

Bin ich von NIS2 betroffen?

Sechs Fragen, keine Technikenntnis nötig. Ergebnis in unter fünf Minuten.

1 Bin ich in einem der 18 NIS2-Sektoren tätig?

Maßgeblich sind Anlage 1 und Anlage 2 des BSIG. Wer in keinem der Sektoren tätig ist, ist nicht direkt reguliert, kann aber über die Lieferkette in der Pflicht stehen.

ANLAGE 1 · HOCHKRITISCH 11

- Energie
- Verkehr und Transport
- Bankwesen
- Finanzmarktinfrastuktur
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- IKT-Dienste (B2B)
- Öffentliche Verwaltung
- Weltraum

ANLAGE 2 · SONSTIGE KRITISCHE 7

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemische Industrie
- Lebensmittelverarbeitung
- Verarbeitendes Gewerbe (inkl. Maschinenbau)
- Digitale Dienste (Marktplätze, Suchmaschinen)
- Forschungseinrichtungen

⚠ Sonderfall, größenunabhängig betroffen: DNS-Dienste, TLD-Registrare, qualifizierte Vertrauensdiensteanbieter und TK-Anbieter gelten ohne Schwellenprüfung sofort als besonders wichtige Einrichtung.

✓ **JA** Weiter zu Frage 2

✗ **NEIN** Weiter zu Frage 4: indirekte Betroffenheit

2 Steht mein Sektor in Anlage 1 oder in Anlage 2?

Die Anlage entscheidet, welche Einstufung überhaupt erreichbar ist. Die Größe entscheidet danach, ob sie erreicht wird.

ANLAGE 1

Einstufung als besonders wichtige Einrichtung möglich

ANLAGE 2

höchstens Einstufung als wichtige Einrichtung

→ **DANN** In beiden Fällen weiter zu Frage 3

3 Erfülle ich die Schwellenwerte nach § 28 BSIG?

Ein Wert genügt: entweder die Zahl der Mitarbeitenden oder Umsatz und Bilanzsumme gemeinsam.

● Besonders wichtige Einrichtung	≥ 250 Mitarbeitende	oder > 50 Mio. € Umsatz und > 43 Mio. € Bilanzsumme
● Wichtige Einrichtung	≥ 50 Mitarbeitende	oder > 10 Mio. € Umsatz und > 10 Mio. € Bilanzsumme
● Nicht direkt reguliert	< 50 Mitarbeitende	und < 10 Mio. € Umsatz

⚠ Konzernklausel, die häufigste Fehlerquelle: Gehört das Unternehmen zu einem Konzern, der die Schwellenwerte überschreitet, zählt die wirtschaftliche Einheit, nicht die einzelne Gesellschaft.

✓ **JA** Die Einstufung steht fest: direkt reguliert

✗ **NEIN** Weiter zu Frage 4

4 Bin ich kritischer Zulieferer oder IT-Dienstleister für ein NIS2-pflichtiges Unternehmen?

Gemeint sind Lieferungen, Daten oder IT-Leistungen für Unternehmen, die selbst unter NIS2 fallen.

✓ **JA** **Indirekt betroffen**

✗ **NEIN** Weiter zu Frage 5

5 Bin ich IKT-Dienstleister für ein Finanzunternehmen?

IT-Dienste, Software oder Infrastruktur für Banken, Versicherungen, Zahlungsdienstleister und andere von DORA regulierte Institute.

✓ **JA** **DORA-relevant**

✗ **NEIN** Weiter zu Frage 6

6 Entwickle oder verkaufe ich Produkte mit digitalen Elementen?

Hardware oder Software, die in der EU verkauft wird und eine Netzwerkverbindung oder Software-Komponenten enthält.

✓ **JA** **CRA-pflichtig**

✗ **NEIN** **Nicht direkt reguliert**

Was das Ergebnis bedeutet

ERGEBNIS	BEDEUTUNG	NÄCHSTER SCHRITT
Besonders wichtige Einrichtung	Direkt und streng reguliert	BSI-Registrierung nachholen, ISMS aufbauen, § 38 BSIG beachten
Wichtige Einrichtung	Direkt reguliert, reaktive Aufsicht	BSI-Registrierung nachholen, Maßnahmen nach § 30 BSIG umsetzen
Größenunabhängig betroffen	Direkt reguliert ohne Schwellenprüfung	Sofort das BSI kontaktieren, Pflichten klären
Indirekt betroffen (Lieferkette)	Keine Gesetzespflicht, faktische Pflicht	Kundenanforderungen proaktiv erfüllen, ISO 27001 aufbauen
DORA-relevant	IKT-Dienstleister für den Finanzsektor	DORA Art. 28 bis 30, IKT-Register aufbauen (→ Kap. 10)
CRA-pflichtig	Produkthersteller mit digitalen Elementen	Security-by-Design, SBOM, Meldeprozess bis Sept. 2026 (→ Kap. 11)
Nicht direkt reguliert	Kein gesetzlicher Status	Betroffenheit dokumentieren (Datum und Begründung), bei Wachstum neu prüfen