SECJUR

# Die NIS2-Richtlinie ist da: So bereiten Sie Ihr Unternehmen 2026 auf die Umsetzung vor

Whitepaper

Diese Marktführer arbeiten mit SECJUR:

PETER KÖLLN · Masterplan.com · SWT STAHLWERK THÜRINGEN · 1KOMMA5° · YUNEX TRAFFIC · OTTO DÖRNER · deepset · EDEKABANK · Nordzucker · yfood · demeter · STADTWERKE KAMP-LINTFORT

## 1. Einleitung

### 1.1 Warum NIS2?

Die Digitalisierung hat in den vergangenen Jahren nahezu alle Wirtschaftsbereiche tiefgreifend verändert. Mit ihr wächst jedoch nicht nur die Effizienz, sondern auch die Abhängigkeit von vernetzten Systemen, digitalen Lieferketten und automatisierten Produktionsprozessen.

Inmitten wirtschaftlicher und politischer Volatilität gewinnen Fragen der Informationssicherheit rasant an Bedeutung. Cyberangriffe auf Unternehmen nehmen zu, werden gezielter, koordinierter und verursachen teils existenzbedrohende Schäden.

Vor diesem Hintergrund wurde die NIS2-Richtlinie ins Leben gerufen. Sie ist die überarbeitete und deutlich verschärfte Nachfolgerin der ursprünglichen NIS-Richtlinie aus dem Jahr 2016 und verfolgt das Ziel, das Cybersicherheitsniveau innerhalb der Europäischen Union auf ein einheitlich hohes Niveau zu heben.

Die Richtlinie definiert konkrete Mindeststandards für die Sicherheit von Netz- und Informationssystemen, schafft einheitliche Meldepflichten und adressiert insbesondere solche Sektoren, deren Ausfall massive Auswirkungen auf die Gesellschaft und Wirtschaft hätte.

## 1.2 Kritische Branchen im Fokus der Cybersicherheit

Die Erweiterung des Anwendungsbereichs durch die NIS2-Richtlinie markiert einen tiefgreifenden Paradigmenwechsel im europäischen Sicherheitsverständnis. Zahlreiche Branchen, die bislang nicht unter den Begriff der „kritischen Infrastruktur“ fielen, werden nun regulatorisch stärker in die Pflicht genommen – und das mit gutem Grund: Ihre Rolle für die wirtschaftliche Stabilität, Versorgungssicherheit und das gesellschaftliche Funktionieren ist unübersehbar.

Unternehmen in diesen Sektoren – von industriellen Herstellern über Logistiknetzwerke bis hin zu digitalen Dienstleistern – sind zunehmend digitalisiert, global vernetzt und auf sensible Systeme angewiesen. Automatisierte Steuerungen, cloudbasierte Plattformen, Zulieferprozesse und Datenflüsse werden dabei zu potenziellen Einfallstoren für gezielte Angriffe.

Was viele dieser Organisationen vereint: Sie waren bislang nicht der primäre Fokus gesetzlicher Sicherheitsvorgaben. Mit NIS2 ändert sich das grundlegend. Die Richtlinie verpflichtet nun auch Betreiber sogenannter „wichtiger Einrichtungen“ – darunter viele Mittelständler und industrielle Unternehmen – zu einem strukturierten Schutz ihrer digitalen Infrastrukturen und Prozesse. Ziel ist es, das Sicherheitsniveau auf breiter Front zu erhöhen und damit das Gesamtrisiko für Gesellschaft und Wirtschaft deutlich zu senken.

## 1.3 Ziel dieses Whitepapers

Dieses Whitepaper richtet sich an Entscheiderinnen und Entscheider in Unternehmen, die direkt oder indirekt in den Anwendungsbereich der NIS2-Richtlinie fallen – insbesondere aus mittelständischen und industriellen Strukturen. Dazu zählen Geschäftsführungen, IT-Leitungen, Compliance-Verantwortliche sowie Fachkräfte aus den Bereichen Informationssicherheit, Produktion und Lieferkettensteuerung.

Ziel ist es, praxisnah und verständlich über die Anforderungen der NIS2 aufzuklären, branchenspezifische Herausforderungen greifbar zu machen und konkrete Wege für eine strukturierte und ressourcenschonende Umsetzung aufzuzeigen. Im Mittelpunkt stehen dabei nicht nur gesetzliche Pflichten, sondern auch die Chance, Cybersicherheit als strategischen Erfolgsfaktor zu etablieren.

Denn klar ist: Mit NIS2 wird IT-Sicherheit zur Führungsaufgabe.

# 2. Was ist die NIS2-Richtlinie genau?

Stand: Juli 2025

## 2.1 Hintergrund und Zielsetzung der Richtlinie

Die EU-Richtlinie NIS 2 ist eine überarbeitete Version der NIS-1-Richtlinie, die strengere Cybersicherheitsstandards für Unternehmen mit mindestens 50 Mitarbeitenden und 10 Millionen Euro Umsatz in bestimmten Sektoren vorschreibt.

Mit der NIS2-Richtlinie (Richtlinie (EU) 2022/2555) hat die Europäische Union im Jahr 2022 einen neuen Rechtsrahmen geschaffen, um das steigende Risiko von Cyberangriffen zu adressieren. Sie ersetzt die bisherige NIS-Richtlinie von 2016 und reagiert auf die Erfahrungen aus deren Umsetzung: unklare Zuständigkeiten, uneinheitliche Sicherheitsniveaus und eine zu enge Auswahl betroffener Unternehmen.

NIS2 verfolgt daher ein klares Ziel: Die Etablierung eines gemeinsamen, hohen Cybersicherheitsniveaus innerhalb der EU. Dabei geht es nicht nur um den Schutz technischer Systeme, sondern auch um die Resilienz gesellschaftlich relevanter Funktionen – von der Energieversorgung über die Lebensmittelproduktion bis hin zu Onlineplattformen.

Die Richtlinie schreibt europaweit einheitliche Mindeststandards für die Sicherheit von Netz- und Informationssystemen vor, führt Meldepflichten bei Sicherheitsvorfällen ein und verlangt von den Mitgliedstaaten, effektive Aufsichts- und Durchsetzungsmechanismen zu etablieren.

## 2.2 Wer ist betroffen?

Die NIS2-Richtlinie richtet sich an Unternehmen und Organisationen, deren Ausfall potenziell erhebliche Auswirkungen auf Wirtschaft, Gesellschaft oder öffentliche Sicherheit hätte.

**Sie unterscheidet dabei zwei Kategorien von Einrichtungen:**

**„Wesentliche Einrichtungen“:**

z. B. in den Sektoren Energie, Verkehr, Gesundheit, digitale Infrastruktur.

**„Wichtige Einrichtungen“:**

z. B. in den Bereichen Abfallwirtschaft, Chemie – und neu: Lebensmittelproduktion, -verarbeitung und -vertrieb.

Grundsätzlich gilt NIS2 für Unternehmen mit mehr als 50 Mitarbeitenden oder über 10 Millionen Euro Jahresumsatz bzw. Bilanzsumme.

Aber: Auch kleinere Unternehmen können erfasst werden, wenn sie kritische Dienstleistungen für größere Betreiber erbringen oder systemrelevant sind, etwa durch Alleinstellungsmerkmale in der Lieferkette.

## 2.3 Relevanz für Unternehmen in kritischen und wichtigen Sektoren

Mit der NIS2-Richtlinie wurden zahlreiche Branchen neu als „kritisch“ oder „wichtig“ im Sinne der Versorgungssicherheit und öffentlichen Ordnung eingestuft. Damit trägt die EU der Tatsache Rechnung, dass digitale Angriffe auf Unternehmen weitreichende Auswirkungen auf ganze Volkswirtschaften und gesellschaftliche Grundfunktionen haben können – vergleichbar mit Strom-, Wasser- oder Gesundheitsinfrastrukturen.

Für betroffene Unternehmen bedeutet das: Sie müssen sich auf umfangreiche neue Anforderungen vorbereiten – unabhängig davon, ob sie Versorger, Hersteller, Dienstleister oder Zulieferer sind.

Im Zentrum stehen unter anderem systematische Risikomanagementprozesse, technische und organisatorische Schutzmaßnahmen, verpflichtende Mitarbeiterschulungen sowie strikte Meldepflichten bei Sicherheitsvorfällen. Besonders stark betroffen sind Unternehmen mit automatisierter Produktion, digitalisierten Lieferketten, Plattformarchitekturen oder hohem Datenaufkommen.

## 2.4 Fristen, Umsetzung und aktuelle Lage in Deutschland

Die NIS2-Richtlinie ist seit dem **16. Januar 2023** auf europäischer Ebene in Kraft. Mitgliedstaaten waren verpflichtet, die Vorgaben bis zum **17. Oktober 2024** in nationales Recht zu überführen.

In Deutschland jedoch kam es durch politische Entwicklungen zu Verzögerungen: Ein erster Gesetzesentwurf scheiterte vor der Bundestagswahl im Februar 2025. Derzeit liegt (Stand August 2025) ein überarbeiteter Referentenentwurf des Bundesinnenministeriums vor. Die Verabschiedung durch Bundestag und Bundesrat wird für Herbst 2025 erwartet.

Für Unternehmen bedeutet das: Obwohl das nationale Gesetz noch aussteht, bleibt die Verpflichtung zur Umsetzung bestehen. Die Grundprinzipien der NIS2 sind verbindlich – und Unternehmen, die untätig bleiben, setzen sich bereits heute einem erheblichen Risiko aus.

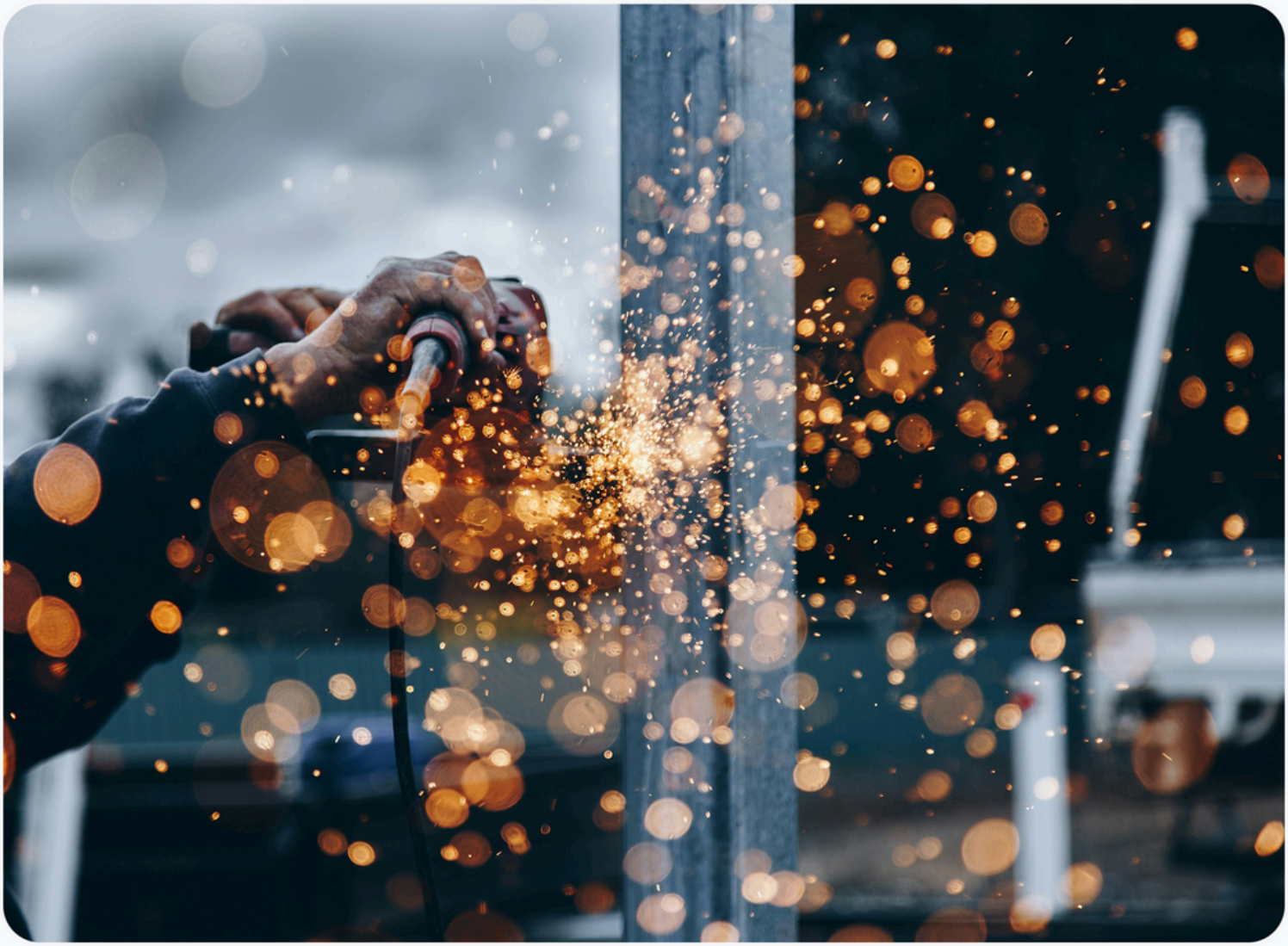
## 2.5 Sanktionen bei Nichteinhaltung

Die NIS2-Richtlinie sieht empfindliche Sanktionen für Verstöße vor.
Die Höhe der Bußgelder orientiert sich an der Größe und Einstufung des Unternehmens:

- **Wesentliche Einrichtungen:** Bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes (je nachdem, welcher Betrag höher ist).
- **Wichtige Einrichtungen:** Bis zu 7 Millionen Euro oder 1,4 % des Umsatzes.

Neben finanziellen Sanktionen drohen weitere Konsequenzen: etwa die Offenlegung des Vorfalls, Einschränkungen des Geschäftsbetriebs oder – besonders schwerwiegend – abhängig von der Rechtsform auch eine persönliche Haftung der Geschäftsführung und eine Entbindung von ihren Aufgaben.

Unternehmen betroffener Branchen sollten diese Risiken ernst nehmen. Denn gerade in einem sensiblen Sektor wie diesem sind Datenschutz, Prozesssicherheit und Vertrauen zentrale Erfolgsfaktoren – und ein Vorfall kann wirtschaftlich und reputativ verheerend wirken.



# 3. Wie die NIS2 in Unternehmen umgesetzt werden muss

Die NIS2-Richtlinie ist keine abstrakte Vorschrift – sie bringt konkrete, überprüfbare und zum Teil tiefgreifende Veränderungen für Unternehmen verschiedener Branchen mit sich. Die Anforderungen betreffen nicht nur IT-Abteilungen, sondern wirken tief in Produktionsprozesse, Qualitätsmanagement, Einkauf, Schulungswesen und das Lieferantenmanagement hinein.

Für betroffene Betriebe bedeutet das: NIS2 ist kein IT-Projekt, sondern ein organisationsweiter Transformationsprozess.

## 3.1 Umsetzung technischer und organisatorischer Maßnahmen

Kernstück der NIS2-Anforderungen ist der Aufbau eines systematischen Cybersicherheits- und Risikomanagements. Unternehmen müssen künftig technische und organisatorische Maßnahmen umsetzen, die über gängige Sicherheitspraktiken hinausgehen.

Dazu zählen:

- **Risikoanalysen für alle kritischen Geschäfts-** und Produktionsprozesse
- **Einführung und Dokumentation** von Sicherheitsrichtlinien und Zugriffskontrollen
- **Schutzmaßnahmen wie Firewalls,** Netzsegmentierung und regelmäßige Schwachstellenscans
- **Awareness-Schulungen für Mitarbeitende,** insbesondere in Produktion, Lager und Verwaltung
- **Integration von Cybersicherheit** in bestehende Qualitäts- und Auditstrukturen (z. B. HACCP)

Diese Maßnahmen müssen nicht nur implementiert, sondern regelmäßig überprüft und dokumentiert werden – mit klar zugewiesenen Verantwortlichkeiten und Nachweisen für Audits oder Behörden.

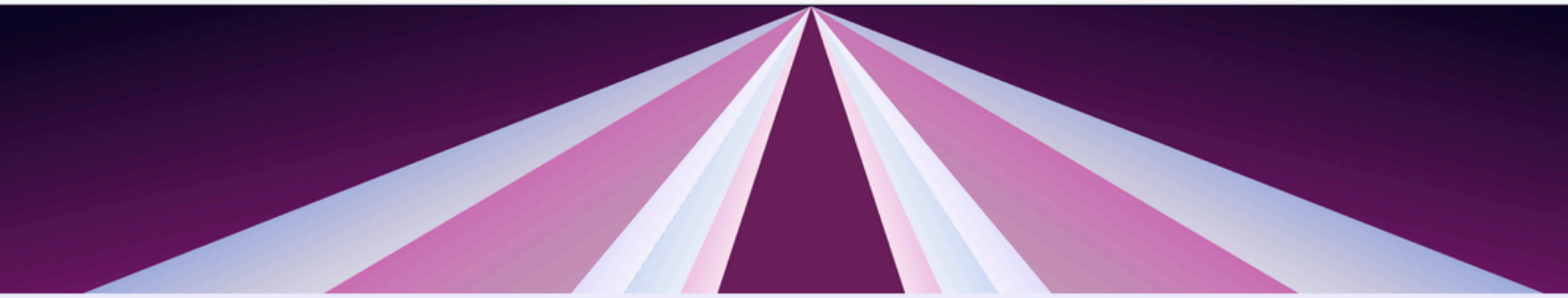
## 3.2 Schutz der Lieferkette und Datenintegrität

NIS2 verpflichtet Unternehmen dazu, nicht nur ihre eigenen Systeme abzusichern, sondern auch die Cybersicherheit innerhalb der Lieferkette zu berücksichtigen.

**Für Betriebe heißt das konkret:**

- Zulieferer, Spediteure, Lohnverarbeiter und IT-Dienstleister müssen sicherheitstechnisch bewertet und vertraglich eingebunden werden.
- Datenflüsse entlang der Lieferkette – etwa zur Rückverfolgbarkeit, Lagerverwaltung oder Rezeptfreigabe – sind durch geeignete technische Maßnahmen zu schützen.
- Der Einsatz von Technologien zur Datenintegrität, etwa digitale Signaturen oder Blockchain-basierte Dokumentation, kann erforderlich werden, um die Unverfälschbarkeit sicherheitskritischer Informationen zu gewährleisten.

Insbesondere Schnittstellen zu Partnern mit niedrigerem Cybersicherheitsniveau gelten künftig als Risiko – und müssen entsprechend abgesichert oder regelmäßig überprüft werden.



## 3.3 Neue Anforderungen an Vorfallmanagement und Meldepflichten

NIS2 verpflichtet Unternehmen zur Einrichtung eines strukturierten Systems zur Erkennung, Bewertung und Meldung von IT-Sicherheitsvorfällen.

Besonders relevant sind hierbei:

- **Frühwarnpflicht:** Innerhalb von 24 Stunden nach Feststellung eines sicherheitsrelevanten Vorfalls muss eine erste Meldung an die zuständige Behörde erfolgen.
- **Detailmeldung:** Innerhalb von 72 Stunden ist eine umfassende technische und organisatorische Beschreibung nachzureichen.
- **Abschlussbericht:** Spätestens einen Monat nach dem Vorfall ist eine finale Bewertung inkl. Ursachenanalyse und ergriffener Maßnahmen vorzulegen.
- **Transparenzpflicht:** In schwerwiegenden Fällen kann eine Information der Öffentlichkeit oder betroffener Geschäftspartner erforderlich sein.

Unternehmen benötigen daher klar definierte interne Meldeketten, ein Incident-Response-Team, ein sicheres Berichtswesen und regelmäßig getestete Notfallpläne. Spontane Reaktionen „im Ernstfall“ reichen nicht mehr aus – es gilt, proaktiv vorbereitet zu sein.


# 4. Der SECJUR-Vorteil: Wie wir unterstützen

Die Umsetzung der NIS2-Richtlinie stellt viele Unternehmen vor eine doppelte Herausforderung: Einerseits müssen sie komplexe regulatorische Anforderungen erfüllen – andererseits fehlen häufig Ressourcen, Know-how oder die organisatorische Struktur, um dies effizient umzusetzen.

**Genau hier setzt SECJUR an. Mit unserem modularen Compliance-as-a-Service-Ansatz kombinieren wir Technologie, Fachwissen und Automatisierung in einer ganzheitlichen Lösung.**

Unser Ziel: Unternehmen befähigen, die Anforderungen von NIS2 und anderen Standards rechtskonform, effizient und dauerhaft zu erfüllen – ohne Mehraufwand für interne Teams.

## 4.1 Gap-Analyse und Maßnahmenplan

Auf Basis unseres Assessments führen wir eine detaillierte Soll-Ist-Analyse durch. Dabei identifizieren wir systematisch alle Sicherheitslücken, Prozessdefizite und organisatorischen Schwachstellen im Hinblick auf die NIS2-Anforderungen.

Das Ergebnis ist ein priorisierter Maßnahmenplan, der konkrete Handlungsempfehlungen liefert – inkl. Verantwortlichkeiten und Umsetzungsaufwand. So entsteht eine belastbare Grundlage für eine gezielte und ressourcenschonende Compliance-Strategie.

## 4.2 Risikomanagement: Effektiv, intelligent, automatisiert

Ein zentrales Element der NIS2-Richtlinie ist der systematische Umgang mit Risiken. Unternehmen müssen in der Lage sein, cyberbezogene, organisatorische und technische Risiken frühzeitig zu erkennen, zu bewerten und zu steuern – nicht nur im eigenen Betrieb, sondern auch entlang der gesamten Lieferkette.

Für viele Unternehmen ist das ein neues Terrain – insbesondere, wenn bisher kein zertifiziertes Informationssicherheits-Managementsystem (ISMS) vorhanden ist.

Mit SECJUR gelingt der Einstieg ins Risikomanagement mühelos – dank Automatisierung, KI-Unterstützung und intuitiver Nutzerführung.

## 4.3 Automatisierte Umsetzung mit KI und Plattform

Die eigentliche Umsetzung der Maßnahmen erfolgt über unsere digitale Plattform – unterstützt durch künstliche Intelligenz, vorgefertigte Module und geführte Prozesse.

Ob IT-Sicherheitsrichtlinien, Dokumentation, Awareness-Schulungen oder Risikoanalysen: SECJUR digitalisiert und automatisiert alle relevanten Compliance-Bausteine – revisionssicher, benutzerfreundlich und vollständig nachvollziehbar.

Das spart nicht nur Zeit, sondern reduziert auch externe Beratungskosten und minimiert Fehlerquellen.

## 4.4 Laufende Compliance-Überwachung

Compliance endet nicht mit der Erstumsetzung – sie muss gepflegt, überprüft und an neue Entwicklungen angepasst werden.

Regelmäßige Compliance-Updates stellen sicher, dass der erreichte Standard auch in Zukunft eingehalten werden kann. Risiken werden frühzeitig erkannt – bevor sie zum Problem werden.

## 4.5 Weitere integrierte Standards: ISO 27001, DSGVO & Whistleblowing

SECJUR denkt Compliance ganzheitlich: Unsere Plattform bildet nicht nur die Anforderungen der NIS2-Richtlinie ab, sondern integriert auf Wunsch auch weitere gesetzliche und normative Vorgaben – etwa die DSGVO, ISO 27001 oder die Anforderungen des Hinweisgeberschutzgesetzes.

So entsteht ein zentrales, auditfähiges System für alle sicherheits- und datenschutzrelevanten Aufgaben.

Für Unternehmen bedeutet das: **Ein Login, eine Plattform – und vollständige Übersicht über alle relevanten Compliance-Verpflichtungen.**

**Mit SECJUR** setzen Sie nicht nur NIS2 um – Sie etablieren eine nachhaltige, zukunftssichere Sicherheits- und Compliancekultur in Ihrem Unternehmen.

> Mit der Durchsetzung der NIS2 ist ab Beginn 2026 zu rechnen.

**Niklas Hanitsch**
Rechtsanwalt & Geschäftsführer, SECJUR

Mitglied der Bundesfachkommission Cybersicherheit des Wirtschaftsrats