

CHECKLISTE · TOMORIS TOOLBOX

Informationssicherheit in der Gemeinde: Checkliste für den Basisschutz

Verantwortung, Überblick, Konten, Updates, Datensicherung, Dienstleister und Meldestellen, nach dem BSI-Kommunalprofil und dem Österreichischen Informationssicherheitshandbuch

STAND

25.10.2026

UMFANG

PDF, 8 Seiten

ONLINE

tomoris.com/downloads/gemeinde-informationssicherheit-checkliste

AUF EINEN BLICK

§ 24

Abs. 3 NISG 2026:
Gemeinden nicht im
Sektor Verwaltung

Art. 32

DSGVO: Sicherheit der
Verarbeitung gilt

Art. 37

DSGVO: Datenschutzbe-
auftragte für Behörden

GovCERT

Meldestelle für die öf-
fentliche Verwaltung

FÜR WEN

- Bürgermeisterinnen und Bürgermeister, die die Verantwortung tragen
- Amtsleitung, die Abläufe und Zuständigkeiten im Gemeindeamt organisiert
- Gemeinde-IT und IT-Dienstleister von Gemeinden
- Gemeindeverbände und kleine öffentliche Einrichtungen

WORUM ES GEHT

Gemeindeämter verarbeiten täglich personenbezogene Daten von Bürgerinnen und Bürgern, oft mit wenig eigenem IT-Personal und vielen externen Dienstleistern. Diese Checkliste bündelt den Basisschutz für Gemeinden: wer verantwortlich ist, welcher Überblick nötig ist, wie Konten, Updates, Schutz vor Schadsoftware und Datensicherung geregelt sein sollten, worauf bei Fernwartung, Cloud und Auslagerung zu achten ist und an wen Sie sich im Vorfall wenden. Sie stützt sich auf das Österreichische Informationssicherheitshandbuch, das BSI-Profil Basis-Absicherung Kommunalverwaltung und die DSGVO und ordnet ein, welche Rolle das NISG 2026 für Gemeinden spielt.

Diese Checkliste ist eine Empfehlung von TOMORIS und ersetzt keine Rechtsberatung. Das BSI-Profil stammt aus Deutschland und dient als Vorbild. Maßgeblich sind DSGVO, NISG 2026 und das für Ihre Gemeinde geltende Landes- und Bundesrecht in der geltenden Fassung; ob Einrichtungen in Gemeindehand unter das NISG 2026 fallen, ist im Einzelfall zu prüfen.

INHALT

01	Ausgangslage für Gemeinden	2
02	Verantwortung und Organisation	3
03	Überblick über Systeme, Verfahren und Partner	4
04	Konten, Updates, Schadsoftware, Datensicherung	4
05	Fernwartung, Cloud und externe Dienstleister	5
06	Sicherheitsvorfall und Meldestellen	5
07	Mitarbeitende einbinden	6
08	Fahrplan in fünf Schritten	7
09	Quellen	8

01

Ausgangslage für Gemeinden

Was rechtlich gilt und welche Leitfäden helfen

NISG 2026

Gemeinden und Gemeindeverbände sind vom Sektor öffentliche Verwaltung ausdrücklich ausgenommen (§ 24 Abs. 3). Die NIS-2-Richtlinie hätte es den Mitgliedstaaten erlaubt, die lokale Ebene einzubeziehen (Art. 2 Abs. 5 lit. a). Ob Einrichtungen einer Gemeinde in einem anderen Sektor erfasst sind, ist gesondert zu prüfen.

DSGVO

Gilt für jede Gemeinde: geeignete technische und organisatorische Maßnahmen für ein dem Risiko angemessenes Schutzniveau (Art. 32), Pflicht zur Benennung einer oder eines Datenschutzbeauftragten für Behörden und öffentliche Stellen (Art. 37 Abs. 1 lit. a).

Österreichisches Informationssicherheitshandbuch

Herausgegeben von Bundeskanzleramt und A-SIT, Version 4.4.0 vom 06.11.2023; beschreibt den Aufbau eines Informationssicherheits-Managementsystems in Unternehmen und der öffentlichen Verwaltung.

BSI-Profil Basis-Absicherung Kommunalverwaltung

Deutsches Profil, Version 4.0 vom 13.11.2023, von der Arbeitsgruppe kommunale Basis-Absicherung mit den kommunalen Spitzenverbänden erarbeitet und vom BSI veröffentlicht; definiert Mindestmaßnahmen für Kommunalverwaltungen als Einstieg. Für Österreich ein gut übertragbares Vorbild, keine Rechtspflicht.

Die Checkliste ist eine Empfehlung von TOMORIS und folgt den genannten Leitfäden. Das BSI-Profil versteht sich ausdrücklich als Einstieg: Mittelfristig soll darauf ein Sicherheitskonzept nach der Standard-Absicherung aufbauen, weil Gemeinden regelmäßig Daten mit höherem Schutzbedarf verarbeiten.

02 —

Verantwortung und Organisation

Wer zuständig ist, auch wenn eine Person mehrere Rollen hat

- ☐ Bürgermeisterin oder Bürgermeister bzw. Amtsleitung übernimmt die Verantwortung für Informationssicherheit und stellt Mittel bereit (BSI-Profil, Zielgruppe; Handbuch, Managementverantwortung).
- ☐ Eine verantwortliche Person benannt, die das Thema vorantreibt (BSI-Profil zu ISMS.1.A4).
- ☐ Leitlinie zur Informationssicherheit beschlossen und bekannt gemacht; das BSI-Profil verweist dazu auf eine eigene Handreichung für Kommunalverwaltungen (BSI-Profil, Rahmenbedingungen).
- ☐ Zuständigkeiten festgelegt; dieselbe Person darf mehrere Aufgaben übernehmen, wenn die nötigen Verantwortlichkeiten definiert sind (BSI-Profil zu ORP.1).
- ☐ Ansprechperson für schwierige technische Sicherheitsfragen festgelegt; das kann ein externer Dienstleister sein (BSI-Profil zu ORP.1.A15).
- ☐ Datenschutzbeauftragte oder Datenschutzbeauftragter benannt und frühzeitig in Sicherheitsfragen eingebunden (Art. 37 DSGVO; BSI-Profil zu CON.2).
- ☐ Überblick über die rechtlichen und vertraglichen Anforderungen an das Gemeindeamt (BSI-Profil, ORP.5).

03 —

Überblick über Systeme, Verfahren und Partner

Was Sie kennen müssen, bevor Sie schützen

- ☐ Liste aller Standorte und Systeme: Gemeindeamt, Bauhof, Schule, Kindergarten, Server, Arbeitsplätze, Netzwerkgeräte, Drucker.
- ☐ Liste der Fachanwendungen und Online-Dienste mit Verantwortlichen und Anbietern.
- ☐ Liste der externen Dienstleister und Cloud-Dienste mit Zugriffen und Verträgen.
- ☐ Schutzbedarf eingeschätzt; bei personenbezogenen Daten ist er in Gemeinden in der Regel höher als die Basis-Absicherung (BSI-Profil, Schutzbedarf).
- ☐ Verfahren mit besonderen rechtlichen Vorgaben gekennzeichnet; sie brauchen zusätzliche Maßnahmen (BSI-Profil, Handlungsempfehlung).

Die Listen sind die Grundlage für alle weiteren Punkte: für Updates, Datensicherung, Berechtigungen und den Notfall. Halten Sie sie aktuell und so, dass sie auch bei einem Ausfall der IT greifbar sind.

04 —

Konten, Updates, Schadsoftware, Datensicherung

Der technische Basisschutz nach den Bausteinen des BSI

Technischer Basisschutz (Anforderungen laut BSI-Profil Basis-Absicherung Kommunalverwaltung)

BEREICH	WAS GEREGLT SEIN SOLL	BAUSTEIN
Konten und Rechte	Benutzende geregelt einrichten und löschen, Berechtigungen vergeben, ändern und entziehen und dokumentieren, Funktionen trennen, Passwortgebrauch und Anmeldung regeln; alle in die Anmeldeverfahren eingewiesen	ORP.4.A1 bis A9, A22, A23, A19
Administration	Geregelte Administration, getrennte Rollen für Anwendungs- und Systemadministration; externe Administratoren setzen den Baustein ebenfalls um	OPS.1.1.2
Updates	Konzept für Patches und Änderungen, Zuständigkeiten, Umgang mit Autoupdates, regelmäßige Aktualisierung	OPS.1.1.3.A1 bis A3, A15
Schadsoftware	Virenschutz, den Benutzende nicht abschalten können; Mitarbeitende kennen die Ansprechperson bei Verdacht	OPS.1.1.4
Datensicherung	Einflussfaktoren erheben, Verfahren und Pläne festlegen, regelmäßig sichern, Sicherungen schützen und sicher aufbewahren, regelmäßig testen; beim Aufbewahrungsort die lokale Gefahrenlage wie Hochwasser berücksichtigen	CON.3.A1, A2, A4, A5, A12, A14, A15

**Verschlüsselung
und Löschen**

Kryptokonzept für personenbezogene Daten und Kommunikation; geregeltes Löschen und Vernichten

CON.1, CON.6

Prüfen Sie die Datensicherung mit einer Kopie, die von Angriffen und Störungen im Gemeindeamt getrennt ist, und testen Sie die Wiederherstellung. Einzelheiten zum Vorgehen enthält die Backup-Checkliste 3-2-1-1-0 von TOMORIS.

05

Fernwartung, Cloud und externe Dienstleister

Die Verantwortung bleibt beim Gemeindeamt

- ☐ Fernwartung nur mit aktuellen, als sicher eingestuften Protokollen und festgelegten Werkzeugen; Abläufe geregelt (BSI-Profil zu OPS.1.2.5.A8, A9).
- ☐ Fernwartung durch Dritte aufgezeichnet und vertraglich geregelt; Dokumentation der Zugänge vor Unbefugten geschützt (OPS.1.2.5.A7, A19).
- ☐ Vor der Vergabe von Cloud-Diensten Anforderungen festgelegt, Datenschutzbeauftragte früh eingebunden, Vertrag mit Leistung, Verantwortlichen, Art und Ort der Verarbeitung (OPS.2.2.A2, A8, A9).
- ☐ Anforderungen an Cloud-Dienste regelmäßig anhand aktueller Nachweise kontrolliert; Beendigung schon bei Vertragsbeginn geregelt (OPS.2.2.A13, A14).
- ☐ Bei Auslagerung bleibt die Verantwortung für die Informationssicherheit bei der Dienststelle; Anforderungen vorab definiert, Ausstiegsstrategie im Vertrag (BSI-Profil zu OPS.2.3).
- ☐ Bei sensiblen Daten Verschwiegenheit mit Dienstleistern vereinbart (BSI-Profil zu OPS.2.3.A4); bei Auftragsverarbeitung Vertrag nach Art. 28 DSGVO.

06

Sicherheitsvorfall und Meldestellen

Wer zu verständigen ist und wie Sie vorbereitet sind

Das BSI-Profil sieht die Basis-Anforderungen der Vorfallbehandlung vor: definieren, was ein Sicherheitsvorfall ist, Richtlinie und Zuständigkeiten festlegen, Betroffene informieren, Vorfälle beheben und die Betriebsumgebung sicher wiederherstellen (DER.2.1.A1 bis A6). Für eine vollständige Basis-Absicherung kommt das Notfallmanagement dazu (DER.4).

Anlaufstellen in Österreich (laut deren eigenen Angaben)

STELLE	WOFÜR	KONTAKT
GovCERT Austria	Computer Emergency Response Team der öffentlichen Verwaltung; Meldung sonstiger Vorfälle in der öffentlichen Verwaltung, für Gemeinden freiwillig	reports@govcert.gv.at
CERT.at	Nationales CERT, Ansprechpartner für IT-Sicherheit, koordiniert bei Angriffen	team@cert.at, reports@cert.at
Bundeskriminalamt	Hinweise und Hilfe bei Verdacht auf Internetkriminalität; Anzeige nicht per E-Mail, sondern bei jeder Polizeidienststelle	against-cybercrime@bmi.gv.at
Datenschutzbehörde	Meldung einer Verletzung des Schutzes personenbezogener Daten, möglichst binnen 72 Stunden (Art. 33 DSGVO)	Online- oder PDF-Formular der Datenschutzbehörde

Notfallkontakte Ihrer Gemeinde (zum Ausfüllen)

ROLLE	NAME	ERREICHBAR UNTER
Bürgermeister/in	_____	_____
Amtsleitung	_____	_____
IT-Verantwortliche/r	_____	_____
IT-Dienstleister, Notfallnummer	_____	_____
Datenschutzbeauftragte/r	_____	_____

Organisationen der öffentlichen Verwaltung können am aktiven Informationsaustausch mit GovCERT Austria teilnehmen; das Bundesministerium für Inneres entscheidet darüber, die Organisation nennt zwei Kontaktpersonen.

07

Mitarbeitende einbinden

Sensibilisierung, Eintritt, Austritt und Homeoffice

- ☐ Leitung sensibilisiert, Mitarbeitende in den sicheren Umgang mit IT eingewiesen und nach Aufgaben geschult; fortlaufend, nicht nur einmal (BSI-Profil zu ORP.3.A1, A3, A6).
- ☐ Eintritt und Austritt geregelt: Konten, Rechte und Schlüssel werden rechtzeitig vergeben und entzogen (BSI-Profil, ORP.2 und ORP.4).
- ☐ Homeoffice nur nach Regeln, wenn es genutzt wird (BSI-Profil, OPS.1.2.4).

- ☐ Alle wissen, an wen sie einen Verdacht auf Schadsoftware oder einen Vorfall melden (BSI-Profil zu OPS.1.1.4.A7).

08

Fahrplan in fünf Schritten

Vom Einstieg zum dauerhaften Sicherheitsmanagement, Empfehlung von TOMORIS

- 1 Verantwortung klären**
 Leitung entscheidet, eine verantwortliche Person wird benannt, Datenschutzbeauftragte sind eingebunden.
- 2 Überblick schaffen**
 Systeme, Fachanwendungen, Dienstleister und Verträge erfassen.
- 3 Basisschutz umsetzen**
 Die Punkte dieser Checkliste abarbeiten, beginnend mit Datensicherung, Updates, Konten und Fernwartung.
- 4 Notfall vorbereiten**
 Kontakte, Abläufe und Wiederanlauf festhalten, zum Beispiel mit der Vorlage für ein IT-Notfallhandbuch, und einmal im Jahr üben.
- 5 Weiterentwickeln**
 Mittelfristig ein Sicherheitskonzept nach der Standard-Absicherung bzw. ein Managementsystem nach dem Österreichischen Informationssicherheitshandbuch aufbauen.

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, BGBl. I Nr. 94/2025, geltende Fassung im RIS**
§ 8 Abs. 4, § 24 Abs. 3, § 46, gelesen am 25.10.2026
www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gese...
- 2 **Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie), deutsche Fassung auf EUR-Lex**
Art. 2 Abs. 5 lit. a, gelesen am 25.10.2026
eur-lex.europa.eu/eli/dir/2022/2555/oj/deu
- 3 **Verordnung (EU) 2016/679 (DSGVO), deutsche Fassung auf EUR-Lex**
Art. 28, 32, 33 und 37, gelesen am 25.10.2026
eur-lex.europa.eu/eli/reg/2016/679/oj/deu
- 4 **Österreichische Datenschutzbehörde: Meldung Data Breach**
Meldewege und Formular, gelesen am 25.10.2026
dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach
- 5 **Österreichisches Informationssicherheitshandbuch, Version 4.4.0 (06.11.2023), Bundeskanzleramt und A-SIT**
Einführung und Management Summary, gelesen am 25.10.2026
www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf
- 6 **BSI: IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung, Version 4.0 (13.11.2023)**
Abschnitte 5, 6 und 9.1, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmi...
- 7 **BSI IT-Grundschutz-Kompodium, Baustein DER.2.1 Behandlung von Sicherheitsvorfällen (Edition 2023)**
Basis-Anforderungen A1 bis A6, gelesen am 25.10.2026
www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-K...
- 8 **GovCERT Austria: Startseite, Meldung sonstiger Vorfälle, Teilnahme und Leistungen**
Aufgabe, Meldeadresse, Teilnahme am Informationsaustausch, gelesen am 25.10.2026
www.govcert.gv.at
- 9 **CERT.at: Über uns**
Rolle als nationales CERT, Kontakt, gelesen am 25.10.2026
www.cert.at/de/ueber-uns
- 10 **Bundeskriminalamt: Cybercrime-Competence-Center und Meldestelle against Cybercrime**
Meldestelle für Internetkriminalität, gelesen am 25.10.2026
www.bundeskriminalamt.at/306/start.html