

Austrian NIS-2 implementation acts - NISG 2026 and NISV 2026 - now in effect

5.10.2026 - | Wolf Theiss

This Client Alert is available in both English and German.

The Austrian Network and Information Systems Security Act 2026 (NISG 2026), implementing the NIS-2 Directive, is applicable in Austria since 1 October 2026. It is supplemented by the NIS Regulation 2026 (NISV 2026) of the Cybersecurity Authority, which further specifies risk management requirements. Both local companies and Austrian subsidiaries of international groups operating critical infrastructure are affected.

The NISG 2026 establishes a strict supervisory and control regime for companies in a wide range of critical sectors, including energy, transport, banking, healthcare, digital infrastructure, ICT service management and public administration. It explicitly assigns responsibility for cybersecurity to senior management and introduces severe consequences for non-compliance, including temporary disqualification from management duties. Entities are classified as either essential or important based on the sector in which they operate and their size, with stricter obligations applying to essential entities.

1. Required action

- **Check applicability:** Companies operating in critical sectors should promptly determine whether they fall within the scope of NISG 2026.
 - **Wide scope:** NISG 2026 significantly expands coverage compared to its predecessor and will affect more companies than may be expected. The number of covered sectors has more than doubled, now including manufacturing, postal services, waste management, chemicals, food production and space, among others.
 - **Group relief:** Consolidation of key figures within corporate groups does not apply where organisational, technical and operational independence with respect to networks and information systems exists.
- **Reporting:** Establish incident reporting channels to meet the notification deadlines for significant cyber incidents (initial early warning within 24 hours, incident notification within 72 hours and final report within one month). This requirement has applied since 1 October 2026.
- **Registration:** Complete formal registration with the Cybersecurity Authority (Cybersicherheitsbehörde) no later than 31 December 2026.
- **Self-declaration:** Submit information on the implemented cybersecurity risk management measures to the competent authority within 12 months of the registration obligation arising, i.e. earliest by 30 September 2027.
- **Governance:** Responsibility for implementing and monitoring risk management measures rests explicitly with the management board or executive directors.
- **Training:** Management and employees are subject to mandatory cybersecurity training requirements.
- **Supply chain security:** Risk management measures must also cover cybersecurity throughout the supply chain. This is often the most challenging aspect and may require the review and updating of supplier contracts and related documentation.
- **Risk assessment and risk management requirements:** The Cybersecurity Authority's NIS

Regulation 2026 (NISV 2026) extends the risk management requirements of Implementing Regulation (EU) 2024/2690, originally designed for certain digital service providers, to all essential and important entities. It also lists risk categories that must be considered (technological, human, ICT supply chain and location-related risks), as well as criteria for significant incidents, with a single criterion being sufficient.

2. Sanctions and enforcement

- **Control:** The Cybersecurity Authority will have extensive audit rights, including on-site inspections and security scans.
- **Disqualification:** Members of the management body of essential entities may be temporarily prohibited from exercising their management functions in cases of serious breaches.
- **Naming and shaming:** In cases of inadequate measures, the Cybersecurity Authority may impose additional requirements and inform the public.
- **Fines:**
 - Breaches of essential obligations may result in fines of up to EUR 10 million or 2% of global turnover for essential entities or EUR 7 million or 1.4% of global turnover for important entities. These fines primarily target breaches such as failure to provide training, inadequate implementation of risk management measures and failure to report significant cybersecurity incidents.
 - For certain other obligations, such as registration requirements, fines of up to EUR 50,000 may be imposed, increasing to EUR 100,000 for repeated offences.

3. Impact on Austrian subsidiaries within international groups

- **Conduct a scope analysis:** Which entities in Austria or elsewhere in the EU are likely to fall within the scope of NISG 2026? How are they structured?
 - Austrian subsidiaries must assess whether they qualify as “essential” or “important” entities under NISG 2026 by applying the relevant size thresholds and lists of critical sectors.
 - Independently operated subsidiaries may benefit from relief regarding the consolidation of corporate figures, preventing automatic threshold exceedances across an entire group.
- Companies within the scope of NISG 2026 must register with the Austrian Cybersecurity Authority and implement risk management measures, including documented policies and controls as well as cybersecurity training for employees and executives.

4. Conclusion

While the formal deadlines for registration and self-declaration extend into late 2026 and 2027, the core obligations, particularly those relating to risk management and incident reporting, apply immediately. To avoid penalties, companies should implement the necessary compliance measures without delay.

Österreichisches NIS-2-Umsetzungsgesetz - NISG 2026 und NISV 2026 - ab sofort in Kraft

Das österreichische Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) zur

Umsetzung der NIS-2-Richtlinie ist seit 1. Oktober 2026 in Österreich anwendbar. Ergänzt wird es durch die NIS-Verordnung 2026 (NISV 2026) der Cybersicherheitsbehörde, welche die Anforderungen an das Risikomanagement näher konkretisiert. Betroffen sind sowohl österreichische Unternehmen als auch österreichische Tochtergesellschaften internationaler Konzerne, die kritische Infrastrukturen betreiben.

Das NISG 2026 etabliert ein strenges Aufsichts- und Kontrollregime für Unternehmen in einer Vielzahl kritischer Sektoren, darunter Energie, Verkehr, Banken, Gesundheitswesen, digitale Infrastruktur, Verwaltung von IKT-Diensten und öffentliche Verwaltung. Es weist die Verantwortung für Cybersicherheit ausdrücklich der obersten Führungsebene zu und sieht erhebliche Konsequenzen bei Verstößen vor, einschließlich eines vorübergehenden Ausschlusses von Leitungsfunktionen. Unternehmen werden abhängig von ihrem Tätigkeitsbereich und ihrer Größe als wesentliche oder wichtige Einrichtungen eingestuft, wobei für wesentliche Einrichtungen strengere Anforderungen gelten.

1. Erforderliche Maßnahmen

- **Anwendbarkeit prüfen:** Unternehmen, die in kritischen Sektoren tätig sind, sollten unverzüglich prüfen, ob sie in den Anwendungsbereich des NISG 2026 fallen.
 - **Weiter Anwendungsbereich:** Das NISG 2026 erweitert den Anwendungsbereich gegenüber seinem Vorgängergesetz erheblich und wird mehr Unternehmen erfassen, als häufig angenommen wird. Die Zahl der betroffenen Sektoren hat sich mehr als verdoppelt und umfasst nun unter anderem auch die verarbeitende Industrie, Postdienste, Abfallwirtschaft, Chemie, Lebensmittelproduktion und den Weltraumsektor.
 - **Erleichterungen für Unternehmensgruppen:** Eine Konsolidierung relevanter Kennzahlen innerhalb von Unternehmensgruppen erfolgt nicht, sofern organisatorische, technische und operative Unabhängigkeit hinsichtlich der Netz- und Informationssysteme besteht.
- **Meldewesen:** Es sind geeignete Meldekanäle für Sicherheitsvorfälle einzurichten, um die Meldefristen für erhebliche Cybervorfälle einzuhalten (erste Frühwarnung innerhalb von 24 Stunden, Vorfallsmeldung innerhalb von 72 Stunden sowie Abschlussbericht innerhalb eines Monats). Diese Verpflichtung gilt bereits seit dem 1. Oktober 2026.
- **Registrierung:** Die formelle Registrierung bei der Cybersicherheitsbehörde muss spätestens bis zum 31. Dezember 2026 erfolgen.
- **Selbsterklärung:** Informationen zu den umgesetzten Cybersicherheits-Risikomanagementmaßnahmen sind innerhalb von zwölf Monaten nach Entstehen der Registrierungspflicht an die zuständige Behörde zu übermitteln, somit frühestens bis zum 30. September 2027.
- **Governance:** Die Verantwortung für die Umsetzung und Überwachung der Risikomanagementmaßnahmen liegt ausdrücklich beim Vorstand bzw. bei der Geschäftsführung.
- **Schulungen:** Für Management und Mitarbeitende gelten verpflichtende Anforderungen hinsichtlich Cybersicherheitsschulungen.
- **Sicherheit der Lieferkette:** Die Risikomanagementmaßnahmen müssen auch die Cybersicherheit entlang der gesamten Lieferkette erfassen. Dies stellt häufig die größte Herausforderung dar und kann eine Überprüfung und Aktualisierung von Lieferantenverträgen sowie entsprechender Dokumentation erforderlich machen.
- **Anforderungen an Risikoanalyse und Risikomanagement:** Die NIS-Verordnung 2026 (NISV 2026) der Cybersicherheitsbehörde erstreckt die Risikomanagementanforderungen der Durchführungsverordnung (EU) 2024/2690, die ursprünglich für bestimmte Anbieter digitaler Dienste konzipiert wurden, auf alle wesentlichen und wichtigen Einrichtungen. Zudem legt sie zu berücksichtigende Risikokategorien (technologische, menschliche, IKT-

lieferkettenbezogene und standortbezogene Risiken) sowie Kriterien für erhebliche Sicherheitsvorfälle fest, wobei bereits die Erfüllung eines einzelnen Kriteriums ausreicht.

2. Sanktionen und Durchsetzung

- Kontrollen: Die Cybersicherheitsbehörde erhält weitreichende Prüfungsrechte, einschließlich Vor-Ort-Kontrollen und Sicherheitsscans.
- Ausschluss von Leitungsfunktionen: Mitglieder der Leitungsorgane wesentlicher Einrichtungen können bei schwerwiegenden Verstößen vorübergehend an der Ausübung ihrer Leitungsfunktion gehindert werden.
- „Naming and shaming“: Bei unzureichenden Maßnahmen kann die Cybersicherheitsbehörde zusätzliche Anforderungen auferlegen und die Öffentlichkeit informieren.
- Geldbußen:
 - Verstöße gegen wesentliche Verpflichtungen können mit Geldbußen von bis zu EUR 10 Millionen oder 2 % des weltweiten Jahresumsatzes bei wesentlichen Einrichtungen bzw. EUR 7 Millionen oder 1,4 % des weltweiten Jahresumsatzes bei wichtigen Einrichtungen geahndet werden. Diese Sanktionen betreffen insbesondere Verstöße wie unterlassene Schulungen, die unzureichende Umsetzung von Risikomanagementmaßnahmen oder die Nichtmeldung erheblicher Cybervorfälle.
 - Für bestimmte andere Verpflichtungen, etwa Registrierungspflichten, können Geldbußen von bis zu EUR 50.000 verhängt werden. Bei wiederholten Verstößen erhöht sich dieser Betrag auf bis zu EUR 100.000.

3. Auswirkungen auf österreichische Tochtergesellschaften internationaler Konzerne

- Anwendungsbereich analysieren: Welche Gesellschaften in Österreich oder anderen EU-Mitgliedstaaten fallen voraussichtlich in den Anwendungsbereich des NISG 2026? Wie sind diese strukturiert?
 - Österreichische Tochtergesellschaften müssen prüfen, ob sie anhand der maßgeblichen Größenkriterien und der Listen kritischer Sektoren als wesentliche oder wichtige Einrichtungen im Sinne des NISG 2026 einzustufen sind.
 - Operativ unabhängige Tochtergesellschaften können von Erleichterungen bei der Konsolidierung von Unternehmenskennzahlen profitieren, wodurch eine automatische Überschreitung relevanter Schwellenwerte innerhalb eines Konzerns vermieden werden kann.
- Unternehmen, die in den Anwendungsbereich des NISG 2026 fallen, müssen sich bei der österreichischen Cybersicherheitsbehörde registrieren und Risikomanagementmaßnahmen implementieren. Dazu gehören dokumentierte Richtlinien und Kontrollmechanismen sowie Cybersicherheitsschulungen für Mitarbeitende und Führungskräfte.

4. Fazit

Während die formellen Fristen für Registrierung und Selbsterklärung bis Ende 2026 bzw. 2027 reichen, gelten die wesentlichen Verpflichtungen, insbesondere im Bereich Risikomanagement und Vorfallsmeldung, bereits unmittelbar. Um Sanktionen zu vermeiden, sollten Unternehmen die erforderlichen Compliance-Maßnahmen daher unverzüglich umsetzen.

<https://www.wolftheiss.com/insights/austrian-nis-2-implementation-acts-nisg-2026-and-nisv-2026-now-in-effect>