Teil 1:
Rechtliche Anforderungen des NISG 2026

1. Einleitung

Mit der NIS-2-Richtlinie (EU) 2022/2555 und ihrer nationalen Umsetzung im Netz- und Informationssystemsicherheitsgesetz 2026 (NISG) hat sich der Umgang mit Cybersicherheit in Österreich grundlegend verändert. Was bisher oft freiwillig oder branchenspezifisch geregelt war, ist für viele Einrichtungen seit 1. Oktober 2026 Pflicht, verantwortlich für die Einhaltung der gefordertern Maßnahmen sind die Leitungsorgane.

Dieses Buch begleitet beide Seiten dieser Aufgabe: Teil 1 arbeitet die rechtlichen Anforderungen des NISG 2026 fundiert auf: Wer ist betroffen, welche Pflichten bestehen, welche Fristen gelten, welche Konsequenzen drohen bei Nichteinhaltung. Teil 2 setzt dort an, wo viele Compliance-Ratgeber aufhören: bei der tatsächlichen Umsetzung im betrieblichen Alltag. Eine rechtlich korrekte Maßnahme, die im Tagesgeschäft nicht gelebt wird, schützt nicht.

Beide Teile lassen sich einzeln lesen, ergänzen sich aber: Wo sinnvoll, verweist Teil 2 auf die passenden rechtlichen Grundlagen in Teil 1. Teil 2 folgt dabei einer durchgängigen Methodik: Was die Realität in Unternehmen ist, warum das jeweilige Thema relevant ist, und wie die Umsetzung in der Praxis gelingt – ergänzt um Fallbeispiele und konkrete Werkzeuge.

Dieses Buch ersetzt keine rechtliche oder fachliche Einzelfallberatung. Es soll die Grundlage schaffen, das NISG 2026 nicht als Pflichtübung abzuhaken, sondern als Chance zu nutzen, Informationssicherheit im eigenen Unternehmen wirksam zu verankern.

Zitierhinweise

Soweit im Folgenden Paragraphen ohne Gesetzesangabe zitiert werden, ist jeweils das österreichische NISG 2026 gemeint. Der Begriff NIS-2 steht für das gesamte Rechtsregime aufbauend auf Basis der EU-weit geltenden NIS-2-Richtlinie. Die Abkürzung ErläutRV bzw der Begriff Erläuterungen bezieht sich auf die Erläuterungen zur Regierungsvorlage zum NISG 2026.

2. Ausgangssituation: Was ist NIS?

2.1. Allgemeines

Die Abkürzung NIS steht für die Sicherheit von Netz- und Informationssystemen. Sie bildet den zentralen Regelungsgegenstand der Richtlinie (EU) 2022/2555 (im Folgenden: NIS-2-Richtlinie) sowie des Netz- und Informationssystemsicherheitsgesetzes 2026 (im Folgenden: NISG).

Adressiert werden dabei nicht nur klassische IT-Systeme, sondern sämtliche Netz- und Informationssysteme sowie sonstige digitale Komponenten, die für die Erbringung von Diensten und den Betrieb einer Einrichtung von Bedeutung sind:

Netz- und Informationssysteme im Sinne des NISG umfassen:

- Kommunikationsnetze
- Geräte oder Gruppen miteinander verbundener oder zusammenhängender Geräte, die die automatische Verarbeitung digitaler Daten durchführen
- digitale Daten, die von einem Kommunikationsnetz, Geräten oder Gruppen miteinander verbundener oder zusammenhängender Geräte, die die automatische Verarbeitung digitaler Daten durchführen, zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.[1]

Die Begriffe sind bewusst technologieneutral und weit gefasst, um sowohl klassische IT-Infrastrukturen als auch moderne Cloud-, Plattform- und OT-Umgebungen zu erfassen. Für Unternehmen bedeutet dies, dass nicht nur zentrale IT-Systeme, sondern auch Produktionsanlagen und Steuerungssysteme, aber auch ausgelagerte IT-Services in den Anwendungsbereich fallen können.

Die Sicherheit von Netz- und Informationssystemen ist die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau Beeinträchtigungen der Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten und Diensten abzuwehren.[2]

Damit stellt das Gesetz klar, dass Cybersicherheit nicht nur den Schutz vor Totalausfällen betrifft. Bereits die Beeinträchtigung eines einzelnen Schutzziels – etwa durch Datenabfluss, Manipulation oder Identitätsmissbrauch – kann einen relevanten Cybersicherheitsvorfall darstellen. Die Schutzziele bilden daher den zentralen Bewertungsmaßstab für unternehmerische Risiken, Sicherheitsmaßnahmen und Pflichten nach NIS-2.

2.2. Schutzziele von Informationssicherheit

Die Sicherheit von Netz- und Informationssystemen beruht auf allgemein anerkannten Schutzzielen der Informationssicherheit. Diese Schutzziele beschreiben, welche Eigenschaften von Daten und Diensten zu schützen sind, um ein angemessenes Sicherheitsniveau zu gewährleisten.

Das NISG übernimmt dabei die Systematik der NIS-2-Richtlinie und definiert die Sicherheit von Netz- und Informationssystemen als die Fähigkeit, Beeinträchtigungen der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und Diensten abzuwehren.

1 § 3 Z 1.
2 § 3 Z 2.

Bedeutung für Unternehmen:

Für Unternehmen sind die Schutzziele kein theoretisches Konstrukt, sondern:

- Grundlage des Cyber-Risikomanagements,
- Maßstab für technische und organisatorische Maßnahmen,
- Kriterium für die Bewertung von Sicherheitsvorfällen (zB Meldepflichten).

Ein Cybersicherheitsvorfall liegt vor, wenn die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Diensten, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt ist.[3]

Die Schutzziele bilden zugleich den Maßstab für zahlreiche Verpflichtungen des NISG und der Durchführungsverordnung (EU) 2024/2690 zur Richtlinie (EU) 2022/2555 der Kommission (im Folgenden: DVO (EU) 2024/2690), insbesondere für die Risikomanagementmaßnahmen sowie für die Beurteilung, ob ein Sicherheitsvorfall als erheblich einzustufen und damit meldepflichtig ist.

2.3. Verfügbarkeit

Verfügbarkeit bedeutet, dass Daten, IT-Systeme und digitale Dienste für berechtigte Nutzer jederzeit innerhalb der vorgesehenen Zeit nutzbar sind.

Im NIS-2-Kontext ist die Verfügbarkeit insbesondere deshalb von zentraler Bedeutung, weil Ausfälle oder Unterbrechungen von Netz- und Informationssystemen erhebliche Auswirkungen auf Gesellschaft, Wirtschaft und öffentliche Sicherheit haben können.

Bedeutung für Unternehmen

Für Unternehmen ist die Verfügbarkeit besonders kritisch, da Ausfälle beispielsweise unmittelbar zu:

- Produktionsstillständen,
- Lieferverzögerungen,
- Umsatzausfällen,
- Reputationsschäden

führen können.

Praxisbeispiele

Eine Beeinträchtigung der Verfügbarkeit liegt etwa vor bei:

- einem Ransomware-Angriff, der zentrale Systeme verschlüsselt,
- einem Denial-of-Service-Angriff auf einen Online-Dienst,
- einem Ausfall des Rechenzentrums oder Cloud-Dienstes, der den Geschäftsbetrieb lahmlegt.

3 Vgl § 3 Z 30.

Rechtliche Einordnung

Die Sicherstellung der Verfügbarkeit ist ein zentrales Schutzziel nach NIS-2. Unternehmen müssen daher geeignete Maßnahmen setzen, um Ausfälle zu verhindern, zu erkennen und rasch zu beheben.

2.4. Authentizität

Authentizität beschreibt die Eigenschaft, dass die Identität von Personen, Systemen oder Komponenten sowie die Herkunft von Daten eindeutig und überprüfbar ist.

Bedeutung für Unternehmen

Authentizität ist für Unternehmen wesentlich, um sicherzustellen, dass:

- nur berechtigte Personen auf Systeme zugreifen,
- Daten tatsächlich von der angegebenen Quelle stammen,
- digitale Kommunikation vertrauenswürdig ist.

Praxisbeispiele

Eine Beeinträchtigung der Authentizität liegt etwa vor bei:

- kompromittierten Benutzerkonten durch Phishing,
- Missbrauch von Administrator-Zugängen,
- Spoofing-Angriffen, bei denen Systeme oder Absender vorgetäuscht werden.

Rechtliche Einordnung

Die NIS-2-Richtlinie nennt Authentizität ausdrücklich als Schutzziel der Sicherheit von Netz- und Informationssystemen. Einrichtungen müssen daher Maßnahmen setzen, um Identitätsmissbrauch und unbefugten Zugriff zu verhindern. Die DVO (EU) 2024/2690 konkretisiert dies unter anderem durch Anforderungen an Zugriffskontrollen und Identitätsmanagement.

2.5. Integrität

Integrität bezeichnet die Eigenschaft von Daten und Systemen, vollständig, unverändert und korrekt zu bleiben.

Bedeutung für Unternehmen

Verlust der Integrität kann zu:

- falschen Geschäftsentscheidungen,
- fehlerhaften Produktionsprozessen,
- Sicherheitsrisiken

führen, selbst wenn Systeme weiterhin verfügbar sind.

Praxisbeispiele

Eine Beeinträchtigung der Integrität liegt etwa vor bei:

- Manipulation von Produktions- oder Logistikdaten,
- unbefugter Änderung von Konfigurationsdateien,
- Verfälschung von Daten bei der Übertragung.

Rechtliche Einordnung

Der Schutz der Integrität ist ein gleichrangiges Schutzziel neben Verfügbarkeit, Authentizität und Vertraulichkeit. Auch rein integritätsbezogene Vorfälle können als Sicherheitsvorfälle im Sinne von NIS-2 relevant sein.

2.6. Vertraulichkeit

Vertraulichkeit bezeichnet die Eigenschaft von Daten und Informationen, nur für berechtigte Personen, Stellen oder Systeme zugänglich zu sein.

Bedeutung für Unternehmen

Für Unternehmen betrifft Vertraulichkeit insbesondere:

- Geschäfts- und Betriebsgeheimnisse,
- Kunden- und Mitarbeiterdaten,
- Finanzdaten
- Sicherheits- und Zugangsinformationen.

Praxisbeispiele

Eine Beeinträchtigung der Vertraulichkeit liegt etwa vor bei:

- Datendiebstahl durch Cyberkriminelle,
- unbefugtem Zugriff auf interne Dokumente,
- Fehlkonfigurationen von Cloud-Speichern, die Daten öffentlich zugänglich machen.

Rechtliche Einordnung

Die NIS-2-Richtlinie und das NISG 2026 verstehen Vertraulichkeit als ein zentrales Schutzziel der Sicherheit von Netz- und Informationssystemen. Die DVO (EU) 2024/2690 konkretisiert dies durch Anforderungen an den Schutz vor unbefugter Offenlegung, insbesondere durch Zugriffsbeschränkungen und Schutz gespeicherter und übertragener Daten.

Sicherheitsvorfälle können daher auch dann melde- oder bewertungsrelevant sein, wenn ausschließlich die Vertraulichkeit von Daten betroffen ist, etwa bei Datenlecks oder Cyberangriffen ohne unmittelbaren Systemausfall.

Technische und organisatorische Maßnahmen zum Schutz der Vertraulichkeit umfassen unter anderem Zugriffsbeschränkungen und Schutz vor unbefugter Offenlegung, beispielsweise das Need-to-know-Prinzip.[4]

4 Vgl Anhang DVO (EU) 2024/2690, Ziffer 11.2.2 lit a.

3. Gesetzgebung

3.1. NIS-Richtlinie und NISG 2018 oder wie alles begann

3.1.1. NIS-Richtlinie (EU) 2016/1148

Die ursprüngliche NIS-Richtlinie, nämlich die Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-Richtlinie) war der erste Rechtsakt für Cybersicherheit auf EU-Ebene und die zentrale Maßnahme der ersten Europäischen Cybersicherheitsstrategie[5], die von der Kommission bereits 2013 vorgestellt wurde. Sie zielte darauf ab, ein hohes gemeinsames Sicherheitsniveau für Netz- und Informationssysteme in der Union zu gewährleisten.

Die EU-Mitgliedstaaten mussten nationale Cybersicherheitsstrategien entwickeln, zuständige Behörden und Computer-Notfallteams (Computer Security Incident Response Teams; im Folgenden: CSIRTs) einrichten sowie Betreiber wesentlicher Dienste identifizieren.

Die Umsetzungsgesetze zur NIS-Richtlinie verpflichteten Betreiber wesentlicher Dienste und bestimmte Anbieter digitaler Dienste, Sicherheitsmaßnahmen umzusetzen und Vorfälle zu melden.

Die Richtlinie förderte auch die Zusammenarbeit über die NIS-Kooperationsgruppe und das CSIRT-Netzwerk.

Ziel war (und ist) es, ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der gesamten Europäischen Union zu erreichen.

Die NIS-Richtlinie war ein wichtiger erster Schritt, um die Cybersicherheit in der EU zu stärken. Ihre Defizite, insbesondere die uneinheitliche Anwendung in den verschiedenen Mitgliedstaaten, fehlende Krisenreaktion und der sehr begrenzte Anwendungsbereich[6], führten zur NIS-2-Richtlinie, die deutlich umfassender, verbindlicher und harmonisierter ist.

3.1.2. NIS-Gesetz 2018

Das Netz- und Informationssystemsicherheitsgesetz (im Folgenden: NISG 2018) setzte die NIS-Richtlinie in Österreich um.[7] Es trat zeitgleich mit dem Inkrafttreten des NISG 2026 zur Umsetzung der NIS-2-Richtlinie außer Kraft[8], sodass seit 1. Oktober 2026 nur mehr das NISG 2026 gilt.[9] Es ist daher deutlich zwischen NISG 2018 und dem geltenden NISG 2026 zu unterscheiden.

5 Cybersicherheitsstrategie der Europäischen Union, JOIN(2013) 1 final, 7.2.2013.
6 Erwägungsgründe 4 bis 6 NIS-2-RL.
7 § 48 Z 1.
8 § 51 Abs 1.
9 § 51 Abs 1.

3.1.2.1. Anwendungsbereich NISG 2018

Das NISG 2018 galt für Betreiber wesentlicher Dienste in den Sektoren

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung
- Digitale Infrastruktur

sowie für

- Anbieter digitaler Dienste (Online-Marktplatz, eine Online-Suchmaschine oder einen Cloud-Computing-Dienst jeweils ab mittlerer Unternehmensgröße) sowie für
- Einrichtungen der öffentlichen Verwaltung (teilweise).[10]

Die Ermittlung der Betreiber wesentlicher Dienste erfolgte – anders als bei Anbietern digitaler Dienste – mittels **Bescheid**.[11] In Österreich waren rund hundert Betreiber wesentlicher Dienste im Anwendungsbereich des NISG 2018 und erhielten einen entsprechenden Bescheid.

Dies hat sich mit dem NISG 2026 grundlegend geändert. Anstelle der Betreiber wesentlicher Dienste und Anbieter digitaler Dienste im Sinne des NISG 2024 gibt es nun wesentliche und wichtige Einrichtungen im Sinne des NISG 2026. Diese müssen selbst feststellen, ob sie in den Anwendungsbereich des NISG 2026 fallen und müssen sich ohne behördliche Aufforderung registrieren.[12] Bescheide zum Anwendungsbereich gibt es im Rahmen des NISG 2026 nur mehr in Ausnahmefällen (zB größenunabhängige Einstufung als wesentliche oder wichtige Einrichtung aufgrund der besonderen Bedeutung der Einrichtung für den Sektor[13]).

3.1.2.2. Inhalt NISG 2018

Das NISG 2018 legte Aufgaben, Zuständigkeiten und Befugnisse für die mit der Umsetzung betrauten Behörden fest. Der Bundeskanzler nahm dabei strategische Aufgaben[14], beispielsweise Festlegung strategischer Ziele und Politik- und Regulierungsmaßnahmen wahr,[15] während der Bundesminister für Inneres für operative Aufgaben zuständig war,[16] beispielsweise die Überprüfung der Sicherheitsvorkehrungen von Betreibern wesentlicher Dienste und die Einhaltung der Meldepflichten.[17]

10 § 2 NISG 2018.
11 § 16 Abs 4 Z 1 NISG 2018.
12 S 29 Abs 2.
13 § 26 Abs 1.
14 § 4 Abs 1 NISG 2018.
15 § 8 Abs 1 NISG 2018.
16 § 5 Abs 1 NISG 2018.
17 § 5 Abs 5 NISG 2018.

Nähere Regelungen für die Sicherheitsvorkehrungen fanden sich in der NIS-Verordnung 2019.[18]

3.1.2.3. NIS-Verordnung 2019

In der Netz- und Informationssystemsicherheitsverordnung 2019 (NIS-Verordnung 2019)[19] waren die Kriterien für Sicherheitsvorfälle, Schwellenwerte für die Definition von wesentlichen Diensten in den einzelnen Sektoren und Festlegung von Kategorien und Maßnahmen hinsichtlich Sicherheitsvorkehrungen festgelegt.

3.1.2.4. Geltungsdauer NISG 2018 und zugehörige Verordnungen

Das NISG 2018 und die auf seiner Grundlage erlassenen Verordnungen traten mit Inkrafttreten des NISG 2026 außer Kraft.[20]

Bescheide zur Ermittlung der Betreiber wesentlicher Dienste, die gemäß NISG 2018 erlassen wurden, wurden mit Inkrafttreten des NISG 2026 gegenstandslos.[21]

Für Bescheide für Aufgaben der Computernotfallteams CSIRTs (Computer Security Incident Response Teams) und der qualifizierten Stellen gibt es Übergangsbestimmungen.[22]

3.1.3. Unterschiede NISG 2018 und NISG 2026

	NISG 2018	NISG 2026
Rechtsgrundlage	NIS-Richtlinie (EU) 2016/1148	NIS-2-Richtlinie (EU) 2022/2555
Behörde	Bundeskanzler als strategische Behörde; Bundesminister für Inneres als operative Behörde	Zentrale Cybersicherheitsbehörde: Bundesamt für Cybersicherheit
Anwendungsbereich	„Betreiber wesentlicher Dienste" und „digitale Diensteanbieter"; wenige Sektoren mit Schwellenwerten; öffentliche Verwaltung	18 Sektoren mit „wesentlichen" und „wichtigen" Einrichtungen größenabhängig, öffentliche Verwaltung
Identifikation	Ermittlung Betreiber wesentlicher Dienste mit Bescheid	Selbstidentifikation aufgrund Gesetz und Registrierungspflicht
Scope	wesentlicher Dienst	gesamte Einrichtung

18 Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV), BGBl II 2019/215.

19 Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV), BGBl II 2019/215.

20 § 51 Abs 1.

21 § 51 Abs 5.

22 § 51 Abs 5.

	NISG 2018	NISG 2026
Governance	Keine ausdrückliche Verantwortung der Geschäftsleitung	Klare Verantwortung der Leitungsorgane, einschließlich Überwachungs- und Schulungspflichten
Risikomanagement-maßnahmen	Pflicht zu angemessenen technischen und organisatorischen Sicherheitsmaßnahmen	Konkrete Anforderungen an Risikomanagement, Governance, Lieferkettensicherheit, Business Continuity, Verschlüsselung, Authentifizierung uvm
Lieferkettensicherheit	geregelt	Explizite Anforderungen an Sicherheitsmaßnahmen in der Lieferkette; Aufnahme Lieferkettensicherheit in Selbstdeklaration
Schulungen und Awarenessbildung	keine konkreten Vorgaben	Verpflichtende Schulungen und Sensibilisierung für Mitarbeitende und Leitungsorgane
Nachweis Wirksamkeit	Prüfung durch qualifizierte Stelle alle drei Jahre	Selbstdeklaration; Prüfung durch unabhängige Stelle nur auf Aufforderung
Strafen	bis zu EUR 50.000, im Wiederholungsfall bis zu 100.000	Wesentliche Einrichtungen bis zu EUR 10 Millionen oder bis zu 2 % des weltweiten Jahresumsatzes; Wichtige Einrichtungen bis zu EUR 7 Millionen oder bis zu 1,4 % des weltweiten Jahresumsatzes; bei weniger sanktionsrelevanten Vergehen bis zu EUR 50.000, im Wiederholungsfall bis zu 100.000

3.1.3.1. Einrichtungsbezogene Einstufung statt dienstbezogener Betrachtung im NISG 2026

Eine pauschale Überleitung früherer Betreiber wesentlicher Dienste nach dem NISG 2018 in die neue NIS-2-Systematik wurde nicht vorgesehen.[23]

Das NISG 2026 löst sich von der bisherigen Betrachtung wesentlicher Dienste.[24] Die Einstufung erfolgt nicht mehr anhand einzelner wesentlicher Dienste, sondern „einrichtungsbezogen".[25] Es ergibt sich damit ein echter Systemwechsel.

> **Achtung: gesamte Einrichtung im NISG 2026**
>
> Die Qualifikation als wesentliche oder wichtige Einrichtung knüpft nicht mehr an einzelne Dienste an. Risikomanagementmaßnahmen und Berichtspflichten treffen die Einrichtung (die jeweilige juristische Person) grundsätzlich insgesamt und sind nicht auf deren wesentliche Dienste beschränkt.

Die konkreten Anforderungen gelten in der Einrichtung jedoch nicht gleichermaßen, sondern unterscheiden sich für einzelne Bereiche auf Grundlage der Risikoeinschätzung.[26]

23 ErläutRV NISG 2026 zu § 24, S 26.
24 ErläutRV NISG 2026 zu § 24, S 26.
25 § 24.
26 Vgl §§ 32, 34 NISG.

3.2. NIS-2-Richtlinie

3.2.1. Allgemeines

Die NIS-2-Richtlinie ist zusammen mit dem Cyber Resilience Act der wohl weitreichendste europäische Cybersicherheitsrechtsakt der Europäischen Union.[27]

Die NIS-2-Richtlinie verstärkt die Zusammenarbeit und die Rolle der EU-Agentur für Cybersicherheit (ENISA) bei der Unterstützung der Mitgliedstaaten in Fragen der Cybersicherheit. Es handelt sich bei NIS-2 um eine Weiterentwicklung und Ausweitung der NIS-Richtlinie, um auf die sich ständig ändernde Bedrohungslandschaft und die wachsende Bedeutung der Cybersicherheit in der EU zu reagieren.

3.2.2. Gründe für die Entstehung der NIS-2-Richtlinie

Die NIS-2-Richtlinie ist nicht als bloße Fortschreibung der ursprünglichen NIS-Richtlinie konzipiert, sondern als strukturelle Neuausrichtung des unionsrechtlichen Cybersicherheitsrahmens. Bei beiden Rechtsakten stützt sich der Unionsgesetzgeber auf Art 114 AEUV als Binnenmarktharmonisierungskompetenz. Die Überprüfung der NIS-Richtlinie hat jedoch gezeigt, dass die angestrebte Angleichung der nationalen Rechtsordnungen nur unzureichend erreicht wurde.[28]

Zentrale Ursache hierfür waren erhebliche Unterschiede in der nationalen Umsetzung.

Diese betrafen insbesondere

- den Anwendungsbereich,
- die Konkretisierung der Sicherheitsanforderungen,
- die Ausgestaltung der Meldepflichten sowie
- die Regelungen zu Aufsicht und Durchsetzung.

Der den Mitgliedstaaten eingeräumte Umsetzungsspielraum führte dazu, dass Einrichtungen mit grenzüberschreitender Tätigkeit mit uneinheitlichen und teilweise widersprüchlichen Anforderungen konfrontiert waren, was zusätzliche Kosten verursachte und die grenzüberschreitende Erbringung von Waren und Dienstleistungen erschwerte.[29]

Darüber hinaus hob der Unionsgesetzgeber richtigerweise hervor, dass Cybersicherheit aufgrund der Intensität des grenzüberschreitenden Austauschs keine rein nationale Angelegenheit mehr darstellt. Eine unangemessene Ausgestaltung oder Umsetzung von Cybersicherheitsanforderungen in einem Mitgliedstaat kann

27 *Vinzenz Heußler/Arno Spiegel/Jakob Zanol* in *Hysek* (Hrsg), Praxishandbuch Digital Operational Resilience Act|DORA (2025), 298.
28 Erwägungsgrund 4 NIS-2-RL.
29 Erwägungsgrund 4 NIS-2-RL.