



NIS-2-Compliance für Stadtwerke

Anforderungen kennen und sicher umsetzen



Stadtwerte im Fokus der Cybersicherheitsregulierung

Stadtwerte und kommunale Versorgungsunternehmen beliefern Millionen von Bürgerinnen und Bürgern mit Strom, Gas, Wasser, Wärme und digitaler Infrastruktur. Sie vereinen damit mehrere regulierte Sektoren unter einem Dach. Genau diese systemrelevante Rolle macht sie zu einem bevorzugten Angriffsziel für Cyberkriminalität.

Viele Stadtwerte zählen aufgrund ihrer Versorgungsrelevanz zu den besonders wichtigen Einrichtungen im Sinne von NIS-2 und unterliegen daher strengeren Anforderungen und einer intensiveren Aufsicht. Hinzu kommt: Die operative Technologie (OT) in Leitstellen und Steuerungssystemen ist oft historisch gewachsen und häufig nur unzureichend auf moderne Cyberbedrohungen ausgerichtet.

Mit der NIS-2-Richtlinie (EU) 2022/2555 hat der europäische Gesetzgeber auf die wachsende Bedrohungslage reagiert. Auch für Unternehmen, die bereits von der NIS-1-Richtlinie betroffen waren, werden die Anforderungen deutlich verschärft. Sie sind umfassender, greifen tiefer in bestehende Strukturen und Prozesse ein und regeln erstmals auch explizit die persönliche Haftung der Geschäftsleitung.

Typische NIS-2-relevante Bereiche bei Stadtwerten:

- Strom- und Gasversorgung
- Trinkwasser und Abwasser
- Fernwärme
- Telekommunikation / Breitband
- Abfallwirtschaft





Von NIS-1 zu NIS-2: Was sich für Stadtwerke in Deutschland ändert

NIS-1-Umsetzung bis 5. Dez. 2025	NIS-2-Umsetzung ab 6. Dez. 2025
Keine Registrierungspflicht	Verpflichtende Registrierung und Bewertung
Begrenzter Sektorenumfang (z. B. Energie, Verkehr, Gesundheit, Wasser, digitale Infrastruktur)	Deutlich erweiterter Sektorenkatalog (u. a. Energie, Trinkwasser, Abwasser, digitale Dienste, Abfallwirtschaft, Industrie)
Betreiber wesentlicher Dienste mit sektorspezifischen Schwellwerten (z. B. Energieversorger ab 500 Megawatt)	Unternehmen ab 50 Mitarbeitern oder ab 10 Mio. € Jahresumsatz (in relevanten Sektoren); nahezu alle Stadtwerke
Keine explizite Regelung zur persönlichen Verantwortung der Geschäftsleitung	Explizite Verantwortung der Geschäftsleitung: Eigene Fortbildung, Genehmigung und Überwachung von Maßnahmen sowie Haftbarkeit bei Verstößen
Meldepflichten weniger konkret, weniger standardisiert und weniger zeitkritisch	Mehrstufige, klar definierte und zeitkritische Meldepflichten (24h / 72h / 30 Tage)
Fokus auf technische und operative Sicherheitsmaßnahmen	Ganzheitlicher Ansatz: Governance, Organisation, Technik und Lieferkette

NIS-2-Anforderungen: Was auf Stadtwerke zukommt

Die NIS-2-Richtlinie definiert ein umfassendes Set an Anforderungen. Diese sind technischer und organisatorischer Natur und greifen tief in bestehende Strukturen, Prozesse und Verantwortlichkeiten ein.

Für Stadtwerke bedeutet das eine besondere Herausforderung: Neben klassischen IT-Systemen sind auch OT-Systeme in Leitstellen und Steuerung einbezogen. Gleichzeitig müssen Organisation und Prozesse – etwa im Risikomanagement, Incident Handling oder in der Zusammenarbeit mit Dienstleistern – deutlich weiterentwickelt werden. Hinzu kommen erweiterte regulatorische Pflichten, insbesondere im Hinblick auf Meldeprozesse und die persönliche Verantwortung der Geschäftsleitung. Zudem sind interne Ressourcen und Fachkompetenzen in der Informationssicherheit in vielen Fällen nur begrenzt vorhanden.

Pflichten im Überblick

Organisatorische und technische Maßnahmen entsprechen dem aktuellen Stand der Technik:

- Durchführung regelmäßiger Risikoanalysen und -bewertungen
- Einführung eines strukturierten Incident- und Krisenmanagements
- Business-Continuity- und Notfallmanagement-Konzepte
- Absicherung von Lieferketten, IT-Dienstleistern und OT-Systemen
- Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen für alle Mitarbeiter
- Mehrstufige Meldepflichten bei Sicherheitsvorfällen
(24h Erstmeldung, 72h Folgemeldung, 30 Tage Abschlussbericht)
- Technische Schutzmaßnahmen: Netzwerksicherheit, Zugriffskontrolle, Verschlüsselung, Patch-Management

Persönliche Haftung der Geschäftsleitung

NIS-2 stellt klar: Die Einhaltung der Cybersicherheitsanforderungen liegt in der persönlichen Verantwortung der Geschäftsleitung. Diese Pflicht ist nicht delegierbar. Bei Verstößen drohen empfindliche Bußgelder für wesentliche Einrichtungen bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes, für wichtige Einrichtungen bis zu 7 Millionen Euro oder 1,4 % des Umsatzes. Darüber hinaus kann die Aufsichtsbehörde Managern die Ausübung von Leitungsaufgaben vorübergehend untersagen.



Wie Consileon Stadtwerke begleitet

Consileon begleitet Stadtwerke auf dem gesamten Weg zur NIS-2-Compliance von der ersten Standortbestimmung bis zur dauerhaften Umsetzungsbegleitung. Die Herausforderungen der NIS-2-Umsetzung sind komplex: technisch, organisatorisch und regulatorisch. Klassische, überwiegend manuelle Ansätze stoßen dabei schnell an ihre Grenzen. Consileon verbindet tiefes Branchen-Know-how mit modernsten KI-gestützten Methoden zu einem leistungsstarken, wirtschaftlich tragfähigen Angebot.



1. Betroffenheitsanalyse

Wir prüfen, ob und in welcher Einstufung (besonders wichtige oder wichtige Einrichtung) Ihr Stadtwerk von NIS-2 betroffen ist. Basis ist eine strukturierte Analyse Ihrer Unternehmensmerkmale, Sektorenzugehörigkeit und Versorgungsleistungen.



2. Registrierungsberatung

NIS-2 verpflichtet betroffene Einrichtungen zur Registrierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Wir begleiten Sie durch den Prozess – von der Vorbereitung der erforderlichen Informationen bis zur vollständigen Antragsstellung – oder übernehmen diesen vollständig.



3. NIS-2-Audit

Mit KI-gestützten Analyseverfahren prüfen wir systematisch bestehende Richtlinien, Prozesse und technische Maßnahmen gegen die NIS-2-Anforderungen und identifizieren Lücken und Handlungsfelder für Ihr Unternehmen (Red Flags).



4. Geschäftsleitungs-Schulung

Wir schulen Ihre Geschäftsleitung gezielt zu den persönlichen Haftungsrisiken unter NIS-2. Sie erhalten ein Grundverständnis über organisatorische und technische Maßnahmen, Pflichten und Nachweisführung und sind in der Lage, NIS-2-Compliance als integralen Bestandteil Ihrer Governance zu verankern.



5. Beratung und Umsetzungsbegleitung

Wir begleiten ihr Stadtwerk bei der Ausgestaltung, in der operativen Umsetzung und der Einführung eines passgenauen Sicherheitsmanagements. Unser modularer Ansatz erlaubt es, genau dort anzusetzen, wo Ihr größter Handlungsbedarf liegt.



6. Continuous Compliance Management

Einmalige Umsetzung reicht nicht: NIS-2 erfordert dauerhaftes Monitoring und laufende Anpassung. Unser Ansatz etabliert einen kontinuierlichen Compliance-Prozess mit automatisierten Überwachungsroutinen, strukturierter Dokumentation und regelmäßigen Status-Reportings für Ihre Geschäftsleitung.

Ihr Weg zur steuerbaren Compliance

NIS-2 ist kein einmaliges Projekt, sondern ein dauerhaftes Pflichtenregime. Viele Stadtwerke stehen vor der Herausforderung, Compliance-Strukturen ohne zusätzliches Fachpersonal aufzubauen. Consileon hilft Ihnen dabei, NIS-2 als integralen Bestandteil Ihrer Governance zu verankern und dauerhaft handlungsfähig zu bleiben – pragmatisch, aufwandsarm und mit KI-Unterstützung.



Ganzheitlicher Ansatz

Consileon begleitet Sie von der Erstanalyse bis zum laufenden Compliance-Management: Strategie, Organisation, IT/OT-Technik und Schulung aus einer Hand. Dank langjähriger Erfahrung in der kommunalen Energie- und Versorgungswirtschaft verstehen wir Ihre Herausforderungen.



KI-gestützte Dokumentprüfung

Der Consileon Compliance Manager analysiert Ihre Dokumente KI-gestützt, strukturiert und reproduzierbar. Abweichungen und Compliancelücken werden erkannt und Maßnahmen vorgeschlagen. Reduzieren Sie den Aufwand um 50 % ohne Abstriche bei Qualität oder regulatorischer Sicherheit.



Rechtliche Klarheit


NIS-2-Compliance ist auch eine rechtliche Herausforderung. Deshalb arbeiten wir eng mit einer führenden deutschen Kanzlei im Bereich IT- und Digitalrecht mit umfangreicher Erfahrung in NIS-2-Projekten bei Unternehmen der kritischen Infrastruktur zusammen. Gemeinsam bieten wir Ihnen technische und juristische Beratung aus einer Hand.

Ihre Vorteile:

- Klarheit über Ihre Betroffenheit und den aktuellen Umsetzungsstand
- Strukturierte Gap-Analysen mit direktem Handlungsplan
- Entlastung Ihrer internen Ressourcen durch KI-gestützte Automatisierung
- Rechtssichere Dokumentation für Audits und Behörden
- Geschäftsleitung dauerhaft steuerungsfähig – nicht haftungsexponiert
- Modularer Einstieg: Starten Sie dort, wo Ihr Handlungsdruck am größten ist

FAZIT





Viele Stadtwerke wissen nicht genau, ob und in welchem Umfang sie von NIS-2 betroffen sind. Gleichzeitig beginnen Aufsichtsbehörden mit der Durchsetzung. Wir analysieren Ihre individuelle Betroffenheit und zeigen Ihnen einen pragmatischen Weg zur NIS-2-Compliance.

“

Lösungen für morgen. Heute.

Ihre Vision, unser Antrieb. Mit über 550 Mitarbeiterinnen und Mitarbeitern ist Consileon Ihr starker Partner für Top-Managementberatung sowie Lösungen mit IT- und KI-Bezug.

Wir unterstützen Sie von der Konzeption bis zur Umsetzung in allen Bereichen der Digitalisierung und helfen Ihnen dabei, wichtige Herausforderungen von morgen mit Technikkompetenz zu lösen.

Gilles Schneider ist Geschäftsbereichsleiter Public Sector bei Consileon und begleitet seit vielen Jahren öffentliche Einrichtungen und kommunale Unternehmen bei strategischen und regulatorischen Transformationsvorhaben. Gerne bespricht er mit Ihnen die Auswirkungen von NIS-2 auf Ihr Stadtwerk, mögliche Handlungsfelder sowie pragmatische Wege zur nachhaltigen und steuerbaren Compliance.



Gilles Schneider
Geschäftsbereichsleiter Public Sector

 +49 173 4096437
 Gilles.Schneider@consileon.de