überblick

NISG 2026

schönherr

:überblick

NISG 2026

*Mit Kundmachung im Bundesgesetzblatt BGBl. I Nr. 94/2025 vom 23.12.2025 wurde die NIS-2-Richtlinie in Österreich durch das Netz- und Informationssystemsicherheitsgesetz 2026 („**NISG 2026**“) umgesetzt.*

Das NISG 2026 stärkt die **Aufsicht** spürbar, hebt die Anforderungen an **Cybersicherheitsmaßnahmen** auf ein neues Niveau – und definiert **klare Melde- und Nachweispflichten**.

Institutioneller Rahmen

Das NISG 2026 etabliert das **Bundesamt für Cybersicherheit** als monokratische Behörde unter dem BMI ("**Cybersicherheitsbehörde**"). Die Computer-Notfallteams ("**CSIRTs**") bleiben tragende Säulen der operativen Abwehr von Cybersicherheitsvorfällen.

Einstufung

Wesentliche Einrichtungen	Wichtige Einrichtungen
Größenunabhängig: u.a. qualifizierte Vertrauensdiensteanbieter, TLD-Namenregister, DNS-Diensteanbieter	**Größenunabhängig**: u.a. Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher Kommunikations-dienste (sofern nicht bereits als wesentlich einzustufen)
Größenabhängig: Einrichtungen der in Anlage 1 genannten Art, die ein großes Unternehmen betreiben	**Größenunabhängig**: Einrichtungen der Landesverwaltung
Größenabhängig: Einrichtungen, die ein mittleres Unternehmen betreiben und Anbieter öffentlicher elektronischer Kommunikations-netze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste	**Größenabhängig**: Einrichtungen der in den Anlagen 1 und 2 genannten Art, die ein großes oder mittleres Unternehmen betreiben (sofern nicht bereits als wesentlich einzustufen)

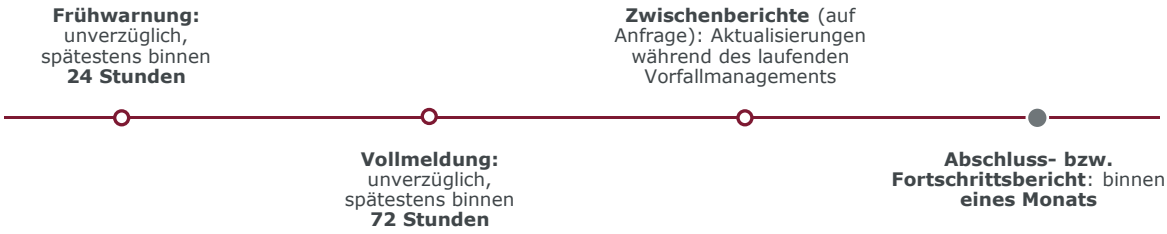
Darüber hinaus kann die Cybersicherheitsbehörde Einrichtungen der in den Anlagen 1 oder 2 genannten Art, die aufgrund ihrer Unternehmensgröße weder wesentlich noch wichtig sind, aus im NISG 2026 **näher definierten Gründen** mit Bescheid als wesentliche Einrichtung oder als wichtige Einrichtung **einstufen**.

Governance

Leitungsorgane sind gemäß NISG 2026 **persönlich** für das Risikomanagement verantwortlich und müssen dessen Umsetzung **aktiv** überwachen. Dazu zählen verpflichtende **Cybersicherheitsschulungen** für sie selbst sowie regelmäßige Schulungen für Mitarbeitende. Als Leitungsorgane gelten nur natürliche Personen auf **Geschäftsführungs- bzw. Vorstandsebene;** Prokurist*innen oder Funktionen wie der/die CISO zählen grundsätzlich nicht dazu.

Meldewesen

(ausgenommen sind Vertrauensdiensteanbieter; für sie gelten Sonderregeln)



Aufsicht und Maßnahmen

Wesentliche Einrichtungen unterliegen einer **ex-ante-Aufsicht**, während **wichtige Einrichtungen** primär einer anlassbezogenen **ex-post-Aufsicht** unterstehen. Der Maßnahmenkatalog reicht von Auskunfts- und Vorlagepflichten über Ad-hoc-Prüfungen und Sicherheitsscans bis hin zur Bestellung eines Überwachungsbeauftragten; in **Extremfällen** können zudem Gewerbeberechtigungen entzogen und die Ausübung von Leitungsfunktionen vorübergehend untersagt werden.

Wesentliche und wichtige Einrichtungen müssen innerhalb von zwei Jahren nach Aufforderung durch die Cybersicherheitsbehörde den Nachweis der technischen, operativen und organisatorischen Umsetzung der Risikomanagementmaßnahmen vorlegen; operative und organisatorische Aspekte können auch durch gültige Zertifikate (etwa ISO/IEC 27001) bestätigt werden. Für **wesentliche Einrichtungen** verkürzt sich die Nachweisfrist für operative und organisatorische Maßnahmen auf **zwei Monate**.

Sanktionen

- **Wesentliche Einrichtungen**: bis EUR 10 Mio oder 2 % des weltweiten Vorjahresumsatzes
- **Wichtige Einrichtungen**: bis EUR 7 Mio oder 1,4 % des weltweiten Vorjahresumsatzes
- **Öffentliche Stellen**: kein Geldbußensystem – alternatives Sanktionsregime ("*naming and shaming*" Lösung)
- **Keine Doppelsanktion** bei gleichzeitigem Verstoß gegen DSGVO

Zeitplan NISG 2026

Praxisfolgen für Unternehmen und öffentliche Stellen

Prüfung der Einstufung	**Soll-Ist-Abgleich der Risikomanagementmaßnahmen**	**Schärfung der Meldeorganisation**
Anhand der Unternehmens-größe und Tätigkeitsart – Einrichtung **"wesentlich"** oder **"wichtig"**	**Schwerpunkte** u.a. auf Informationssicherheit, Lieferkettensicherheit, Bewältigung von Sicherheits-vorfällen, Identity & Access Management mit Multi-Faktor-Authentifizierung, Notfall- und Wiederanlauf-pläne sowie Schulungen	Prozesse, Tools und Verantwortlichkeiten müssen gewährleisten, dass **Frühwarnungen** binnen 24 Stunden und **Voll-meldungen** binnen 72 Stunden abgesetzt werden können
Registrierung rechtzeitig **vorbereiten**	Besonderer Fokus auf die **Qualität der Risikoanalyse** und die **Dokumentation der Wirksamkeitskontrollen** (Selbstdeklaration und Prüfreport)	Öffentliche Verwaltung sollte interne Vorkehrungen im Lichte der **Vorbildfunktion** prüfen (hohes Cyber-sicherheitsniveau)

kontakt

Felix Schneider

Rechtsanwalt, Österreich

T: +43 1 534 37 50213
E: f.schneider@schoenherr.eu

Christopher Drolz

Associate, Österreich

T: +43 1 534 37 50356
E: ch.drolz@schoenherr.eu

www.schoenherr.eu