By PwC Deutschland | 31. August 2026

Sector Shorts: NIS2 – Die Rechtsabteilung als strategischer Schlüssel zur Compliance

NIS2 ist weit mehr als nur eine Aktualisierung der Cybersicherheitsvorgaben für Betreiber kritischer Infrastruktur. Die Richtlinie weitet den Kreis der betroffenen Unternehmen gegenüber NIS1 deutlich aus, verschärft die Anforderungen an Governance, Risikomanagement und steht zugleich im Zusammenspiel mit weiteren Regulierungen wie DORA, CRA, AI Act oder auch der DSGVO. Für Unternehmen bedeutet das: Die Umsetzung ist kein reines IT-Projekt. Wer NIS2 rechtssicher und praxistauglich verankern will, braucht früh eine klare rechtliche Einordnung, belastbare Verantwortlichkeiten und ein gutes Zusammenspiel der Bereiche IT, Informationssicherheit und Operations mit Recht und Compliance.

Der erste Schritt führt über den Anwendungsbereich

Für viele Unternehmen beginnt NIS2 mit einer ganz praktischen Frage: Sind wir überhaupt vom Anwendungsbereich erfasst? In Deutschland ist diese Frage im BSIG geregelt und erfasst neben KRITIS-Anbietern Unternehmen definierter Sektoren, die eine bestimmte Größe überschreiten. Die Umsetzung der Richtlinie in nationales Recht der EU-Mitgliedsstaaten hat dazu geführt, dass der Anwendungsbereich je Mitgliedstaat variieren kann.

Gerade hier ist die Rechtsabteilung gefragt. Sie sorgt für eine belastbare Einordnung, begleitet die Registrierung, behält Fristen im Auge und bewertet nationale Besonderheiten in internationalen Strukturen.

Governance braucht rechtliche Klarheit

Der Pflichtenkatalog der NIS2-Richtlinie umfasst geeignete, verhältnismäßige und wirksame technische und organisatorische Cybersicherheits-Maßnahmen. Dazu zählen unter anderem Risikoanalyse, Incident Response, Business Continuity, Lieferkettensicherheit, Cyberhygiene und Schulungen.

Die Rechtsabteilung übernimmt dabei u.a. die Rolle einer Auslegungs-, Koordinations- und Harmonisierungsinstanz für das interne Regelwerk. Sie muss dafür sorgen, dass die Implementierung regulatorischer Anforderungen auch rechtlich überwacht wird. So prüft sie, ob Policies, Rollenmodelle, Rechte- und Incident-Response-Konzepte rechtlich klar formuliert und konsistent sind und die rechtlichen Anforderungen abbilden.

Incident-Response-Management: Wenn der Ernstfall eintritt, zählt Struktur

Die Effektivität der Governance zeigt sich, wenn es zu einem Vorfall kommt: Die Rechtsabteilung tut gut daran, darauf hinzuwirken, dass die Abläufe bei einem Vorfall mit den Stakeholdern eingeübt werden. Denn ein Sicherheitsvorfall ist nie nur ein technisches Ereignis. Er löst zugleich Meldepflichten, Kommunikationsanforderungen und Abstimmungsbedarf gegenüber Behörden, Versicherungen, Geschäftspartnern und weiteren Stakeholdern aus.

NIS2 verlangt hier keine abstrakte Theorie, sondern belastbare und erprobte Abläufe. Aufbauend auf bestehenden Strukturen können Prävention, Reaktion, Nachbereitung, Dokumentation kontinuierlich verbessert werden.

Besonderer Schwerpunkt ist die Umsetzung der gesetzlichen Meldearchitektur: Sie sieht ein mehrstufiges Verfahren mit früher Erstmeldung, Folgemeldung, ggf. Zwischen- und Fortschrittsmeldung sowie Abschlussmeldung vor. Für Unternehmen ist entscheidend, diese Pflichten mit anderen Meldewegen, -vorgaben und -fristen zu verzahnen.

Lieferkette und Vertragsmanagement rücken in den Fokus

NIS2 macht die Lieferkette ausdrücklich zum Teil des Risikomanagements. Sicherheitsanforderungen müssen an Dienstleister weitergegeben und vertraglich festgesetzt werden. Vorhandene und neu abzuschließende Verträge sind daher auf Sicherheitsstandards, Kontrollmechanismen, Haftung,

Vertragsstrafen und Kündigungsrechte zu überprüfen.

Hier kommt der Rechtsabteilung eine klassische Steuerungsfunktion zu: Sie begleitet Due-Diligence-Prüfungen, entwickelt standardisierte Vertragsklauseln und passt bestehende Verträge und Anhänge an. So wird aus einer regulatorischen Vorgabe ein belastbares Lieferketten- und Vertragsmanagement.

Haftung und Sanktionen: Management früh einbinden

Mit NIS2 rückt auch die Geschäftsleitung stärker in den Fokus. Die Rechtsabteilung sollte deshalb früh zu Risiken, Regressmöglichkeiten und geeignete Absicherungsmaßnahmen beraten. Insbesondere zur Absicherung gehören Dokumentation, Reporting- und Überwachungsstrukturen.

Fazit

NIS2 ist damit vor allem eines: ein unternehmensweites Governance- und Compliance-Thema mit erheblicher rechtlicher Tiefe. Nur wenn die Rechtsabteilung von Anfang an bei der Implementierung eingebunden ist, lässt sich die digitale Resilienz des Unternehmens haftungs- und rechtssicher gestalten. Eine frühzeitige, interdisziplinäre Verzahnung schafft regulatorische Sicherheit.

Schlagwörter

Compliance, Gesetzgebung, Legal, künstliche Intelligenz