

LEITFADEN · TOMORIS TOOLBOX

NIS2: Meldepflichten bei Sicherheitsvorfällen auf einen Blick

Fristen, Inhalte und Empfänger der Meldungen nach NISG 2026 und NIS-2-Richtlinie, mit Checkliste zur Vorbereitung

STAND

22.10.2026

UMFANG

PDF, 7 Seiten

ONLINE

tomoris.com/downloads/nis2-meldepflichten

AUF EINEN BLICK

24 h

Frühwarnung ab Kenntnisnahme des Vorfalls

72 h

Meldung mit erster Bewertung

1 Monat

Abschlussbericht nach der Meldung

10 Mio. €

Strafrahmen wesentliche Einrichtung oder 2 % Umsatz

FÜR WEN

- Geschäftsführung und Leitungsorgane wesentlicher und wichtiger Einrichtungen in Österreich
- IT-Leitung, Informationssicherheits- und Notfallverantwortliche
- IT-Dienstleister, die ihre Kunden bei Sicherheitsvorfällen unterstützen

WORUM ES GEHT

Seit 1. Oktober 2026 gilt in Österreich das NISG 2026. Wesentliche und wichtige Einrichtungen müssen erhebliche Cybersicherheitsvorfälle in festen Stufen melden: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht spätestens einen Monat danach. Dieses Dokument zeigt Fristen, Inhalte und Empfänger mit den Fundstellen im Gesetz und hilft, die Meldekette vorzubereiten, bevor der Ernstfall eintritt.

Dieses Dokument gibt einen Überblick und ersetzt keine Rechtsberatung. Maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung; Verordnungen der Cybersicherheitsbehörde, etwa nach § 35 Abs. 3, können Details ergänzen.

INHALT

01	Für wen die Meldepflicht gilt	2
02	Wann ein Vorfall erheblich ist	3
03	Die Meldekette: 24 Stunden, 72 Stunden, ein Monat	3
04	Wohin Sie melden	4
05	Kunden und Datenschutz nicht vergessen	5
06	Checkliste: meldefähig vor dem Ernstfall	5
07	Was bei Verstößen droht	6
08	Quellen	7

01

Für wen die Meldepflicht gilt

NISG 2026 seit 1. Oktober 2026: Meldepflicht für wesentliche und wichtige Einrichtungen, freiwillige Meldung für alle.

Das Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026, BGBl. I Nr. 94/2025) setzt die NIS-2-Richtlinie in Österreich um. Kundgemacht am 23. Dezember 2025, gelten seine Pflichten seit 1. Oktober 2026 (§ 51 Abs. 2: neun Monate nach der Kundmachung, mit dem folgenden Monatsersten).

Die Meldepflicht nach § 34 trifft wesentliche und wichtige Einrichtungen. Wer dazu zählt, regeln § 24 (Einstufung), § 25 (Unternehmensgröße) und § 26 (größenunabhängige Einstufung) samt den Sektoren der Anlagen 1 und 2.

Auch wer nicht unter das Gesetz fällt, kann Cybersicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle freiwillig an das nationale CSIRT melden (§ 37 Abs. 2), auf Wunsch ohne Angaben zur eigenen Identität (§ 37 Abs. 3).

02 —

Wann ein Vorfall erheblich ist

Die zwei Kriterien aus § 35 NISG 2026, die Beurteilungsmerkmale und die EU-Schwellen für digitale Anbieter.

Melden müssen Sie jeden erheblichen Cybersicherheitsvorfall. Ein Cybersicherheitsvorfall ist ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Diensten beeinträchtigt (§ 3 Z 30). Erheblich ist er nach § 35 Abs. 1, wenn er

- schwerwiegende Betriebsstörungen der Dienste oder schwerwiegende finanzielle Verluste für die Einrichtung verursacht hat oder verursachen kann, oder
- andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

Bei der Beurteilung zählen unter anderem die Abhängigkeit anderer Sektoren von Ihrem Dienst, mögliche Folgen für Umwelt, öffentliche Sicherheit und Gesundheit, Ihr Marktanteil, das betroffene geografische Gebiet und die betroffenen Systeme (§ 35 Abs. 2). Nähere Kriterien kann die Cybersicherheitsbehörde per Verordnung festlegen (§ 35 Abs. 3).

Für DNS-Diensteanbieter, TLD-Namenregister, Cloud- und Rechenzentrumsanbieter, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste und verwalteter Sicherheitsdienste, Online-Marktplätze, Online-Suchmaschinen, Plattformen sozialer Netzwerke und Vertrauensdiensteanbieter legt die Durchführungsverordnung (EU) 2024/2690 konkrete Schwellen fest, etwa einen direkten finanziellen Verlust von mehr als 500.000 Euro oder 5 % des Jahresumsatzes, je nachdem, welcher Wert niedriger ist (Art. 3 Abs. 1 lit. a). Geplante Wartungsarbeiten gelten nicht als erheblicher Vorfall (Art. 3 Abs. 2).

03 —

Die Meldekette: 24 Stunden, 72 Stunden, ein Monat

Frühwarnung, Meldung, Zwischenbericht, Abschlussbericht und Fortschrittsbericht mit Frist, Inhalt und Fundstelle.

Die drei Pflichtstufen, gerechnet ab Kenntnisnahme (§ 34 Abs. 2 NISG 2026)



24 h

Frühwarnung

Unverzüglich, spätestens 24 Stunden nach Kenntnisnahme: gegebenenfalls Verdacht auf rechtswidrige Handlungen und grenzüberschreitende Auswirkungen.



72 h

Meldung

Unverzüglich, spätestens 72 Stunden nach Kenntnisnahme: Aktualisierung und erste Bewertung samt Schweregrad und Auswirkungen.



1 Monat

Abschlussbericht

Spätestens einen Monat nach der Meldung, nicht nach dem Vorfall: Ursachen, Abhilfemaßnahmen, Auswirkungen.

Alle Stufen im Detail (§ 34 Abs. 2 NISG 2026, Art. 23 Abs. 4 NIS-2-Richtlinie)

STUFE	FRIST	INHALT	FUNDSTELLE
Frühwarnung	unverzüglich, spätestens 24 Stunden nach Kenntnisnahme	gegebenenfalls: Verdacht auf rechtswidrige und schuldhaftige Handlungen, mögliche grenzüberschreitende Auswirkungen	§ 34 Abs. 2 Z 1 NISG 2026, Art. 23 Abs. 4 lit. a
Meldung	unverzüglich, spätestens 72 Stunden nach Kenntnisnahme	Aktualisierung der Frühwarnung, erste Bewertung samt Schweregrad und Auswirkungen, gegebenenfalls Kompromittierungsindikatoren	§ 34 Abs. 2 Z 2, Art. 23 Abs. 4 lit. b
Zwischenbericht	auf Ersuchen des CSIRT oder der Cybersicherheitsbehörde	relevante Statusaktualisierungen	§ 34 Abs. 2 Z 3, Art. 23 Abs. 4 lit. c
Abschlussbericht	spätestens einen Monat nach der Meldung, nicht nach dem Vorfall	ausführliche Beschreibung mit Schweregrad und Auswirkungen; Art der Bedrohung und wahrscheinliche Ursachen; getroffene und laufende Abhilfemaßnahmen; gegebenenfalls grenzüberschreitende Auswirkungen	§ 34 Abs. 2 Z 4, Art. 23 Abs. 4 lit. d
Fortschrittsbericht	wenn der Vorfall bei Fälligkeit des Abschlussberichts noch andauert	Stand der Bewältigung; der Abschlussbericht folgt spätestens einen Monat nach Ende der Vorfallsbehandlung	§ 34 Abs. 2 Z 5, Art. 23 Abs. 4 lit. e

- Die Fristen laufen ab Kenntnisnahme des erheblichen Vorfalls, nicht ab seinem Beginn.
- Vertrauensdiensteanbieter melden Vorfälle, die ihre Vertrauensdienste betreffen, statt binnen 72 schon binnen 24 Stunden (§ 34 Abs. 2, Satz nach Z 5).
- Mitzuliefern sind alle Informationen, mit denen CSIRT und Behörde grenzüberschreitende Auswirkungen beurteilen können (§ 34 Abs. 2).
- Das CSIRT antwortet spätestens 24 Stunden nach Eingang der Frühwarnung mit einer ersten Rückmeldung, auf Wunsch mit Orientierungshilfe für Abhilfemaßnahmen (§ 34 Abs. 4).

04 —

Wohin Sie melden

An das zuständige CSIRT. Es leitet die Meldung an das Bundesamt für Cybersicherheit weiter.

Gemeldet wird an das für Sie zuständige sektorspezifische CSIRT, gibt es keines, an das nationale CSIRT. Das CSIRT leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter (§ 34 Abs. 1). Zuständige Behörde ist das Bundesamt für Cybersicherheit (§ 3a Abs. 1).

- Öffentliche Verwaltung: das GovCERT als sektorspezifisches CSIRT (§ 8 Abs. 4).
- Gesundheitswesen: das Austrian HealthCERT (§ 8a Abs. 3 Gesundheitstelematikgesetz 2012, neu gefasst mit BGBl. I Nr. 94/2025).

- Andere Sektoren: das sektorspezifische CSIRT; solange keines besteht, das nationale CSIRT (§ 8 Abs. 3). Bis ein nationales CSIRT nach neuem Recht ermächtigt ist, längstens zwei Jahre, nimmt das bisher ermächtigte nationale CSIRT diese Aufgaben wahr (§ 51 Abs. 6).

Welche CSIRTs ermächtigt sind, macht die Cybersicherheitsbehörde öffentlich bekannt (§ 8 Abs. 5). Halten Sie Meldeadresse und Meldeweg fest, bevor Sie sie im Vorfall suchen müssen.

05

Kunden und Datenschutz nicht vergessen

Empfänger Ihrer Dienste unverzüglich informieren und parallel die 72-Stunden-Meldung nach DSGVO prüfen.

Beeinträchtigt der Vorfall Ihre Dienste, informieren Sie die Empfänger Ihrer Dienste unverzüglich und nennen, soweit möglich, Maßnahmen, die diese selbst ergreifen können (§ 34 Abs. 3).

Sind personenbezogene Daten betroffen, gilt daneben die Datenschutz-Grundverordnung: Der Verantwortliche meldet die Verletzung unverzüglich und möglichst binnen 72 Stunden der Aufsichtsbehörde, es sei denn, sie führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen (Art. 33 Abs. 1 DSGVO). In Österreich ist das die Datenschutzbehörde (§ 18 Abs. 1 DSG).

Zwei Meldungen, zwei Empfänger: Die NIS2-Meldung geht an das CSIRT, die Datenschutzmeldung an die Datenschutzbehörde. Prüfen Sie beide im selben Vorfall.

06

Checkliste: meldefähig vor dem Ernstfall

Zehn Punkte, damit die 24-Stunden-Frist im Vorfall nicht zur Hürde wird.

- ☐ Zuständiges CSIRT und Meldeweg sind festgelegt und dokumentiert (§ 34 Abs. 1).
- ☐ Verantwortliche für die Meldung samt Vertretung sind benannt und auch außerhalb der Bürozeiten erreichbar.
- ☐ Die Kriterien aus § 35 sind auf Ihre Dienste übertragen: Welche Ausfälle, Schäden oder Datenabflüsse lösen eine Meldung aus?
- ☐ Der Zeitpunkt der Kenntnisnahme wird im Vorfall sofort festgehalten, denn ab ihm laufen 24 und 72 Stunden.
- ☐ Vorlagen für Frühwarnung, Meldung und Abschlussbericht enthalten die Inhalte aus § 34 Abs. 2.
- ☐ Ein Vorfallsprotokoll ist vorgesehen: Zeitleiste, Entscheidungen, betroffene Systeme, Kompromittierungsindikatoren.

- ☐ Die Information der Empfänger Ihrer Dienste nach § 34 Abs. 3 ist vorbereitet: wer, an wen, über welchen Kanal.
- ☐ Der Datenschutz ist eingebunden; die Prüfung nach Art. 33 DSGVO läuft parallel.
- ☐ IT-Dienstleister und Lieferanten geben Vorfälle, die Sie betreffen, unverzüglich an Sie weiter; das ist vertraglich geregelt.
- ☐ Die Meldekette wird regelmäßig geübt, zum Beispiel als Planspiel mit Geschäftsführung, IT und Kommunikation.

Die Checkliste ist eine Empfehlung von TOMORIS zur Vorbereitung. Gesetzlich vorgegeben sind Fristen, Inhalte und Empfänger der Meldungen (§ 34 NISG 2026).

07

Was bei Verstößen droht

Verwaltungsstrafen nach § 45 NISG 2026 für verletzte Melde- und Informationspflichten.

Wer die Meldepflicht samt Berichtspflichten (§ 34 Abs. 1 und 2) oder die Information der Empfänger der Dienste (§ 34 Abs. 3) verletzt, begeht eine Verwaltungsübertretung (§ 45 Abs. 1 Z 4 und 5).

10 Mio. €

Wesentliche Einrichtung

oder 2 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, es gilt der höhere Betrag (§ 45 Abs. 2).

7 Mio. €

Wichtige Einrichtung

oder 1,4 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, es gilt der höhere Betrag (§ 45 Abs. 3).

NÄCHSTER SCHRITT

Selbst prüfen oder gemeinsam umsetzen

KOSTENLOS PRÜFEN

NIS2-Betroffenheitscheck

tomoris.com/tools/nis2-check

UMSETZUNG BESPRECHEN

Kontakt aufnehmen

tomoris.com/contact

contact@tomoris.com

08 —

Quellen

Alle Aussagen sind belegt. Gesetzestexte gelten in der jeweils geltenden Fassung.

- 1 **NISG 2026, BGBl. I Nr. 94/2025, authentische Kundmachung im RIS**
§§ 3 Z 30, 3a, 8, 24 bis 26, 34, 35, 37, 45, 51 sowie Art. 3 (§ 8a GTelG 2012), gelesen am 22.10.2026
www.ris.bka.gv.at/eli/bgbl/i/2025/94
- 2 **NISG 2026, geltende Fassung im RIS**
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 3 **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), Art. 23 Berichtspflichten**
ABl. L 333 vom 27.12.2022
eur-lex.europa.eu/eli/dir/2022/2555/oj
- 4 **Durchführungsverordnung (EU) 2024/2690, Art. 3 Erhebliche Sicherheitsvorfälle**
ABl. L vom 18.10.2024
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj
- 5 **Verordnung (EU) 2016/679 (DSGVO), Art. 33 Meldung an die Aufsichtsbehörde**
eur-lex.europa.eu/eli/reg/2016/679/oj
- 6 **Datenschutzgesetz (DSG), § 18 Datenschutzbehörde als Aufsichtsbehörde**
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...