DriveLock

NIS-2 & NISG 2026

Ausgangslage

Mit der NIS-2-Richtlinie (EU 2022/2555) reagiert die Europäische Union auf eine deutlich verschärfte Cyberbedrohungslage. Ziel ist ein **einheitlich hohes Cybersicherheitsniveau** in allen Mitgliedstaaten. Die Richtlinie erweitert den Geltungsbereich erheblich, verschärft Pflichten und fordert Verantwortung explizit von der **Management- und Leitungsebene** ein.

Österreich hat diese Vorgaben durch das **Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026)** umgesetzt, das das bisherige NISG 2018 ablöst.

Zeitliche Eckdaten (Österreich)

- **Inkrafttreten:** 1. Oktober 2026
- **Registrierung bei der Behörde:** bis spätestens 31. Dezember 2026
- **Selbstdeklaration:** innerhalb von 12 Monaten nach Registrierung

Wichtig: Zum Stichtag müssen die zentralen technischen, organisatorischen und operativen Maßnahmen bereits wirksam umgesetzt sein.

Wer ist betroffen?

Das NISG 2026 umfasst deutlich mehr Organisationen als bisher.
Betroffen sind **öffentliche und private Einrichtungen** aus:

- **Anlage 1 – Sektoren mit hoher Kritikalität**
  (z. B. Energie, Verkehr, Bankwesen, Gesundheitswesen, digitale Infrastruktur, öffentliche Verwaltung)

- **Anlage 2 – weitere kritische Sektoren**
  (z. B. produzierendes Gewerbe, Chemie, Post- und Kurierdienste, Abfallwirtschaft, Lebensmittel)

Die Einordnung als **„wesentliche" oder „wichtige" Einrichtung** erfolgt anhand von **Sektor und Unternehmensgröße** (EU-KMU-Schwellenwerte).
Zusätzlich gibt es **größenunabhängige Sonderfälle** (z. B. Vertrauensdienste) sowie eine relevante **indirekte Betroffenheit über Lieferketten und IT-Dienstleister.**

Governance & Verantwortung der Leitung

Ein zentrales Element von NIS-2 / NISG 2026 ist die persönliche Verantwortung der Management- und Leitungsebene:

- Management- und Leitungsebenen müssen die Umsetzung der Cybersicherheitsmaßnahmen **aktiv überwachen**
- Eine reine Delegation an IT oder Security reicht nicht mehr aus
- **Verpflichtende Cybersicherheitsschulungen** für Management- und Leitungsebenen sind vorgesehen
- Governance-Pflichten sind **haftungsrelevant**

Cybersicherheit wird damit klar als **Management- und Organisationsthema** positioniert.

Risikomanagement & Meldepflichten

Das Gesetz definiert zehn zentrale Mindestmaßnahmen im Bereich Cybersicherheit (Art. 21 Abs. 2), u. a.:

- Risikoanalyse und Incident Management
- Business Continuity & Krisenmanagement
- Lieferkettensicherheit
- Zugriffskontrolle & Multi-Faktor-Authentifizierung
- Schulungen & Awareness
- Einsatz von Kryptografie und Verschlüsselung

Bei erheblichen Cybervorfällen gelten klare Meldefristen:

- **24 Stunden:** Frühwarnung
- **72 Stunden:** qualifizierte Meldung
- **1 Monat:** Abschlussbericht

In der Praxis liegt die Herausforderung häufig weniger in der Technik als in **klaren Entscheidungs-, Kommunikations- und Eskalationsprozessen.**

Orientierung an Standards & Best Practices

Die gesetzlichen Vorgaben sind bewusst technologieoffen formuliert.
Als Orientierungsrahmen eignen sich etablierte Standards und Frameworks wie:

- **ISO/IEC 27001 & 27002**
- **NIST Cybersecurity Framework**
- **CIS Critical Security Controls**
- **BSI IT-Grundschutz**
- **TeleTrust – Handreichung Stand der Technik in der IT-Sicherheit**

Diese decken zentrale Sicherheitsdomänen wie Inventarisierung, Secure Configuration, Malware Defense, Data Protection, Awareness, Vulnerability Management, Privilege Control und Incident Response ab und lassen sich gut auf die NIS-2-Anforderungen abbilden.

Zentrale Erkenntnisse für Organisationen

- **NISG 2026 ist kein IT-Projekt,** sondern ein Management- und Governance-Thema
- Der **1.10.2026** markiert den Beginn der Wirksamkeit – nicht den Start der Vorbereitung
- Die größten Umsetzungsrisiken liegen erfahrungsgemäß in **Scope-Fehlern, Lieferketten und ungeübten Meldeprozessen**
- Organisationen mit bestehenden ISMS-, NIST- oder CIS-basierten Kontrollen haben einen klaren Vorteil, müssen diese jedoch auf **österreichische Fristen und Nachweispflichten** ausrichten

Merksatz

Der 1. Oktober 2026 ist der Startpunkt der Wirksamkeit – nicht der Beginn der Vorbereitung. Wer Scope, Governance und Meldeprozesse früh sauber klärt, reduziert Risiko und Druck erheblich.

NIS-2 / NISG 2026 – 3 Schritte, die jetzt zählen

1. Klarheit schaffen
→ Betroffenheit, Scope und verantwortliche Rechtseinheiten festlegen.

2. Verantwortung übernehmen
→ Management einbinden, Governance regeln, Mindestmaßnahmen umsetzen.

3. Vorbereitung absichern
→ Meldeprozesse testen, Lieferkette prüfen, Registrierung & Nachweise vorbereiten.

NIS-2 / NISG 2026 wirft noch Fragen auf?

Gerne stehen wir bei der Umsetzung beratend und operativ zur Seite – praxisnah, strukturiert und realistisch.

DriveLock

DriveLock SE
Landsberger Straße 396
81241 München

+49 (89) 546 36 49-0
info@drivelock.com

ÜBERZEUGEN SIE SICH

Jetzt unverbindlich
30 Tage gratis testen

Sprechen Sie mit
unseren Experten