TOMORIS
MORE THAN IT

FREE DOWNLOAD

TEMPLATE · TOMORIS TOOLBOX

NIS2 Incident Report: Template for Early Warning, Notification, and Final Report

A worksheet to fill in: information for each reporting stage under § 34 NISG 2026, significance under the NISV 2026, customer information, GDPR review, and log

UPDATED
Oct 25, 2026

LENGTH
PDF, 11 pages

ONLINE
tomoris.com/en/downloads/nis2-vorfallmeldung-vorlage

AT A GLANCE

24 h
Early warning after becoming aware

72 h
Notification with an initial assessment

1 month
Final report after the notification

9
Criteria for “significant in any case” in § 5 NISV 2026

WHO IT IS FOR

- Essential and important entities under the NISG 2026
- Information security officers, IT management, and incident response managers
- IT service providers who support customers during an incident or report on their behalf with power of representation

Adaptation for your own use permitted; redistribute unchanged

WHAT THIS COVERS

Essential and important entities report a significant cybersecurity incident to the competent CSIRT in stages: early warning within 24 hours of becoming aware, notification within 72 hours, and a final report no later than one month after the notification (§ 34 NISG 2026). Reports are submitted via the NIS2-Services application in the Unternehmensserviceportal (Austrian business service portal). This worksheet collects internally what you need for this: master data, points in time, the significance review under § 35 NISG 2026 and § 5 NISV 2026, the information for each reporting stage with references, informing your customers, the parallel review under Art. 33 GDPR, and a log.

This template must be adapted to your entity and does not replace legal advice. It collects information internally; reports are submitted via the reporting channel of the competent CSIRT. The legal texts of the NISG 2026, the NISV 2026, and the GDPR in their current versions and the information requested in the reporting portal are authoritative.

Usage: You may adapt this template for your own use; you may redistribute it only in unchanged form.

CONTENTS

01 How to Work with the Template 3
02 Part A: Master Data and Reporting Channel 3
03 Part B: Points in Time, Deadlines, and Log 4
04 Part C: Significance Checklist 5
05 Part D: Early Warning within 24 Hours 7
06 Part E: Notification within 72 Hours 8
07 Part F: Intermediate, Progress, and Final Report 8
08 Part G: Recipients of the Services and Data Protection 9
09 Sources 11

01

How to Work with the Template

Collect internally, report via NIS2-Services: what the worksheet does and what it does not replace.

This template is an internal worksheet. You submit the report itself via the NIS2-Services application, which the Federal Office for Cyber Security (Bundesamt für Cybersicherheit, BCS) provides through the Unternehmensserviceportal. Only if the reporting portal is temporarily unavailable for technical reasons does the BCS name PDF forms for each report type as an alternative reporting channel. The recipient is the CSIRT responsible for you; it forwards the report to the cybersecurity authority without undue delay (§ 34 para. 1 NISG 2026). According to its own website, the BCS is still working on a connection via the Portalverbund (Austrian government portal network) for public administration entities (as of October 5, 2026).

The reporting stages under § 34 para. 2 NISG 2026

24 h
Early warning
Without undue delay, no later than 24 hours after becoming aware of the significant incident (no. 1).

72 h
Notification
Without undue delay, no later than 72 hours after becoming aware; trust service providers within 24 hours (sentence after no. 5).

if needed
Intermediate report
At the request of the CSIRT or the cybersecurity authority (no. 3); progress report if the incident is ongoing (no. 5).

1 month
Final report
No later than one month after submission of the notification, not after the incident (no. 4).

The structure and workflow of the template are a TOMORIS recommendation: you fill in Part A in advance and everything else during the incident. The law prescribes the deadlines, content, and recipients of the reports (§ 34 NISG 2026), significance (§ 35 NISG 2026, §§ 5 to 7 NISV 2026), and the obligations under Art. 33 GDPR. The field names follow the BCS forms for the alternative reporting channel (version 1.0, as of October 1, 2026); in the portal, the information requested there applies.

02

Part A: Master Data and Reporting Channel

Fill in advance: who reports, to which CSIRT, with which access, and with which deputy.

Master data of the entity (§ 29 para. 2 NISG 2026 and BCS forms)

ITEM	BASIS	ENTRY
Name; unique identifier, e.g., KUR (business register code), commercial register number, or ZVR number (register of associations)	§ 29 para. 2 no. 1, form	_____ _____
Essential or important; sectors and type under Annex 1 or 2; member states in which you provide services	§ 24, § 29 para. 2 no. 3, 4, 7	_____ _____

Competent CSIRTs, all of them if several sectors apply	§ 34 para. 1	_____ _____
Contact point: phone number and email address	§ 29 para. 6	_____ _____
Main contact person during an incident and deputy	Form	_____ _____
Registered with the cybersecurity authority on; persons authorized to report in NIS2-Services	§ 29 para. 3	_____ _____
Trust service provider? Then notification within 24 hours	§ 34 para. 2	yes / no
IT service provider with power of representation: name, scope	Explanatory notes NISV	_____ _____
Data protection officer or other contact point	Art. 33(3) GDPR	_____ _____

According to the BCS forms, the competent bodies are GovCERT for public administration (§ 8 para. 4 NISG 2026), Austrian HealthCERT for healthcare, and the national CERT for all other sectors; addresses for the alternative reporting channel: reports@govcert.gv.at, reports@a-healthcert.at, and reports@cert.at. Reporting obligations can also be fulfilled by a third party with the appropriate power of representation, such as your IT service provider (explanatory notes on § 5 NISV 2026). A supplier's report does not release you from your obligation: if the incident is significant for both entities, both report (BCS).

03

Part B: Points in Time, Deadlines, and Log

From the moment of becoming aware, the 24 and 72 hours run, including on weekends. This part covers points in time, deadlines, and the log.

The early warning and notification are due within 24 and 72 hours, respectively, after becoming aware of the significant incident (§ 34 para. 2 no. 1 and 2 NISG 2026). According to the BCS, the 24 hours also run on weekends, even if you do not offer your services then. The law does not define exactly what “becoming aware” means. The BCS forms ask for the start and the first detection or awareness, each with date and time in Central European Time.

Points in time and deadlines (CET or CEST)

POINT IN TIME	BASIS	DUE BY	DONE ON, BY
Start of the incident, if known	Form	–	_____
First detected or became aware	§ 34 para. 2 no. 1	–	_____
Decision on significance (Part C)	§ 35, § 5 NISV	–	_____
Early warning: awareness plus 24 hours	§ 34 para. 2 no. 1	_____	_____
CSIRT response: early warning plus 24 hours	§ 34 para. 4	_____	_____
Notification: awareness plus 72 hours; incident ID	§ 34 para. 2 no. 2	_____	_____

Final report: notification plus one month	§ 34 para. 2 no. 4	_____	_____
With a progress report: end of handling plus one month	§ 34 para. 2 no. 5	_____	_____

TOMORIS recommendation: if in doubt, calculate the deadlines from the earliest documented point in time and keep a log from the first observation. It provides the information for all reports and, if personal data is affected, serves as documentation under Art. 33(5) GDPR.

Incident log: observations, decisions, submissions with incident ID, CSIRT requests, customer information, criminal complaints

DATE, TIME	EVENT, DECISION, SUBMISSION	WHO	EVIDENCE
_____	_____ _____ _____ _____	_____	_____
_____	_____ _____ _____ _____	_____	_____
_____	_____ _____ _____ _____	_____	_____
_____	_____ _____ _____ _____	_____	_____
_____	_____ _____ _____ _____	_____	_____
_____	_____ _____ _____ _____	_____	_____

04

Part C: Significance Checklist

§ 35 NISG 2026 and the criteria of § 5 NISV 2026; for digital providers, the EU thresholds of IR 2024/2690.

You must report every significant cybersecurity incident, meaning an event that compromises the availability, authenticity, integrity, or confidentiality of data or services (§ 3 no. 30 NISG 2026) and is significant. The NISV 2026 (BGBl. II No. 290/2026, promulgated on October 1, 2026) lists in § 5 cases that are significant in any case. According to the explanatory notes, “is capable of causing” in § 5 para. 1 no. 1 to 3 means that the effect is to be expected in the near future in the ordinary course of events. Check what has occurred or is imminent in this way.

- ☐ § 35 para. 1 NISG 2026: severe operational disruption of the services or severe financial losses for the entity (no. 1), or considerable material or non-material damage to other persons (no. 2).
- ☐ § 5 para. 1 no. 1 NISV 2026: direct financial loss exceeding €500,000 or 5% of annual turnover in the previous financial year, whichever is lower.
- ☐ No. 2: leakage of trade secrets within the meaning of § 26b UWG (Austrian Unfair Competition Act) or of information subject to secrecy under § 6 IFG (Austrian Freedom of Information Act).

- [ ] No. 3 and 4: death or serious damage to the health of a natural person.
- [ ] No. 5: successful, suspected malicious, and unauthorized access to network and information systems that is likely to cause severe operational disruption.
- [ ] No. 6 with § 7: at least two incidents in six months that are not significant on their own, with the same apparent root cause and impact, which together exceed the threshold from no. 1.
- [ ] No. 7 and 8: outage or limited availability of the services for more than 24 hours, for more than 100,000 users or 10% of users (whichever is lower), or in the territory of at least one federal state.
- [ ] No. 9: the incident has activated crisis management or disaster recovery plans of business continuity management.
- [ ] Exclusion under § 6 NISV 2026: only a scheduled interruption of operations or the planned consequences of scheduled maintenance work. This is not a significant incident.

The general criteria continue to apply alongside § 5 NISV 2026. Under § 35 para. 2 NISG 2026, these include the dependence of other sectors on your service, effects on the environment, public safety, or health, your market share, the affected area including cross-border impact, the affected systems, the severity of the threat, exploited vulnerabilities, and experience with similar incidents.

> For entities under IR (EU) 2024/2690 (DNS, TLD name registries, cloud, data centers, content delivery networks, managed services and managed security services, online marketplaces, search engines, social networks, trust services), its Art. 3 and 4 and, depending on the type, Art. 5 to 14 apply; according to the explanatory notes, § 5 NISV 2026 governs the other entities. Managed services and managed security services additionally under Art. 10: completely unavailable for more than 30 minutes, limited for more than one hour for more than 5% or 1 million users in the Union (whichever is lower), or data compromised by a suspected malicious act or for this group of users.

Result of the review

RESULT	ENTRY
Significant: yes / no / still open; criteria met	_____ _____ _____ _____
Reasoning in two or three sentences	_____ _____ _____ _____ _____ _____ _____ _____
Decided by, date, time; review again on	_____ _____ _____ _____

05

Part D: Early Warning within 24 Hours

Reduced to the essentials: so that the CSIRT is informed and you get support if needed.

Where applicable, state whether there is a suspicion that the incident was caused by unlawful or malicious acts or could have a cross-border impact (§ 34 para. 2 no. 1 NISG 2026). According to the BCS, the early warning should be reduced to the essentials and can only be submitted once; if the more detailed information is already available, you can submit the notification directly within the 24 hours. Take the entity, contact person, and points in time from Parts A and B.

Early warning information (§ 34 para. 2 no. 1 NISG 2026, fields of the BCS form)

ITEM	BASIS	ENTRY
Short name of the incident; internal reference code	Form	_____ _____
Affected sectors; trust service affected?	Form	_____ _____
Suspicion of unlawful or malicious acts	§ 34 para. 2 no. 1	yes / no / unknown
Impact only in Austria? Otherwise, affected countries	§ 34 para. 2 no. 1	_____ _____
Brief description: possible causes, immediate effects, affected systems	Form	_____ _____ _____ _____
Impact and severity: on your services, other companies in the industry, suppliers	Form	_____ _____ _____ _____
Already publicly known?	Form	yes / no
Support from the CSIRT requested? What kind?	§ 34 para. 4	_____ _____

The report does not replace a criminal complaint to the police (note in the BCS form); if a criminal background is suspected, the CSIRT provides guidance on reporting to law enforcement authorities (§ 34 para. 4 NISG 2026). A report in Austria does not automatically fulfill reporting obligations in other member states (BCS).

06

Part E: Notification within 72 Hours

Update the early warning, initial assessment with severity and impact, and indicators of compromise where available.

The notification updates the early warning where applicable and contains an initial assessment, including severity and impact, as well as indicators of compromise where available (§ 34 para. 2 no. 2 NISG 2026). According to the BCS, information from the early warning is carried over and can be updated; the notification can also be submitted only once.

Additional notification information (§ 34 para. 2 no. 2 NISG 2026, fields of the BCS form)

ITEM	BASIS	ENTRY
Is the incident still ongoing? If not: resolved on	Form	_____ _____
Causes: malicious act (such as ransomware, DoS), system failure, human error, external event, supply chain; known vulnerabilities	Form	_____ _____ _____ _____
Indicators of compromise: IP addresses, URLs, domains, file hashes, network or email data	§ 34 para. 2 no. 2	_____ _____ _____ _____
Initial assessment of severity and impact; criteria from Part C	§ 34 para. 2 no. 2	_____ _____ _____ _____
Recurring incident? Previous incident ID	§ 7 NISV, form	_____ _____
Mitigation and recovery measures taken or planned	Form	_____ _____ _____ _____
Recipients of the services informed? (Part G)	§ 34 para. 3	yes / no / unknown
Criminal complaint or report to other authorities, including abroad: when, where, case number	Form	_____ _____

07

Part F: Intermediate, Progress, and Final Report

What follows the notification: on request, if the incident is ongoing, and no later than one month after the notification.

Reports after the notification (§ 34 para. 2 no. 3 to 5 NISG 2026, BCS guidance)

Intermediate report	At the request of the CSIRT or the cybersecurity authority: relevant status updates (no. 3); according to the BCS, possibly several times.
Progress report	If the incident is still ongoing when the final report is due, a progress report by then; the final report follows no later than one month after incident handling ends (no. 5).

Final report	No later than one month after the notification (no. 4), only once and not for an ongoing incident; after that, nothing more is possible, not even a withdrawal (BCS). If all information is already available within the deadlines and handling is complete, the final report alone is sufficient according to the BCS; however, anyone who waits for more precise information in order to skip the early warning and notification does not report on time.
Withdrawal	If the presumed basis for the reporting obligation no longer applies: after the early warning or notification, before the final report, with reasons (BCS; explanatory notes on § 5 NISV 2026).

Content of the final report (§ 34 para. 2 no. 4 NISG 2026, fields of the BCS form)

ITEM	BASIS	ENTRY
Detailed description of the incident, including severity and impact	No. 4 lit. a	_____ _____ _____ _____
Type of threat and underlying root causes that likely triggered the incident	No. 4 lit. b	_____ _____ _____ _____
Mitigation measures applied and ongoing	No. 4 lit. c	_____ _____ _____ _____
Cross-border impact, where applicable	No. 4 lit. d	_____ _____
Incident successfully resolved on	Form	_____ _____
Follow-up measures against similar incidents	Form	_____ _____ _____ _____

08

Part G: Recipients of the Services and Data Protection

Inform customers under § 34 para. 3 NISG 2026 and check the notification under Art. 33 GDPR in parallel.

If the significant incident affects the provision of your service, inform the recipients of your services without undue delay and, where possible, communicate any measures or remedies they can take in response (§ 34 para. 3 NISG 2026).

Information for recipients of the services

ITEM	ENTRY
Affected service and affected recipients	_____ _____ _____ _____
Channel and sender; informed on, approved by	_____ _____ _____ _____
Measures that recipients can take themselves	_____ _____ _____ _____

Model text, to be adapted to your case: “Dear Sir or Madam, on [MM/DD/YYYY] we detected a cybersecurity incident affecting [service]. [Scope] is affected. We have initiated [measures]. Please [measure for recipients]. Your contact person: [name, function, contact details]. We will update you again on [MM/DD/YYYY].”

If personal data is affected, the controller notifies the supervisory authority of the breach without undue delay and, where feasible, within 72 hours after having become aware of it, 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). According to the BCS, this obligation remains unaffected alongside the NIS2 report.

- [ ] Categories and approximate number of affected persons and records identified, risk to rights and freedoms assessed (Art. 33(1) and (3) GDPR); the breach is documented with facts, effects, and remedial action, even if there is no notification obligation (Art. 33(5)).
- [ ] Notification to the Data Protection Authority: nature of the breach, contact details of the data protection officer or another contact point, likely consequences, measures taken or proposed; after 72 hours, with reasons for the delay; provide missing information in phases (Art. 33(1), (3), and (4)).
- [ ] Likely high risk: affected persons notified without undue delay, unless an exception under Art. 34(3) applies (Art. 34(1)).
- [ ] As a processor: controller informed without undue delay (Art. 33(2)).

Pending, not applicable law: on November 19, 2025, the European Commission proposed a Digital Omnibus Regulation (COM(2025) 837). Under it, notification to the supervisory authority would only be required in the case of a likely high risk and, where feasible, within 96 hours, via a single entry point operated by ENISA. As of October 25, 2026, the proposal has not been adopted; Art. 33 GDPR applies unchanged.

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

09

Sources

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

1 **NISG 2026, BGBl. I No. 94/2025, current version in the RIS**
Version as of October 25, 2026, unchanged since the original version; §§ 3 no. 30, 8, 24, 29, 34, 35; accessed October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

2 **NISV 2026, BGBl. II No. 290/2026, authentic promulgation in the RIS**
§§ 5 to 7; current version unchanged on October 25, 2026; 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**
On § 5: scope, reporting by representatives, withdrawal, “is capable of causing”; accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...

4 **Federal Office for Cyber Security: Reporting obligation and deadlines**
NIS2-Services, alternative reporting channel, report types, withdrawal; page dated October 5, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/303/meldepflicht-und-friste...

5 **Federal Office for Cyber Security: Law and documents, reporting forms for the alternative reporting channel**
Forms for early warning, notification, final report, and withdrawal, version 1.0, as of October 1, 2026; accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/501/start.html

6 **Federal Office for Cyber Security: Frequently asked questions, reports**
Weekends, suppliers, several member states; page dated September 25, 2026, accessed October 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/meldungen.html

7 **Implementing Regulation (EU) 2024/2690, significant incidents**
Art. 1, 3, 4, and 10; OJ L of October 18, 2024
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2690

8 **Regulation (EU) 2016/679 (GDPR), Art. 33 and 34**
Notification to the supervisory authority and communication to data subjects
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

9 **Datenschutzgesetz (DSG, Austrian Data Protection Act), § 18 Data Protection Authority**
§ 18 para. 1, version as of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...

10 **Commission proposal for a Digital Omnibus Regulation, COM(2025) 837**
Explanatory memorandum and Art. 33 GDPR and Art. 23a NIS2 Directive in the proposed version; procedure 2025/0360(COD)
eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837