2/2026
25 – 48

Kurzmeldung
Digital Omnibus
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

NIS-2 – spät, aber doch!

NIS-2 Umsetzung und Entwicklungen in der Cybersecurity

Interview mit Otmar Lendl, cert.at.

NISG 2026: Neues und Altbekanntes

Rainer Knyrim, Gregor Brandstetter

Checkliste NISG 2026

Hans-Jürgen Pollirer

Bereits erstes Auskunftsbegehren kann exzessiv sein

Martin Baumann, Felix Mikolasch

Judikaturüberblick: Datenschutz von juristischen Personen

Janos Böszörmenyi, Denise Stahleder

VwGH: Rechtmäßigkeit Videoüberwachungen Privater muss sich aus DSGVO ergeben

Viktoria Haidinger, Michael Löffler

BVwG: Auskunftsrecht umfasst keine spezifischen Suchmethoden

Viktoria Haidinger, Michael Löffler

ISSN 2313-5409

dako.manz.at

MANZ


Rainer Knyrim
Gründer und Partner bei Knyrim Trieb Rechtsanwälte OG


Gregor Brandstetter
Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte OG

NISG 2026: Neues und Altbekanntes

Netz- und Informationssystemsicherheitsgesetz 2026; NIS-2-RL; Risikomanagement; Gefahrenabwehr. Als verfrühtes Weihnachtsgeschenk an alle CISOs und sonst mit Cybersicherheit Befassten wurde am 23. 12. 2025 mit BGBl I 2025/94 die österr Umsetzung der NIS-2-RL,[1] das NISG 2026, verlautbart. Es tritt mit dem nach Ablauf von neun Monaten ab Kundmachung folgenden Monatsersten in Kraft, also dem 1. 10. 2026.[2] Das NISG 2026 enthält im Vergleich zum NISG – der noch in Kraft stehenden Umsetzung der NIS(-1)-RL – viel Neues, aber auch Altbekanntes.

Bei einem ersten Blick stößt man auf Vertrautes: Erfasste Einrichtungen müssen

- (1) prüfen und deklarieren, ob und wieso sie unter das Regime des NISG 2026 fallen,
- (2) Risikomanagementmaßnahmen implementieren,
- (3) bestimmte Sicherheitsvorfälle melden und
- (4) ihre Governance-Strukturen anpassen.

Diese Pflichten sollen im Folgenden überblicksartig – also ohne Anspruch auf Vollständigkeit, dafür aber auf Verständlichkeit – dargestellt werden.

Anwendungsbereich und Registrierung

Grundsätzlich ist es das Ziel des Richtliniengebers, bestimmte (**für die Gesellschaften wichtige) Sektoren besonders zu schützen**. Die alte Liste mit sieben Sektoren (und einer Auffangkategorie) wird zu diesem Zweck auf 18 Sektoren ausgeweitet. Die erfassten Sektoren reichen gem § 2 NISG 2026 von Energie über Verkehr, Bankwesen, Gesundheitswesen, Digitale Infrastruktur, Abfallbewirtschaftung, Forschung, chemische Stoffe, Lebensmittel, Handel und Warenherstellung bis hin zum Weltraum. In den Anl 1 und 2 zum NISG 2026 finden sich weiterführende **Informationen zur Abgrenzung** der einzelnen Sektoren, leider oft abermals mit Verweisen auf verschiedenstes Materienrecht. Da auch der in der digitalisierten Gesellschaft stetig an Bedeutung gewinnende Betrieb von Rechenzentren und Cloud-Computing-Diensten, die in Konzernstrukturen von einer darauf spezialisierten Tochter erbracht werden,[3] erfasst ist, werden oft Unternehmen in weiteren Branchen und Tätigkeitsfeldern vom Regime erfasst sein.

Neben diesem „qualitativen Element", also der Beurteilung des Tätigkeitsfeldes einer Einrichtung, ist auch ein **„quantitatives Element"** zu prüfen. Vom Anwendungsbereich erfasst sind nämlich nur Einrichtungen, die ein mittleres oder großes Unternehmen iSd entsprechenden Empfehlung der EK zur Definition vom KMU[4] betreiben.

Hinweis

Ein mittleres Unternehmen ist ein solches, das entweder 50 oder mehr Mitarbeitende beschäftigt oder dessen Jahresumsatz und Jahresbilanz 10 Mio Euro oder mehr beträgt.

Dabei sind die Zahlen verbundener Unternehmen und Partnerunternehmen (ggf anteilig entsprechend den jeweiligen Beteiligungen) hinzuzurechnen. Bei Unternehmen, die konsolidierte Jahresabschlüsse erstellen, wird die Verbundenheit angenommen. Diesfalls können die Zahlen des konsolidierten Jahresabschlusses herangezogen werden.

UA nach **problematisch** ist der **Ausnahmetatbestand** des § 25 Abs 4 NISG 2026. In diesem wird bestimmt, dass die Zahlen von Partner- oder verbundenen Unternehmen dann nicht miteinzubeziehen sind, wenn das Zielunternehmen (also jenes konkret zu prüfende Unternehmen) *„organisatorisch, technisch und operativ unabhängig"* von den Partner- oder verbundenen Unternehmen ist. In den Erläut wird dazu ausgeführt, dass diese Ausnahme der „Öffnungsklausel" in ErwGr 16 entspricht. In diesem ErwGr wird festgehalten, dass der **Grad der Unabhängigkeit** gegenüber Partner- und verbundenen Unternehmen **berücksichtigt** werden kann. Das

[1] RL 2022/2555/EU des EP und des Rates vom 14. 12. 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der VO (EU) 910/2014 und der RL 2018/1972/EU sowie zur Aufhebung der RL 2016/1148/EU (NIS-2-RL). [2] § 51 NISG 2026. [3] Vgl *Knyrim/Briegl*, NIS-2: die Anwendung im Konzern, Dako 2024/39. [4] Empfehlung (2003/361/EG) der EK vom 6. 5 2023 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen.

Problem daran ist, dass der EuGH in der Rs *Karen Millen Fashion* erkannt hat, *„dass die Begründungserwägungen eines Gemeinschaftsrechtsakts rechtlich nicht verbindlich sind und weder herangezogen werden können, um von den Bestimmungen des betreffenden Rechtsakts abzuweichen, noch, um diese Bestimmungen in einem Sinne auszulegen, der ihrem Wortlaut offensichtlich widerspricht“*.[5] Da Art 2 Abs 1 NIS-2-RL aber unzweideutig festhält, dass der Anwendungsbereich sich auf mittlere und große Unternehmen iSd Empfehlung erstreckt, kann davon uA nach nicht mit Verweis auf einen ErwGr abgewichen werden.

Neu ist im NISG 2026 die Schaffung einer eigenen Cybersicherheitsbehörde.

Wenn jedenfalls die „passende“ Kategorie gefunden ist, hat sich die Einrichtung gem § 29 Abs 2 NISG 2026 bei der zuständigen **Cybersicherheitsbehörde** zu registrieren. Neu ist im NISG 2026 auch die Schaffung einer eigens zuständigen Behörde. Momentan ist eine Abteilung des BMI zuständig, dies sollte dem alten NISG-2024-Entwurf[6] folgend auch ursprünglich beibehalten werden. Die Registrierung muss innerhalb von drei Monaten ab Inkrafttreten, also bis zum 1. 1. 2027, mittels Eingabe in ein über das Unternehmensserviceportal abrufbares Online-Formular erfolgen. Die Erläut bringen dazu ein Online-Formular ins Spiel. Nach der Registrierung sind auch Änderungen binnen drei Monaten ab Tag der Änderung zu melden. Verstöße gegen Registrierung und Bekanntgabe von Änderungen sind mit Geldstrafe in Höhe von bis zu € 50.000,– und im Wiederholungsfall bis zu € 100.000,– strafbewehrt.

Risikomanagementmaßnahmen und Selbstdeklaration

Auch im NISG 2026 nimmt die Verpflichtung zur Herstellung eines hohen Sicherheitsniveaus durch technische, operative und organisatorische Maßnahmen eine zentrale Stellung ein. Diese allgemeine Pflicht wird durch den **Katalog verpflichtender Inhalte** in § 32 Abs 4 NISG 2026 konkretisiert. Dabei sind wieder „alte Bekannte“ wie die Pflicht zur Durchführung von Risikoanalysen oder zur Einrichtung bestimmter Prozesse zur Bewältigung von Cybersicherheitsvorfällen. Nicht gänzlich neu, aber definitiv als moderne Schwerpunkte erkennbar sind das erweiterte Lieferkettenmanagement sowie die Pflicht zur Cyberhygiene und zur Implementierung von Mehrfaktor-Authentifizierungen.

Zu den Risikomanagementmaßnahmen sind für bestimmte Arten von Einrichtungen spezifische Regelungen in der **Durchführungsverordnung** 2024/2690 der EK (in der Folge „DurchführungsVO“)[7] zu finden. Weitere Durchführungsrechtsakte können durch die EK erlassen werden.

Praxistipp

Unternehmen kann weiterhin eine Orientierung an der Norm ISO 27001 und dem Österreichischen Informationssicherheitshandbuch empfohlen werden (www.sicherheitshandbuch.gv.at/).

Innerhalb von zwölf Monaten ab Eintritt der Registrierungspflicht sind der Cybersicherheitsbehörde Informationen zu den umgesetzten Risikomanagementmaßnahmen, insb hinsichtlich der genutzten Netz- und Informationssysteme, und der Sicherheit der Lieferketten als **Selbstdeklaration** zu übermitteln. Die technische, operative und organisatorische **Umsetzung der Risikomanagementmaßnahmen** ist der Cybersicherheitsbehörde von wichtigen Einrichtungen **binnen zwei Jahren** nach Aufforderung inklusive einer durchgeführten Prüfung nachzuweisen, wobei die Prüfung nicht länger als zwei Jahre zurückliegen darf. Wesentliche Einrichtungen müssen die operative sowie organisatorische Umsetzung der Risikomanagementmaßnahmen innerhalb von zwei Monaten, die technische Umsetzung innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde nachweisen. Die ersten Aufforderungen dürfen ab 1. 10. 2028 erteilt werden. Die **Nichtumsetzung** von Risikomanagementmaßnahmen ist mit **Geldstrafe** von bis zu 10 Mio Euro für wesentliche und 7 Mio Euro für wichtige Einrichtungen zu ahnden. Das Unterlassen der Selbstdeklaration ist mit Strafe iHv € 50.000,– bzw € 100.000,– im Wiederholungsfall bedroht.

Berichts- und Meldepflichten bei erheblichen Cybersicherheitsvorfällen

Wie schon bisher sollen nicht alle Cybersicherheitsvorfälle (vormals Sicherheitsvorfälle) eine Meldepflicht auslösen, sondern nur jene, deren Folgen eine gewisse **Erheblichkeit** – sei es in Bezug auf die Einrichtung selbst oder Dritte – erreichen.

Dabei unterscheidet das NISG 2026 zwischen Beinahe-Cybersicherheitsvorfällen, Cybersicherheitsvorfällen und erheblichen Cybersicherheitsvorfällen (s blaue Rechtecke in Abb 1, Seite 30) und nicht so eindeutig zwischen unerheblichen Cybersicherheitsvorfällen und (normalen?) Cybersicherheitsvorfällen (siehe farbloses Rechteck in Abb 1, Seite 30).

In einem ersten Schritt ist jedenfalls zu prüfen, ob ein Ereignis eine **tatsächliche Beeinträchtigung** von *„Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind“*[8] zur Folge hatte.

[5] EuGH 19. 6. 2014, C-345/13, *Karen Millen Fashion*, Rn 31.
[6] ME NISG 2024, 326/ME 27. GP. [7] VO (EU) 2024/2690 DurchführungsVO der EK. [8] § 3 Z 20 NISG 2026.

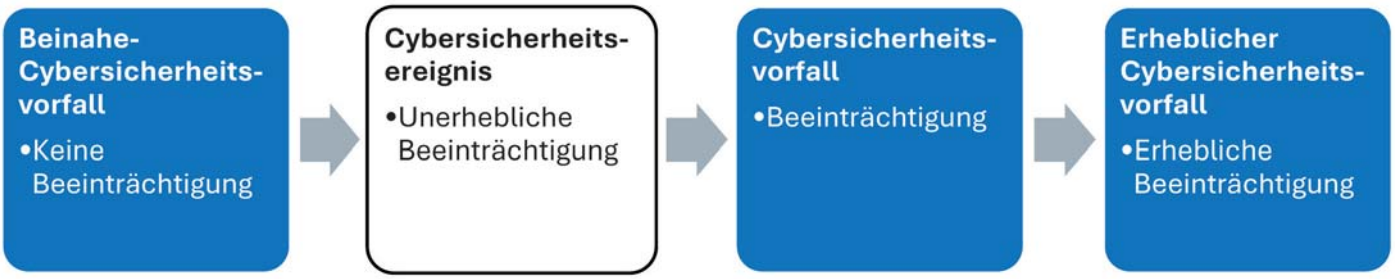

Abb 1: Kategorien von Ereignissen

„**Verfügbarkeit**“ meint dabei, dass die Daten oder Dienste zugriffsbereit bzw betriebsbereit sind und die Nutzer diese verwenden können. Sind Daten bspw nicht abrufbar oder ein Dienst nicht nutzbar, ist (unabhängig von der Dauer) von einem Cybersicherheitsvorfall auszugehen. Der Begriff „**Authentizität**“ meint, dass die Echtheit bzw der Ursprung von Daten und Diensten nachweisbar ist. Gemeint sind damit uA nach Situationen, in denen falsche oder fremde Daten oder Dienste im Netz- und Informationssystem abrufbar sind. In diesen Fällen wird auch immer eine Beeinträchtigung der Integrität vorliegen. **Integrität** meint dabei die Unversehrtheit von Daten und Diensten. Typische Beeinträchtigungen liegen vor, sobald Daten und Dienste durch Angriffe oder technische bzw menschliche Fehler manipuliert oder beschädigt wurden. Zuletzt bedeutet „**Vertraulichkeit**“, dass Daten und Dienste nicht von dazu nicht berechtigten Personen gelesen oder genutzt wurden. Jede Offenlegung gegenüber Unberechtigten ist dabei eine Beeinträchtigung (sollten personenbezogene Daten von einer Beeinträchtigung der Vertraulichkeit betroffen sein, können dadurch auch die Meldepflichten der Art 33, 34 DSGVO ausgelöst werden).

Wurde die Beeinträchtigung abgewehrt oder trat sie aus anderen Gründen nicht ein, handelt es sich bloß um einen **Beinahe-Cybersicherheitsvorfall**. Es besteht in diesem Fall keine Meldepflicht. Es können aber einerseits **freiwillige Meldungen** gem § 37 NISG 2026 abgegeben werden und andererseits gem § 36 NISG 2026 mit anderen Einrichtungen Vereinbarungen über den Austausch von Informationen zur Cybersicherheit geschlossen werden. Kam es zu einer solchen Beeinträchtigung, ist im Prüfschema zur Meldepflicht fortzufahren.

Dabei fällt leider der Blick schnell auf die Erläut zur **Definition von „Cybersicherheitsvorfall“**, in denen ergänzend ausgeführt wird, dass bei der Beurteilung, ob ein Cybersicherheitsvorfall vorliegt, *„insb die Anzahl der betroffenen Nutzer, die Dauer der Störung, die geografische Ausbreitung der Störung sowie die Auswirkung auf wirtschaftliche oder gesellschaftliche Tätigkeiten zu berücksichtigen“* sind (s farbloses Rechteck in Abb 1, Seite 30). Mit dieser Wortfolge wird offensichtlich auf die Definition von „Sicherheitsvorfall“ des NISG rekurriert. Im NISG waren diese Aspekte bei der Prüfung der Erheblichkeit eines Sicherheitsvorfalls zu berücksichtigen (vgl § 3 Z 6 NISG). Dieser **Rückgriff auf die Definition der alten Rechtslage** ist insofern **problematisch**, als § 35 NISG 2026 eigene Kriterien für die Erheblichkeit nennt, die nicht deckungsgleich mit jenen nach NISG sind. Insb ist die Dauer der Störung (bis auf manche von der DurchführungsVO erfasste Sektoren) nicht beachtlich. MaW kann sich eine Einrichtung bei Unterlassen der Meldepflicht nicht darauf berufen, die (tatsächliche) Beeinträchtigung hätte nur kurz angedauert. Die diesbezüglichen Ausführungen der Erläut haben also unangewendet zu bleiben. Die Schaffung einer vierten Kategorie (s farbloses Rechteck in Abb 1, Seite 30) war vom Gesetzgeber uA nach nicht gewollt.

Vielmehr hat nach der Prüfung der Beeinträchtigung und der entsprechenden Unterscheidung zwischen einem Beinahe-Cybersicherheitsvorfall und einem Cybersicherheitsvorfall **nur mehr die Erheblichkeit beurteilt** zu werden. Diese soll – der allgemeinen Umschreibung in § 35 Abs 1 NISG 2026 nach – bei schwerwiegenden Betriebsstörungen und/oder erheblichen materiellen oder immateriellen Schäden der Einrichtung oder Dritter gegeben sein. Die DurchführungsVO nennt etwas dramatisch den Tod einer natürlichen Person als Beispiel.

Hinweis

Wichtig ist, dass bereits die Eignung zur Verursachung solcher Störungen und Schäden ausreicht, um eine Meldepflicht auszulösen!

Da diese allgemeine Beschreibung noch wenig aussagekräftig ist, legen einerseits § 35 Abs 2 NISG 2026 und andererseits die DurchführungsVO weitere spezielle Kriterien fest, anhand derer das Vorliegen einer der Tatbestände nach § 35 Abs 1 NISG 2026 beurteilt werden kann. Im Ergebnis besteht somit ein durchaus umfassender Kriterienkatalog.

Praxistipp

Zur Bändigung des Katalogs wird empfohlen, die für eine spezifische Einrichtung anwendbaren Kriterien in eine tabellarische Übersicht zu überführen, die Zeile für Zeile „abgearbeitet“ werden kann. So kann verhindert werden, im Anlassfall verschiedene Rechtsquellen erst erschließen zu müssen.

Sollte man zu dem Ergebnis kommen, dass ein erheblicher Sicherheitsvorfall vorliegt, löst dies die Meldepflicht gem § 34 NISG 2026 aus. Die Meldepflicht besteht dabei primär gegenüber den nach § 8 NISG 2026 eingesetzten (sektorspezifischen oder nationalen) **Computer-Notfallteams** („CSIRTs“), welche die Meldungen an die Cybersicherheitsbehörde weiterleiten. Der Meldung angeschlossen werden kann ein Ersuchen, der betroffenen Einrichtung Orientierungshilfen (auch hinsichtlich der Einbindung von Strafverfolgungsbehörden), operative Beratung für die Durchführung möglicher Abhilfemaßnahmen oder technische Unterstützung bereitzustellen.

Nur soweit der Cybersicherheitsvorfall auch den von der betroffenen Einrichtung erbrachten Dienst beeinträchtigt, sind ebenfalls die **Empfänger dieses Dienstes zu informieren** (§ 34 Abs 3 NISG 2026). Wenn möglich, sind den Empfängern auch Maßnahmen mitzuteilen, die sie als Reaktion auf eine ggf bestehende Bedrohung ergreifen können.

Der verpflichtende Inhalt der Meldung an die CSIRT ist in § 34 Abs 2 NISG 2026 festgehalten. **Verstöße** gegen die Meldepflichten sind mit **Geldstrafe** von bis zu 10 Mio Euro für wesentliche und 7 Mio Euro für wichtige Einrichtungen zu ahnden.

Governance-Pflichten und Haftung des Leitungsorgans

Mit dem NISG 2026 steht endgültig fest, dass Cybersicherheit kein reines IT-Thema mehr ist. § 31 Abs 1 NISG 2026 normiert die Verantwortlichkeit der Leitungsorgane erfasster Einrichtungen. Leitungsorgane sind die nach außen zur Führung der Geschäfte einer Einrichtung Berufenen. Die Erläut halten fest, dass davon die **Personen auf Geschäftsführungs- und Vorstandsebene umfasst** sind. Keine Leitungsorgane sind Prokuristen oder der CISO.

Bei Verstößen gegen die Aufsichtspflichten kommt die Verantwortlichenhaftung nach § 9 VStG zur Anwendung.

Die **Pflichten der Leitungsorgane** umfassen die Sicherstellung und Beaufsichtigung der Einhaltung der Risikomanagementmaßnahmen sowie die Teilnahme an einschlägigen Schulungen, die die Einrichtungen den Mitarbeitern anzubieten haben.

Auch wenn Art 20 NIS-2-RL vorsieht, dass Leitungsorgane bei **Verstößen gegen ihre Aufsichtspflichten** nach diesem Artikel (umgesetzt in § 31 NISG 2026) verantwortlich gemacht werden können, hat sich der österr Gesetzgeber gegen das Vorsehen einer Verwaltungsstrafe für Leitungsorgane bei Verstößen gegen die sie treffenden Pflichten entschieden. Die Erläut zu § 45 NISG 2026 bestätigen aber, dass die **Verantwortlichenhaftung nach § 9 VStG** zur Anwendung kommt. Für Behörden und sonstige Stellen der öffentlichen Verwaltung einschließlich der Gebietskörperschaften sowie in Formen des Privatrechts eingerichtete Stellen der öffentlichen Verwaltung[9] gibt es ein alternatives Haftungsregime, nach welchem keine Geldstrafen verhängt werden können, sondern in letzter Konsequenz die zuständige Bezirksverwaltungsbehörde die Nichteinhaltung veröffentlicht. Ob dieses Vorgehen effektiv die Einhaltung sicherstellen wird, bleibt abzuwarten.

Fazit und Handlungsempfehlung

Dem NISG 2026 unterliegen deutlich mehr Branchen als bisher. Ebenso unterliegen die Leitungsorgane der erfassten Einrichtungen nun explizit der Verantwortung und einer Schulungspflicht. Das NISG 2026 sieht verschiedene Risikomaßnahmen, eine Selbstdeklaration sowie eine Prüf- und Nachweispflicht zu diesen vor. Weiters ermöglicht es einen freiwilligen Informationsaustausch zwischen Einrichtungen über Cybersicherheitsbedrohungen auf Basis entsprechender Vereinbarungen. Zur Vorbereitung auf das Inkrafttreten am 1. 10. 2026 sollten Unternehmen daher nun insb folgende **Handlungsempfehlungen** umsetzen:

- Prüfen Sie die Anwendbarkeit des NISG 2026 auf Ihr Unternehmen. Beachten Sie dabei Partner- und verbundene Unternehmen.
- Aktualisieren Sie Ihre Risikomanagementmaßnahmen und bereiten Sie die Selbstdeklaration vor.
- Führen Sie Schulungen der Mitarbeiter und Leitungsorgane durch.
- Bereiten Sie den Prüfablauf bei Verdacht auf einen Cybersicherheitsvorfall, insb durch Zusammenstellung der anwendbaren Kriterien, vor.
- Machen Sie sich mit den anwendbaren Fristen und Sanktionen vertraut. Versuchen Sie abzuschätzen, welche Maßnahmen die Cybersicherheitsbehörde Ihrem Unternehmen allenfalls auftragen könnte.
- Schließen Sie mit anderen Einrichtungen Vereinbarungen über den freiwilligen Informationsaustausch zu Cybersicherheitsbedrohungen.

Dako 2026/14

[9] Obacht ist in der Privatwirtschaftsverwaltung insofern geboten, als dort keine Amtshaftung besteht. Sollten also die anderen eine Schadenersatzpflicht begründeten Voraussetzungen vorliegen, haftet grundsätzlich das Organ selbst.

Zum Thema

Über die Autoren

Dr. Rainer Knyrim ist Gründer und Partner bei Knyrim Trieb Rechtsanwälte OG. Mag. Gregor Brandstetter, BA, ist Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte OG.
E-Mail: kt@kt.at