TOMORIS
MORE THAN IT

FREE DOWNLOAD

GUIDE · TOMORIS TOOLBOX

NIS2: Security Incident Reporting Obligations at a Glance

Deadlines, content, and recipients of reports under the NISG 2026 (Austrian Network and Information Systems Security Act 2026) and the NIS2 Directive, with a preparation checklist

UPDATED
Oct 25, 2026

LENGTH
PDF, 7 pages

ONLINE
tomoris.com/en/downloads/nis2-meldepflichten

AT A GLANCE

24 h
Early warning after becoming aware of the incident

72 h
Notification with an initial assessment

1 month
Final report after the notification

€10 million
Maximum fine for an essential entity, or 2% of turnover

WHO IT IS FOR

- Executives and management bodies of essential and important entities in Austria
- IT management, information security officers, and incident response managers
- IT service providers who support their customers during security incidents

Redistribution in unchanged form permitted

WHAT THIS COVERS

Since October 1, 2026, the NISG 2026 (Austrian Network and Information Systems Security Act 2026) has applied in Austria. Essential and important entities must report significant cybersecurity incidents in fixed stages: early warning within 24 hours, notification within 72 hours, and a final report no later than one month after that. This document shows deadlines, content, and recipients with the references in the law. It helps you prepare the reporting chain before an emergency occurs.

This document provides an overview and does not replace legal advice. The legal text in its current version is authoritative; regulations of the cybersecurity authority, currently the NISV 2026, add details.

CONTENTS

01 Who the Reporting Obligation Applies To 2
02 When an Incident Is Significant 3
03 The Reporting Chain: 24 Hours, 72 Hours, One Month 4
04 Where to Report 5
05 Don't Forget Customers and Data Protection 5
06 Checklist: Ready to Report Before an Emergency 6
07 Penalties for Violations 7
08 Sources 7

01

Who the Reporting Obligation Applies To

NISG 2026 since October 1, 2026: mandatory reporting for essential and important entities, voluntary reporting for everyone.

The Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026, Austrian Network and Information Systems Security Act 2026, BGBl. I No. 94/2025) transposes the NIS2 Directive in Austria. It was promulgated on December 23, 2025, and its obligations have applied since October 1, 2026 (§ 51 para. 2: nine months after promulgation, on the first day of the following month).

The reporting obligation under § 34 applies to essential and important entities. Who qualifies is governed by § 24 (classification), § 25 (company size), and § 26 (size-independent classification), together with the sectors in Annexes 1 and 2.

Even organizations that are not covered by the law can voluntarily report cybersecurity incidents, cyber threats, and near misses to the national CSIRT (§ 37 para. 2), anonymously if they wish (§ 37 para. 3).

02

When an Incident Is Significant

The two criteria from § 35 NISG 2026, the assessment factors, the criteria of the NISV 2026 (Austrian NIS Regulation 2026), and the EU thresholds for digital providers.

You must report every significant cybersecurity incident. A cybersecurity incident is an event that compromises the availability, authenticity, integrity, or confidentiality of data or services (§ 3 no. 30). Under § 35 para. 1, it is significant if it

- has caused or is capable of causing severe operational disruption of the services or severe financial losses for the entity, or
- has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The assessment takes into account, among other things, the dependence of other sectors on your service, possible effects on the environment, public safety, and health, your market share, the geographic area affected, and the systems affected (§ 35 para. 2). The cybersecurity authority has set out more detailed criteria in the NISV 2026 (§ 35 para. 3; BGBl. II No. 290/2026, in force since the end of October 1, 2026). According to the explanatory notes of the Federal Office for Cyber Security (Bundesamt für Cybersicherheit), its § 5 applies to entities in sectors outside Implementing Regulation (EU) 2024/2690. Under it, an incident is significant in any case if it

- has caused or is capable of causing a direct financial loss exceeding €500,000 or 5% of annual turnover in the previous financial year, whichever is lower (§ 5 para. 1 no. 1 NISV 2026),
- has caused or is capable of causing the leakage of trade secrets (§ 26b UWG, Austrian Unfair Competition Act) or of information that must be kept secret under § 6 IFG (Austrian Freedom of Information Act) (no. 2),
- has caused or is capable of causing the death of a person or serious damage to a person's health (no. 3 and 4),
- involves successful, suspected malicious, and unauthorized access to network and information systems that is likely to cause severe operational disruption (no. 5),
- causes or is capable of causing the services to fail or be restricted for more than 100,000 users or 10% of users, whichever is lower, or in the territory of at least one federal state for more than 24 hours (no. 7 and 8),
- has triggered crisis management or disaster recovery plans of business continuity management (no. 9), or
- counts as a recurring incident: at least twice in six months, with the same apparent root cause and impact, and together above the loss threshold from no. 1 (no. 6, § 7). Scheduled maintenance does not count as a significant incident (§ 6).

> For DNS service providers, TLD name registries, cloud and data center service providers, content delivery network providers, managed service and managed security service providers, online marketplaces, online search engines, social networking platforms, and trust service providers, Implementing Regulation (EU) 2024/2690 sets specific thresholds, such as a direct financial loss exceeding €500,000 or 5% of annual turnover, whichever is lower (Art. 3(1)(a)). Scheduled maintenance work does not count as a significant incident (Art. 3(2)).

03

The Reporting Chain: 24 Hours, 72 Hours, One Month

Early warning, notification, intermediate report, final report, and progress report with deadline, content, and reference.

The three mandatory stages, counted from becoming aware (§ 34 para. 2 NISG 2026)

24 h
Early warning
Without undue delay, no later than 24 hours after becoming aware: where applicable, suspicion of unlawful acts and cross-border impact.

72 h
Notification
Without undue delay, no later than 72 hours after becoming aware: update and initial assessment, including severity and impact.

1 month
Final report
No later than one month after the notification, not after the incident: root causes, mitigation measures, impact.

All stages in detail (§ 34 para. 2 NISG 2026, Art. 23(4) NIS2 Directive)

STAGE	DEADLINE	CONTENT	REFERENCE
Early warning	without undue delay, no later than 24 hours after becoming aware	where applicable: suspicion of unlawful or malicious acts, possible cross-border impact	§ 34 para. 2 no. 1 NISG 2026, Art. 23(4)(a)
Notification	without undue delay, no later than 72 hours after becoming aware	update of the early warning, initial assessment including severity and impact, indicators of compromise where available	§ 34 para. 2 no. 2, Art. 23(4)(b)
Intermediate report	at the request of the CSIRT or the cybersecurity authority	relevant status updates	§ 34 para. 2 no. 3, Art. 23(4)(c)
Final report	no later than one month after the notification, not after the incident	detailed description including severity and impact; type of threat and likely root causes; mitigation measures applied and ongoing; cross-border impact where applicable	§ 34 para. 2 no. 4, Art. 23(4)(d)
Progress report	if the incident is still ongoing when the final report is due	status of incident handling; the final report follows no later than one month after incident handling ends	§ 34 para. 2 no. 5, Art. 23(4)(e)

- The deadlines run from becoming aware of the significant incident, not from when it began.
- Trust service providers report incidents affecting their trust services within 24 hours instead of 72 (§ 34 para. 2, sentence after no. 5).
- You must provide all information that enables the CSIRT and the authority to assess cross-border impact (§ 34 para. 2).
- The CSIRT responds no later than 24 hours after receiving the early warning with initial feedback and, on request, guidance on mitigation measures (§ 34 para. 4).

04

Where to Report

To the competent CSIRT. It forwards the report to the Federal Office for Cyber Security.

Reports go to the sector-specific CSIRT responsible for you or, if there is none, to the national CSIRT. The CSIRT forwards the report to the cybersecurity authority without undue delay (§ 34 para. 1). The competent authority is the Federal Office for Cyber Security (§ 3a para. 1).

- Public administration: GovCERT as the sector-specific CSIRT (§ 8 para. 4).
- Healthcare: Austrian HealthCERT (§ 8a para. 3 Gesundheitstelematikgesetz 2012 (GTelG 2012, Austrian Health Telematics Act 2012), as amended by BGBl. I No. 94/2025).
- Other sectors: the sector-specific CSIRT; as long as none exists, the national CSIRT (§ 8 para. 3). Until a national CSIRT is authorized under the new law, for no more than two years, the previously authorized national CSIRT performs these tasks (§ 51 para. 6).

> The cybersecurity authority publishes which CSIRTs are authorized (§ 8 para. 5). Record the reporting address and reporting channel before you have to look for them during an incident.

05

Don't Forget Customers and Data Protection

Inform recipients of your services without undue delay and check the 72-hour notification under the GDPR in parallel.

If the incident affects your services, inform the recipients of your services without undue delay and, where possible, name measures they can take themselves (§ 34 para. 3).

If personal data is affected, the General Data Protection Regulation also applies: the controller notifies the supervisory authority of the breach without undue delay and, where feasible, within 72 hours, unless it is unlikely to result in a risk to the rights and freedoms of natural persons (Art. 33(1) GDPR). In Austria, this is the Austrian Data Protection Authority (Datenschutzbehörde) under § 18 para. 1 DSG (Austrian Data Protection Act).

> Two reports, two recipients: the NIS2 report goes to the CSIRT, the data protection notification to the Data Protection Authority. Check both for the same incident.

Updated Oct 25, 2026 · Redistribution unchanged permitted

06

Checklist: Ready to Report Before an Emergency

Ten items so that the 24-hour deadline does not become a hurdle during an incident.

- [ ] The competent CSIRT and the reporting channel are defined and documented (§ 34 para. 1).
- [ ] The people responsible for reporting, including deputies, are named and reachable outside office hours.
- [ ] The criteria from § 35 are applied to your services: which outages, damage, or data leaks trigger a report?
- [ ] The time of becoming aware is recorded immediately during an incident, because the 24 and 72 hours run from that point.
- [ ] Templates for the early warning, notification, and final report contain the content required by § 34 para. 2.
- [ ] An incident log is planned: timeline, decisions, affected systems, indicators of compromise.
- [ ] Informing the recipients of your services under § 34 para. 3 is prepared: who, to whom, and through which channel.
- [ ] Data protection is involved; the review under Art. 33 GDPR runs in parallel.
- [ ] IT service providers and suppliers pass on incidents that affect you without undue delay; this is governed by contract.
- [ ] The reporting chain is practiced regularly, for example as a tabletop exercise with management, IT, and communications.

This checklist is a TOMORIS recommendation for preparation. The law prescribes the deadlines, content, and recipients of the reports (§ 34 NISG 2026).

Updated Oct 25, 2026 · Redistribution unchanged permitted

07

Penalties for Violations

Administrative penalties under § 45 NISG 2026 for breaches of reporting and information obligations.

Anyone who breaches the reporting obligation, including the reporting duties (§ 34 para. 1 and 2), or the obligation to inform the recipients of the services (§ 34 para. 3) commits an administrative offense (§ 45 para. 1 no. 4 and 5).

€10 million

Essential entity

or 2% of the company's total worldwide annual turnover in the previous year, whichever is higher (§ 45 para. 2).

€7 million

Important entity

or 1.4% of the company's total worldwide annual turnover in the previous year, whichever is higher (§ 45 para. 3).

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

NIS2 applicability check (German)
tomoris.com/tools/nis2-check

DISCUSS IMPLEMENTATION

Get in Touch
tomoris.com/en/contact

contact@tomoris.com

08

Sources

All statements are supported by sources. Legislation applies in its current version.

1 **NISG 2026, BGBl. I No. 94/2025, authentic promulgation in the RIS**
§§ 3 no. 30, 3a, 8, 24 to 26, 34, 35, 37, 45, 51, and Art. 3 (§ 8a GTelG 2012), accessed October 22, 2026
www.ris.bka.gv.at/eli/bgbl/i/2025/94

2 **NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§§ 5 to 7 significance, § 9 entry into force, accessed October 25, 2026
www.ris.bka.gv.at/eli/bgbl/II/2026/290

3 **Federal Office for Cyber Security: Explanatory notes on the NISV 2026 (PDF)**
On § 5: scope outside Implementing Regulation (EU) 2024/2690
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...

4 **NISG 2026, current version in the RIS**
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

5 **Directive (EU) 2022/2555 (NIS2 Directive), Art. 23 reporting obligations**
OJ L 333 of December 27, 2022
eur-lex.europa.eu/eli/dir/2022/2555/oj

6 **Implementing Regulation (EU) 2024/2690, Art. 3 significant incidents**
OJ L of October 18, 2024
eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

7 **Regulation (EU) 2016/679 (GDPR), Art. 33 notification to the supervisory authority**
eur-lex.europa.eu/eli/reg/2016/679/oj

8 **Datenschutzgesetz (DSG, Austrian Data Protection Act), § 18 Data Protection Authority as supervisory authority**
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...