NISG 2026

Checkliste für Unternehmen

Praxis-Selbstcheck für Betroffenheit, Governance, Risikomanagement, Meldepflichten und Nachweise.

Stand: 1. Oktober 2026

Das NISG 2026 (BGBl. I Nr. 94/2025) tritt am 1.10.2026 in Kraft und setzt die NIS-2-Richtlinie in Österreich um. Diese Checkliste dient als praxisorientierte Ersteinschätzung und Umsetzungsübersicht.

Unternehmensdaten

Unternehmen	_____
Ansprechperson	_____
Datum des Checks	_____
Nächste Überprüfung	_____

So verwenden Sie die Checkliste

1. Prüfen Sie zuerst, ob Ihr Unternehmen voraussichtlich in den Anwendungsbereich fällt.
2. Bewerten Sie danach die organisatorischen und technischen Maßnahmen mit Ja / Teilweise / Nein.
3. Übertragen Sie offene Punkte in den Maßnahmenplan auf der letzten Seite und vergeben Sie Verantwortliche und Fristen.

Wichtig

Die genaue Betroffenheit hängt insbesondere von Tätigkeit, Sektor, Unternehmensgröße, Konzernstruktur und Sondertatbeständen ab. Die Checkliste ersetzt keine individuelle rechtliche oder technische Beratung.

01

Bin ich vom NISG 2026 betroffen?

Der Anwendungsbereich knüpft insbesondere an die Art der Einrichtung, den Sektor und die Unternehmensgröße an. Bestimmte Einrichtungen sind unabhängig von ihrer Größe erfasst.

A. Tätigkeits- und Sektorcheck

☐ Energie	☐ Abwasser	☐ Abfallbewirtschaftung
☐ Verkehr	☐ Digitale Infrastruktur	☐ Chemische Stoffe: Produktion, Herstellung und Handel
☐ Bankwesen	☐ Verwaltung von IKT-Diensten (B2B)	☐ Lebensmittel: Produktion, Verarbeitung und Vertrieb
☐ Finanzmarktinfrastrukturen	☐ Öffentliche Verwaltung	☐ Verarbeitendes Gewerbe / Herstellung von Waren
☐ Gesundheitswesen	☐ Weltraum	☐ Anbieter digitaler Dienste
☐ Trinkwasser	☐ Post- und Kurierdienste	☐ Forschung

Hinweis: Entscheidend sind die konkreten Arten von Einrichtungen und Teilsektoren gemäß Anlagen 1 und 2 NISG 2026 - nicht jede Tätigkeit innerhalb eines Oberbegriffs ist automatisch erfasst.

B. Größencheck

> **Schwellenwerte nach § 25**
>
> Groß: mindestens 250 Mitarbeitende ODER (Umsatz > 50 Mio. EUR UND Bilanzsumme > 43 Mio. EUR). Mittel: mindestens 50 Mitarbeitende ODER (Umsatz > 10 Mio. EUR UND Bilanzsumme > 10 Mio. EUR), sofern nicht bereits groß.

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Unternehmensgröße anhand Mitarbeitenden, Umsatz und Bilanzsumme korrekt ermittelt.	☐	☐	☐
Partner-/verbundene Unternehmen und die Ausnahme bei technischer/organisatorischer Unabhängigkeit geprüft.	☐	☐	☐

C. Größenunabhängige / besondere Fälle

Prüffrage / Maßnahme	Ja	Teilw.	Nein
DNS-Dienst, TLD-Namenregister oder qualifizierter Vertrauensdiensteanbieter?	☐	☐	☐
Öffentliches Kommunikationsnetz / öffentlich zugänglicher Kommunikationsdienst?	☐	☐	☐

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Behördliche Einstufung als wesentliche/wichtige Einrichtung?	☐	☐	☐
Als kritische Einrichtung nach RL (EU) 2022/2557 ermittelt?	☐	☐	☐
Besondere Bedeutung: einziger Anbieter, erhebliche Auswirkungen oder Systemrisiko?	☐	☐	☐

> **Ersteinschätzung**
>
> Treffen Sektor-/Tätigkeitskriterien und die Größenkriterien zu oder liegt ein Sonderfall vor, sollte die NISG-Einstufung verbindlich geprüft und dokumentiert werden. Auch nicht direkt erfasste Lieferanten können von NISG-Kunden künftig Sicherheitsnachweise und vertragliche Cybersecurity-Anforderungen erhalten.

02

Governance & Verantwortlichkeiten

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Geschäftsleitung stellt Einhaltung der Cyber-Risikomaßnahmen sicher und beaufsichtigt sie.	☐	☐	☐
Cybersecurity-Rollen und Eskalationsverantwortliche sind schriftlich festgelegt.	☐	☐	☐
Leitungsorgane absolvieren spezifische Cybersicherheitsschulungen.	☐	☐	☐
Mitarbeitende erhalten regelmäßig angemessene Cybersicherheitsschulungen.	☐	☐	☐
Schulungen werden mit Teilnahme, Inhalt und Wiederholung dokumentiert.	☐	☐	☐
Management-Review zu Risiken, Vorfällen und offenen Maßnahmen ist etabliert.	☐	☐	☐

03

Risikomanagementmaßnahmen nach § 32 NISG 2026

Die Maßnahmen müssen technisch, operativ und organisatorisch angemessen sowie verhältnismäßig sein und einem gefahrenübergreifenden Ansatz folgen.

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Risikoanalyse für Systeme, Dienste, Bedrohungen, Schwachstellen und Auswirkungen.	☐	☐	☐
Informationssicherheitskonzept mit Richtlinien und Mindeststandards.	☐	☐	☐
Incident Management: Erkennung, Eskalation, Eindämmung, Behebung, Nachbereitung.	☐	☐	☐
Business Continuity: kritische Prozesse, Abhängigkeiten und Notbetrieb geregelt.	☐	☐	☐
Backups: geschützte Sicherungen, Restore-Tests und Wiederanlaufziele vorhanden.	☐	☐	☐
Krisenmanagement mit Rollen, Kommunikationswegen und Entscheidungsbefugnissen.	☐	☐	☐
Kritische Anbieter/Dienstleister sind identifiziert und nach Cyberrisiko bewertet.	☐	☐	☐
Verträge enthalten angemessene Sicherheits-, Melde-, Audit- und Mitwirkungspflichten.	☐	☐	☐

03

Risikomanagementmaßnahmen - Fortsetzung

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Beschaffung: Sicherheitsanforderungen vor Erwerb von IKT definiert.	☐	☐	☐
Entwicklung/Wartung: sichere Change- und Patch-Prozesse.	☐	☐	☐
Schwachstellen werden erkannt, priorisiert, behoben und	☐	☐	☐

Prüffrage / Maßnahme	Ja	Teilw.	Nein
dokumentiert.			
Wirksamkeit der Maßnahmen wird regelmäßig getestet/bewertet.	☐	☐	☐
Cyberhygiene: Patchen, sichere Konfiguration, Phishing-/Endpoint-Schutz, Awareness.	☐	☐	☐
Kryptografie/Verschlüsselung ist geregelt und risikobasiert umgesetzt.	☐	☐	☐
Personalsicherheit bei Eintritt, Rollenwechsel und Austritt geregelt.	☐	☐	☐
Zugriffskontrolle nach Least Privilege; privilegierte Konten besonders geschützt.	☐	☐	☐
Asset-Inventar für Hardware, Software, Cloud, Konten und relevante Daten.	☐	☐	☐
MFA/starke Authentifizierung für relevante privilegierte, Remote- und Cloud-Zugänge.	☐	☐	☐
Sensible Sprach-, Video- und Textkommunikation ist angemessen geschützt.	☐	☐	☐
Abgesicherte alternative Notfallkommunikation ist vorgesehen.	☐	☐	☐

> **Praxisregel**
>
> Ein Häkchen bei „Ja“ sollte belegbar sein. Typische Nachweise sind Richtlinien, Protokolle, Schulungsnachweise, Risikoanalysen, Asset-Listen, Backup- und Restore-Tests, Lieferantenbewertungen, technische Konfigurationen sowie Incident- und Krisenübungen.

Lieferkette - zusätzlicher Kurzcheck

☐ Kritische Lieferanten nach Kritikalität und Zugriff auf Systeme/Daten klassifiziert	☐ Meldepflichten für Vorfälle vertraglich vereinbart	☐ Regelmäßige Neubewertung kritischer Dienstleister vorgesehen
☐ Sicherheitsniveau vor Beauftragung geprüft	☐ Zugänge von Dienstleistern zeitlich und technisch begrenzt	☐ Exit-/Wechsel-Szenario für kritische Anbieter vorhanden

04

Meldepflichten bei erheblichen Cybersicherheitsvorfällen

> **Die Zeit läuft ab Kenntnisnahme**
>
> Für erhebliche Cybersicherheitsvorfälle sieht § 34 NISG 2026 gestufte Meldungen an das zuständige CSIRT vor. Der Prozess muss so vorbereitet sein, dass die Fristen auch nachts, am Wochenende und bei eingeschränkter IT-Verfügbarkeit eingehalten werden können.

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Kriterien für die Eskalation eines potenziell erheblichen Vorfalls sind definiert.	☐	☐	☐
24/7-Eskalationskette und Vertretung sind festgelegt.	☐	☐	☐
Zuständiges CSIRT und Kontaktdaten sind hinterlegt.	☐	☐	☐
24-Stunden-Frühwarnung ist als Prozess/Vorlage vorbereitet.	☐	☐	☐
72-Stunden-Vorfallsmeldung ist als Prozess/Vorlage vorbereitet.	☐	☐	☐
Zwischenberichte auf Ersuchen sind organisatorisch vorbereitet.	☐	☐	☐
Abschlussbericht innerhalb eines Monats ist vorbereitet.	☐	☐	☐
Unterrichtung betroffener Diensteempfänger ist geregelt.	☐	☐	☐
Meldeprozess wurde praktisch/Tabletop getestet.	☐	☐	☐

Zeitplan im Ernstfall

Frist	Schritt	Inhalt / Vorbereitung
≤ 24 h	**Frühwarnung**	Erste Information zum erheblichen Vorfall; soweit relevant Verdacht auf rechtswidrige Handlungen / grenzüberschreitende Auswirkungen.
≤ 72 h	**Vorfallsmeldung**	Aktualisierung und erste Bewertung von Schweregrad und Auswirkungen; gegebenenfalls Kompromittierungsindikatoren.
≤ 1 Monat	**Abschlussbericht**	Ausführliche Beschreibung, Ursachen, Abhilfemaßnahmen und weitere gesetzlich geforderte Angaben.

05

Registrierung & Nachweise

Prüffrage / Maßnahme	Ja	Teilw.	Nein
Registrierung über USP ist intern zugeordnet und terminiert.	☐	☐	☐
Registrierungsdaten nach § 29 Abs. 2 sind vorbereitet.	☐	☐	☐
Kontaktstelle mit Telefonnummer und E-Mail ist festgelegt.	☐	☐	☐
Registrierung bis spätestens 31.12.2026 eingeplant (bereits Betroffene).	☐	☐	☐
Änderungen werden fristgerecht (2 Wochen / 3 Monate) gemeldet.	☐	☐	☐
Selbstdeklaration zu Risikomaßnahmen ist bis spätestens 30.09.2027 eingeplant.	☐	☐	☐
Nachweise zur Wirksamkeit werden strukturiert und aktuell gehalten.	☐	☐	☐

06

Maßnahmenplan

Übertragen Sie alle mit „Teilweise“ oder „Nein“ bewerteten Punkte in diese Übersicht. Priorisieren Sie zuerst Pflichten mit kurzer Frist und Maßnahmen, die hohe Betriebsrisiken reduzieren.

Offene Maßnahme	Priorität	Verantwortlich	Zieltermin	Status

Abschlussbewertung

Abschlusskriterium	Ja	Teilw.	Nein
Betroffenheit wurde nachvollziehbar geprüft und dokumentiert.	☐	☐	☐
Registrierung und Fristen sind organisatorisch abgesichert.	☐	☐	☐
Geschäftsleitung und Mitarbeitende sind geschult.	☐	☐	☐
Risikomanagementmaßnahmen nach § 32 sind dokumentiert und wirksam umgesetzt.	☐	☐	☐
24-/72-Stunden-Meldeprozess ist praktisch einsatzfähig.	☐	☐	☐
Lieferkettensicherheit und Nachweise sind in Beschaffung und Vertragsmanagement verankert.	☐	☐	☐

Empfehlung für die nächste Überprüfung

Mindestens jährlich sowie zusätzlich bei wesentlichen Änderungen von Diensten, Systemen, Lieferanten, Unternehmensgröße oder nach einem erheblichen Cybersicherheitsvorfall.

07

Nächste Schritte

Nutzen Sie die Checkliste als Startpunkt für eine dokumentierte NISG-Umsetzung.

☐ Betroffenheit und Einstufung intern bzw. fachlich bestätigen.	☐ Geschäftsleitung und Mitarbeitende schulen; Nachweise zentral dokumentieren.	☐ Registrierung bis Ende 2026 und Selbstdeklaration 2027 verbindlich terminieren.
☐ Offene Punkte aus der Checkliste priorisieren und Verantwortliche benennen.	☐ Incident- und Meldeprozess als Tabletop-Übung testen.	

> **Schulungen als Pflichtbestandteil**
>
> § 31 NISG 2026 verlangt spezifische Cybersicherheitsschulungen für Leitungsorgane und regelmäßige entsprechende Schulungen für Mitarbeitende. Schulungsplanung, Teilnahme und Wiederholung sollten nachvollziehbar dokumentiert werden.

Rechtsgrundlagen & weiterführende Informationen

- RIS - NISG 2026, BGBl. I Nr. 94/2025, Fassung 01.10.2026
- WKO - NISG 2026 & NIS 2: Pflichten für Unternehmen
- WKO / BMI - Fragen und Antworten zu NISG 2026

Hinweis: Diese Checkliste ist eine allgemeine Orientierungshilfe und stellt keine Rechts-, Datenschutz- oder IT-Sicherheitsberatung dar. Maßgeblich sind die jeweils geltenden gesetzlichen Bestimmungen, Verordnungen und behördlichen Vorgaben. Stand: 01.10.2026.

ROOKIE LEARNING

rookie-learning.com