NIS 2

Hohe Anforderungen an die Cybersicherheit

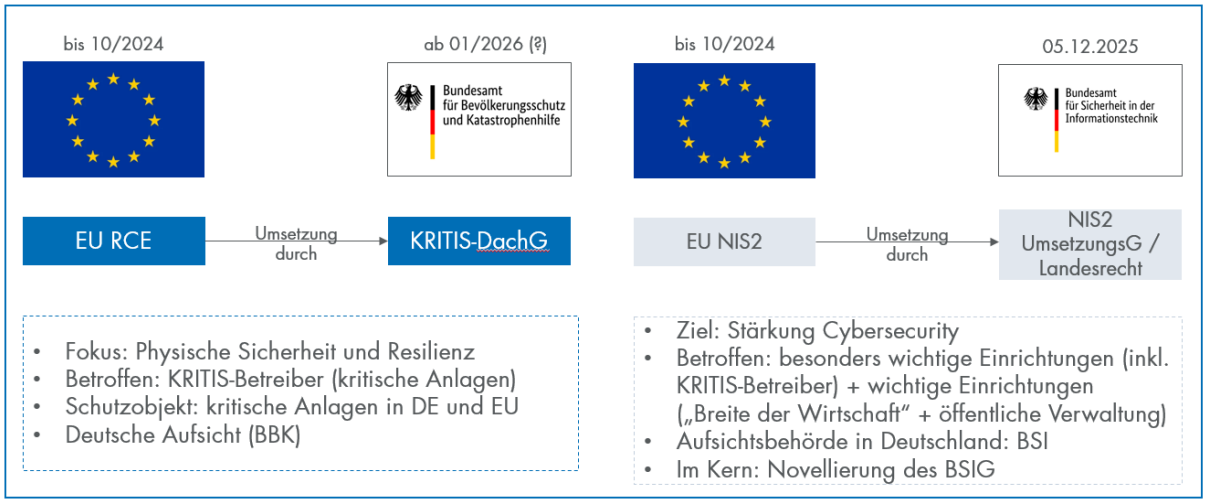
Spätestens seit Inkrafttreten der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union – NIS 2 (EU 2022/2555) sollte das Thema Cybersicherheit in Unternehmen Chefsache sein. NIS 2 hat den Maßnahmen- und Pflichtenkatalog bezüglich Cybersecurity für Unternehmen noch einmal deutlich erweitert. Dieser gilt nicht mehr nur für „kritische Infrastrukturen“ im engeren Sinne, sondern stellt flächendeckend hohe Anforderungen an die Cybersicherheit für Unternehmen. NIS 2 ist grundsätzlich für öffentliche und private Einrichtungen anwendbar. In bestimmten Sektoren sind Unternehmen sogar größenunabhängig betroffen.

Fact Sheet zur NIS 2-Umsetzung

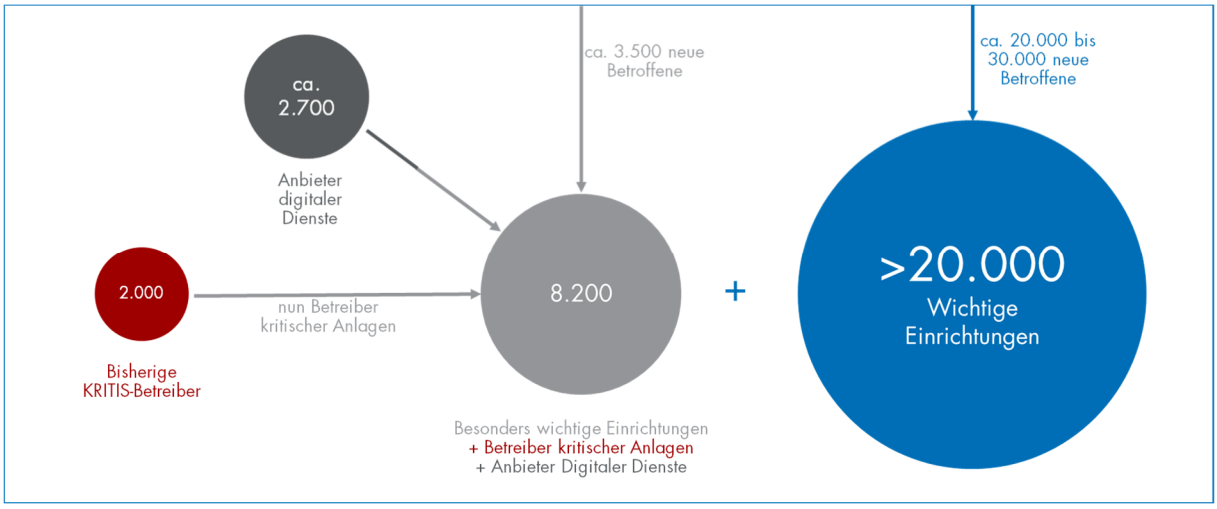
Hintergrund und Grundlagen zur NIS 2

Die Umsetzung der NIS 2 (Network and Information Security) -Richtlinie ist ein Teil der EU-Cybersicherheitsstrategie zur Stärkung und Vereinheitlichung des IT-Sicherheitsniveaus innerhalb der EU. In Deutschland erfolgt die Umsetzung durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“ (NIS2-Umsetzungsgesetz), wodurch insbesondere das BSIG erheblich umgestaltet wird.

Aufgrund einer „hybriden Bedrohungslage“ nimmt die EU-Cybersicherheitsstrategie mit der „CER“ (Critical Entities Resilience)-Richtlinie auch den physischen Schutz kritischer Anlagen (Sabotage, Naturkatastrophen etc.) in den Blick. Die CER-RL wird durch das KRITIS-Dachgesetz (KRITIS-DachG) umgesetzt. Das KRITIS-DachG hat den Deutschen Bundestag passiert; erforderlich ist aktuell (Stand 5. März 2026) noch die Zustimmung des Bundesrats.



Von der NIS 2-Umsetzung werden nicht mehr nur Betreiber “kritische Infrastrukturen” (“KRITIS”), sondern wird die Breite der Wirtschaft betroffen sein. Der Gesetzgeber geht von circa 30.000 zusätzlich betroffenen Unternehmen bzw. Einrichtungen aus.



Wann gelten die NIS 2-Regelungen?

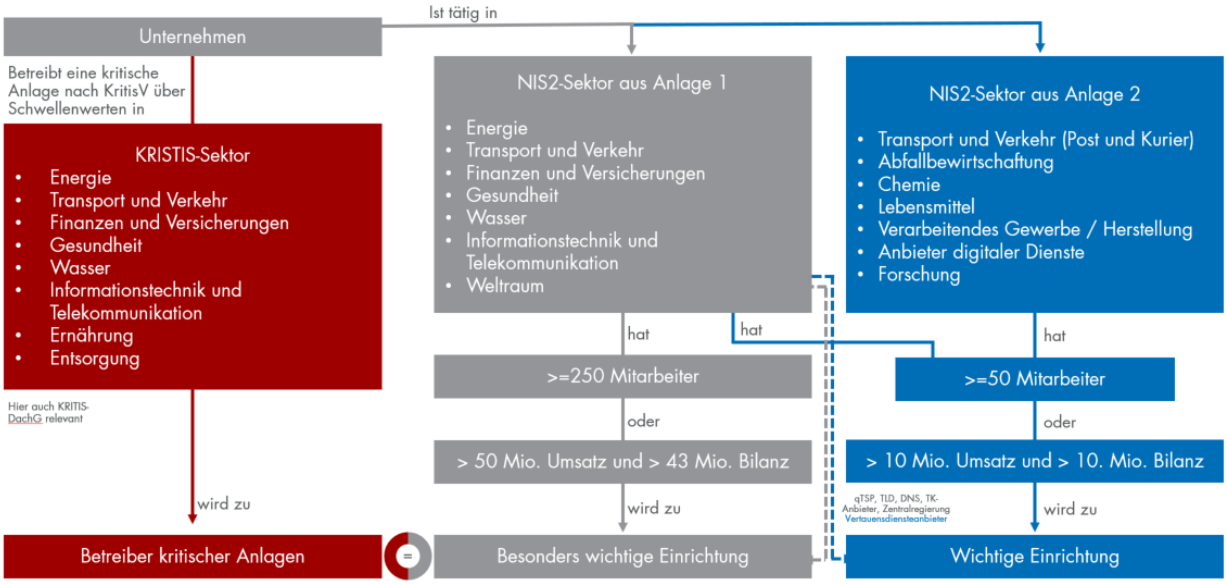
Die NIS 2 Richtlinie bedarf der Umsetzung durch die EU-Mitgliedstaaten. Die Umsetzungsfrist ist am 17. Oktober 2024 abgelaufen. Deutschland hat das NIS2-Umsetzungsgesetz, durch das im Wesentlichen das BSIG novelliert wird, am 5. Dezember 2025 verkündet. Die **Pflichten gelten seit dem 6. Dezember 2025** für die betroffenen Unternehmen in Deutschland.

Anwendungsbereich:

Um zu ermitteln, ob ein Unternehmen bzw. eine Einrichtung in den Anwendungsbereich des BSIG fällt, müssen im Wesentlichen die folgenden Fragen beantwortet werden:

- Fällt die Geschäftstätigkeit in einen der Sektoren? **Ausnahmen können für „vernachlässigbare" Geschäftstätigkeiten gelten*
- Werden die Schwellenwerte aus § 28 BSIG bzw. der (neuen) BSI-KRITIS-VO erreicht?

Es wird zwischen „wichtigen Einrichtungen" und „besonders wichtigen Einrichtungen" sowie „Betreibern kritischer Anlagen" (als eine Kategorie „besonders wichtiger Einrichtungen").



Die Grafik gibt eine Übersicht. Für eine genaue Einordnung bedarf es einer Prüfung im Einzelfall, bei der auch Einzelfragen der Berechnung, die Behandlung von Konzernunternehmen, Nebentätigkeiten eines Unternehmens und auch zu Zuordnung eines Unternehmens zu mehreren Sektoren zu klären sind. Wir unterstützen hierbei gern.

NIS 2-Pflichtenkreis für betroffene Unternehmen

Unter den Anwendungsbereich von NIS 2 fallende Unternehmen müssen mehrere Pflichten erfüllen, darunter:

Risikomanagementmaßnahmen (§§ 30, 31 BSIG):

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaß-nahmen im Bereich der Sicherheit in der Informationstechnik,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Meldepflichten (§ 32 BSIG) 24h/72h/30 Tage, ggf. Zwischenmeldungen an das BSI

Registrierungspflichten (§§ 33, 34 BSIG) Frist: 3 Monate ab dem Zeitpunkt, in dem das betroffene Unternehmen die Voraussetzungen für eine wichtige / besonders wichtige Einrichtung erfüllt

Unterrichtungspflichten (§ 35 BSIG)

Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen (§ 38 BSIG) Die Geschäftsleitungen, die diese Pflichten verletzen, haften gegenüber der Einrichtung für einen hierdurch schuldhaft verursachten Schaden

Nachweispflichten für Betreiber kritischer Anlagen (§ 39 BSIG): Audits, Prüfungen, Zertifizierungen. Alle drei Jahre, Stichproben durch BSI

Ggf. Benennung eines Vertreters (§ 60 Abs. 3 BSIG)

Sanktionen

Bei Nichteinhaltung der Pflichten können besonders wichtige Einrichtungen mit einem Bußgeld in Höhe von bis zu 10 Mio. EUR (oder 2 % des globalen Umsatzes) belegt werden; wichtige Einrichtungen mit einem Bußgeld in Höhe von bis zu 7 Mio. EUR (oder 1,4 % des globalen Umsatzes).

Sofern besonders wichtige Einrichtungen bei Defiziten bezüglich der Cybersecurity den Anordnungen des BSI nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann vorübergehend die Betriebsgenehmigung ganz oder teilweise ausgesetzt werden oder unzuverlässigen Geschäftsleitungen die Ausübung ihrer Tätigkeit vorübergehend untersagt werden.

Unser Beratungsansatz

Unsere Anwältinnen und Anwälte bieten für die Umsetzung von NIS 2 umfassende Rechts- und Strategieberatung an. Wir verfolgen dabei einen ganzheitlichen Beratungsansatz bestehend aus IT-Sicherheitsrecht, Datenschutz, Compliance & Riskmanagement, Versicherungsrecht (etwa Fragen zu einer Cyber Versicherung), Äußerungs- und Medienrecht (Reputationsschutz) und gegebenenfalls Strafrecht.

Sofern es um eher technische Fragen wie die konkrete Umsetzung und Angemessenheit der geforderten Risikomanagementmaßnahmen einschließlich einer technischen Gap-Analyse geht, setzen wir auf die enge Zusammenarbeit mit spezialisierten Kooperationsunternehmen.