NIS2-Checkliste 2026 für Österreich

NISG 2026 (BGBl. I Nr. 94/2025) — Schritt für Schritt zur Registrierung & Umsetzung · Stand: Juni 2026

ERSTREGISTRIERUNG	SELBSTDEKLARATION	INKRAFTTRETEN NISG 2026
31.12.2026	30.09.2027	01.10.2026

Diese Checkliste führt in sechs Schritten durch das NISG 2026 — von der Betroffenheit über die Registrierung bis zu Meldewesen und Selbstdeklaration. Sie bildet die **Mindestschritte** ab; das Abhaken bedeutet nicht automatisch „100 % konform".

Schritt 1 Betroffenheit klären

- [ ] In einem der **18 Sektoren** (Anlage 1 oder 2) tätig?
- [ ] Größenschwelle: ab **50 Mitarbeitenden** — oder, davon unabhängig, ab **> 10 Mio. € Umsatz UND > 10 Mio. € Bilanzsumme** (kumulativ)?
- [ ] Größenunabhängige Sonderfälle geprüft (qualifizierte Vertrauensdienste, DNS, öffentliche Kommunikationsnetze)?
- [ ] Einstufung bestimmt: **wesentlich, wichtig oder außerhalb**?
- [ ] DORA-Vorrang geprüft (Finanzsektor, § 24 Abs. 7)?

Schritt 2 Registrieren — bis 31.12.2026

- [ ] Die **sieben § 29-Pflichtangaben** zusammengetragen (Name, Kontakt, Sektor/Teilsektor/Art, Mitgliedstaaten, IP-Bereiche, Niederlassungen, Schwellenwert-/Einstufungsangaben)?
- [ ] Kontaktstelle benannt (mind. Telefon + E-Mail, § 29 Abs. 6)?
- [ ] **Bis 31.12.2026** elektronisch bei der Cybersicherheitsbehörde registriert (§ 29 Abs. 3)?
- [ ] Prozess für Änderungsmeldungen etabliert (Z 1–5 binnen 2 Wochen, Z 6–7 binnen 3 Monaten)?

Schritt 3 Risikomanagement umsetzen (§ 32)

Die zehn gesetzlichen Mindestinhalte (§ 32 Abs. 4) — gefahrenübergreifend, Stand der Technik:

- [ ] a) Risikoanalyse & Sicherheitskonzepte
- [ ] b) Bewältigung von Sicherheitsvorfällen (Incident Handling)
- [ ] c) Aufrechterhaltung des Betriebs (Backup, Wiederherstellung, Krisenmanagement)
- [ ] d) Sicherheit der Lieferkette (inkl. unmittelbarer Anbieter)
- [ ] e) Sicherheit bei Erwerb, Entwicklung & Wartung (inkl. Schwachstellenmanagement)
- [ ] f) Bewertung der Wirksamkeit der Maßnahmen
- [ ] g) Cyberhygiene & Schulungen
- [ ] h) Kryptografie & ggf. Verschlüsselung
- [ ] i) Personalsicherheit, Zugriffskontrolle, Asset-Management
- [ ] j) Multi-Faktor-Authentifizierung & gesicherte Kommunikation

Schritt 4 Governance & Schulung (§ 31)

- [ ] Leitungsorgan stellt die § 32-Maßnahmen sicher und **beaufsichtigt** sie (§ 31 Abs. 1)?
- [ ] Leitungsorgan an Cybersicherheitsschulungen teilgenommen (§ 31 Abs. 2)?
- [ ] Mitarbeitenden werden regelmäßig Schulungen angeboten?
- [ ] Aufsicht/Beschlüsse prüffest dokumentiert?

Schritt 5 Meldewesen vorbereiten (§ 34 / § 35)

- [ ] Erheblichkeitsschwelle (§ 35) intern definiert und bekannt?
- [ ] Meldekette eingeübt: **24 h** Frühwarnung, **72 h** Meldung, **1 Monat** Abschlussbericht (§ 34 Abs. 2)?
- [ ] Klar, dass Vorfälle an das **CSIRT** gehen (nicht direkt an die Behörde)?
- [ ] Empfänger-Unterrichtung vorgesehen, wenn die Diensterbringung beeinträchtigt ist (§ 34 Abs. 3)?

Schritt 6 Nachweise & Selbstdeklaration (§ 33)

- [ ] **Selbstdeklaration der § 32-Maßnahmen bis 30.9.2027 vorbereitet (§ 33 Abs. 1)?**
- [ ] **Auf eine mögliche Prüfung durch eine unabhängige Stelle vorbereitet?**
- [ ] **Nachweise prüffest und versioniert abgelegt?**

Kostenloser Sofort-Check: Sind Sie im Geltungsbereich?
In 2 Minuten zur voraussichtlichen NISG-Einstufung — Sektor + Größe wählen.
nisg26.at/nis2-betroffenheit-pruefen

Hinweis: Diese Checkliste dient der Orientierung und ersetzt keine Rechtsberatung. Ein vollständiges Abhaken ist kein automatischer Konformitätsnachweis — die § 32-Maßnahmen sind gesetzliche Mindestinhalte, deren Ausgestaltung von Größe, Risiko und Stand der Technik abhängt (§ 32 Abs. 3/4). Eine **verbindliche Einstufung** trifft allein die zuständige Behörde mit Bescheid. Maßgeblich ist der Gesetzestext (BGBl. I Nr. 94/2025). Quellen: ris.bka.gv.at · nis.gv.at · wko.at.