MANZ – QUALITÄT SEIT 1849

03 | 2026 | 165–244 | ecolex

ecolex

FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT

Schwerpunkt

Schwerpunkt: NISG 2026

> Cybersicherheit
> Vergleich zum NISG 2018

Recht hören. Der ecolex-Podcast!

Flexibility Purchase Agreements

Corporate Social Responsibility 2.0

Politische Werbung: Infopflichten

UVP-Rückblick 2025

Interne Untersuchung

Cyber Resilience Act

ECOLEX.MANZ.AT

ISSN 1022-9418

MANZ

NISG Reloaded: Österreichs neuer Rechtsrahmen für Cybersicherheit

Anwendungsbereich, Pflichten und Sanktionssystem

BEITRAG. Nach einer neunmonatigen Legisvakanz tritt das NISG 2026[1] am 1. 10. 2026 in Kraft und begründet ein grundlegend neues Regulierungsregime für die Cybersicherheit in Österreich. Gleichzeitig tritt das bisherige NISG 2018[2] samt den zugehörigen Verordnungen[3] außer Kraft. Das Gesetz etabliert das Bundesamt für Cybersicherheit als zentrale Aufsichtsbehörde, erweitert den Anwendungsbereich erheblich und konkretisiert die Pflichten der betroffenen Einrichtungen. Erstmals verankert es eine ausdrückliche Verantwortung der Leitungsorgane für die Cybersicherheits-Governance. Zugleich führt es ein gestuftes Sanktionssystem ein, das empfindliche Geldbußen ermöglicht. Dieser Beitrag erläutert die maßgeblichen Eckpunkte zu Anwendungsbereich, Pflichten und Sanktionsregime. ecolex 2026/94

Mag. **Felix Schneider** ist Rechtsanwalt der Schönherr Rechtsanwälte GmbH.

A. Gesetzlicher Rahmen und Inkrafttreten

Das NISG 2026 dient der Umsetzung der NIS-2-RL[4] sowie der Durchführung der VO (EU) 2021/887 über das Europäische Kompetenzzentrum für Cybersicherheit.[5] Die Kundmachung erfolgte am 23. 12. 2025. Gem § 51 NISG 2026 treten alle Bestimmungen neun Monate nach Kundmachung mit dem nächstfolgenden Monatsersten in Kraft; das Gesetz gilt daher ab 1. 10. 2026.

Mit dem Inkrafttreten treten das NISG 2018 sowie die NISV und die QuaSteV außer Kraft. Verordnungen auf Grundlage des NISG 2026 können bereits seit dem Tag nach der Kundmachung erlassen werden; sie werden jedoch erst mit dem Inkrafttreten des Stammgesetzes wirksam.

Institutionell verankert das NISG 2026 das Bundesamt für Cybersicherheit als zuständige Behörde mit bundesweiter Zuständigkeit. Es ist unmittelbar dem BM für Inneres nachgeordnet. Diese neue Behörde übernimmt die Funktion einer zentralen Anlaufstelle, nimmt Koordinierungs- und Aufsichtsfunktionen wahr und vertritt Österreich in den einschlägigen unionsrechtlichen Gremien. Zugleich fungiert sie als nationales Koordinierungszentrum für Cybersicherheit.

Das nationale CSIRT[6] und die sektoralen CSIRTs werden in einen strukturierten Aufsichts- und Kooperationsverbund eingebettet. Für die koordinierte Offenlegung von Schwachstellen ist das nationale CSIRT zuständig. Übergangsweise nehmen das bisherige nationale CSIRT[7] sowie die nach dem NISG 2018 bestellten qualifizierten Stellen[8] definierte Aufgaben wahr.

B. Anwendungsbereich und Einstufung

Der sachliche Anwendungsbereich orientiert sich an der Systematik der NIS-2-RL. Er erfasst wesentliche und wichtige Einrichtungen in insg 18 Sektoren und Teilsektoren, die für grundlegende gesellschaftliche und wirtschaftliche Funktionen kritisch sind. Diese Sektoren sind in § 2 sowie in den Anl 1 und 2 zum NISG 2026 konkretisiert.

Die Einstufung als wesentliche oder wichtige Einrichtung folgt grundsätzlich einer Kombination aus Sektorzuordnung und Unternehmensgröße.

Die Einstufung als wesentliche oder wichtige Einrichtung folgt grds einer Kombination aus Sektorzuordnung und Unternehmensgröße. Wesentliche Einrichtungen[9] sind insb solche der in Anl 1 genannten Art, die ein großes Unternehmen betreiben. Anbieter öffentlicher elektronischer Kommunikationsnetze oder -dienste gelten bereits als wesentlich, wenn sie zumindest ein mittleres Unternehmen betreiben.

Unabhängig von ihrer Größe gelten stets als wesentliche Einrichtungen:

- qualifizierte Vertrauensdiensteanbieter,
- TLD-Namenregister,
- DNS-Diensteanbieter sowie
- Einrichtungen, die nach der CER-RL[10] als kritische Einrichtungen ermittelt wurden.

Ferner kann die Cybersicherheitsbehörde Einrichtungen größenunabhängig als wesentlich einstufen.[11]

Wichtige Einrichtungen sind Einrichtungen der in den Anl 1 und 2 genannten Art, die ein großes oder mittleres Unterneh-

1) Netz- und InformationssystemsicherheitsG 2026 (NISG 2026), BGBl I 2025/94.
2) Netz- und InformationssystemsicherheitsG (NISG), BGBl I 2018/111.
3) Netz- und InformationssystemsicherheitV (NISV), BGBl II 2019/215 sowie V über qualifizierte Stellen (QuaSteV), BGBl II 2019/226.
4) RL (EU) 2022/2555, ABl L 2022/333, 80.
5) VO (EU) 2021/887, ABl L 2021/202, 1.
6) Computer Security Incident Response Team.
7) Vgl § 51 Abs 6 NISG 2026.
8) Vgl § 51 Abs 7 NISG 2026.
9) Vgl § 24 Abs 1 NISG 2026.
10) RL (EU) 2022/2557, ABl L 2022/333, 164.
11) Vgl dazu § 26 NISG 2026.

men betreiben und nicht bereits als wesentliche Einrichtung gelten. Hinzu kommen größenunabhängig eingestufte Einrichtungen[12] sowie bestimmte Anbieter von Kommunikationsnetzen oder -diensten und Vertrauensdiensteanbieter.

Für Einrichtungen der öffentlichen Verwaltung bestehen besondere Regeln. Auf Bundesebene gelten Verwaltungseinheiten grds als wesentliche Einrichtungen; auf Landesebene als wichtige Einrichtungen.[13] Das Gesetz sieht jeweils spezifische Ausnahmen vor.

Die Abgrenzung großer und mittlerer Unternehmen erfolgt auf Grundlage der EU-KMU-Definition[14] und basiert auf einer kombinierten Betrachtung von Mitarbeiterzahl, Jahresumsatz und Bilanzsumme. Für die Anwendung des NISG 2026 werden die maßgeblichen Schwellenwerte gem § 25 konkretisiert und herangezogen. Ein großes Unternehmen liegt vor, wenn mind 250 Beschäftigte oder ein Jahresumsatz von über 50 Mio Euro bei gleichzeitig über 43 Mio Euro Bilanzsumme erreicht werden. Als mittleres Unternehmen gilt ein Unternehmen ab 50 Beschäftigten oder ab einem Jahresumsatz von über 10 Mio Euro bei einer Bilanzsumme von über 10 Mio Euro. Unter bestimmten funktionsbezogenen Voraussetzungen können verbundene Unternehmen und Partnerunternehmen bei der Schwellenwertprüfung unberücksichtigt bleiben.[15]

Für Einrichtungen, die in den Anwendungsbereich der DORA-VO fallen, gehen deren einschlägige Bestimmungen vor.

Das Gesetz enthält zudem Kollisions- und Territorialregeln. Für bestimmte Anbieter – namentlich etwa DNS-Dienste, TLD-Register, Cloud- und Rechenzentrumsdienste, CDN-Betreiber sowie Anbieter verwalteter Dienste und verwalteter Sicherheitsdienste – gelten besondere Anknüpfungsregeln an die Hauptniederlassung. Drittlandsansässige Anbieter, die Dienste in Österreich erbringen, müssen einen Zustellungsbevollmächtigten in der EU benennen; bei Unterlassung erfolgt die Durchsetzung unmittelbar nach österr Recht.[16]

Für Einrichtungen, die in den Anwendungsbereich der DORA-VO[17] fallen, gehen deren einschlägige Bestimmungen vor.[18] IKT-Drittdienstleister iSd DORA unterfallen zusätzlich dem NISG 2026.[19]

Kriterium	Wesentliche Einrichtung	Wichtige Einrichtung
Sektorbezug	Anlage 1 (Sektoren mit hoher Kritikalität)	Anlagen 1 und 2 (sonstige kritische Sektoren)
Unternehmensgröße	Großes Unternehmen; teils mittlere Unternehmen bei Kommunikationsnetzen/-diensten	Großes oder mittleres Unternehmen
Größenunabhängige Erfassung	u.a. qualifizierte Vertrauensdiensteanbieter, TLD-Register, DNS, kritische Einrichtungen (CER), behördliche Einstufung	u.a. behördliche Einstufung, Anbieter von Kommunikationsnetzen oder -diensten, Vertrauensdiensteanbieter
Öffentliche Verwaltung	Bundesebene grundsätzlich wesentlich; Landesebene wichtig (jeweils mit Ausnahmen)	Landesebene wichtig
DORA-Vorrang	ja, soweit einschlägig	ja, soweit einschlägig

Tabelle 1: Einstufung wesentliche vs wichtige Einrichtungen

C. Pflichten: Registrierung, Governance und Risikomanagement

1. Registrierungspflicht

Das NISG 2026 sieht ein Register der wesentlichen und wichtigen Einrichtungen vor. Dieses Register wird von der Cybersicherheitsbehörde geführt. Alle betroffenen Einrichtungen müssen der Behörde strukturierte Angaben elektronisch übermitteln.[20]

Die Erstregistrierung hat innerhalb von drei Monaten ab Inkrafttreten des Gesetzes zu erfolgen. Bei einem Inkrafttreten am 1. 10. 2026 endet diese Frist am 1. 1. 2027. Einrichtungen, die erst später in den Anwendungsbereich fallen, müssen sich binnen drei Monaten ab Erfüllung der Voraussetzungen registrieren.

2. Governance-Pflichten der Leitungsorgane

Die Governance-Pflichten[21] nach § 31 NISG 2026 adressieren ausdrücklich die Leitungsorgane. Prokuristen und Chief Information Security Officers (CISO) sind nicht unmittelbar normadressiert. Leitungsorgane sind ausdrücklich für die Sicherstellung und Überwachung der Risikomanagementmaßnahmen verantwortlich und haben eigene sowie betriebsweite Cybersicherheitsschulungen sicherzustellen.

Diese ausdrückliche Verankerung der Cybersicherheits-Governance auf der Leitungsebene ist sanktionsbewehrt. Sie spiegelt den Risikoverantwortungsansatz der NIS-2-RL wider und markiert eine wesentliche Neuerung gegenüber dem bisherigen Rechtsrahmen.

3. Risikomanagementmaßnahmen

Das Kernstück der operativen Pflichten bilden die Risikomanagementmaßnahmen nach § 32 NISG 2026. Sie müssen geeignet und verhältnismäßig sein, den Stand der Technik berücksichtigen und ein dem Risiko angemessenes Schutzniveau gewährleisten.

Das Gesetz verlangt einen gefahrenübergreifenden Ansatz. Dieser muss mind folgende Bereiche abdecken:

- Risikoanalyse und Informationssicherheitskonzepte,
- Bewältigung von Sicherheitsvorfällen,
- Notfall- und Krisenmanagement einschließlich Backup und Wiederherstellung,
- Sicherheit der Lieferkette,
- Security by Design mit Schwachstellenmanagement, Bewertung der Wirksamkeit, Cyberhygiene und Schulungen, Einsatz von Kryptografie sowie
- sichere Authentifizierungs- und Kommunikationsverfahren.

Die Cybersicherheitsbehörde kann nähere Anforderungen durch Verordnung festlegen. Sie kann ferner EU-Durchfüh-

12) Vgl § 24 Abs 2 NISG 2026.
13) Vgl § 24 Abs 3, 4, 5 und 6 NISG 2026.
14) Vgl Empfehlung der Kommission (2003/361/EG) betr die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen, ABl L 2003/124, 36.
15) Vgl § 25 Abs 4 NISG 2026.
16) Vgl § 28 Abs 2 NISG 2026.
17) VO (EU) 2022/2554, ABl L 2022/333, 1.
18) Vgl § 24 Abs 7 NISG 2026.
19) Vgl § 24 Abs 8 NISG 2026.
20) Vgl § 29 Abs 2 NISG 2026.
21) Vgl § 31 NISG 2026.

rungsrechtsakte auch sektorübergreifend für anwendbar erklären.

Für bestimmte digitale Sektoren – namentlich etwa DNS-Diensteanbieter, TLD-Register, Cloud-Anbieter, Rechenzentrumsdienste, CDN-Betreiber, Anbieter verwalteter Dienste und verwalteter Sicherheitsdienste – gilt die DurchführungsVO (EU) 2024/2690 der EK unmittelbar.[22)]

4. Nachweis der Wirksamkeit

Der Nachweis der Wirksamkeit erfolgt in gestufter Form. Innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht ist der Behörde eine strukturierte Selbstdeklaration zu übermitteln.[23)] Diese muss die implementierten Maßnahmen, die eingesetzten Systeme, die Lieferkettensicherheit und die Ergebnisse der Risikoanalyse umfassen.

Zusätzlich kann die Behörde eine Prüfung durch eine unabhängige Stelle verlangen. Der technische, operative und organisatorische Umsetzungsnachweis ist dann binnen zwei Jahren zu erbringen. Anerkannte gültige Zertifikate können die operative und organisatorische Umsetzung belegen. Für wesentliche Einrichtungen gelten nach Aufforderung verkürzte Fristen. Erste Aufforderungen zum externen Nachweis dürfen frühestens nach Ablauf von 2 Jahren ab Inkrafttreten des Gesetzes erfolgen.[24)]

D. Melderegeln und Incident-Handling

Erhebliche Cybersicherheitsvorfälle lösen ein gestuftes Meldewesen[25)] aus:

Zunächst ist unverzüglich, spätestens binnen 24 Stunden ab Kenntnis, eine Frühwarnung zu erstatten. Diese enthält eine Ersteinschätzung und Verdachtsmomente, insb hinsichtlich rechtswidriger Handlungen und grenzüberschreitender Auswirkungen. Sodann folgt eine strukturierte Vorfallmeldung binnen 72 Stunden mit einer aktualisierten Bewertung von Schweregrad und Auswirkungen sowie relevanten Kompromittierungsindikatoren.

Auf Ersuchen des CSIRT oder der Behörde sind Zwischenberichte zu erstatten. Spätestens einen Monat nach Abgabe der 72-Stunden-Meldung ist ein Abschlussbericht vorzulegen. Dieser muss eine vollständige Darstellung des Vorfalls, seiner Ursachen, der ergriffenen Maßnahmen und allfälliger grenzüberschreitender Aspekte enthalten. Bei noch andauernden Vorfällen ist anstelle des Abschlussberichts ein Fortschrittsbericht vorzulegen; der Abschlussbericht folgt dann binnen eines Monats nach Beendigung der Vorfallbehandlung.

Zusätzlich zur behördlichen Meldung müssen betroffene Einrichtungen grds ihre Diensteempfänger unverzüglich informieren und – soweit möglich – Abhilfemaßnahmen empfehlen.

Ein erheblicher Cybersicherheitsvorfall liegt vor, wenn der Vorfall schwerwiegende Betriebsstörungen oder finanzielle Verluste verursacht hat oder verursachen kann oder wenn er Dritte erheblich beeinträchtigt hat oder beeinträchtigen kann.[26)] Die Erheblichkeit ist daher bereits dann zu bejahen, wenn eine qualifizierte Gefährdungslage vorliegt.[27)] Bei der Beurteilung der Erheblichkeit sind ua Abhängigkeiten in anderen Sektoren, Auswirkungen auf Umwelt, öffentliche Ordnung und Gesundheit, Marktanteile, geografische Reichweite sowie technische Merkmale und betroffene Systeme zu berücksichtigen. Die Cybersicherheitsbehörde kann weitere Kriterien durch Verordnung festlegen.

Branchenspezifische Besonderheiten bestehen im Gesundheitssektor. Dort erstatten Einrichtungen ihre Meldungen an das Austrian HealthCERT. Diese Kanalisierung dient der Bündelung sektorspezifischer Expertise.[28)]

E. Aufsicht, Durchsetzung und Rechtsschutz

1. Aufsichtsinstrumente

Die Cybersicherheitsbehörde verfügt über ein abgestuftes Instrumentarium zur Aufsicht. Sie kann Kontrollen der Umsetzung von Risikomanagementmaßnahmen vor Ort oder aus der Ferne durchführen. Ferner ist sie befugt, Sicherheitsscans vorzunehmen, umfassende Informationen einschließlich dokumentierter Sicherheitskonzepte anzufordern und Zugang zu Daten, Dokumenten und sonstigen Informationen zu verlangen. Schließlich kann sie Ad-hoc-Prüfungen anordnen oder Prüfungen durch unabhängige Stellen begleiten.

Diese Aufsichtsinstrumente gelten für wesentliche und wichtige Einrichtungen gleichermaßen, wenngleich in unterschiedlicher Ausprägung. Die Eingriffsintensität ist bei wesentlichen Einrichtungen typischerweise höher.[29)]

2. Durchsetzungsinstrumente

Bei Verstößen stehen der Behörde wirksame Durchsetzungsinstrumente zur Verfügung. Sie kann erforderliche Maßnahmen mit Bescheid anordnen und Pflichtverletzungen öffentlich bekannt machen, um Risiken zu reduzieren. Gegenüber wesentlichen Einrichtungen kann sie befristet Überwachungsbeauftragte einsetzen, die die Umsetzung von Risikomanagement- und Meldepflichten sicherstellen.

Kommt eine wesentliche Einrichtung Anordnungen nicht fristgerecht nach, kann die Behörde bei zuständigen Stellen die Aussetzung von Genehmigungen oder Zertifikaten anregen. Bei der Auswahl der Maßnahmen hat die Behörde insb zu berücksichtigen: Schwere und Dauer des Verstoßes, Wiederholungscharakter, Schadensausmaß, Vorsatz oder Fahrlässigkeit, Kooperationsbereitschaft der Einrichtung sowie deren bisheriger Compliance-Stand.

3. Rechtsschutz

Der Rechtsschutz gegen behördliche Maßnahmen ist gewährleistet. Gegen Bescheide der Cybersicherheitsbehörde steht die Beschwerde an das BVwG offen. Gegen Bescheide der Bezirksverwaltungsbehörden, die für die Verhängung von Geldstrafen zuständig sind, ist die Beschwerde an die LVwG vorgesehen.[30)]

---

22) DurchführungsVO (EU) 2024/2690, ABl L 2024/2690, 1.
23) Vgl § 33 Abs 1 NISG 2026.
24) Vgl § 33 Abs 2 NISG 2026.
25) Vgl § 34 NISG 2026.
26) Siehe dazu auch *Drolz*, Mögliche Konsequenzen sowie Prävention eines Cyber-Vorfalls, GRCaktuell 2023, 49.
27) Es ist daher davon auszugehen, dass die Abgrenzung zw meldepflichtigen und nicht meldepflichtigen Vorfällen in der praktischen Anwendung mit erheblichen Auslegungsfragen verbunden sein wird.
28) Vgl § 8a GTelG 2012.
29) Vgl §§ 38f NISG 2026.
30) Vgl § 41 Abs 1 und 2 NISG 2026.

F. Sanktionsregime und Verantwortlichkeit

1. Zuständigkeit und Unternehmensverantwortlichkeit

Die Verhängung von Verwaltungsstrafen obliegt den Bezirksverwaltungsbehörden. Die Cybersicherheitsbehörde hat diese bei Verdacht eines Verstoßes zu befassen. Das Gesetz sieht eine ausdrückliche Unternehmensverantwortlichkeit vor: Juristische Personen und eingetragene Personengesellschaften können bestraft werden, wenn Verstöße durch Leitungspersonen begangen wurden oder wenn mangelhafte Aufsicht durch Leitungspersonen die Verstöße ermöglicht hat.

Eine Doppelbestrafung mit Geldbußen nach der DSGVO wird vermieden. Bei der Strafbemessung sind die im Durchsetzungsregime genannten Faktoren zu berücksichtigen.

2. Strafdrohungen

Die Höchststrafen orientieren sich an der Einstufung der betroffenen Einrichtung.[31] Für wesentliche Einrichtungen betragen sie bis zu 10 Mio Euro oder bis zu 2% des weltweiten Vorjahresumsatzes, wobei der jeweils höhere Betrag maßgeblich ist. Für wichtige Einrichtungen liegen die Höchststrafen bei bis zu 7 Mio Euro oder bis zu 1,4% des weltweiten Vorjahresumsatzes.

3. Tatbestände

Die Höchststrafen können bei folgenden Verstößen verhängt werden: unterlassene Schulungen von Leitungsorganen und Beschäftigten, Nichtumsetzung von Risikomanagementmaßnahmen, Verstöße gegen Melde- und Berichtsfristen sowie die Nichtbefolgung behördlicher Durchsetzungsanordnungen.

Daneben sieht § 45 Abs 4 NISG 2026 eigenständige Tatbestände mit einer Strafdrohung bis € 50.000,– vor; im Wiederholungsfall bis € 100.000,–. Erfasst sind etwa verspätete oder unrichtige Registrierungen, die Vereitelung von Kontrollen, die Nichtbereitstellung angeforderter Informationen oder die Behinderung eines Überwachungsbeauftragten.

4. Sonderregime für die öffentliche Verwaltung

Für Behörden und sonstige Stellen der öffentlichen Verwaltung – einschließlich in Privatrechtsform organisierter Verwaltungseinheiten – gilt ein gesondertes, verfassungsrechtlich abgesichertes Regime ohne Geldstrafen.[32] Bei Nichteinhaltung der Verpflichtungen hat die Bezirksverwaltungsbehörde den Verstoß festzustellen und eine Frist zur Herstellung des rechtmäßigen Zustands zu setzen. Erfolgt die Herstellung nicht fristgerecht, ist die Nichteinhaltung öffentlich bekannt zu machen, sofern dem keine überwiegenden öffentlichen Interessen entgegenstehen.

G. Zeitliche Roadmap und praktische Implikationen

Für die Praxis ist die zeitliche Staffelung der Pflichten zentral. Mit dem Inkrafttreten am 1. 10. 2026 beginnt die dreimonatige Frist zur Erstregistrierung; sie endet daher am 1. 1. 2027. Innerhalb von zwölf Monaten nach Eintritt der Registrierungspflicht – also bis 1. 10. 2027 – ist die Selbstdeklaration zu übermitteln. Eine erste behördliche Aufforderung zum externen Umsetzungsnachweis darf frühestens zwei Jahre nach Inkrafttreten – also ab 1. 10. 2028 – erfolgen; die Vorlage ist dann binnen zwei Jahren zu erbringen, für wesentliche Einrichtungen nach Aufforderung teilweise binnen zwei Monaten.

Diese Staffelung ermöglicht angemessene Implementierungs- und Testzyklen. Sie verlangt allerdings frühzeitige Gap-Analysen und die Abstimmung mit Branchenstandards.

Praxistipp

- Das Gesetz verlangt einen integrierten Sicherheitslebenszyklus. Leitungsorgane müssen Verantwortung übernehmen, regelmäßige Schulungen sicherstellen und den Nachweis der Wirksamkeit aktiv unterstützen. Die Pflichten zu Lieferkettensicherheit, Security by Design und sicherer Authentifizierung erfordern belastbare Prozesse für das Third-Party-Risk-Management und technische Mindeststandards.
- Das Meldewesen mit Frühwarnung, Vorfallmeldung und Abschlussbericht verlangt erprobte Reaktionspläne, abgestimmte Kommunikationswege und verlässliche Dokumentationsprozesse. Sektorspezifisch empfiehlt sich die frühzeitige Einbindung der brancheneigenen CSIRT. Im Gesundheitswesen sollte die prozessuale Anbindung an das Austrian HealthCERT vorbereitet werden, um Doppelgleisigkeiten zu vermeiden.
- Drittlandsansässige Anbieter ohne EU-Niederlassung müssen einen Zustellungsbevollmächtigten in Österreich oder einem anderen MS benennen. Andernfalls drohen unmittelbare nationale Aufsichts- und Durchsetzungsmaßnahmen.
- Schließlich sollten Unternehmen die Möglichkeit eur Zertifizierungsschemata im Blick behalten. Eine rechtzeitige Prüfung geeigneter Zertifizierungen kann den späteren Nachweisaufwand erheblich reduzieren.

Schlussstrich

Das NISG 2026 markiert eine grundlegende Neuausrichtung der österr Cyberregulierung. Es verbindet einen weiten, risikobasierten Anwendungsbereich mit konkretisierten Pflichten und scharfen Durchsetzungsmechanismen. Die ausdrückliche Verankerung der Cybersicherheitsverantwortung auf Leitungsebene unterscheidet das neue Regime deutlich von seinem Vorgänger.

Die zeitliche Architektur – Inkrafttreten am 1. 10. 2026, Registrierung bis 1. 1. 2027, Selbstdeklaration binnen zwölf Monaten, gestufte Nachweissystematik – schafft einerseits Planungssicherheit, andererseits einen ambitionierten Umsetzungsfahrplan.

Offene Fragen betreffen die angekündigten Detailverordnungen der Cybersicherheitsbehörde, sektorspezifische Konkretisierungen und die Nutzung eur Durchführungsrechtsakte. Unternehmen sollten diese Rechtsentwicklung frühzeitig in ihre Compliance-Planung einbeziehen. Wer jetzt Governance-, Risiko- und Lieferkettenprozesse konsolidiert, Melde- und Untersuchungskapazitäten aufbaut und Nachweissysteme etabliert, wird die behördlichen Anforderungen nicht nur erfüllen, sondern Cybersicherheit als Führungsaufgabe nachhaltig verankern.

[31] Vgl insb § 45 NISG 2026.
[32] Vgl § 46 NISG 2026.