Cloud-Infrastruktur

Souveräne Smart City

[07.10.2026] Smarter, vernetzter, bürgerfreundlicher und trotzdem digital souverän. Städte und Gemeinden müssen sich modernisieren und gleichzeitig die Herrschaft über ihre digitale Zukunft behalten. Eine standardisierte und interoperable Cloud-Architektur hilft dabei.

Eine Smart City umfasst weit mehr als eine perfekt orchestrierte Verkehrsleittechnik und eine reibungslos funktionierende Abfallwirtschaft. Auch ein durchgängig digitales Angebot von Bürgerdienstleistungen, Nachhaltigkeitsinitiativen sowie der sichere Betrieb der gesamten Infrastruktur gehören zum Spektrum einer modernen Stadtplanung. Die Grundlage hierfür ist eine belastbare technische Infrastruktur mit offenen Schnittstellen und interoperablen Systemen sowie eine IT-Architektur, die mit den wachsenden Anforderungen Schritt hält.

Datenhoheit jenseits des Serverstandorts

Gleichzeitig mit der Entscheidung für die technische Grundlage muss eine politische Frage einhergehen. Wer kontrolliert die Daten? Kommunen, die auf die proprietären Plattformen großer Technologiekonzerne setzen, erkaufen sich kurzfristige Bequemlichkeit mit langfristigem Kontrollverlust. Im Mittelpunkt steht dabei der US-amerikanische Cloud Act. Demnach können Daten, die bei US-Anbietern liegen, dem Zugriff außereuropäischer Behörden unterliegen, selbst wenn die Server in europäischen Rechenzentren stehen. Vertragliche Zusicherungen einzelner Anbieter ändern daran wenig, da sie die Reichweite ausländischer Gesetzgebung nicht aufheben können. Das ist besonders kritisch bei sensiblen Bürger-, Register- und Verfahrensdaten. Anders ausgedrückt: Wer kommunale Daten auf Hyperscaler-Plattformen verarbeitet, gibt im Zweifel die Hoheit über kritische Fachverfahren aus der Hand.

Neben der Datensouveränität gibt es ein weiteres, oft unterschätztes Problem: die Abhängigkeit von einzelnen Anbietern. Proprietäre Cloud-Umgebungen binden Kommunen an bestimmte Technologie-Stacks, Lizenzmodelle und Migrationskosten. Das macht einen späteren Anbieterwechsel technisch und wirtschaftlich schwierig. Gerade für öffentliche Einrichtungen, die langfristig planen und haushaltsrechtlich gebunden sind, bedeutet der sogenannte Vendor Lock-in eine schwierige Lage.

Regeln für Sicherheit und Souveränität

Dieser Handlungsdruck wird durch regulatorische Vorschriften für den Datenschutz, die Informationssicherheit und die Nachvollziehbarkeit verstärkt. So hat der Gesetzgeber mit dem im Dezember 2025 in Kraft getretenen NIS2-Umsetzungsgesetz die Cyber-Sicherheitspflichten erheblich ausgeweitet. Dazu zählen ein systematisches Risikomanagement, Meldepflichten bei Sicherheitsvorfällen und Anforderungen an die Lieferkette.

Auch wo kommunale IT-Dienstleister landesrechtlich reguliert sind, steigt das geforderte Sicherheitsniveau im gesamten öffentlichen Sektor spürbar. Parallel dazu formuliert die Deutsche Verwaltungs-Cloud-Strategie (DVS) des IT-Planungsrats klare Erwartungen an souveräne und interoperable Cloud-Infrastrukturen. Kommunen müssen künftig belegen, dass sie sensible Daten im EU-Rechtsraum

verarbeiten und die Kontrolle über kritische Systeme behalten.

Offene Standards schaffen Wahlfreiheit

Offene Standards bieten einen Ausweg aus der Abhängigkeit. Open-Source-Technologien schaffen Transparenz, ermöglichen die Nachnutzung durch andere Verwaltungen und geben Kommunen die Freiheit, Systeme weiterzuentwickeln, ohne an einen einzigen Hersteller gebunden zu sein. Was eine Kommune entwickelt, können andere übernehmen, anstatt jede Lösung erneut zu beschaffen.

Das technische Fundament dafür liefert der Sovereign Cloud Stack (SCS) der Open Source Business Alliance. Er definiert eine standardisierte und interoperable Cloud-Architektur, die speziell für den Einsatz in der öffentlichen Verwaltung entwickelt wurde. Wenn mehrere Anbieter diesem Stack folgen, entstehen vergleichbare Dienste, zwischen denen Verwaltungen wechseln oder Lasten verteilen können, ohne ihre Architektur neu aufzubauen. Auf dieser gemeinsamen Basis können Bund, Länder und Kommunen zu einem föderalen Verbund verknüpft werden, der eigene Erweiterungen einbringt und voneinander profitiert.

Souveräne Cloud mit geprüftem Betrieb

Die noris Sovereign Cloud (nSC) zeigt, wie sich dieser Anspruch produktiv umsetzen lässt. Sie überführt den Sovereign Cloud Stack in eine zertifizierte Produktivumgebung, die vollständig auf Open-Source-Standards basiert und keine Abhängigkeit von proprietären Hyperscaler-Technologien aufweist. Die Plattform wird ausschließlich in deutschen Hochsicherheitsrechenzentren betrieben, die nach BSI C5 zertifiziert und mit der DVS konform sind. Damit entsteht für Kommunen eine Infrastruktur, die Skalierbarkeit und Automatisierung bietet, ohne die digitale Souveränität preiszugeben. Da die Plattform auf offenen Standards aufsetzt, bleibt ein Anbieterwechsel möglich.

Souveränität ohne nachweisbare Sicherheit ist ein leeres Versprechen – so viel steht fest. Die Rechenzentren von noris network sind nach ISO 27001, BSI IT-Grundschutz und EN 50600 zertifiziert und somit auf hohe Informationssicherheit und Betriebskontinuität ausgelegt. Der Betrieb erfolgt mit 100-prozentiger regenerativer Energie, was durch Zertifizierungen nach ISO 14001 und ISO 50001 belegt ist.

()

Dieser Beitrag ist in der Ausgabe Oktober 2026 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Cloud-Infrastruktur, Smart City