

NISG 2026

Das österreichische Gesetz zur Sicherung von Netz- und Informationssystemen gemäß der EU-Richtlinie NIS2

Was ist NISG 2026?

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) ist ein österreichisches Bundesgesetz zur Umsetzung der dazugehörigen EU-Richtlinie und regelt erstmals verbindliche Mindestanforderungen an Cyber-Security-Maßnahmen sowie verpflichtende Meldeprozesse für Unternehmen und Einrichtungen in ausgewählten kritischen und wirtschaftlich relevanten Sektoren in Österreich.

Während sich frühere Regelungen primär auf klassische Betreiber kritischer Infrastrukturen konzentrierten, erfasst das NISG 2026 nun auch eine Vielzahl von Industrie-, Digital- und Dienstleistungsunternehmen, sofern sie in bestimmten Sektoren tätig sind und definierte Größenkriterien erfüllen.

Für Unternehmen bedeutet das:

- verpflichtende organisatorische und technische Sicherheitsmaßnahmen,
- formalisierte Meldeprozesse bei Cybervorfällen,
- sowie eine stärkere Einbindung der Unternehmensleitung in die Steuerung der Cyber Security.

Da der operative Anwendungsbeginn am **01.10.2026** liegt, müssen betroffene Organisationen bereits jetzt interne Zuständigkeiten klären, Reporting-Prozesse aufsetzen und die Maßnahmenumsetzung vorbereiten.

Wer ist betroffen?

Das Gesetz unterscheidet:

- **Wesentliche Einrichtungen** und
- **Wichtige Einrichtungen**

Erfasst sind Organisationen aus insgesamt **18 Sektoren** gem. § 2 NISG 2026, u.a. Energie, Verkehr, Gesundheitswesen, digitale Infrastruktur, öffentliche Verwaltung sowie verarbeitendes Gewerbe.

Die Einstufung erfolgt in der Regel anhand von:

- Unternehmensgröße (Mitarbeiteranzahl, Umsatz und Bilanzsumme)
- wirtschaftlicher Bedeutung,
- sowie sektoraler Kritikalität.

Wichtig

Auch Unternehmen, welche nicht als „wesentliche“ oder „wichtige“ Einrichtung eingestuft sind, können über Lieferketten- und Vertragsanforderungen indirekt betroffen sein. NISG-pflichtige Unternehmen müssen Sicherheitsrisiken entlang der Lieferkette berücksichtigen und geben entsprechende Cyber-Security-Maßnahmen und Meldepflichten häufig an ihre Zulieferer weiter.

Kernpflichten für betroffene Einrichtungen

Governance

CyberSecurity wird zur Leitungsaufgabe, indem das Management die Umsetzung und Wirksamkeit der Risikomanagementmaßnahmen sicherstellen und überwachen muss.

Risikomanagementmaßnahmen

Einrichtungen müssen u.a. Risikoanalysen durchführen sowie u. a. Maßnahmen zu

- Reaktion auf Sicherheitsvorfälle,
- Business Continuity und
- Lieferketten- und Zugriffssicherheit (z.B. Mehrfaktor-Authentifizierung) implementieren.

Meldepflichten bei Cyber-Vorfällen

Bei erheblichen Sicherheitsvorfällen gelten gestufte Meldefristen:

- Frühwarnung: bis 24h nach Kenntnisnahme
- Vorfallsmeldung: bis 72h nach Kenntnisnahme
- Abschlussbericht: spätestens einen Monat nach der Übermittlung der Vorfallsmeldung

Registrierung & Nachweisführung

Betroffene Einrichtungen müssen sich innerhalb von drei Monaten ab Inkrafttreten (§ 29 Abs. 3) registrieren und strukturierte Angaben elektronisch an die zuständige Behörde übermitteln.

Aufsicht & Sanktionen

Die Einhaltung des NISG 2026 wird durch die neue nationale **Cybersicherheitsbehörde** (dem Bundesministerium für Inneres nachgeordnete organisatorische Behörde) überwacht.

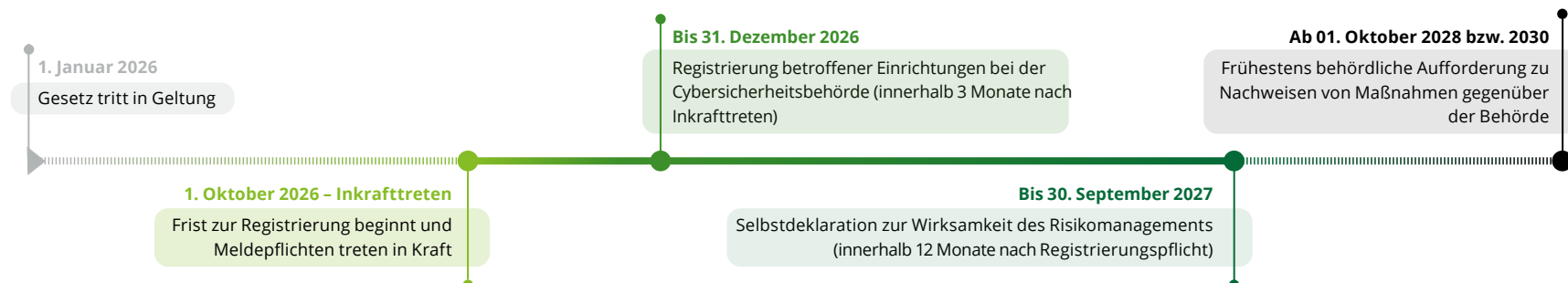
Sanktionsrahmen:

- **Wesentliche Einrichtungen:** bis zu 10 Mio. EUR oder 2 % weltweiter Jahresumsatz
- **Wichtige Einrichtungen:** bis zu 7 Mio. EUR oder 1,4 % weltweiter Jahresumsatz (je nachdem, welcher Betrag höher ist)

Was Unternehmen jetzt konkret tun sollten

- 01** Betroffenheitsanalyse durchführen
- 02** Rollen & Verantwortlichkeiten festlegen
- 03** Gap-Analyse gegenüber gesetzlichen Anforderungen durchführen
- 04** Berichtspflichten bei Sicherheitsvorfällen definieren und vorbereiten
- 05** Registrierung & Nachweisfähigkeit sicherstellen
- 06** Umsetzungs-Roadmap erstellen

Timeline





Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk von Mitgliedsunternehmen und deren verbundene Unternehmen innerhalb der „Deloitte Organisation“. DTTL („Deloitte Global“), jedes ihrer Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen. DTTL erbringt keine Dienstleistungen für Kundinnen und Kunden. Weitere Informationen finden Sie unter www.deloitte.com/about.

Deloitte Legal bezieht sich auf die ständige Kooperation mit Jank Weiler Operenyi, der österreichischen Rechtsanwaltskanzlei im internationalen Deloitte Legal-Netzwerk.

Deloitte ist ein global führender Anbieter von Dienstleistungen aus den Bereichen Audit & Assurance, Tax, Strategy, Risk & Transactions und Technology & Transformation. Mit einem weltweiten Netzwerk von Mitgliedsunternehmen und den mit ihnen verbundenen Unternehmen innerhalb der „Deloitte Organisation“ in mehr als 150 Ländern und Regionen betreuen wir vier von fünf Fortune Global 500® Unternehmen. „Making an impact that matters“ – ca. 470.000 Mitarbeiterinnen und Mitarbeiter von Deloitte teilen dieses gemeinsame Verständnis für den Beitrag, den wir als Unternehmen stetig für unsere Klientinnen und Klienten, Mitarbeiterinnen und Mitarbeiter sowie die Gesellschaft erbringen. Mehr Information finden Sie unter www.deloitte.com.

Diese Kommunikation enthält lediglich allgemeine Informationen, die eine Beratung im Einzelfall nicht ersetzen können. Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk an Mitgliedsunternehmen oder mit ihnen verbundene Unternehmen innerhalb der „Deloitte Organisation“ bieten im Rahmen dieser Kommunikation keine professionelle Beratung oder Services an. Bevor Sie die vorliegenden Informationen als Basis für eine Entscheidung oder Aktion nutzen, die Auswirkungen auf Ihre Finanzen oder Geschäftstätigkeit haben könnte, sollten Sie qualifizierte, professionelle Beratung in Anspruch nehmen.

DTTL, seine Mitgliedsunternehmen, mit ihnen verbundene Unternehmen, ihre Mitarbeiterinnen und Mitarbeiter sowie ihre Vertreterinnen und Vertreter übernehmen keinerlei Haftung, Gewährleistung oder Verpflichtungen (weder ausdrücklich noch stillschweigend) für die Richtigkeit oder Vollständigkeit der in dieser Kommunikation enthaltenen Informationen. Sie sind weder haftbar noch verantwortlich für Verluste oder Schäden, die direkt oder indirekt in Verbindung mit Personen stehen, die sich auf diese Kommunikation verlassen haben. DTTL, jedes seiner Mitgliedsunternehmen und mit ihnen verbundene Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen.

Kontakt



Karin Mair
Managing Partner |
Technology & Transformation und
Strategy, Risk & Transactions

+43 1 537 00-4840
kmair@deloitte.at



Georg Schwondra
Partner |
Cyber

+43 1 537 00-3760
gschwondra@deloitte.at