

GUIDE · TOMORIS TOOLBOX

NIS2 and Municipalities: Who Is Covered and What Applies

The exclusion under § 24 para. 3 NISG 2026, review questions for water, wastewater, waste and energy operations, and what every municipality should do anyway

UPDATED

Oct 25, 2026

LENGTH

PDF, 12 pages

ONLINE

tomoris.com/en/downloads/nis2-gemeinden-leitfaden

AT A GLANCE

§ 24

Para. 3: municipalities outside public administration

Annex 1

Drinking water, wastewater, energy: review each operation

50

Employees: threshold for a medium-sized operation

Art. 32

GDPR: data security applies to every municipality

WHO IT IS FOR

- Mayors, municipal office directors and municipal executive boards
- Municipal IT and IT service providers for municipalities
- Municipal associations, for example for water, wastewater and waste
- Management of municipal enterprises such as public utilities and supply companies

WHAT THIS COVERS

The NISG 2026 (Austrian Network and Information Systems Security Act 2026) has applied since October 1, 2026. Municipalities and municipal associations are expressly not part of the public administration sector (§ 24 para. 3). Their operations for drinking water, wastewater, waste or energy can still be covered. This guide explains the legal situation, the review questions for the municipality, association and operation, and what every municipality should do anyway.

This guide provides an overview and does not replace legal advice. The text of the law in its current version is decisive, in particular §§ 24 to 26 and Annexes 1 and 2 NISG 2026. The review questions, first steps and guides are TOMORIS recommendations.

CONTENTS

01	The short answer	2
02	The legal situation under § 24 NISG 2026	3
03	When municipalities and their operations are still covered	4
04	Determining size correctly	6
05	Review questions for the municipality, association and operation	7
06	If a legal entity is covered	8
07	What every municipality should do anyway	8
08	Common misconceptions	10
09	Sources	11

01

The short answer

As an administration, the municipality is not covered. Its operations can be, and data protection applies anyway.

No

Municipality as public administration

Municipalities and municipal associations are not entities in the public administration sector (§ 24 para. 3 NISG 2026).

Review

Municipal operations and associations

Anyone who performs an activity listed in Annex 1 or 2, such as drinking water, wastewater, waste or energy, is covered from medium size upward, unless a restriction in the annex applies (§ 24 para. 1 no. 3, para. 2 no. 1, § 25).

Yes

Data protection and supply chain

Security of processing under Art. 32 GDPR applies to every municipality. Covered partners must manage the security of their supply chain (§ 32 para. 4 lit. d NISG 2026).

The Federal Office for Cybersecurity answers the question in its FAQ as follows: municipalities, “and thus also cities,” and municipal associations are expressly excluded from the public administration sector, “but not generally excluded from the scope.” They are covered if they operate in another sector listed in Annex 1 or 2, such as drinking water, wastewater, waste management, energy, transport or digital infrastructure, and meet the size criteria for medium-sized or large enterprises.

Whether an entity is essential or important follows directly from § 24 NISG 2026; no administrative decision is required. Covered entities must register themselves (§ 29). In addition, the cybersecurity authority classifies smaller entities listed in Annexes 1 and 2 by administrative decision if one of the grounds in § 26 para. 3 applies.

02 —

The legal situation under § 24 NISG 2026

Public administration is classified by level, not by size. The law expressly excludes municipalities and municipal associations.

The NISG 2026 (BGBl. I No. 94/2025) transposes the NIS 2 Directive and has applied since October 1, 2026 (§ 51 paras. 1 and 2). It classifies public administration by level, not by size. Under § 24 para. 3, entities in the public administration sector are entities that meet all three criteria:

- No. 1: They were established to perform tasks in the public interest that are not of an industrial or commercial nature.
- No. 2: They are subject to the supervision of the federal government or a state or are bound by the instructions of a supreme body, the majority of their management or supervisory body is appointed by federal or state bodies, the federal government or a state holds at least 50% of the capital, or they are members of the federal government.
- No. 3: They are authorized to issue administrative decisions that affect the rights of individuals in the cross-border movement of persons, goods, services or capital.

The paragraph ends with the words “with the exception of municipalities and municipal associations.” According to the explanatory notes to the government bill, the option to include the local level, which domestically means the municipalities, was “not used.” In one place, the explanatory notes go further (“In addition to the municipalities, educational institutions ... are also not considered essential or important entities”). The text of the law is decisive, and it excludes municipalities only from the public administration sector; the BCS reads it the same way.

Public administration sector under § 24 NISG 2026

LEVEL	WHO IS COVERED	CLASSIFICATION
Federal	Entities under para. 3 that handle matters of federal administration and are a federal authority or have legal personality	essential, regardless of size (para. 1 no. 1 lit. d, para. 4)
State	Offices of the state governments and district administrative authorities, as well as entities under para. 3 with legal personality that handle matters of state administration	important, also regardless of size according to the explanatory notes (para. 2 no. 2, para. 5)

Municipalities and municipal associations	expressly not part of the sector, according to the BCS this includes cities; § 24 para. 5 names only the district administrative authorities, not the municipal authorities of statutory cities	no classification as public administration (para. 3)
Other exclusions	predominantly national security, public security or law enforcement; universities, higher education and schools; the judiciary; the legislature; the Austrian National Bank	neither essential nor important, except as trust service providers (para. 6)

This is consistent with the NIS 2 Directive: it covers the public administration of central government and, following a risk-based assessment, the regional level, regardless of size (Art. 2(2)(f)). Member States may include public administration entities at the local level, but they are not required to (Art. 2(5)(a)).

Special case Vienna: The Vienna municipal authority also performs the function of the Office of the State Government (Art. 108 B-VG (Austrian Federal Constitutional Law)), which § 24 para. 5 names as an entity at the state level. According to the explanatory notes, this requires a “differentiated assessment,” “particularly since the ‘local level’ ... is not meant to be covered by the public administration sector.” The law does not address this specifically; review Vienna entities case by case.

03

When municipalities and their operations are still covered

The exclusion applies only to the public administration sector. In the other sectors, activity and size count, not the owner.

The exclusion appears only in the definition of the public administration sector. In the other sectors, the following applies: entities of a type listed in Annex 1 are essential if they operate a large enterprise (§ 24 para. 1 no. 3); entities of a type listed in Annex 1 or 2 are important if they operate a medium-sized or large enterprise (§ 24 para. 2 no. 1). An entity is any natural or legal person or registered partnership that can exercise rights and be subject to obligations in its own name (§ 3 no. 10). The Directive expressly refers to “public or private entities” (Art. 2(1)), and an enterprise is any entity engaged in an economic activity, regardless of its legal form (Art. 1 of the Annex to Recommendation 2003/361/EC).

Types of entities likely to be relevant for municipalities and their operations (excerpt from Annexes 1 and 2, abridged)

SECTOR	TYPE OF ENTITY	RESTRICTION IN THE LAW
Drinking water (Annex 1 no. 6)	Suppliers and distributors of “water intended for human consumption” (§ 3 no. 2 LMSVG (Austrian Food Safety and Consumer Protection Act))	only suppliers excluded whose general activity is the distribution of other commodities and goods and for whom drinking water is a non-essential part of that activity; the exclusion does not mention water supply companies
Wastewater (Annex 1 no. 7)	Undertakings that collect, dispose of or treat urban, domestic or industrial wastewater	not if this is only a non-essential part of their general activity
Waste (Annex 2 no. 2)	Waste collectors and waste treatment operators (§ 2 para. 6 nos. 3 and 4 AWG 2002 (Austrian Waste Management Act 2002))	not if waste management is not their (economic) principal activity

Energy (Annex 1 no. 1)	for example electricity undertakings that carry out supply, distribution system operators for electricity and natural gas, operators of district heating and of recharging points	electricity producers only if commercial or professional activity is their principal activity
Transport (Annex 1 no. 2 lit. d)	Road authorities responsible for traffic management and traffic control; operators of intelligent transport systems (§ 2 no. 1 IVS-G (Austrian Intelligent Transport Systems Act))	public bodies not if traffic management or the operation of intelligent transport systems is only a non-essential part of their general activity
Health (Annex 1 no. 5)	Healthcare providers, according to the explanatory notes for example hospitals and emergency medical services	long-term care and nursing homes not covered according to the explanatory notes and the BCS; review case by case depending on the setup
Digital infrastructure (Annex 1 no. 8)	Providers of public electronic communications networks or publicly available communications services	no size threshold (§ 24 para. 1 no. 2, para. 2 no. 3 lit. a)
ICT service management (Annex 1 no. 9)	Managed service providers (MSPs); according to the BCS also internal IT service providers that manage systems of other companies in a group with administrative access	only excluded if operated and used exclusively by the entity concerned

According to the Federal Office for Cybersecurity (BCS), whether an activity is principal or ancillary generally does not matter. The law contains restrictions only for certain types: electricity producers (principal activity), drinking water suppliers whose general activity is the distribution of other commodities and goods, wastewater and road authorities (non-essential part of the general activity), and waste management (principal economic activity). Otherwise, according to the BCS, even subordinate activities can bring the entire entity, meaning the legal person, into scope. For wastewater, according to the explanatory notes, every activity of the undertaking counts toward its general activity, including non-economic ones; for waste management, non-economic activities are excluded from the outset.

Photovoltaics, recharging points, networks: Anyone who feeds surplus electricity from a photovoltaic system into the grid but generates primarily for their own use is generally not covered by the NISG 2026, according to the BCS. Publicly accessible recharging points, on the other hand, can fall under “operators of recharging points.” Whether a municipal fiber network is a public communications network depends on § 4 no. 9 TKG 2021 (Austrian Telecommunications Act 2021), to which § 3 no. 4 NISG 2026 refers; no size threshold protects you here.

04 —

Determining size correctly

Medium-sized enterprise from 50 employees or more than €10 million in turnover and balance sheet total, calculated according to the SME Recommendation.

Size categories under § 25 NISG 2026 and their consequence

SIZE	THRESHOLD	EFFECT FOR AN ANNEX 1 OR 2 ACTIVITY
Large	at least 250 employees, or annual turnover above €50 million and annual balance sheet total above €43 million (§ 25 para. 2)	Annex 1: essential (§ 24 para. 1 no. 3); Annex 2: important (§ 24 para. 2 no. 1)
Medium	at least 50 employees, or annual turnover above €10 million and annual balance sheet total above €10 million (§ 25 para. 3)	important (§ 24 para. 2 no. 1); providers of public communications networks: essential (§ 24 para. 1 no. 2)
Small	neither medium nor large	only in case of size-independent classification, for example as a network provider (§ 24 para. 2 no. 3) or by administrative decision (§ 26)

- Employees are counted in annual work units; apprentices as well as maternity and parental leave are not counted (Art. 5 of the Annex to Recommendation 2003/361/EC).
- The most recent financial statements are decisive; a change in status only takes effect after two consecutive financial years (Art. 4(1) and (2) of the Annex).
- Linked enterprises count at 100%, partner enterprises proportionally from a 25% holding (Art. 3 and Art. 6(2) of the Annex).
- Public control of 25% or more does not rule out SME status, because Art. 3(4) of the Annex does not apply (§ 25 para. 1, Art. 2(1) NIS 2 Directive); ownership by the municipality alone does not make a municipal company large. However, sister companies controlled by the same municipality can count as linked (Art. 3(3) of the Annex). Whether the municipality's own data counts is an open question.
- A municipality with an annual budget below €10 million and fewer than 5,000 inhabitants does not make an enterprise a partner enterprise, even with a holding of 25% or more, as long as it is not linked to it (Art. 3(2), second subparagraph, (d) of the Annex).
- Figures are not added if the entity is organizationally, technically and operationally independent with regard to its network and information systems (§ 25 para. 4). If an operation shares IT with the municipality, review this especially carefully.

Open question: If a municipality runs an operation itself, for example water supply without a separate company, the municipality as a legal person is the entity (§ 3 no. 10). Neither § 25 nor the explanatory notes expressly answer whether only the operation or the entire municipality then counts for size. According to the explanatory notes on § 24, a covered entity is classified in its entirety, and its obligations apply to all its services. Clarify such cases with your legal counsel or the cybersecurity authority.

05 —

Review questions for the municipality, association and operation

Six questions for each legal entity separately, plus the documents you need for the review.

Review questions per legal entity: municipality, association, company (TOMORIS recommendation)

QUESTION	IF YES	REFERENCE
1. Is the legal entity a municipality or a municipal association?	No classification as public administration; continue with question 2.	§ 24 para. 3
2. Does it perform an activity of a type listed in Annex 1 or 2 without the applicable restriction taking effect?	Continue with question 3. If no: not covered, record the result.	Annexes 1 and 2
3. Does it provide public communications networks or services, or is it a trust service provider?	Covered regardless of size, at least as an important entity.	§ 24 para. 1 no. 1 lit. a, no. 2, para. 2 no. 3
4. Is it at least a medium-sized enterprise?	Annex 1 and large: essential. Otherwise: important.	§ 24 para. 1 no. 3, para. 2 no. 1, § 25
5. Is it a critical entity under Directive (EU) 2022/2557 or classified by administrative decision?	Essential, or as specified in the administrative decision.	§ 24 para. 1 no. 1 lit. e and f, § 26
6. Is it covered under questions 3 to 5?	Register and implement the obligations (next section).	§§ 29, 31 to 34

- ☐ List of all legal entities with holdings, capital shares and voting rights
- ☐ Articles of association, partnership and association agreements, service descriptions of the operations
- ☐ Financial statements for the last two years: turnover, balance sheet total, employees in annual work units
- ☐ Overview of who operates and uses which IT, including IT service providers
- ☐ Documented result with date, rationale and legal references, acknowledged by the competent body

The review questions and the document list are a TOMORIS recommendation; legally decisive are §§ 24 to 26 NISG 2026 including Annexes 1 and 2. Repeat the review after each set of financial statements and whenever new activities are added.

06 —

If a legal entity is covered

Registration, the key obligations and the special rule of § 46 instead of fines for municipalities and public bodies.

Covered entities register within three months of entry into force; entities added later register within three months of meeting the requirements (§ 29 para. 3). The BCS gives two dates for initial registration: in its FAQ (as of September 25, 2026), December 31, 2026; on the “Registration” page (as of October 2, 2026), generally January 1, 2027, and at the latest January 4, 2027, due to § 33 para. 2 AVG (Austrian General Administrative Procedure Act). Register before the end of the year. Registration is done independently, without being asked, via “NIS2-Services” in the Business Service Portal (USP); for public administration entities, the BCS has announced a connection via the Portalverbund (Austrian portal network). Required information includes the sector, type of entity and thresholds, as well as a point of contact with telephone number and email address (§ 29 paras. 2 and 6).

- Governance: management bodies ensure and oversee the risk management measures and take part in cybersecurity training (§ 31).
- Risk management with at least the content of § 32 para. 4 lit. a to j; under § 2 NISV 2026 (Austrian NIS Regulation 2026), the Annex to Implementing Regulation (EU) 2024/2690 also applies to the other types of entities in Annexes 1 and 2.
- Self-declaration within twelve months after the registration obligation arises (§ 33 para. 1).
- Reporting of significant cybersecurity incidents to the CSIRT, early warning no later than 24 hours after becoming aware (§ 34 paras. 1 and 2).

No fines for municipalities: For authorities and other public administration bodies, including territorial authorities and bodies established under private law, the district administrative authority establishes non-compliance by decision and sets a deadline, in derogation from § 45. If it expires, the authority publishes non-compliance after finality and an opportunity to comment (§ 46 para. 2, constitutional provision). § 39 para. 4 (suspensions, prohibition of management functions) does not apply to these bodies (§ 39 para. 6); orders under § 39 paras. 1 to 3 remain possible. The explanatory notes say outsourced legal entities may also fall under this rule.

07 —

What every municipality should do anyway

Data security under the GDPR, supply chain requirements, six first steps and two guides for orientation.

Regardless of the NISG 2026, the GDPR applies. Under Art. 32(1), the municipality as controller implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including encryption (lit. a), confidentiality, integrity, availability and resilience of systems (lit. b), timely restoration after an incident (lit. c) and regular testing (lit. d). It reports personal data breaches to the supervisory authority without undue delay and, where feasible, within 72 hours, unless the breach is unlikely to result in a risk (Art. 33(1)); if the breach is likely to result in a high risk, it also notifies the data subjects (Art. 34(1)).

Covered entities must manage the security of their supply chain (§ 32 para. 4 lit. d NISG 2026). As guidance for contracts, the BCS names, among other things, cybersecurity requirements, the obligation to report incidents without undue delay, a right to audit and the remediation of vulnerabilities; a general reference in the terms and conditions is not enough. If municipal IT supports a covered association or operation, it should expect such requirements. If the municipal IT or a municipal IT company operates systems for other legal entities, such as associations, companies or neighboring municipalities, also review whether it is itself a managed service provider (Annex 1 no. 9).

1

Assign responsibility

Municipal leadership determines who coordinates information security and provides time and resources. The BSI profile is aimed at the administrative leadership, which provides resources and is responsible for the security level and its risks (Section 5.1).

2

Create an overview

Record tasks, specialized procedures, applications, IT systems, locations and service providers; for specialized tasks and applications, the BSI profile names an existing task structure plan as a possible starting point (Section 7.2).

3

Implement basic protection

Start with data backup including tested restoration, timely updates, managed permissions and protection against malware, guided by the modules CON.3, OPS.1.1.3, ORP.4 and OPS.1.1.4 of the BSI profile.

4

Prepare for incidents

Define who decides, whom you notify and how you assess the notification under Art. 33 GDPR. Entities outside the NISG 2026 can also report incidents to the national CSIRT voluntarily and without disclosing their identity (§ 37 paras. 2 and 3).

5

Review service providers and contracts

Agree with IT service providers on incident reporting obligations, access, remote maintenance and sub-contractors.

6

Train and practice

Raise employee awareness regularly (BSI profile, module ORP.3) and practice for emergencies. For covered entities, training is mandatory (§ 31 para. 2 NISG 2026).

Two freely available guides for orientation (recommendation)

Austrian Information Security Handbook

Published by the Federal Chancellery with A-SIT, freely available online. Version 4 describes how to build an information security management system in companies and public administration, follows ISO/IEC 27001 and 27002 and allows custom checklists.

BSI municipal administration baseline profile

IT-Grundschutz profile, created by the working group of the German municipal umbrella associations (AG koBA) and published by the BSI, version 4.0 of November 13, 2023. Based on BSI Standard 200-2, it defines minimum measures for municipal administrations, applies with the Kompendium Edition 2023 and cites German legal bases. It is not mandatory for Austrian municipalities, but it offers practical orientation.

State law: We have not found a separate state law on the cybersecurity of municipalities (as of October 25, 2026). However, some state regulations contain requirements for the IT security of municipalities, for example:

- Upper Austria: If its municipalities or municipal associations make fully automated decisions as holders of private rights, the Oö. ITEG requires, among other things, documented data and information security measures, retention of logs and log files for at least six months, and data availability and integrity according to the state of the art (§ 1 no. 2, § 3 para. 3).
- Carinthia: The municipal service center provides ICT services and advises municipalities and municipal associations on IT security (§ 109 para. 1 lit. h and para. 2 K-GMG). The induction course for municipal employees covers ICT security and is mandatory for everyone who joined on or after January 1, 2012 (§ 4 para. 1 lit. e and para. 6 K-GAPV).
- Vienna: For mobile work, the use of private ICT devices is also permitted with the civil servant's consent, provided ICT security is maintained (§ 26d para. 5 Dienstordnung 1994 (Vienna Civil Service Code 1994)).

The steps and guides are TOMORIS recommendations. Legally required for every municipality are, among others, Art. 32 to 34 GDPR, and for covered entities additionally §§ 31 to 34 NISG 2026; state law may contain further requirements. Under Recital 13 of the NIS 2 Directive, Member States should strive to ensure that excluded entities also achieve a high level of cybersecurity.

08

Common misconceptions

Five assumptions that lead municipalities and their operations to the wrong conclusions.

“The municipality is excluded, so its operations are too.”

The exclusion applies only to the public administration sector (§ 24 para. 3). Municipalities, associations and companies with activities under Annex 1 or 2 review their status like any other enterprise.

“A municipal company is always large.”

No, not automatically. The rule under which public control of 25% or more rules out SME status does not apply (§ 25 para. 1). What counts are employees, turnover and balance sheet total, including linked and partner enterprises, and sister companies as well.

“With fewer than 50 employees, we are definitely out.”

Not necessarily: turnover and balance sheet total each above €10 million also make an enterprise medium-sized (§ 25 para. 3), linked enterprises are included, and providers of public communications networks are covered regardless of size (§ 24 para. 2 no. 3 lit. a).

“An ancillary operation does not count.”	Only for certain types in the energy, transport, drinking water, wastewater and waste management sectors does the law restrict coverage to the principal activity or an essential share (Annexes 1 and 2). Otherwise, according to the BCS, even subordinate activities can bring the whole entity into scope.
“The authority will contact us if we are covered.”	Classification follows from the law. Covered entities register themselves (§ 29 paras. 2 and 3), according to the BCS independently and without being asked by the authority.

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.

- NISG 2026, current version in the RIS, including Annexes 1 and 2**
§§ 3, 24 to 26, 29, 31 to 34, 37, 39, 45, 46, 51, Annexes 1 and 2; version of October 25, 2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009173
- Government bill 308 d. B. XXVIII. GP, explanatory notes on the NISG 2026 (PDF)**
On §§ 24, 25 and 46 and on Annex 1 nos. 5 and 7 and Annex 2 no. 2
www.parlament.gv.at/dokument/XXVIII/I/308/fname_1723246.pdf
- Federal Office for Cybersecurity: FAQ sectors**
Municipalities, principal and ancillary activities, photovoltaics, recharging points, managed service providers, nursing homes; as of September 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/sektoren.html
- Federal Office for Cybersecurity: FAQ supply chain**
Contractual obligations of suppliers; as of September 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/lieferkette.html
- Federal Office for Cybersecurity: FAQ registration**
Who is subject to the registration obligation?, form via USP or Portalverbund; as of September 25, 2026
www.bundesamt-cybersicherheit.gv.at/faq/registrierung.html
- Federal Office for Cybersecurity: Registration**
Initial registration, NIS2-Services in the USP, Portalverbund for public administration; as of October 2, 2026
www.bundesamt-cybersicherheit.gv.at/303/registrierung.html
- NISV 2026, BGBl. II No. 290/2026, in the RIS**
§ 2 requirements for risk management measures, § 9 entry into force
www.ris.bka.gv.at/eli/bgbl/II/2026/290
- Directive (EU) 2022/2555 (NIS 2 Directive)**
Recital 13, Art. 2(1), (2)(f) and (5)(a)
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- Commission Recommendation 2003/361/EC concerning the definition of SMEs**
Annex Art. 1 to 6
eur-lex.europa.eu/eli/reco/2003/361/oj/deu
- Regulation (EU) 2016/679 (General Data Protection Regulation)**
Art. 32 security of processing, Art. 33 and 34 notification and communication
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- Abfallwirtschaftsgesetz 2002 (Austrian Waste Management Act 2002), § 2 in the RIS**
§ 2 para. 6 nos. 3 and 4: waste collectors and waste treatment operators
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009173
- Bundes-Verfassungsgesetz (Austrian Federal Constitutional Law), Art. 108 in the RIS**
Vienna: municipal authority is also the Office of the State Government
www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009173

- 13 **Oö. Informationstechnologien-Einsatz-Gesetz (Oö. ITEG), LGBL No. 46/2025, in the RIS**
§ 1 no. 2, § 3 paras. 1 and 3
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=LrOO&Gesetzesnumm...
- 15 **Kärntner Gemeinde-Ausbildungs- und Prüfungsverordnung (K-GAPV), § 4 in the RIS**
Para. 1 lit. e and para. 6: induction course including ICT security
ris.bka.gv.at/eli/lgbL/KA/2022/53/P4/LKT40020758
- 17 **Austrian Information Security Handbook (Federal Chancellery, A-SIT)**
Version 4: foreword, preface, introduction and target group guides
www.sicherheitshandbuch.gv.at
- 14 **Kärntner Gemeindemitarbeiterinnengesetz (K-GMG), § 109 in the RIS**
Para. 1 lit. h and para. 2: ICT and IT security; in force since January 1, 2026
ris.bka.gv.at/eli/lgbL/KA/2011/96/P109/LKT40020810
- 16 **Wiener Dienstordnung 1994, § 26d in the RIS**
Para. 5: private ICT devices for mobile work; in force since September 1, 2025
ris.bka.gv.at/eli/lgbL/WI/1994/56/P26d/LWI40017661
- 18 **BSI: IT-Grundschutz profile Basis-Absicherung Kommunalverwaltung**
Version 4.0 of November 13, 2023, Sections 5 to 7 and 9
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmi...