

LEITFADEN · TOMORIS TOOLBOX

NIS2 und Gemeinden: wer betroffen ist und was gilt

Die Ausnahme nach § 24 Abs. 3 NISG 2026, Prüffragen für Wasser-, Abwasser-, Abfall- und Energiebetriebe und was jede Gemeinde ohnehin tun sollte

STAND

25.10.2026

UMFANG

PDF, 12 Seiten

ONLINE

tomoris.com/downloads/nis2-gemeinden-leitfaden

AUF EINEN BLICK

§ 24

Abs. 3: Gemeinden nicht im Sektor öffentliche Verwaltung

Anlage 1

Trinkwasser, Abwasser, Energie: Betriebe gesondert prüfen

50

Beschäftigte: ab hier gilt ein Betrieb als mittelgroß

Art. 32

DSGVO: Datensicherheit gilt für jede Gemeinde

FÜR WEN

- Bürgermeisterinnen und Bürgermeister, Amtsleitungen und Gemeindevorstände
- Gemeinde-IT und IT-Dienstleister von Gemeinden
- Gemeindeverbände, etwa für Wasser, Abwasser und Abfall
- Geschäftsführungen kommunaler Betriebe wie Stadtwerke und Versorgungsunternehmen

WURUM ES GEHT

Seit 1. Oktober 2026 gilt das NISG 2026. Gemeinden und Gemeindeverbände zählen ausdrücklich nicht zum Sektor öffentliche Verwaltung (§ 24 Abs. 3). Ihre Betriebe für Trinkwasser, Abwasser, Abfall oder Energie können trotzdem erfasst sein. Dieser Leitfaden zeigt die Rechtslage, die Prüffragen für Gemeinde, Verband und Betrieb und was jede Gemeinde ohnehin tun sollte.

Dieser Leitfaden gibt einen Überblick und ersetzt keine Rechtsberatung. Maßgeblich ist der Gesetzestext in der jeweils geltenden Fassung, insbesondere §§ 24 bis 26 und die Anlagen 1 und 2 NISG 2026. Prüffragen, erste Schritte und Leitfäden sind Empfehlungen von TOMORIS.

INHALT

01	Die Kurzantwort	2
02	Die Rechtslage nach § 24 NISG 2026	3
03	Wann Gemeinden und ihre Betriebe trotzdem erfasst sind	4
04	Die Größe richtig ermitteln	6
05	Prüffragen für Gemeinde, Verband und Betrieb	7
06	Wenn ein Rechtsträger erfasst ist	8
07	Was jede Gemeinde ohnehin tun sollte	9
08	Häufige Missverständnisse	11
09	Quellen	12

01

Die Kurzantwort

Als Verwaltung ist die Gemeinde nicht erfasst. Ihre Betriebe können es sein, und Datenschutz gilt ohnehin.

Nein

Gemeinde als öffentliche Verwaltung

Gemeinden und Gemeindeverbände sind keine Einrichtungen im Sektor der öffentlichen Verwaltung (§ 24 Abs. 3 NISG 2026).

Prüfen

Kommunale Betriebe und Verbände

Wer eine Tätigkeit aus Anlage 1 oder 2 ausübt, etwa Trinkwasser, Abwasser, Abfall oder Energie, ist ab mittlerer Größe erfasst, sofern keine Einschränkung der Anlage greift (§ 24 Abs. 1 Z 3, Abs. 2 Z 1, § 25).

Ja

Datenschutz und Lieferkette

Die Sicherheit der Verarbeitung nach Art. 32 DSGVO gilt für jede Gemeinde. Erfasste Partner müssen die Sicherheit ihrer Lieferkette regeln (§ 32 Abs. 4 lit. d NISG 2026).

Das Bundesamt für Cybersicherheit beantwortet die Frage in seinen FAQ so: Gemeinden, „somit auch Städte“, und Gemeindeverbände sind im Sektor öffentliche Verwaltung ausdrücklich ausgenommen, „aber nicht pauschal vom Anwendungsbereich ausgeschlossen“. Betroffen sind sie, wenn sie in einem anderen Sektor der Anlage 1 oder 2 tätig sind, etwa Trinkwasser, Abwasser, Abfallwirtschaft, Energie, Verkehr oder digitale Infrastruktur, und die Größenkriterien für mittlere oder große Unternehmen erfüllen.

Ob eine Einrichtung wesentlich oder wichtig ist, folgt unmittelbar aus § 24 NISG 2026; ein Bescheid ist dafür nicht nötig. Erfasste Einrichtungen müssen sich selbst registrieren (§ 29). Daneben stuft die Cybersicherheitsbehörde kleinere Einrichtungen der Anlagen 1 und 2 mit Bescheid ein, wenn einer der Gründe des § 26 Abs. 3 vorliegt.

02

Die Rechtslage nach § 24 NISG 2026

Öffentliche Verwaltung wird nach Ebene eingestuft, nicht nach Größe. Gemeinden und Gemeindeverbände nimmt das Gesetz ausdrücklich aus.

Das NISG 2026 (BGBl. I Nr. 94/2025) setzt die NIS-2-Richtlinie um und gilt seit 1. Oktober 2026 (§ 51 Abs. 1 und 2). Die öffentliche Verwaltung stuft es nach Ebene ein, nicht nach Größe. Einrichtungen im Sektor der öffentlichen Verwaltung sind nach § 24 Abs. 3 Einrichtungen, die alle drei Merkmale erfüllen:

- Z 1: Sie wurden eingerichtet, um im öffentlichen Interesse liegende Aufgaben nicht gewerblicher Art zu erfüllen.
- Z 2: Sie unterstehen der Aufsicht von Bund oder Land oder sind an Weisungen eines obersten Organs gebunden, ihr Leitungs- oder Aufsichtsorgan wird mehrheitlich von Stellen des Bundes oder der Länder eingesetzt, Bund oder Land halten mindestens 50 vH des Kapitals, oder sie sind Mitglieder der Bundesregierung.
- Z 3: Sie sind ermächtigt, Bescheide zu erlassen, die Rechte Einzelner im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren.

Der Absatz endet mit den Worten „mit Ausnahme der Gemeinden sowie Gemeindeverbände“. Laut den Erläuterungen zur Regierungsvorlage wurde von der Möglichkeit, die lokale Ebene, innerstaatlich die Gemeinden, einzubeziehen, „kein Gebrauch gemacht“. An einer Stelle formulieren die Erläuterungen weiter („Neben den Gemeinden gelten auch Bildungseinrichtungen ... nicht als wesentliche oder wichtige Einrichtungen“). Maßgeblich ist der Gesetzestext, der Gemeinden nur aus dem Sektor öffentliche Verwaltung ausnimmt; so liest es auch das BCS.

Sektor öffentliche Verwaltung nach § 24 NISG 2026

EBENE	WER ERFASST IST	EINSTUFUNG
Bund	Einrichtungen nach Abs. 3, die Angelegenheiten der Bundesverwaltung besorgen und Bundesbehörde sind oder Rechtspersönlichkeit besitzen	wesentlich, unabhängig von der Größe (Abs. 1 Z 1 lit. d, Abs. 4)

Land	Ämter der Landesregierungen und Bezirkshauptmannschaften sowie Einrichtungen nach Abs. 3 mit Rechtspersönlichkeit, die Angelegenheiten der Landesverwaltung besorgen	wichtig, laut Erläuterungen ebenfalls unabhängig von der Größe (Abs. 2 Z 2, Abs. 5)
Gemeinden und Gemeindeverbände	ausdrücklich nicht Teil des Sektors, laut BCS auch Städte; § 24 Abs. 5 nennt nur die Bezirkshauptmannschaften, nicht die Magistrate der Statutarstädte	keine Einstufung als öffentliche Verwaltung (Abs. 3)
Weitere Ausnahmen	überwiegend nationale Sicherheit, öffentliche Sicherheit oder Strafverfolgung; Universitäts-, Hochschul- und Schulwesen; Gerichtsbarkeit; Gesetzgebung; Österreichische Nationalbank	weder wesentlich noch wichtig, außer als Vertrauensdiensteanbieter (Abs. 6)

Das deckt sich mit der NIS-2-Richtlinie: Sie erfasst die öffentliche Verwaltung der Zentralregierung und, nach einer risikobasierten Bewertung, der regionalen Ebene unabhängig von der Größe (Art. 2 Abs. 2 lit. f). Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene können die Mitgliedstaaten einbeziehen, müssen es aber nicht (Art. 2 Abs. 5 lit. a).

Sonderfall Wien: Der Wiener Magistrat hat auch die Funktion des Amtes der Landesregierung (Art. 108 B-VG), das § 24 Abs. 5 als Einrichtung der Landesebene nennt. Laut den Erläuterungen bedarf es einer „differenzierten Betrachtung“, „zumal die ‚lokale Ebene‘ ... vom Sektor der öffentlichen Verwaltung nicht umfasst sein soll“. Das Gesetz regelt das nicht eigens; prüfen Sie Wiener Einrichtungen im Einzelfall.

03

Wann Gemeinden und ihre Betriebe trotzdem erfasst sind

Die Ausnahme gilt nur für den Sektor öffentliche Verwaltung. In den anderen Sektoren zählen Tätigkeit und Größe, nicht die Eigentümerin.

Die Ausnahme steht nur in der Begriffsbestimmung des Sektors öffentliche Verwaltung. In den übrigen Sektoren gilt: Einrichtungen einer Art aus Anlage 1 sind wesentlich, wenn sie ein großes Unternehmen betreiben (§ 24 Abs. 1 Z 3); Einrichtungen einer Art aus Anlage 1 oder 2 sind wichtig, wenn sie ein mittleres oder großes Unternehmen betreiben (§ 24 Abs. 2 Z 1). Einrichtung ist jede natürliche oder juristische Person oder eingetragene Personengesellschaft, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann (§ 3 Z 10). Die Richtlinie nennt ausdrücklich „öffentliche oder private Einrichtungen“ (Art. 2 Abs. 1), und als Unternehmen gilt jede Einheit, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform (Art. 1 Anhang Empfehlung 2003/361/EG).

Arten von Einrichtungen, die bei Gemeinden und ihren Betrieben naheliegen (Auszug aus Anlage 1 und 2, gekürzt)

SEKTOR	ART DER EINRICHTUNG	EINSCHRÄNKUNG IM GESETZ
Trinkwasser (Anlage 1 Z 6)	Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ (§ 3 Z 2 LMSVG)	nur Lieferanten ausgenommen, deren allgemeine Tätigkeit die Lieferung anderer Rohstoffe und Güter ist und für die Trinkwasser dabei ein nicht wesentlicher Teil ist; Unternehmen der Wasserversorgung nennt die Ausnahme nicht

Abwasser (Anlage 1 Z 7)	Unternehmen, die kommunales, häusliches oder industrielles Abwasser sammeln, entsorgen oder behandeln	nicht, wenn das nur ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
Abfall (Anlage 2 Z 2)	Abfallsammler und Abfallbehandler (§ 2 Abs. 6 Z 3 und 4 AWG 2002)	nicht, wenn die Abfallbewirtschaftung nicht ihre (wirtschaftliche) Haupttätigkeit ist
Energie (Anlage 1 Z 1)	etwa Elektrizitätsunternehmen als Versorger, Verteilernetzbetreiber für Strom und Erdgas, Betreiber von Fernwärme und von Ladepunkten	Stromerzeuger nur bei gewerblicher oder beruflicher Haupttätigkeit
Verkehr (Anlage 1 Z 2 lit. d)	Straßenverkehrsbehörden, die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind; Betreiber intelligenter Verkehrssysteme (§ 2 Z 1 IVS-G)	öffentliche Stellen nicht, wenn Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme nur ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
Gesundheit (Anlage 1 Z 5)	Gesundheitsdienstleister, laut Erläuterungen etwa Krankenanstalten und Einrichtungen des Rettungswesens	Langzeitpflege und Pflegeheime laut Erläuterungen und BCS nicht erfasst; je nach Ausgestaltung im Einzelfall prüfen
Digitale Infrastruktur (Anlage 1 Z 8)	Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher Kommunikationsdienste	keine Größenschwelle (§ 24 Abs. 1 Z 2, Abs. 2 Z 3 lit. a)
Verwaltung von IKT-Diensten (Anlage 1 Z 9)	Anbieter verwalteter Dienste (MSP); laut BCS auch interne IT-Dienstleister, die mit administrativem Zugriff Systeme anderer Gesellschaften eines Unternehmensverbunds betreuen	nur ausgenommen, wenn ausschließlich von der betroffenen Einrichtung betrieben und genutzt

Ob eine Tätigkeit Haupt- oder Nebensache ist, spielt laut Bundesamt für Cybersicherheit (BCS) grundsätzlich keine Rolle. Einschränkungen enthält das Gesetz nur bei einzelnen Arten: Stromerzeuger (Haupttätigkeit), Trinkwasserlieferanten, deren allgemeine Tätigkeit die Lieferung anderer Rohstoffe und Güter ist, Abwasser und Straßenverkehrsbehörden (nicht wesentlicher Teil der allgemeinen Tätigkeit) sowie Abfallbewirtschaftung (wirtschaftliche Haupttätigkeit). Sonst können laut BCS auch untergeordnete Tätigkeiten die gesamte Einrichtung, also die juristische Person, erfassen. Beim Abwasser zählt laut Erläuterungen jede Tätigkeit des Unternehmens zur allgemeinen Tätigkeit, auch eine nicht wirtschaftliche; bei der Abfallbewirtschaftung scheiden nicht wirtschaftliche Tätigkeiten von vornherein aus.

Photovoltaik, Ladepunkte, Netze: Wer Überschussstrom einer Photovoltaikanlage einspeist, aber primär für den Eigenbedarf erzeugt, fällt laut BCS grundsätzlich nicht unter das NISG 2026. Öffentlich zugängliche Ladepunkte können dagegen unter „Betreiber von Ladepunkten“ fallen. Ob ein Glasfasernetz der Gemeinde ein öffentliches Kommunikationsnetz ist, richtet sich nach § 4 Z 9 TKG 2021, auf den § 3 Z 4 NISG 2026 verweist; hier schützt keine Größenschwelle.

04

Die Größe richtig ermitteln

Mittleres Unternehmen ab 50 Beschäftigten oder mehr als 10 Mio. Euro Umsatz und Bilanzsumme, gerechnet nach der KMU-Empfehlung.

Größenklassen nach § 25 NISG 2026 und ihre Folge

GRÖSSE	SCHWELLE	FOLGE BEI TÄTIGKEIT NACH ANLAGE 1 ODER 2
Groß	mindestens 250 Mitarbeiter oder Jahresumsatz über 50 Mio. Euro und Jahresbilanzsumme über 43 Mio. Euro (§ 25 Abs. 2)	Anlage 1: wesentlich (§ 24 Abs. 1 Z 3); Anlage 2: wichtig (§ 24 Abs. 2 Z 1)
Mittel	mindestens 50 Mitarbeiter oder Jahresumsatz über 10 Mio. Euro und Jahresbilanzsumme über 10 Mio. Euro (§ 25 Abs. 3)	wichtig (§ 24 Abs. 2 Z 1); Anbieter öffentlicher Kommunikationsnetze: wesentlich (§ 24 Abs. 1 Z 2)
Klein	weder mittel noch groß	nur bei größenunabhängiger Einstufung, etwa als Netz-anbieter (§ 24 Abs. 2 Z 3) oder per Bescheid (§ 26)

- Beschäftigte zählen in Jahresarbeitseinheiten; Lehrlinge sowie Mutterschafts- und Elternurlaub zählen nicht (Art. 5 Anhang Empfehlung 2003/361/EG).
- Maßgeblich ist der letzte Rechnungsabschluss; ein Statuswechsel wirkt erst nach zwei aufeinanderfolgenden Geschäftsjahren (Art. 4 Abs. 1 und 2 Anhang).
- Verbundene Unternehmen zählen zu 100 %, Partnerunternehmen ab 25 % Beteiligung anteilig (Art. 3 und Art. 6 Abs. 2 Anhang).
- Öffentliche Kontrolle von 25 % oder mehr schließt den KMU-Status nicht aus, denn Art. 3 Abs. 4 Anhang ist nicht anzuwenden (§ 25 Abs. 1, Art. 2 Abs. 1 NIS-2-Richtlinie); die Eigentümerin allein macht eine Gemeindegesellschaft nicht groß. Als verbunden können aber Schwestergesellschaften gelten, die dieselbe Gemeinde beherrscht (Art. 3 Abs. 3 Anhang). Ob Daten der Gemeinde selbst zählen, ist offen.
- Eine Gemeinde mit Haushalt unter 10 Mio. Euro und weniger als 5.000 Einwohnern macht ein Unternehmen auch mit 25 % oder mehr nicht zum Partnerunternehmen, solange sie nicht mit ihm verbunden ist (Art. 3 Abs. 2 UAbs. 2 lit. d Anhang).
- Nicht hinzugerechnet wird, wenn die Einrichtung bei ihren Netz- und Informationssystemen organisatorisch, technisch und operativ unabhängig ist (§ 25 Abs. 4). Teilt ein Betrieb die IT mit der Gemeinde, prüfen Sie das besonders sorgfältig.

Offene Frage: Führt eine Gemeinde einen Betrieb selbst, etwa die Wasserversorgung ohne eigene Gesellschaft, ist die Gemeinde als juristische Person die Einrichtung (§ 3 Z 10). Ob für die Größe dann nur der Betrieb oder die ganze Gemeinde zählt, beantworten weder § 25 noch die Erläuterungen ausdrücklich. Laut den Erläuterungen zu § 24 wird eine erfasste Einrichtung zur Gänze eingestuft, ihre Pflichten gelten für alle ihre Dienste. Klären Sie solche Fälle mit Ihrer Rechtsberatung oder der Cybersicherheitsbehörde.

05

Prüffragen für Gemeinde, Verband und Betrieb

Sechs Fragen für jeden Rechtsträger gesondert, dazu die Unterlagen, die Sie für die Prüfung brauchen.

Prüffragen je Rechtsträger: Gemeinde, Verband, Gesellschaft (Empfehlung von TOMORIS)

FRAGE	WENN JA	FUNDSTELLE
1. Ist der Rechtsträger eine Gemeinde oder ein Gemeindeverband?	Keine Einstufung als öffentliche Verwaltung; weiter mit Frage 2.	§ 24 Abs. 3
2. Übt er eine Tätigkeit einer Art aus Anlage 1 oder 2 aus, ohne dass deren Einschränkung greift?	Weiter mit Frage 3. Wenn nein: nicht erfasst, Ergebnis festhalten.	Anlagen 1 und 2
3. Bietet er öffentliche Kommunikationsnetze oder -dienste an oder ist er Vertrauensdiensteanbieter?	Erfasst unabhängig von der Größe, mindestens als wichtige Einrichtung.	§ 24 Abs. 1 Z 1 lit. a, Z 2, Abs. 2 Z 3
4. Ist er mindestens ein mittleres Unternehmen?	Anlage 1 und groß: wesentlich. Sonst: wichtig.	§ 24 Abs. 1 Z 3, Abs. 2 Z 1, § 25
5. Ist er kritische Einrichtung nach der Richtlinie (EU) 2022/2557 oder per Bescheid eingestuft?	Wesentlich beziehungsweise wie im Bescheid festgelegt.	§ 24 Abs. 1 Z 1 lit. e und f, § 26
6. Ist er nach Frage 3 bis 5 erfasst?	Registrieren und Pflichten umsetzen (nächster Abschnitt).	§§ 29, 31 bis 34

- ☐ Liste aller Rechtsträger mit Beteiligungen, Kapital- und Stimmrechtsanteilen
- ☐ Satzungen, Gesellschafts- und Verbandsverträge, Leistungsbeschreibungen der Betriebe
- ☐ Rechnungsabschlüsse der letzten zwei Jahre: Umsatz, Bilanzsumme, Beschäftigte in Jahresarbeitseinheiten
- ☐ Übersicht, wer welche IT betreibt und nutzt, samt IT-Dienstleistern
- ☐ Dokumentiertes Ergebnis mit Datum, Begründung und Fundstellen, vom zuständigen Organ zur Kenntnis genommen

Prüffragen und Unterlagenliste sind eine Empfehlung von TOMORIS; rechtlich maßgeblich sind §§ 24 bis 26 NISG 2026 samt Anlagen 1 und 2. Wiederholen Sie die Prüfung nach jedem Rechnungsabschluss und bei neuen Tätigkeiten.

06 —

Wenn ein Rechtsträger erfasst ist

Registrierung, die wichtigsten Pflichten und die Sonderregel des § 46 statt Geldstrafen für Gemeinden und öffentliche Stellen.

Erfasste Einrichtungen registrieren sich innerhalb von drei Monaten ab Inkrafttreten, später hinzukommende binnen drei Monaten ab Erfüllung der Voraussetzungen (§ 29 Abs. 3). Das BCS nennt für die erste Registrierung zwei Daten: in den FAQ (Stand 25.9.2026) den 31. Dezember 2026, auf der Seite „Registrierung“ (Stand 2.10.2026) grundsätzlich den 1. Jänner 2027, wegen § 33 Abs. 2 AVG spätestens den 4. Jänner 2027. Registrieren Sie sich vor Jahresende. Registriert wird eigenständig, ohne Aufforderung, über „NIS2-Services“ im Unternehmensserviceportal (USP); für Einrichtungen der öffentlichen Verwaltung kündigt das BCS eine Anbindung über den Portalverbund an. Anzugeben sind unter anderem Sektor, Art der Einrichtung und Schwellenwerte, dazu eine Kontaktstelle mit Telefonnummer und E-Mail-Adresse (§ 29 Abs. 2 und 6).

- Governance: Leitungsorgane stellen die Risikomanagementmaßnahmen sicher, beaufsichtigen sie und nehmen an Cybersicherheitsschulungen teil (§ 31).
- Risikomanagement mit mindestens den Inhalten des § 32 Abs. 4 lit. a bis j; der Anhang der Durchführungsverordnung (EU) 2024/2690 gilt nach § 2 NISV 2026 auch für die übrigen Arten von Einrichtungen der Anlagen 1 und 2.
- Selbstdeklaration binnen zwölf Monaten nach Eintritt der Registrierungspflicht (§ 33 Abs. 1).
- Meldung erheblicher Cybersicherheitsvorfälle an das CSIRT, Frühwarnung spätestens 24 Stunden nach Kenntnisnahme (§ 34 Abs. 1 und 2).

Keine Geldstrafen für Gemeinden: Bei Behörden und sonstigen Stellen der öffentlichen Verwaltung, einschließlich der Gebietskörperschaften und der in Formen des Privatrechts eingerichteten Stellen, stellt abweichend von § 45 die Bezirksverwaltungsbehörde die Nichteinhaltung mit Bescheid fest und setzt eine Frist; verstreicht sie, veröffentlicht sie die Nichteinhaltung nach Rechtskraft und Gelegenheit zur Stellungnahme (§ 46 Abs. 2, Verfassungsbestimmung). § 39 Abs. 4 (Aussetzungen, Verbot von Leitungsaufgaben) gilt für diese Stellen nicht (§ 39 Abs. 6), Anordnungen nach § 39 Abs. 1 bis 3 bleiben möglich. Auch ausgegliederte Rechtsträger können laut Erläuterungen darunterfallen.

07 —

Was jede Gemeinde ohnehin tun sollte

Datensicherheit nach DSGVO, Anforderungen aus der Lieferkette, sechs erste Schritte und zwei Leitfäden zur Orientierung.

Unabhängig vom NISG 2026 gilt die DSGVO. Nach Art. 32 Abs. 1 trifft die Gemeinde als Verantwortliche geeignete technische und organisatorische Maßnahmen für ein dem Risiko angemessenes Schutzniveau, unter anderem Verschlüsselung (lit. a), Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme (lit. b), rasche Wiederherstellung nach einem Zwischenfall (lit. c) und regelmäßige Überprüfung (lit. d). Datenschutzverletzungen meldet sie unverzüglich und möglichst binnen 72 Stunden der Aufsichtsbehörde, außer es besteht voraussichtlich kein Risiko (Art. 33 Abs. 1); bei voraussichtlich hohem Risiko benachrichtigt sie auch die betroffenen Personen (Art. 34 Abs. 1).

Erfasste Einrichtungen müssen die Sicherheit ihrer Lieferkette regeln (§ 32 Abs. 4 lit. d NISG 2026). Das BCS nennt als Anhaltspunkte für Verträge unter anderem Cybersicherheitsanforderungen, die Pflicht, Vorfälle unverzüglich zu melden, ein Prüfrecht und die Behebung von Schwachstellen; ein pauschaler AGB-Hinweis genügt nicht. Betreut die Gemeinde-IT einen erfassten Verband oder Betrieb, sollte sie mit solchen Anforderungen rechnen. Betreibt sie oder eine Gemeinde-IT-Gesellschaft Systeme für andere Rechtsträger, etwa Verbände, Gesellschaften oder Nachbargemeinden, prüfen Sie zusätzlich, ob sie selbst Anbieter verwalteter Dienste ist (Anlage 1 Z 9).

1

Verantwortung festlegen

Die Gemeindeführung bestimmt, wer Informationssicherheit koordiniert, und stellt Zeit und Mittel bereit. Das BSI-Profil richtet sich an die Verwaltungsspitze, die Ressourcen bereitstellt und Sicherheitsniveau samt Risiken verantwortet (Abschnitt 5.1).

2

Überblick schaffen

Erfassen Sie Aufgaben, Fachverfahren, Anwendungen, IT-Systeme, Standorte und Dienstleister; für Fachaufgaben und Anwendungen nennt das BSI-Profil einen vorhandenen Aufgabengliederungsplan als möglichen Ausgangspunkt (Abschnitt 7.2).

3

Grundschutz umsetzen

Beginnen Sie mit Datensicherung samt geprüfter Wiederherstellung, zeitnahen Updates, geregelten Berechtigungen und Schutz vor Schadprogrammen, orientiert an den Bausteinen CON.3, OPS.1.1.3, ORP.4 und OPS.1.1.4 des BSI-Profiles.

4

Vorfälle vorbereiten

Legen Sie fest, wer entscheidet, wen Sie verständigen und wie Sie die Meldung nach Art. 33 DSGVO prüfen. Auch Einrichtungen außerhalb des NISG 2026 können Vorfälle freiwillig und ohne Angabe ihrer Identität an das nationale CSIRT melden (§ 37 Abs. 2 und 3).

5

Dienstleister und Verträge prüfen

Regeln Sie mit IT-Dienstleistern Meldepflichten bei Vorfällen, Zugriffe, Fernwartung und Unterauftragnehmer.

6

Schulen und üben

Sensibilisieren Sie Mitarbeitende regelmäßig (BSI-Profil, Baustein ORP.3) und üben Sie den Ernstfall. Für erfasste Einrichtungen sind Schulungen Pflicht (§ 31 Abs. 2 NISG 2026).

Zwei frei verfügbare Leitfäden zur Orientierung (Empfehlung)

Österreichisches Informationssicherheitshandbuch

Vom Bundeskanzleramt mit A-SIT, frei online. Version 4 beschreibt den Aufbau eines Informationssicherheitsmanagementsystems in Unternehmen und öffentlicher Verwaltung, folgt ISO/IEC 27001 und 27002 und erlaubt eigene Checklisten.

BSI-Profil Basis-Absicherung Kommunalverwaltung

IT-Grundschutz-Profil, erstellt von der Arbeitsgruppe der deutschen kommunalen Spitzenverbände (AG koBA) und vom BSI veröffentlicht, Version 4.0 vom 13. November 2023. Es definiert auf Basis des BSI-Standards 200-2 Mindestmaßnahmen für Kommunalverwaltungen, gilt mit dem Kompendium Edition 2023 und nennt deutsche Rechtsgrundlagen. Für österreichische Gemeinden ist es keine Pflicht, aber eine praxisnahe Orientierung.

Landesrecht: Ein eigenes Landesgesetz zur Cybersicherheit der Gemeinden haben wir (Stand 25. Oktober 2026) nicht gefunden. Einzelne Landesnormen enthalten aber Vorgaben zur IT-Sicherheit von Gemeinden, zum Beispiel:

- **Oberösterreich:** Treffen öö. Gemeinden oder Gemeindeverbände als Träger von Privatrechten vollautomatisierte Entscheidungen, verlangt das Oö. ITEG unter anderem, Maßnahmen zur Daten- und Informationssicherheit zu dokumentieren, Protokolle und Logdateien mindestens sechs Monate zu speichern und Verfügbarkeit und Integrität der Daten nach dem Stand der Technik zu sichern (§ 1 Z 2, § 3 Abs. 3).
- **Kärnten:** Das Gemeinde-Servicezentrum stellt IKT-Dienstleistungen bereit und berät Gemeinden und Gemeindeverbände zur IT-Sicherheit (§ 109 Abs. 1 lit. h und Abs. 2 K-GMG). Der Einführungslehrgang für Gemeindebedienstete umfasst IKT-Sicherheit und ist für alle verpflichtend, die ab 1. Jänner 2012 eingetreten sind (§ 4 Abs. 1 lit. e und Abs. 6 K-GAPV).
- **Wien:** Beim mobilen Arbeiten ist mit Zustimmung des Beamten auch die Nutzung privater IKT-Endgeräte unter Wahrung der IKT-Sicherheit zulässig (§ 26d Abs. 5 Dienstordnung 1994).

Schritte und Leitfäden sind Empfehlungen von TOMORIS. Gesetzlich vorgegeben sind für jede Gemeinde unter anderem Art. 32 bis 34 DSGVO, für erfasste Einrichtungen zusätzlich §§ 31 bis 34 NISG 2026; Landesrecht kann weitere Vorgaben enthalten. Nach Erwägungsgrund 13 der NIS-2-Richtlinie sollen die Mitgliedstaaten bestrebt sein, dass auch ausgenommene Einrichtungen ein hohes Maß an Cybersicherheit erreichen.

08 —

Häufige Missverständnisse

Fünf Annahmen, die bei Gemeinden und ihren Betrieben zu falschen Schlüssen führen.

„Die Gemeinde ist ausgenommen, also auch ihre Betriebe.“

Die Ausnahme gilt nur für den Sektor öffentliche Verwaltung (§ 24 Abs. 3). Gemeinden, Verbände und Gesellschaften mit Tätigkeiten aus Anlage 1 oder 2 prüfen sich wie jedes Unternehmen.

„Eine Gemeindegesellschaft ist immer groß.“

Nein, nicht automatisch. Die Regel, nach der öffentliche Kontrolle von 25 % oder mehr den KMU-Status ausschließt, ist nicht anzuwenden (§ 25 Abs. 1). Es zählen Beschäftigte, Umsatz und Bilanzsumme samt verbundenen und Partnerunternehmen, auch von Schwestergesellschaften.

„Unter 50 Beschäftigten sind wir sicher draußen.“

Nicht unbedingt: Auch Umsatz und Bilanzsumme über je 10 Mio. Euro machen mittelgroß (§ 25 Abs. 3), verbundene Unternehmen zählen mit, und Anbieter öffentlicher Kommunikationsnetze sind unabhängig von der Größe erfasst (§ 24 Abs. 2 Z 3 lit. a).

„Ein Nebenbetrieb zählt nicht.“

Nur bei einzelnen Arten in den Sektoren Energie, Verkehr, Trinkwasser, Abwasser und Abfallwirtschaft schränkt das Gesetz auf Haupttätigkeit oder wesentlichen Anteil ein (Anlagen 1 und 2). Sonst können laut BCS auch untergeordnete Tätigkeiten die ganze Einrichtung erfassen.

„Die Behörde meldet sich, wenn wir betroffen sind.“

Die Einstufung folgt aus dem Gesetz. Erfasste Einrichtungen registrieren sich selbst (§ 29 Abs. 2 und 3), laut BCS eigenständig und ohne Aufforderung durch die Behörde.

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

09 —

Quellen

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

- 1 **NISG 2026, geltende Fassung im RIS, samt Anlagen 1 und 2**
§§ 3, 24 bis 26, 29, 31 bis 34, 37, 39, 45, 46, 51, Anlagen 1 und 2;
Fassung vom 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 2 **Regierungsvorlage 308 d. B. XXVIII. GP, Erläuterungen zum NISG 2026 (PDF)**
Zu §§ 24, 25 und 46 sowie zu Anlage 1 Z 5 und 7 und Anlage 2 Z 2
www.parlament.gv.at/dokument/XXVIII/I/308/fname_1723246.pdf
- 3 **Bundesamt für Cybersicherheit: FAQ Sektoren**
Gemeinden, Haupt- und Nebentätigkeit, Photovoltaik, Ladepunkte,
Managed Service Provider, Pflegeheime; Stand 25.9.2026
www.bundesamt-cybersicherheit.gv.at/faq/sektoren.html
- 4 **Bundesamt für Cybersicherheit: FAQ Lieferkette**
Vertragliche Verpflichtungen von Lieferanten; Stand 25.9.2026
www.bundesamt-cybersicherheit.gv.at/faq/lieferkette.html
- 5 **Bundesamt für Cybersicherheit: FAQ Registrierung**
Wen trifft die Registrierungspflicht?, Formular über USP bzw. Portal-
verbund; Stand 25.9.2026
www.bundesamt-cybersicherheit.gv.at/faq/registrierung.html
- 6 **Bundesamt für Cybersicherheit: Registrierung**
Erstregistrierung, NIS2-Services im USP, Portalverbund für die öffent-
liche Verwaltung; Stand 2.10.2026
www.bundesamt-cybersicherheit.gv.at/303/registrierung.html
- 7 **NISV 2026, BGBl. II Nr. 290/2026, im RIS**
§ 2 Anforderungen an Risikomanagementmaßnahmen, § 9 Inkrafttreten
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- 8 **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)**
Erwägungsgrund 13, Art. 2 Abs. 1, Abs. 2 lit. f und Abs. 5 lit. a
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 9 **Empfehlung 2003/361/EG der Kommission zur Definition der KMU**
Anhang Art. 1 bis 6
eur-lex.europa.eu/eli/reco/2003/361/oj/deu
- 10 **Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)**
Art. 32 Sicherheit der Verarbeitung, Art. 33 und 34 Meldung und Be-
nachrichtigung
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 11 **Abfallwirtschaftsgesetz 2002, § 2 im RIS**
§ 2 Abs. 6 Z 3 und 4: Abfallsammler und Abfallbehandler
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...
- 12 **Bundes-Verfassungsgesetz, Art. 108 im RIS**
Wien: Magistrat zugleich Amt der Landesregierung
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetze...
- 13 **Oö. Informationstechnologien-Einsatz-Gesetz (Oö. ITEG), LGBL Nr. 46/2025, im RIS**
§ 1 Z 2, § 3 Abs. 1 und 3
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrOO&Gesetzesnumm...
- 14 **Kärntner Gemeindemitarbeiterinnengesetz (K-GMG), § 109 im RIS**
Abs. 1 lit. h und Abs. 2: IKT und IT-Sicherheit; in Kraft seit 1.1.2026
ris.bka.gv.at/eli/lgb/KA/2011/96/P109/LKT40020810
- 15 **Kärntner Gemeinde-Ausbildungs- und Prüfungsverordnung (K-GAPV), § 4 im RIS**
Abs. 1 lit. e und Abs. 6: Einführungslehrgang mit IKT-Sicherheit
ris.bka.gv.at/eli/lgb/KA/2022/53/P4/LKT40020758
- 16 **Wiener Dienstordnung 1994, § 26d im RIS**
Abs. 5: private IKT-Endgeräte beim mobilen Arbeiten; in Kraft seit
1.9.2025
ris.bka.gv.at/eli/lgb/WI/1994/56/P26d/LWI40017661
- 17 **Österreichisches Informationssicherheitshandbuch (Bundeskanzleramt, A-SIT)**
Version 4: Zum Geleit, Vorwort, Einführung und zielgruppenspezifische
Leitfäden
www.sicherheitshandbuch.gv.at
- 18 **BSI: IT-Grundschutz-Profil Basis-Absicherung Kommunalver-
waltung**
Version 4.0 vom 13.11.2023, Abschnitte 5 bis 7 und 9
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmi...