NIS2 auf einer Seite

NISG 2026, BGBl. I Nr. 94/2025

1. Okt 2026	31. Dez 2026	24 / 72 Std.	10 / 7 Mio. €
In Kraft	Registrierung	Meldefristen	Strafrahmen

1 WER ERFASST IST: SEKTOR MAL GRÖSSE

GRÖSSE	ANLAGE 1	ANLAGE 2
Ab 250 Mitarbeitern	wesentliche Einrichtung	wichtige Einrichtung
Ab 50 Mitarbeitern	wichtige Einrichtung	wichtige Einrichtung
Darunter	Einstufung per Bescheid möglich	Einstufung per Bescheid möglich

Alternativ zur Mitarbeiterzahl: Umsatz über 50 Mio. Euro und Bilanzsumme über 43 Mio. Euro (groß), Umsatz über 10 Mio. Euro und Bilanzsumme über 10 Mio. Euro (mittel). Zahlen von Partner- und verbundenen Unternehmen werden grundsätzlich hinzugerechnet (§ 25 Abs. 1), nicht jedoch, wenn die Einrichtung organisatorisch, technisch und operativ unabhängig von ihnen ist (§ 25 Abs. 4). Unabhängig von der Größe erfasst sind unter anderem DNS-Dienste, TLD-Namenregister, Vertrauensdienste, Anbieter öffentlicher Kommunikationsnetze, die öffentliche Verwaltung und kritische Einrichtungen nach der CER-Richtlinie (§ 24). Strafrahmen: wesentliche Einrichtungen bis 10 Mio. Euro oder 2 % des weltweiten Umsatzes (§ 45 Abs. 2), wichtige Einrichtungen bis 7 Mio. Euro oder 1,4 % (§ 45 Abs. 3).

2 ZWEI ROLLEN

Direkt erfasst

Registrierung (§ 29). Risikomanagement (§ 32). Meldung binnen 24 und 72 Stunden (§ 34). Die Leitungsorgane haben die Einhaltung sicherzustellen, zu beaufsichtigen und selbst an Schulungen teilzunehmen (§ 31).

Zulieferer

Das Gesetz verpflichtet wesentliche und wichtige Einrichtungen. Wer selbst keine ist, wird über den Vertrag des Auftraggebers erreicht (§ 32 Abs. 4 lit. d). IT-Dienstleister sind häufig selbst erfasst, etwa als MSP, MSSP, Cloud- oder Rechenzentrumsanbieter.

3 WAS VERLANGT WIRD: § 32 ABS. 4, ZUMINDEST ZEHN PUNKTE

- Risikoanalyse und Sicherheitskonzepte
- Betrieb, Backup, Wiederherstellung, Krise
- Erwerb, Entwicklung, Wartung, Schwachstellen
- Cyberhygiene und Schulungen
- Personal, Zugriffskontrolle, Anlagen
- Bewältigung von Vorfällen
- Sicherheit der Lieferkette
- Wirksamkeit der Maßnahmen
- Kryptografie und Verschlüsselung
- Mehr-Faktor-Authentifizierung

4 NACHWEIS

Eine NIS2-Zertifizierung besteht nicht. Das Gesetz kennt die Selbstdeklaration (§ 33 Abs. 1) und, auf Aufforderung, den Nachweis der Umsetzung durch eine unabhängige Stelle (§ 33 Abs. 2). Ein gültiges ISO-27001-Zertifikat kann die operative und organisatorische Umsetzung belegen, die technische nicht.

Wir unterstützen beim Betroffenheits-Check und bei der Gap-Analyse

Wir klären mit Ihnen, ob und wie Sie erfasst sind, und erheben den Ist-Zustand gegen § 32. Die zehn Punkte prüfen wir gegen die zugehörigen Controls der ISO/IEC 27002:2022, auf Wunsch gegen sämtliche Controls der Norm. Eine Bestätigung der Konformität sprechen wir nicht aus.