risikomanagement.



NIS2UmsuCG - Ausschlüsse

Ausschlüsse für Bundesbehörden

Bundesbehörden werden reguliert – aber mit eigenen Ausnahmen. § 46 Abs. 2–3 nennt ausdrücklich Bereiche, in denen die Regulierung nicht gilt, z. B.:

- Verteidigung
- Nationale Sicherheit
- Teilbereiche der inneren Sicherheit
- Behörden unterliegen teilweise anderen Regelungen oder sind komplett ausgenommen.

Der „Ausnahmebescheid“ (nationale Sicherheitsinteressen)

- § 37 NIS2UmsuCG ermöglicht, dass Einrichtungen teilweise oder vollständig von NIS2-Pflichten ausgenommen werden.
- Das gilt nur, wenn: nationale Sicherheit, öffentliche Ordnung, Verteidigung, Strafverfolgung gefährdet wäre.
- Zwei Formen:
 - Einfacher Ausnahmebescheid: Befreiung von Risikomanagement + Meldepflichten
 - Erweiterter Ausnahmebescheid: vollständige Befreiung inkl. Registrierung



Was kann sanktioniert werden? (§65)

Ordnungswidrig handelt ein Unternehmen, wenn z. B.:

- Risikomanagement-Maßnahmen nicht oder unvollständig umgesetzt werden
 - (z. B. Backup, Incident Response, Notfallkonzepte) → §30 Abs. 1
- Dokumentationspflichten verletzt werden
 - (z. B. fehlende Nachweise, unvollständige Protokolle) → §30 Abs. 1 S.3 & §39
- Meldepflichten nicht eingehalten werden
 - Erstmeldung nicht innerhalb 24h
 - Folge-/Abschlussmeldung nicht oder verspätet → §32
- Registrierungs- und Berichtspflichten nicht erfüllt werden
 - (z. B. falsche oder fehlende Angaben an das BSI) → §33 & §34
- Anordnungen des BSI nicht befolgt werden
 - (z. B. Prüfungen, Maßnahmen, Zutritte) → §§16, 17, 35, 36, 40, 61
- Zertifikate oder Kennzeichnungen falsch verwendet werden → §§52–55
- BSI-Prüfern Information oder Zugang verweigert wird
 - (z. B. Räume, Unterlagen, Aufzeichnungen) → §61

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Wie hoch können die Bußgelder sein?

Die Höhe hängt davon ab, ob das Unternehmen:

- „besonders wichtige Einrichtung“ (bwE) oder
- „wichtige Einrichtung“ (wE)

ist – und vom **Gesamtumsatz** des Unternehmens.

1) Bußgelder für schwerwiegende Verstöße (Pflichten nach §§30–32 & §39)

- Besonders wichtige Einrichtungen (bwE)
 - bis zu 10 Mio. € oder
 - bis zu 2 % des weltweiten Jahresumsatzes, wenn Umsatz > 500 Mio. €
- Wichtige Einrichtungen (wE)
 - bis zu 7 Mio. € oder
 - bis zu 1,4 % des weltweiten Jahresumsatzes, wenn Umsatz > 500 Mio. € (§65 Abs. 5 Nr. 1 + Abs. 6 + Abs. 7)

2) Weitere Bußgeldrahmen

- Bis 2 Mio. €: z. B. Verstöße gegen Anordnungen nach §11, §16, §17
- Bis 1 Mio. €: fehlende Nachweise
- Bis 500.000 €: fehlerhafte Angaben, falsche Zertifikate, fehlende Unterrichtung
- Bis 100.000 €: fehlende Erreichbarkeit, Zutrittsverweigerung, Verzögerungen

*Quelle: <https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html>



Wie das NIS2-Umsetzungsgesetz mit anderen Gesetzen zusammenhängt

- **EU-RICHTLINIE (NIS2)** – EU-Vorgaben für Cybersicherheit. Umsetzung in nationales Gesetz
- **NIS2-Umsetzungsgesetz (NIS2UmsuCG)** – Zentrales Gesetz für Cyber Sicherheit in Deutschland
- **EU-Implementing Acts** - Gelten u. a. für Cloud, DNS, TLD, Hosting, Rechenzentren, CDN, Suchmaschinen, soziale Netzwerke. Haben Vorrang vor den nationalen technischen Anforderungen des §30 NIS2UmsuCG
- **BSI-Gesetz (BSIG)** – Grundgesetz der IT-Sicherheit, durch NIS2 aktualisiert & erweitert
- **IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)** – Wird durch NIS2UmsuCG weitgehend **abgelöst**, bleibt aber historisch relevant
- **KRITIS-Dachgesetz (geplant)** – Ersetzt künftig die BSI-Kritisverordnung, Regelt physische Sicherheit kritischer Anlagen (Gebäude, Zutritt, Betriebsumgebung), Wird parallel zu NIS2 gelten
- **Sektorale Spezialgesetze** (EnWG, TKG, Wasser-, Gesundheits-, Verkehrsrecht) – Bleiben bestehen und gelten zusätzlich
- **DORA (Digital Operational Resilience Act – EU-Verordnung)** – Gilt ausschließlich für den Finanzsektor, DORA geht vor NIS2.



Ihre nächsten Schritte

- Prüfen Sie, ob Ihr Unternehmen in den Anwendungsbereich fällt.
 - Offizielle BSI-Prüfung ab sofort verfügbar
 - <https://betroffenheitspruefung-nis-2.bsi.de/>
- Bereiten Sie die Registrierung und Meldewege vor
- Gap-Analyse starten
- Fangen Sie mit der Risiko-Analyse an. Implementieren Sie **angemessene** technische und organisatorische Maßnahmen.
- Implementieren Sie ein Krisen-Management um bei einem Sicherheitsvorfall schnell, fristgerecht und mit entsprechender Berichterstattung reagieren zu können.
- Rahmenwerke und Standards passend zur Branche und Unternehmensgröße unterstützen bei der Umsetzung
 - ISO 27001
 - BSI IT-Grundschutz

Unterstützung durch das BSI



- Starterpaket für Unternehmen
- Virtuelle Kick-off-Seminare für:
 - Betroffenheitsprüfung
 - Registrierung
 - Meldepflichten
 - Risikomanagement
- Weitere Leitfäden & FAQ folgen
- BSI plant zentrale CISO-Struktur für Bundesverwaltung

So können wir Sie unterstützen



- Qualifizierung des Fachpersonals und Schulung der Mitarbeiter im Bereich ISO 27001 (Foundation, Officer, Auditor)
- NIS2 Compliance Prüfung
- 10 % Rabatt auf die gesamte ISO-27001-Reihe

Gutschein Code: ISO-10

Termin buchen und Gutschein nutzen

Vielen
Dank!