Österreichischer Gemeindebund

NETZ- UND INFORMATIONSSICHERHEITSGESETZ 2026

Kurzinformation für Gemeinden

Netz- und Informationssicherheitsgesetz 2026 – verständlicher Überblick, zur Betroffenheit, Pflichten und Fristen

Dieses Rundschreiben beantwortet zwei Fragen

1. Fällt die Gemeinde oder eine kommunale Einrichtung unter das NISG 2026?
2. Wenn ja: Welche rechtlichen Folgen treten ein und welche Schritte sind jetzt zu setzen?

Das Gesetz tritt am 1. Oktober 2026 in Kraft.

Gemeinden und Gemeindeverbände sind gemäß § 24 Abs. 3 NISG 2026 ausdrücklich vom Sektor „öffentliche Verwaltung“ ausgenommen. Sie fallen daher nicht allein aufgrund ihrer Eigenschaft als Gemeinde oder Gemeindeverband unter das NISG 2026. Eine Betroffenheit kann sich jedoch ergeben, wenn sie selbst eine Tätigkeit aus einem anderen NISG-Sektor ausüben, insbesondere in den Bereichen Trinkwasser oder Abwasser.

Frage 1: Fällt meine Gemeinde unter das NISG 2026?

Schritt	Prüffrage	Worauf kommt es an?
1	Rechtsträger feststellen	Wer erbringt den Dienst tatsächlich: die Gemeinde, ein Gemeindeverband, eine kommunale GmbH oder ein anderer selbstständiger Rechtsträger?
2	Sektor prüfen	Erbringt dieser Rechtsträger eine Tätigkeit aus der Anlage 1 oder 2 des NISG 2026? Kommunal besonders relevant sind dabei Wasser, Abwasser, Abfall, Energie, Gesundheitswesen, Verkehrsmanagement sowie verwaltete IT- oder Sicherheitsdienste.
3	Größe ermitteln	Erreicht die Einrichtung die Schwelle eines mittleren oder großen Unternehmens? Dabei können Daten von Partner- oder verbundenen Unternehmen hinzuzurechnen sein.
4	Ausnahme und Sonderfälle prüfen	Zusätzlich sind drei Sonderfälle zu prüfen: Tätigkeiten im Bereich Wasser oder Abwasser können ausgenommen sein, wenn sie lediglich eine untergeordnete Nebentätigkeit darstellen. Im Abfallbereich ist entscheidend, ob die Abfallbewirtschaftung die wirtschaftliche Haupttätigkeit des Rechtsträgers bildet. Bei der Berechnung der Unternehmensgröße ist außerdem zu prüfen, ob Daten der Gemeinde oder verbundener Einrichtungen aufgrund einer organisatorisch, technisch und operativ unabhängigen IT-Struktur außer Betracht bleiben können.

Einstufung bei erfüllter Sektor- und Größenschwelle

Sektor	Mittlere Einrichtung	Große Einrichtung
Anlage 1 – Sektoren mit hoher Kritikalität	Wichtige Einrichtung	Wesentliche Einrichtung
Anlage 2 – sonstige kritische Sektoren	Wichtige Einrichtung	Wichtige Einrichtung*

**eine größenunabhängige Einstufung durch die Cybersicherheitsbehörde ist in gesetzlich bestimmten Ausnahmefällen möglich (§26 NISG 2026)*

Welche kommunalen Tätigkeiten sind besonders relevant?

Fallgruppe	Praktische Einordnung
Nur allgemeine Gemeindeverwaltung	Keine Betroffenheit allein aufgrund der Eigenschaft als Gemeinde: Gemeinde ist vom NISG-Sektor „öffentliche Verwaltung“ ausgenommen (§ 24 Abs. 3).
Trinkwasser oder Abwasser im direkten Betrieb	Die Gemeinde kann selbst erfasst sein, wenn zumindest mittlere Größe vorliegt und die Tätigkeit nicht nur einen unwesentlichen Teil der allgemeinen Tätigkeit bildet. Eine Versorgung der Gemeinde oder wesentlicher Teile davon wird regelmäßig nicht bloß unwesentlich sein.
Abfallbewirtschaftung im direkten Betrieb	Eine Erfassung über den Abfallsektor setzt voraus, dass Abfallbewirtschaftung die wirtschaftliche Haupttätigkeit des Rechtsträgers ist. Bei einer Gemeinde als Ganzes wird das häufig nicht der Fall sein; bei einem eigenständigen Abfallunternehmen dagegen typischerweise schon.
Kommunale GmbH oder Gemeindeverband	Der eigenständige Rechtsträger wird selbst geprüft. Seine Betroffenheit geht nicht automatisch auf die Gemeinde über. Bei der Größenprüfung können Gemeindedaten oder Daten anderer verbundener Einrichtungen jedoch hinzugerechnet werden.
Ausgelagerte Leistung	Erbringt ein unabhängiger Dritter den NISG-relevanten Dienst, ist grundsätzlich dieser Dritte zu prüfen. Bleibt die Gemeinde selbst NISG-pflichtig und lagert lediglich IT-Betrieb oder Teilaufgaben aus, bleiben ihre Pflichten – insbesondere zur Lieferkettensicherheit – bestehen.
Gemeinsame IT- oder Sicherheitsdienste	Erbringt eine kommunale Einrichtung verwaltete IT- oder Sicherheitsdienste für andere Rechtsträger, kann eine Betroffenheit als Managed Service Provider bzw. Managed Security Service Provider bestehen.

Wichtig bei direktem Betrieb

Ist die Gemeinde selbst die betroffene Einrichtung, bezieht sich die NISG-Betroffenheit grundsätzlich auf die Gemeinde als Rechtsträger und nicht nur auf die zuständige Fachabteilung. Die konkreten Sicherheitsmaßnahmen sind jedoch risikobasiert auf jene Netz- und Informationssysteme auszurichten, die für den Betrieb und die Erbringung der relevanten Dienste genutzt werden.

Wie wird die Größe ermittelt?

Größenklasse	Beschäftigte	Finanzielle Alternative
Mittleres Unternehmen	Mindestens 50	Jahresumsatz über 10 Mio. Euro UND Jahresbilanzsumme über 10 Mio. Euro
Großes Unternehmen	Mindestens 250	Jahresumsatz über 50 Mio. Euro UND Jahresbilanzsumme über 43 Mio. Euro

Die Beschäftigtenschwelle und die finanzielle Alternative sind jeweils mit „ODER“ verknüpft. Innerhalb der finanziellen alternative müssen dagegen beide Werte überschritten werden.

Beteiligungen und verbundene Einrichtungen

- **Beteiligungen unter 25 %** bleiben in der Regel außer Betracht; bei Partnerunternehmen werden Daten grundsätzlich anteilig, bei verbundenen Unternehmen grundsätzlich vollständig hinzugerechnet.
- **Bei kleinen Gemeinden** mit weniger als 5.000 Einwohnern und einem Jahreshaushalt unter 10 Mio. Euro kann die Zurechnung als Partnerunternehmen entfallen, sofern keine Verbindung bzw. Beherrschung vorliegt.
- **Keine Hinzurechnung** ist nach § 25 Abs. 4 NISG 2026 erforderlich, wenn die betrachtete Einrichtung hinsichtlich ihrer diensterelevanten Netz- und Informationssysteme organisatorisch, technisch und operativ unabhängig ist. Diese Unabhängigkeit sollte nachvollziehbar dokumentiert werden.

Besonderheit bei der Größenberechnung

Die Berechnung der Beschäftigtenzahl, des Jahresumsatzes und der Jahresbilanzsumme richtet sich gemäß § 25 Abs. 1 NISG 2026 nach der KMU-Empfehlung 2003/361/EG der Europäischen Kommission. Obwohl diese Empfehlung unternehmensbezogene Begriffe verwendet, ist sie auch auf Gemeinden und Gemeindeverbände anzuwenden. Für eine erste kommunale Prüfung können die Beschäftigten in Jahresarbeitseinheiten, das Einzahlungsvolumen der geprüften Finanzierungsrechnung als Jahresumsatz und das Vermögen gemäß geprüfter Vermögensrechnung als Jahresbilanzsumme herangezogen werden. Beteiligungen sowie Partner- und verbundene Einrichtungen sind nach den Vorgaben der KMU-Empfehlung zu berücksichtigen; die Ausnahme des § 25 Abs. 4 NISG 2026 bleibt unberührt.

Frage 2: Meine Gemeinde ist betroffen – wie geht es jetzt weiter?

Die unmittelbare Konsequenz

Die Gemeinde selbst wird dadurch zur wesentlichen oder wichtigen Einrichtung. Die Umsetzung beschränkt sich nicht auf technische Maßnahmen der IT-Abteilung. Das zuständige Leitungsorgan trägt die Gesamtverantwortung und muss insbesondere klare Zuständigkeiten, ausreichende personelle und finanzielle Ressourcen, Schulungen, Sicherheitsmaßnahmen, Meldeprozesse und eine nachvollziehbare Dokumentation sicherstellen. Auch bei einer Auslagerung der IT verbleibt die Verantwortung bei der Gemeinde.

Kommunaler Umsetzungsfahrplan

Zeitraum	Arbeitspaket	Konkretes Ergebnis
Ab sofort	Entscheidung und Organisation	Betroffenheit dokumentieren; Dienste und Rechtsträger abgrenzen; Leitungsorgan, NISG-Koordination und Arbeitsteam benennen; Ressourcen festlegen
Vor 1. Oktober 2026	Bestand und Risiken	Dienste, Systeme, Daten, Standorte, Abhängigkeiten und Lieferanten erfassen; Risiken und Lücken bewerten; priorisierten Maßnahmenplan beschließen.
Bis 31. Dezember 2026	Registrierung	Sektor, Größen- und Kontaktdaten elektronisch übermitteln; erreichbare Kontaktstelle mit Telefonnummer und E-Mail-Adresse vorsehen.
Ab 1. Oktober 2026 laufend	Betrieb und Vorfälle	Maßnahmen betreiben und nachweisen; schulen; erhebliche Vorfälle binnen 24/72 Stunden und grundsätzlich binnen eines Monats melden.
Bis 1. Oktober 2027	Selbstdeklaration	Maßnahmen, Systeme, Lieferkettensicherheit und Risikoanalyse strukturiert an die Cybersicherheitsbehörde übermitteln.
Frühestens ab 1. Oktober 2028	Prüfbereitschaft	Mit Aufforderung zu Prüf- und Wirksamkeitsnachweisen rechnen; Dokumentation laufend aktuell halten.

Was muss praktisch eingerichtet sein?

Verantwortung festlegen:	Zuständiges Leitungsorgan, NISG-Koordination, interne Ansprechpersonen, Budget und regelmäßige Berichterstattung festlegen.
Überblick über Risiken schaffen:	Relevante Dienste, IT-Systeme, Daten, Standorte, Abhängigkeiten und externe Anbieter erfassen und bewerten.
Technische Sicherheit verbessern:	Insbesondere Multi-Faktor-Authentifizierung, Berechtigungs- und Patchmanagement, sichere Fernzugriffe, Protokollierung sowie getestete Backups umsetzen.
Vorfall- und Krisenmanagement vorbereiten:	Interne Eskalationswege, die 24-/72-Stunden-Meldung, Notbetrieb, Kommunikation und Wiederanlauf festlegen und regelmäßig üben.
Externe Dienstleister miteinbeziehen:	Kritische Anbieter erfassen und Sicherheitsanforderungen, Zuständigkeiten sowie Meldepflichten vertraglich regeln.
Umsetzung dokumentieren:	Entscheidungen, Risikoanalysen, Maßnahmen, Tests, Schulungen, Sicherheitsvorfälle und Verbesserungen nachvollziehbar festhalten.

Nach Mitteilung des BMI ist derzeit beabsichtigt, bei der Konkretisierung der Risikomanagementmaßnahmen gemäß § 32 NISG 2026 inhaltlich an die Durchführungsverordnung (EU) 2024/2690 anzuknüpfen. Die entsprechende nationale Verordnung bleibt abzuwarten. Gemeinden sollten die darin enthaltenen technischen und methodischen Anforderungen daher bereits bei ihren Vorbereitungen berücksichtigen.

Folgen bei Nicht-Einhaltung

Aufsicht, Anordnungen und mögliche Sanktionen

Die Cybersicherheitsbehörde kann Informationen, Kontrollen, Sicherheitsscans und die Behebung von Mängeln verlangen (§§ 38 und 39). Für Gemeinden als Gebietskörperschaften sieht § 46 grundsätzlich Bescheid, Sanierungsfrist und bei fortdauernder Nichteinhaltung Veröffentlichung vor. Bei eigenständigen kommunalen Rechtsträgern ist zu klären, ob § 46 oder § 45 gilt. Die Geldstrafen nach § 45 reichen bei Kernpflichten – je nach Einstufung – bis 10 Mio. Euro bzw. 2 % oder bis 7 Mio. Euro bzw. 1,4 % des weltweiten Jahresumsatzes; bei organisatorischen Verstößen bis 50.000 Euro, im Wiederholungsfall bis 100.000 Euro.

Kompakte Übersicht der Rechtsquellen

Thema	Rechtsgrundlage
Betroffenheit, Größe und Einstufung	§§ 24 bis 26 NISG 2026; Anlagen 1 und 2; KMU-Empfehlung 2003/361/EG
Registrierung und Kontaktstelle	§ 29 NISG 2026
Verantwortung und Risikomanagementmaßnahmen	§§ 31 und 32 NISG 2026
Selbstdeklaration, Prüfungen und Prüfstellen	§§ 33 und 7 NISG 2026
Meldung erheblicher Vorfälle	§§ 34 und 35 NISG 2026
Informationsaustausch und freiwillige Meldungen	§§ 36 und 37 NISG 2026
Aufsicht und Durchsetzung	§§ 38 und 39 NISG 2026
Strafbestimmungen und Besonderheiten für öffentliche Stellen	§§ 44 bis 46 NISG 2026

Weiterführende Praxishilfen
Die Wirtschaftskammer Österreich stellt einen umfassenden Überblick, häufig gestellte Fragen und einen Online-Ratgeber zur Prüfung der Betroffenheit nach dem NISG 2026 zur Verfügung.
Dazu die Links zum WKO-Überblick und zu den WKO-FAQ.