

VORLAGE · TOMORIS TOOLBOX

# NIS2-Vorfallmeldung: Vorlage für Frühwarnung, Meldung und Abschlussbericht

Arbeitsblatt zum Ausfüllen: Angaben je Meldestufe nach § 34 NISG 2026, Erheblichkeit nach NISV 2026, Kundeninformation, DSGVO-Prüfung und Protokoll

STAND

25.10.2026

UMFANG

PDF, 10 Seiten

ONLINE

[tomoris.com/downloads/nis2-vorfallmeldung-vorlage](https://tomoris.com/downloads/nis2-vorfallmeldung-vorlage)

## AUF EINEN BLICK

**24 h**

Frühwarnung ab Kenntnisnahme

**72 h**

Meldung mit erster Bewertung

**1 Monat**

Abschlussbericht nach der Meldung

**9**

Kriterien „jedenfalls erheblich“ in § 5 NISV 2026

## FÜR WEN

- Wesentliche und wichtige Einrichtungen nach dem NISG 2026
- Informationssicherheitsbeauftragte, IT-Leitung und Notfallverantwortliche
- IT-Dienstleister, die Kunden im Vorfall unterstützen oder mit Vertretungsbefugnis für sie melden

## WURUM ES GEHT

Wesentliche und wichtige Einrichtungen melden einen erheblichen Cybersicherheitsvorfall in Stufen an das zuständige CSIRT: Frühwarnung binnen 24 Stunden ab Kenntnisnahme, Meldung binnen 72 Stunden, Abschlussbericht spätestens einen Monat nach der Meldung (§ 34 NISG 2026). Übermittelt wird über die Anwendung NIS2-Services im Unternehmensserviceportal. Dieses Arbeitsblatt sammelt intern, was Sie dafür brauchen: Stammdaten, Zeitpunkte, die Prüfung der Erheblichkeit nach § 35 NISG 2026 und § 5 NISV 2026, die Angaben je Meldestufe mit Fundstelle, die Information Ihrer Kunden, die parallele Prüfung nach Art. 33 DSGVO und ein Protokoll.

Diese Vorlage ist an Ihre Einrichtung anzupassen und ersetzt keine Rechtsberatung. Sie sammelt Angaben intern; gemeldet wird über den Meldeweg des zuständigen CSIRT. Maßgeblich sind der Gesetzestext von NISG 2026, NISV 2026 und DSGVO in der jeweils geltenden Fassung sowie die im Meldeportal verlangten Angaben.

### INHALT

|           |                                                             |           |
|-----------|-------------------------------------------------------------|-----------|
| <b>01</b> | So arbeiten Sie mit der Vorlage .....                       | <b>2</b>  |
| <b>02</b> | Teil A: Stammdaten und Meldeweg .....                       | <b>3</b>  |
| <b>03</b> | Teil B: Zeitpunkte, Fristen und Protokoll .....             | <b>4</b>  |
| <b>04</b> | Teil C: Prüfliste Erheblichkeit .....                       | <b>5</b>  |
| <b>05</b> | Teil D: Frühwarnung binnen 24 Stunden .....                 | <b>6</b>  |
| <b>06</b> | Teil E: Meldung binnen 72 Stunden .....                     | <b>7</b>  |
| <b>07</b> | Teil F: Zwischen-, Fortschritts- und Abschlussbericht ..... | <b>8</b>  |
| <b>08</b> | Teil G: Empfänger der Dienste und Datenschutz .....         | <b>9</b>  |
| <b>09</b> | Quellen .....                                               | <b>10</b> |

## 01 —

# So arbeiten Sie mit der Vorlage

Intern sammeln, über NIS2-Services melden: was das Arbeitsblatt leistet und was es nicht ersetzt.

Diese Vorlage ist ein internes Arbeitsblatt. Die Meldung selbst übermitteln Sie über die Anwendung NIS2-Services, die das Bundesamt für Cybersicherheit (BCS) über das Unternehmensserviceportal bereitstellt. Nur wenn das Meldeportal vorübergehend technisch nicht verfügbar ist, nennt das BCS als alternativen Meldeweg PDF-Formulare für jeden Meldetyp. Empfänger ist das für Sie zuständige CSIRT; es leitet die Meldung unverzüglich an die Cybersicherheitsbehörde weiter (§ 34 Abs. 1 NISG 2026). Für Einrichtungen der öffentlichen Verwaltung arbeitet das BCS laut eigener Seite noch an einer Anbindung über den Portalverbund (Stand 5. Oktober 2026).

### Die Meldestufen nach § 34 Abs. 2 NISG 2026



Aufbau und Arbeitsweise der Vorlage sind eine Empfehlung von TOMORIS: Teil A füllen Sie vorab aus, alles Weitere im Vorfall. Gesetzlich vorgegeben sind Fristen, Inhalte und Empfänger der Meldungen (§ 34 NISG 2026), die Erheblichkeit (§ 35 NISG 2026, §§ 5 bis 7 NISV 2026) und die Pflichten nach Art. 33 DSGVO. Die Feldnamen folgen den BCS-Formularen für den alternativen Meldeweg (Version 1.0, Stand 1. Oktober 2026); im Portal gelten die dort verlangten Angaben.

## 02

# Teil A: Stammdaten und Meldeweg

Vorab ausfüllen: wer meldet, an welches CSIRT, mit welchem Zugang und welcher Vertretung.

### Stammdaten der Einrichtung (§ 29 Abs. 2 NISG 2026 und BCS-Formulare)

| ANGABE                                                                                                                 | GRUNDLAGE                   | EINTRAG   |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------|-----------|
| <b>Name; eindeutige Kennziffer, z. B. KUR, Firmenbuchnummer oder ZVR-Zahl</b>                                          | § 29 Abs. 2 Z 1, Formular   | _____     |
| <b>Wesentlich oder wichtig; Sektoren und Art nach Anlage 1 oder 2; Mitgliedstaaten, in denen Sie Dienste erbringen</b> | § 24, § 29 Abs. 2 Z 3, 4, 7 | _____     |
| <b>Zuständige CSIRTs, bei mehreren Sektoren alle</b>                                                                   | § 34 Abs. 1                 | _____     |
| <b>Kontaktstelle: Telefonnummer und E-Mail-Adresse</b>                                                                 | § 29 Abs. 6                 | _____     |
| <b>Hauptansprechperson im Vorfall und Vertretung</b>                                                                   | Formular                    | _____     |
| <b>Registriert bei der Cybersicherheitsbehörde am; meldeberechtigte Personen in NIS2-Services</b>                      | § 29 Abs. 3                 | _____     |
| <b>Vertrauensdiensteanbieter? Dann Meldung binnen 24 Stunden</b>                                                       | § 34 Abs. 2                 | ja / nein |
| <b>IT-Dienstleister mit Vertretungsbefugnis: Name, Umfang</b>                                                          | Erläuterungen NISV          | _____     |
| <b>Datenschutzbeauftragter oder sonstige Anlaufstelle</b>                                                              | Art. 33 Abs. 3 DSGVO        | _____     |

Zuständig sind laut BCS-Formularen das GovCERT für die öffentliche Verwaltung (§ 8 Abs. 4 NISG 2026), das Austrian HealthCERT für das Gesundheitswesen und das nationale CERT für alle weiteren Sektoren; Adressen für den alternativen Meldeweg: reports@govcert.gv.at, reports@a-healthcert.at und reports@cert.at. Berichtspflichten kann bei entsprechender Vertretungsbefugnis auch ein Dritter erfüllen, etwa Ihr IT-Dienstleister (Erläuterungen zu § 5 NISV 2026). Die Meldung eines Lieferanten entbindet Sie nicht: Ist der Vorfall für beide Einrichtungen erheblich, melden beide (BCS).

### 03

## Teil B: Zeitpunkte, Fristen und Protokoll

Ab der Kenntnisnahme laufen 24 und 72 Stunden, auch am Wochenende. Hier stehen Zeitpunkte, Fristen und Protokoll.

Frühwarnung und Meldung sind binnen 24 bzw. 72 Stunden nach Kenntnisnahme des erheblichen Vorfalls fällig (§ 34 Abs. 2 Z 1 und 2 NISG 2026). Die 24 Stunden laufen laut BCS auch am Wochenende, wenn Sie Ihre Dienste dann nicht anbieten. Was „Kenntnisnahme“ genau ist, definiert das Gesetz nicht. Die BCS-Formulare fragen nach Beginn und erstmaligem Erkennen bzw. Kenntnisnahme, jeweils mit Datum und Uhrzeit in mitteleuropäischer Zeit.

### Zeitpunkte und Fristen (MEZ bzw. MESZ)

| ZEITPUNKT                                                          | GRUNDLAGE       | FÄLLIG BIS | ERLEDIGT AM, VON |
|--------------------------------------------------------------------|-----------------|------------|------------------|
| <b>Beginn des Vorfalls, soweit bekannt</b>                         | Formular        | –          | _____            |
| <b>Erstmals erkannt bzw. zur Kenntnis genommen</b>                 | § 34 Abs. 2 Z 1 | –          | _____            |
| <b>Entscheidung über die Erheblichkeit (Teil C)</b>                | § 35, § 5 NISV  | –          | _____            |
| <b>Frühwarnung: Kenntnisnahme plus 24 Stunden</b>                  | § 34 Abs. 2 Z 1 | _____      | _____            |
| <b>Antwort des CSIRT: Frühwarnung plus 24 Stunden</b>              | § 34 Abs. 4     | _____      | _____            |
| <b>Meldung: Kenntnisnahme plus 72 Stunden; Incident-ID</b>         | § 34 Abs. 2 Z 2 | _____      | _____            |
| <b>Abschlussbericht: Meldung plus ein Monat</b>                    | § 34 Abs. 2 Z 4 | _____      | _____            |
| <b>Bei Fortschrittsbericht: Ende der Behandlung plus ein Monat</b> | § 34 Abs. 2 Z 5 | _____      | _____            |

Empfehlung von TOMORIS: Rechnen Sie die Fristen im Zweifel ab dem frühesten dokumentierten Zeitpunkt und führen Sie ab der ersten Beobachtung ein Protokoll. Es liefert die Angaben für alle Berichte und dient, wenn personenbezogene Daten betroffen sind, der Dokumentation nach Art. 33 Abs. 5 DSGVO.

**Vorfallsprotokoll: Beobachtungen, Entscheidungen, Übermittlungen mit Incident-ID, Ersuchen des CSIRT, Kundeninformation, Anzeigen**

| DATUM, UHRZEIT | EREIGNIS, ENTSCHEIDUNG, ÜBERMITTLUNG | WER   | BELEG |
|----------------|--------------------------------------|-------|-------|
| -----          | -----                                | ----- | ----- |
| -----          | -----                                | ----- | ----- |
| -----          | -----                                | ----- | ----- |
| -----          | -----                                | ----- | ----- |
| -----          | -----                                | ----- | ----- |
| -----          | -----                                | ----- | ----- |

**04**

## Teil C: Prüfliste Erheblichkeit

§ 35 NISG 2026 und die Kriterien des § 5 NISV 2026; für digitale Anbieter die EU-Schwellen der DVO 2024/2690.

Melden müssen Sie jeden erheblichen Cybersicherheitsvorfall, also ein Ereignis, das Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder Diensten beeinträchtigt (§ 3 Z 30 NISG 2026) und erheblich ist. Die NISV 2026 (BGBl. II Nr. 290/2026, kundgemacht am 1. Oktober 2026) nennt in § 5 Fälle, die jedenfalls erheblich sind. „Kann verursachen“ in § 5 Abs. 1 Z 1 bis 3 heißt laut Erläuterungen: Die Auswirkung ist bei gewöhnlichem Verlauf der Dinge in naher Zukunft zu erwarten. Kreuzen Sie an, was eingetreten ist oder so bevorsteht.

- ☐ § 35 Abs. 1 NISG 2026: schwerwiegende Betriebsstörungen der Dienste oder schwerwiegende finanzielle Verluste der Einrichtung (Z 1) oder erhebliche materielle oder immaterielle Schäden bei anderen Personen (Z 2).
- ☐ § 5 Abs. 1 Z 1 NISV 2026: direkter finanzieller Verlust von mehr als 500 000 EUR oder 5 % des Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Wert niedriger ist.
- ☐ Z 2: Abfluss von Geschäftsgeheimnissen im Sinne von § 26b UWG oder von Informationen, die nach § 6 IFG der Geheimhaltung unterliegen.
- ☐ Z 3 und 4: Tod oder schwere Schädigung der Gesundheit einer natürlichen Person.
- ☐ Z 5: erfolgreicher, mutmaßlich böswilliger und unbefugter Zugriff auf Netz- und Informationssysteme, der wahrscheinlich schwerwiegende Betriebsstörungen verursacht.
- ☐ Z 6 mit § 7: mindestens zwei für sich nicht erhebliche Vorfälle in sechs Monaten mit derselben offensichtlichen Ursache und Auswirkung, die zusammen die Schwelle aus Z 1 überschreiten.

- ☐ Z 7 und 8: Ausfall oder eingeschränkte Verfügbarkeit der Dienste für mehr als 24 Stunden, für mehr als 100 000 Nutzer oder 10 % der Nutzer (der niedrigere Wert) oder im Gebiet mindestens eines Bundeslandes.
- ☐ Z 9: Der Vorfall hat das Krisenmanagement oder Notfallwiederherstellungspläne des Betriebskontinuitätsmanagements aktiviert.
- ☐ Ausschluss nach § 6 NISV 2026: nur eine planmäßige Betriebsunterbrechung oder geplante Folgen planmäßiger Wartungsarbeiten. Das ist kein erheblicher Vorfall.

Die allgemeinen Kriterien gelten neben § 5 NISV 2026 weiter. Nach § 35 Abs. 2 NISG 2026 zählen etwa die Abhängigkeit anderer Sektoren von Ihrem Dienst, Folgen für Umwelt, öffentliche Sicherheit oder Gesundheit, Ihr Marktanteil, das betroffene Gebiet samt grenzüberschreitender Auswirkungen, die betroffenen Systeme, Schwere der Bedrohung, ausgenutzte Schwachstellen und Erfahrungen mit ähnlichen Vorfällen.

Für Einrichtungen nach der DVO (EU) 2024/2690 (DNS, TLD-Namenregister, Cloud, Rechenzentren, Inhaltszustecknetze, verwaltete Dienste und Sicherheitsdienste, Online-Marktplätze, Suchmaschinen, soziale Netzwerke, Vertrauensdienste) gelten deren Art. 3, 4 und je Art. 5 bis 14; § 5 NISV 2026 regelt laut Erläuterungen die übrigen Einrichtungen. Verwaltete Dienste und Sicherheitsdienste zusätzlich nach Art. 10: mehr als 30 Minuten vollständig nicht verfügbar, mehr als eine Stunde eingeschränkt für mehr als 5 % oder 1 Mio. Nutzer in der Union (der niedrigere Wert) oder Daten durch mutmaßlich böswillige Handlung oder für diesen Nutzerkreis beeinträchtigt.

#### Ergebnis der Prüfung

| ERGEBNIS                                           | EINTRAG        |
|----------------------------------------------------|----------------|
| Erheblich: ja / nein / noch offen; erfüllte Punkte | _____          |
| Begründung in zwei, drei Sätzen                    | _____<br>_____ |
| Entschieden von, Datum, Uhrzeit; erneut prüfen am  | _____          |

## 05

### Teil D: Frühwarnung binnen 24 Stunden

Auf das Wesentliche reduziert: damit das CSIRT informiert ist und Sie bei Bedarf Unterstützung bekommen.

Anzugeben ist gegebenenfalls, ob der Verdacht besteht, dass der Vorfall auf rechtswidrige und schuldhaft Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte (§ 34 Abs. 2 Z 1 NISG 2026). Laut BCS ist die Frühwarnung auf das Wesentliche zu reduzieren und nur einmal möglich; liegen die ausführlicheren Angaben schon vor, können Sie innerhalb der 24 Stunden gleich die Meldung abgeben. Einrichtung, Ansprechperson und Zeitpunkte übernehmen Sie aus Teil A und B.

### Angaben der Frühwarnung (§ 34 Abs. 2 Z 1 NISG 2026, Felder des BCS-Formulars)

| ANGABE                                                                                      | GRUNDLAGE       | EINTRAG               |
|---------------------------------------------------------------------------------------------|-----------------|-----------------------|
| Kurze Bezeichnung des Vorfalls; interner Referenzcode                                       | Formular        | _____                 |
| Betroffene Sektoren; Vertrauensdienst betroffen?                                            | Formular        | _____                 |
| Verdacht auf rechtswidrige und schuldhaft Handlungen                                        | § 34 Abs. 2 Z 1 | ja / nein / unbekannt |
| Nur Auswirkungen in Österreich? Sonst betroffene Staaten                                    | § 34 Abs. 2 Z 1 | _____                 |
| Kurzbeschreibung: mögliche Ursachen, unmittelbare Auswirkungen, betroffene Systeme          | Formular        | _____<br>_____        |
| Auswirkungen und Schweregrad: auf Ihre Dienste, andere Unternehmen der Branche, Lieferanten | Formular        | _____<br>_____        |
| Bereits öffentlich bekannt?                                                                 | Formular        | ja / nein             |
| Unterstützung durch das CSIRT gewünscht? Welche?                                            | § 34 Abs. 4     | _____                 |

Die Meldung ersetzt keine polizeiliche Anzeige (Hinweis im BCS-Formular); bei vermutetem strafrechtlichem Hintergrund gibt das CSIRT Orientierungshilfe für die Meldung an die Strafverfolgungsbehörden (§ 34 Abs. 4 NISG 2026). Eine Meldung in Österreich erfüllt nicht automatisch Meldepflichten in anderen Mitgliedstaaten (BCS).

## 06

## Teil E: Meldung binnen 72 Stunden

Frühwarnung aktualisieren, erste Bewertung mit Schweregrad und Auswirkungen, gegebenenfalls Kompromittierungsindikatoren.

Die Meldung aktualisiert gegebenenfalls die Frühwarnung und enthält eine erste Bewertung samt Schweregrad und Auswirkungen sowie gegebenenfalls die Kompromittierungsindikatoren (§ 34 Abs. 2 Z 2 NISG 2026). Angaben der Frühwarnung werden laut BCS übernommen und können aktualisiert werden; auch die Meldung ist nur einmal möglich.

### Zusätzliche Angaben der Meldung (§ 34 Abs. 2 Z 2 NISG 2026, Felder des BCS-Formulars)

| ANGABE                                                                                                                                             | GRUNDLAGE       | EINTRAG        |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----------------|
| Hält der Vorfall noch an? Wenn nein: behoben am                                                                                                    | Formular        | _____          |
| Ursachen: böswilliges Handeln (etwa Ransomware, DoS), Systemfehler, menschliches Versagen, externes Ereignis, Lieferkette; bekannte Schwachstellen | Formular        | _____<br>_____ |
| Kompromittierungsindikatoren: IP-Adressen, URLs, Domains, Datei-Hashes, Netzwerk- oder E-Mail-Daten                                                | § 34 Abs. 2 Z 2 | _____<br>_____ |

|                                                                                           |                    |                       |
|-------------------------------------------------------------------------------------------|--------------------|-----------------------|
| <b>Erste Bewertung von Schweregrad und Auswirkungen; Kriterien aus Teil C</b>             | § 34 Abs. 2 Z 2    | _____                 |
| <b>Wiederkehrender Vorfall? Frühere Incident-ID</b>                                       | § 7 NISV, Formular | _____                 |
| <b>Getroffene oder geplante Abhilfe- und Wiederherstellungsmaßnahmen</b>                  | Formular           | _____                 |
| <b>Empfänger der Dienste unterrichtet? (Teil G)</b>                                       | § 34 Abs. 3        | ja / nein / unbekannt |
| <b>Anzeige oder Meldung an weitere Behörden, auch im Ausland: wann, wo, Geschäftszahl</b> | Formular           | _____                 |

## 07

# Teil F: Zwischen-, Fortschritts- und Abschlussbericht

Was nach der Meldung folgt: auf Ersuchen, bei andauerndem Vorfall und spätestens einen Monat nach der Meldung.

## Berichte nach der Meldung (§ 34 Abs. 2 Z 3 bis 5 NISG 2026, Hinweise des BCS)

|                            |                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Zwischenbericht</b>     | Auf Ersuchen des CSIRT oder der Cybersicherheitsbehörde: relevante Statusaktualisierungen (Z 3); laut BCS auch mehrfach.                                                                                                                                                                                                                                                                                |
| <b>Fortschrittsbericht</b> | Dauert der Vorfall bei Fälligkeit des Abschlussberichts an, bis dahin ein Fortschrittsbericht; der Abschlussbericht folgt spätestens einen Monat nach Ende der Vorfallsbehandlung (Z 5).                                                                                                                                                                                                                |
| <b>Abschlussbericht</b>    | Spätestens einen Monat nach der Meldung (Z 4), nur einmal und nicht zu einem andauernden Vorfall; danach ist nichts mehr möglich, auch kein Widerruf (BCS). Liegen schon binnen der Fristen alle Angaben vor und ist die Behandlung abgeschlossen, genügt laut BCS der Abschlussbericht; wer aber auf genauere Informationen wartet, um Frühwarnung und Meldung zu ersparen, meldet nicht fristgerecht. |
| <b>Widerruf</b>            | Fällt die vermutete Grundlage der Berichtspflicht weg: nach Frühwarnung oder Meldung, vor dem Abschlussbericht, mit Begründung (BCS; Erläuterungen zu § 5 NISV 2026).                                                                                                                                                                                                                                   |

## Inhalt des Abschlussberichts (§ 34 Abs. 2 Z 4 NISG 2026, Felder des BCS-Formulars)

| ANGABE                                                                                                 | GRUNDLAGE  | EINTRAG |
|--------------------------------------------------------------------------------------------------------|------------|---------|
| <b>Ausführliche Beschreibung des Vorfalls samt Schweregrad und Auswirkungen</b>                        | Z 4 lit. a | _____   |
| <b>Art der Bedrohung und zugrundeliegende Ursachen, die den Vorfall wahrscheinlich ausgelöst haben</b> | Z 4 lit. b | _____   |
| <b>Getroffene und laufende Abhilfemaßnahmen</b>                                                        | Z 4 lit. c | _____   |

|                                                         |            |                |
|---------------------------------------------------------|------------|----------------|
| <b>Gegebenenfalls grenzüberschreitende Auswirkungen</b> | Z 4 lit. d | _____          |
| <b>Vorfall erfolgreich behoben am</b>                   | Formular   | _____          |
| <b>Folgemaßnahmen gegen ähnliche Vorfälle</b>           | Formular   | _____<br>_____ |

## 08

# Teil G: Empfänger der Dienste und Datenschutz

Kunden nach § 34 Abs. 3 NISG 2026 informieren und parallel die Meldung nach Art. 33 DSGVO prüfen.

Beeinträchtigt der erhebliche Vorfall die Erbringung Ihres Dienstes, unterrichten Sie die Empfänger Ihrer Dienste unverzüglich und teilen, soweit möglich, alle Maßnahmen oder Abhilfemaßnahmen mit, die diese als Reaktion ergreifen können (§ 34 Abs. 3 NISG 2026).

## Information der Empfänger der Dienste

| ANGABE                                                      | EINTRAG |
|-------------------------------------------------------------|---------|
| <b>Beeinträchtigter Dienst und betroffene Empfänger</b>     | _____   |
| <b>Kanal und Absender; informiert am, freigegeben von</b>   | _____   |
| <b>Maßnahmen, die die Empfänger selbst ergreifen können</b> | _____   |

Mustertext, an Ihren Fall anzupassen: „Sehr geehrte Damen und Herren, am [Datum] haben wir einen Cybersicherheitsvorfall festgestellt, der [Dienst] beeinträchtigt. Betroffen ist [Umfang]. Wir haben [Maßnahmen] eingeleitet. Bitte [Maßnahme für Empfänger]. Ihre Ansprechperson: [Name, Funktion, Kontakt]. Wir informieren Sie erneut am [Datum].“

Sind personenbezogene Daten betroffen, meldet der Verantwortliche die Verletzung unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt wurde, 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). Diese Pflicht bleibt laut BCS neben der NIS2-Meldung unberührt.

- ☐ Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze erhoben, Risiko für die Rechte und Freiheiten bewertet (Art. 33 Abs. 1 und 3 DSGVO); die Verletzung ist mit Fakten, Auswirkungen und Abhilfemaßnahmen dokumentiert, auch ohne Meldepflicht (Art. 33 Abs. 5).
- ☐ Meldung an die Datenschutzbehörde: Art der Verletzung, Kontakt des Datenschutzbeauftragten oder einer Anlaufstelle, wahrscheinliche Folgen, ergriffene oder vorgeschlagene Maßnahmen; nach 72 Stunden mit Begründung der Verzögerung; Fehlendes schrittweise nachreichen (Art. 33 Abs. 1, 3 und 4).

- ☐ Voraussichtlich hohes Risiko: betroffene Personen unverzüglich benachrichtigt, außer eine Ausnahme nach Art. 34 Abs. 3 greift (Art. 34 Abs. 1).
- ☐ Als Auftragsverarbeiter: Verantwortlichen unverzüglich informiert (Art. 33 Abs. 2).

Im Verfahren, nicht geltend: Die Europäische Kommission hat am 19. November 2025 eine Digital-Omnibus-Verordnung vorgeschlagen (COM(2025) 837). Danach wäre der Aufsichtsbehörde nur bei voraussichtlich hohem Risiko und nach Möglichkeit binnen 96 Stunden zu melden, über eine zentrale Anlaufstelle der ENISA. Mit Stand 25. Oktober 2026 ist der Vorschlag nicht beschlossen; Art. 33 DSGVO gilt unverändert.

#### NÄCHSTER SCHRITT

## Selbst prüfen oder gemeinsam umsetzen

#### KOSTENLOS PRÜFEN

**NIS2-Betroffenheitscheck**  
[tomoris.com/tools/nis2-check](https://tomoris.com/tools/nis2-check)

#### UMSETZUNG BESPRECHEN

**Kontakt aufnehmen**  
[tomoris.com/contact](https://tomoris.com/contact)  
[contact@tomoris.com](mailto:contact@tomoris.com)

### 09

## Quellen

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

- 1 **NISG 2026, BGBl. I Nr. 94/2025, geltende Fassung im RIS**  
Fassung vom 25.10.2026, unverändert seit der Stammfassung; §§ 3 Z 30, 8, 24, 29, 34, 35; gelesen am 25.10.2026  
[www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...)
- 2 **NISV 2026, BGBl. II Nr. 290/2026, authentische Kundmachung im RIS**  
§§ 5 bis 7; geltende Fassung am 25.10.2026 unverändert; gelesen am 25.10.2026  
[www.ris.bka.gv.at/eli/bgbl/II/2026/290](https://www.ris.bka.gv.at/eli/bgbl/II/2026/290)
- 3 **Bundesamt für Cybersicherheit: Erläuterungen zur NISV 2026**  
Zu § 5: Anwendungsbereich, Meldung durch Vertreter, Widerruf, „kann verursachen“; gelesen am 25.10.2026  
[www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...](https://www.bundesamt-cybersicherheit.gv.at/501/files/nisv-2026-erlaeut...)
- 4 **Bundesamt für Cybersicherheit: Meldepflicht und Fristen**  
NIS2-Services, alternativer Meldeweg, Meldetypen, Widerruf; Seite vom 5.10.2026; gelesen am 25.10.2026  
[www.bundesamt-cybersicherheit.gv.at/303/meldepflicht-und-friste...](https://www.bundesamt-cybersicherheit.gv.at/303/meldepflicht-und-friste...)
- 5 **Bundesamt für Cybersicherheit: Recht und Dokumente, Meldeformulare für den alternativen Meldeweg**  
Formulare Frühwarnung, Meldung, Abschlussbericht und Widerruf, Version 1.0, Stand 1.10.2026; gelesen am 25.10.2026  
[www.bundesamt-cybersicherheit.gv.at/501/start.html](https://www.bundesamt-cybersicherheit.gv.at/501/start.html)
- 6 **Bundesamt für Cybersicherheit: Häufig gestellte Fragen, Meldungen**  
Wochenende, Lieferanten, mehrere Mitgliedstaaten; Seite vom 25.9.2026; gelesen am 25.10.2026  
[www.bundesamt-cybersicherheit.gv.at/faq/meldungen.html](https://www.bundesamt-cybersicherheit.gv.at/faq/meldungen.html)
- 7 **Durchführungsverordnung (EU) 2024/2690, erhebliche Sicherheitsvorfälle**  
Art. 1, 3, 4 und 10; ABl. L vom 18.10.2024  
[eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2690](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R2690)
- 8 **Verordnung (EU) 2016/679 (DSGVO), Art. 33 und 34**  
Meldung an die Aufsichtsbehörde und Benachrichtigung der Betroffenen  
[eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679)
- 9 **Datenschutzgesetz (DSG), § 18 Datenschutzbehörde**  
§ 18 Abs. 1, Fassung vom 25.10.2026  
[www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...](https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...)
- 10 **Vorschlag der Kommission für eine Digital-Omnibus-Verordnung, COM(2025) 837**  
Begründung sowie Art. 33 DSGVO und Art. 23a NIS-2-Richtlinie in der vorgeschlagenen Fassung; Verfahren 2025/0360(COD)  
[eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837](https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52025PC0837)