FRANKFORD'S SOLUTIONS

Stand: Juli 2026

NIS2-Readiness-Checkliste für österreichische Unternehmen

Betroffenheit klären, Pflichten kennen, rechtzeitig handeln. Das NISG 2026 gilt ab 1. Oktober 2026.

Diese Checkliste richtet sich an Unternehmen in Österreich, die nicht sicher sind, ob NIS2 sie betrifft und was konkret zu tun ist. Österreich hat die EU-Richtlinie mit dem NISG 2026 umgesetzt, beschlossen im Dezember 2025, in Kraft ab 1. Oktober 2026. Stand: Juli 2026. Diese Checkliste ist eine Orientierungshilfe und keine Rechtsberatung.

1. Betroffenheit prüfen

- [ ] Prüfen Sie, ob Ihre Tätigkeit in einen der 18 NIS2-Sektoren fällt.
  Sektoren mit hoher Kritikalität sind unter anderem Energie, Verkehr, Banken, Gesundheit, Trinkwasser, Abwasser und digitale Infrastruktur. Dazu kommen sonstige kritische Sektoren wie Post, Abfall, Chemie, Lebensmittel, verarbeitendes Gewerbe, digitale Dienste und Forschung.
- [ ] Prüfen Sie die Größenschwellen: ab 50 Beschäftigten oder über 10 Mio. Euro Umsatz und über 10 Mio. Euro Bilanzsumme sind Sie im Anwendungsbereich, sofern Sie in einem der 18 Sektoren tätig sind.
  Kleinere Unternehmen sind nur in Sonderfällen direkt erfasst, etwa DNS-Anbieter oder qualifizierte Vertrauensdienste.
- [ ] Klären Sie, ob Sie als wesentliche oder wichtige Einrichtung gelten.
  Wesentliche Einrichtungen stehen unter strengerer Aufsicht. Die Strafrahmen reichen bis 10 Mio. Euro oder 2 Prozent des weltweiten Jahresumsatzes, bei wichtigen Einrichtungen bis 7 Mio. Euro oder 1,4 Prozent. Es gilt jeweils der höhere Betrag.
- [ ] Machen Sie den kostenlosen Online-Betroffenheitscheck der WKO unter ratgeber.wko.at/NIS2.
- [ ] Prüfen Sie, ob betroffene Kunden NIS2-Anforderungen über Verträge an Sie weitergeben.
  Über die Lieferkette trifft NIS2 auch Unternehmen, die selbst nicht unter das Gesetz fallen.

2. Pflichten der Geschäftsleitung

- [ ] Setzen Sie NIS2 auf die Agenda der Geschäftsführung.
  Die Leitungsorgane müssen die Risikomanagementmaßnahmen billigen und ihre Umsetzung überwachen. Das lässt sich nicht zur Gänze an die IT delegieren. Bei Pflichtverletzungen können die Leitungsorgane persönlich zur Verantwortung gezogen werden.
- [ ] Planen Sie die verpflichtende Cybersicherheitsschulung für die Geschäftsleitung ein.
- [ ] Benennen Sie eine verantwortliche Person für Informationssicherheit samt Vertretung.
  Keine ausdrückliche gesetzliche Pflicht, aber empfehlenswert, damit die Zuständigkeit im Alltag klar ist.
- [ ] Reservieren Sie Budget und Zeit für die Umsetzung im Geschäftsjahr 2026/27.

3. Risikomanagement-Maßnahmen umsetzen

- [ ] Führen Sie eine Risikoanalyse Ihrer Netz- und Informationssysteme durch und dokumentieren Sie das Ergebnis.
- [ ] Erstellen Sie eine schriftliche Informationssicherheitsrichtlinie.
- [ ] Richten Sie einen Prozess für die Bewältigung von Sicherheitsvorfällen ein.
  Wer erkennt einen Vorfall, wer entscheidet, wer kommuniziert. Das muss vorher geklärt sein.
- [ ] Sorgen Sie für Backups und Notfallpläne und testen Sie die Wiederherstellung regelmäßig.
- [ ] Bewerten Sie die Sicherheit Ihrer Lieferkette, vor allem IT-Dienstleister und Software-Lieferanten.
- [ ] Verankern Sie Sicherheitsanforderungen in Einkauf, Entwicklung und Wartung Ihrer Systeme, inklusive Umgang mit Schwachstellen.
- [ ] Führen Sie Multi-Faktor-Authentifizierung ein und vergeben Sie Zugriffsrechte nur nach Bedarf.
- [ ] Setzen Sie Verschlüsselung für sensible Daten und Kommunikation ein.
- [ ] Schulen Sie Ihre Mitarbeiter regelmäßig zu Cyberhygiene und aktuellen Bedrohungen.
- [ ] Legen Sie fest, wie Sie die Wirksamkeit Ihrer Maßnahmen regelmäßig überprüfen.

4. Melde- und Registrierungspflichten

- [ ] Registrieren Sie Ihr Unternehmen zwischen 1. Oktober und 31. Dezember 2026 über das Unternehmensserviceportal (USP).
  Fallen Sie erst später in den Anwendungsbereich, haben Sie ab diesem Zeitpunkt drei Monate Zeit für die Registrierung.
- [ ] Legen Sie fest, wer Sicherheitsvorfälle an die Behörde meldet, und sichern Sie die Erreichbarkeit auch außerhalb der Bürozeiten.
- [ ] Richten Sie Ihren Meldeprozess auf drei Fristen aus: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen eines Monats.
  Die Fristen gelten für erhebliche Sicherheitsvorfälle. Frühwarnung und Meldung laufen ab Kenntnis des Vorfalls. Der Abschlussbericht ist binnen eines Monats nach der Meldung fällig, dauert der Vorfall dann noch an, reicht zunächst ein Fortschrittsbericht.
- [ ] Planen Sie ein, betroffene Kunden zu informieren, wenn ein Vorfall Ihre Leistungen beeinträchtigt.
- [ ] Merken Sie die Selbstdeklaration vor: bis 30. September 2027 melden Sie die umgesetzten Maßnahmen an die Cybersicherheitsbehörde.
  Verstöße gegen Registrierungs- oder Selbstdeklarationspflicht kosten laut WKO bis zu 50.000 Euro, im Wiederholungsfall bis zu 100.000 Euro.

5. Erste Schritte bis Oktober 2026

- [ ] Machen Sie eine Gap-Analyse und leiten Sie daraus einen Maßnahmenplan mit Terminen und Verantwortlichen ab.
- [ ] Sichten Sie Ihre Verträge mit IT-Dienstleistern und ergänzen Sie Sicherheits- und Meldepflichten.

- [ ] Beobachten Sie die Verordnungen der Cybersicherheitsbehörde.
  Technische Detailanforderungen und das Formular für die Selbstdeklaration können noch per Verordnung konkretisiert werden. Hier ist einiges noch im Fluss.
- [ ] Dokumentieren Sie jeden Schritt nachvollziehbar. Im Prüffall zählt der Nachweis.

Frankford's IT-Solutions in Innsbruck unterstützt Sie bei der technischen Umsetzung, von MFA über sichere Softwareentwicklung bis zur Automatisierung Ihrer Prozesse. Melden Sie sich einfach, wenn Sie Fragen haben.

Frankford's IT-Solutions GmbH · Fallmerayerstraße 14, 6020 Innsbruck · frankford-it.at · eduard.frankford@frankford-it.at · Stand: Juli 2026