

Hoheit bewahren

René Petters

Für Kommunen ist Cloud eine Entscheidungsfrage: Zögern führt zu höheren Kosten, Sicherheitsrisiken und Kontrollverlust. Die Cloud bildet somit den Schlüssel zur Verwaltungsmodernisierung – vorausgesetzt, die digitale Souveränität ist gesichert.

Die digitale Transformation der öffentlichen Verwaltung läuft – aber sie läuft nicht von allein. Mit jedem neuen Online-Dienst, jeder Schnittstelle und jedem digitalisierten Prozess steigen die Anforderungen an Kontrolle, Sicherheit und Verlässlichkeit. Kommunen müssen heute schneller liefern, stabiler betreiben und zugleich strenger schützen. Dabei dürfen sie eines nicht verlieren: die Hoheit über Daten, Prozesse und IT-Strukturen. Deshalb wird digitale Souveränität zum Must-have. Und genau deshalb rücken Cloud-Lösungen, die dies gewährleisten können, in den Mittelpunkt.

Digitale Souveränität heißt auf kommunaler Ebene, dass eine Kommune ihre IT selbstbestimmt steuern kann. Sie entscheidet, wo Daten verarbeitet werden. Sie definiert, wer worauf zugreifen darf. Sie setzt Betriebsmodelle so auf, dass sie transparent, prüfbar und rechtssicher bleiben. Das klingt selbstverständlich – ist es aber in vielen Cloud-Konstellationen nicht. Gerade im öffentlichen Sektor besteht ein sehr hoher Schutzbedarf, unter anderem für Bürgerdaten, kritische Fachverfahren oder verwaltungsweite Plattformen. Wenn Abhängigkeiten von einzelnen Anbietern wachsen, die Transpa-

renz über Datenflüsse fehlt oder Zuständigkeiten zwischen Verwaltung, Provider und Dienstleister verschwimmen, wird Souveränität zur Illusion. Dann drohen nicht nur Sicherheits- und Compliance-Risiken, sondern auch ganz praktische Folgen wie Verzögerungen, Kostenüberraschungen, Betriebsausfälle, Vertrauensverlust. Wer kommunal handlungsfähig bleiben will, muss Cloud-Entscheidungen deshalb konsequent an Souveränität ausrichten – technologisch, organisatorisch und rechtlich.

Cloud-Technologien sind aus modernen Verwaltungen nicht mehr wegzudenken. Sie schaffen Tempo, Skalierbarkeit und neue Möglichkeiten für Zusammenarbeit und digitale Services. Für die sichere, souveräne Nutzung stehen mehrere Schlüsselfragen im Mittelpunkt, die Kommunen konsequent beantworten müssen: Wo werden Daten verarbeitet, und unter welchem Rechtsraum? Wie transparent ist der Betrieb in technischer, organisatorischer und finanzieller Hinsicht? Wer trägt die Verantwortung – und ist diese eindeutig, durchgängig und auch dokumentiert? Cloud-Ansätze für mehr Souveränität setzen hier an: Sie verbinden Cloud-Funktionalität mit klarer Datenhoheit, nachvollziehbaren Sicherheits-

mechanismen und überprüfbaren Betriebsprozessen. So wird Cloud zur kontrollierbaren Infrastruktur – und nicht zur Blackbox.

Viele Kommunen starten souverän, indem sie für besonders schutzbedürftige Anwendungen auf Private-Cloud-Umgebungen setzen. Die Vorteile: Die Umgebung ist dediziert, Zuständigkeiten lassen sich klar regeln, Sicherheits- und Zugriffsmodelle sind stringent umsetzbar. Sensible Daten und kritische Verfahren laufen damit in einem Rahmen, der sich technisch wie organisatorisch zuverlässig kontrollieren lässt. GISA unterstützt Kommunen in diesem Kontext mit einem Ansatz, der digitale Souveränität nicht auf einzelne Produkte reduziert, sondern als Zusammenspiel aus Infrastruktur, Governance und Betrieb versteht. Ein zentraler Baustein ist dabei die GISA Business Cloud in zertifizierten Rechenzentren in Deutschland. Sie ermöglicht einen rechtskonformen, kontrollierbaren Cloud-Betrieb, bei dem Daten im deutschen Rechtsraum bleiben und Zugriffs sowie Sicherheitsmechanismen nachvollziehbar geregelt werden. Dabei ist die Private Cloud kein Selbstzweck. Sie schafft dort Souveränität, wo sie zwingend gebraucht wird – bei Daten mit hohem Schutzbedarf, bei Kernverfahren

und bei Plattformen, die die Verwaltung dauerhaft tragen müssen.

Digitale Souveränität bedeutet jedoch nicht Verzicht auf Innovation. Viele Kommunen benötigen flexible Plattformen, etwa für Kollaboration, Webportale, skalierbare Fachanwendungen oder projektbasierte Entwicklungsumgebungen. Hybride Architekturen kombinieren kontrollierte Private-Cloud-Infrastrukturen mit ausgewählten Public-Cloud-Diensten. Sensible Daten und Kernverfahren bleiben stets in der Private Cloud. Weniger kritische Anwendungen können die Skalierbarkeit der Public Cloud nutzen. Das bedeutet: mehr Tempo und Flexibilität ohne pauschale Abhängigkeit. Hybride Modelle funktionieren allerdings nur, wenn sie konsequent gesteuert werden. Ein IT-Dienstleister wie GISA übernimmt in solchen Szenarien die Orchestrierung hybrider Umgebungen. Das schließt Sicherheitskonzepte, Compliance Management und klar definierte Verantwortlichkeiten mit ein. Die Kommune kann entscheiden, was wo läuft und behält eine umfassende Kontrolle über ihre eigenen Daten und Prozesse.

Der Cloud-Betrieb scheitert selten an Rechenleistung, sondern meist an der Organisation. Unklare Rollen, fehlende Governance und mangelnde Transparenz bei Kosten und Sicherheit zählen zu den häufigsten Stolpersteinen in Cloud-Projekten – gerade in hybriden Landschaften. Wenn nicht feststeht, wer Back-up, Monitoring, Incident-

Bearbeitung oder Berechtigungsmanagement verantwortet, entstehen Grauzonen. Das stellt ein nicht unerhebliches Risiko dar. Deshalb müssen Kommunen Governance früh verankern. Erfolgreiche Modelle stehen auf vier Hauptsäulen: dokumentierte Rollen und Zuständigkeiten, die auch im Betrieb tragen; Identity- und Access-Management, das Zugriffe konsequent steuert;



Adrian Grossi/stock.adobe.com

Cloud-Infrastrukturen müssen keine Blackbox sein.

kontinuierliches Monitoring für Sicherheit, Performance und Kosten sowie nachvollziehbare Dokumentation für Prüfungen, Audits und Gremien. GISA begegnet diesen Anforderungen zum Beispiel mit einem ganzheitlichen Ansatz von der strategischen Beratung über Architektur und Migration bis zum operativen Betrieb. Der Nutzen für Kommunen liegt nicht in „mehr Technik“, sondern in mehr Steuerbarkeit. Cloud wird überprüfbar, kalkulierbar und belastbar.

Digitale Souveränität ist kein Projekt mit Enddatum, sondern ein Entwicklungsprozess. Denn Regulierung verändert sich, Technologien verändern sich und auch die Verwaltungsorganisationen selbst ver-

ändern sich. Wer souverän bleiben will, muss seine Cloud-Strategie regelmäßig weiterentwickeln. Dies betrifft sowohl fachliche, technische als auch organisatorische Aspekte. Das gilt auch in der kommunalen Praxis. So müssen Kommunen Workloads neu priorisieren, Sicherheitsanforderungen nachschärfen, Betriebsprozesse anpassen und Kompetenzen im Haus aufbauen oder gezielt ergänzen. Dabei helfen Managed Services und erfahrene Partner, weil sie Betrieb und Weiterentwicklung dauerhaft absichern, ohne dass die Verwaltung die Datenhoheit verliert.

Kommunen können Digitalisierung und Selbstbestimmung verbinden. Sie benötigen dafür aber Ansätze, die ihren spezifischen Anforderungen gerecht werden. Dazu gehören Private- und Hybrid-Modelle, die die Datenhoheit sichern; eine Governance, die Verantwortung klärt sowie ein Betrieb, der transparent und prüfbar bleibt. Denn Cloud-Lösungen schaffen die Grundlage, um digitale Verwaltungsleistungen verlässlich bereitzustellen – heute und langfristig. GISA kann Kommunen dabei unterstützen, diesen Weg strukturiert zu gehen und setzt dabei auf deutsche Cloud-Infrastruktur, hybride Architekturen, klare Governance und verlässlichen Betrieb. Die Verwaltung behält dabei die Kontrolle – und gewinnt gleichzeitig die Flexibilität, die Digitalisierung erfordert.

René Petters ist Business Line Manager öffentlicher Sektor beim IT-Dienstleister und Cloud Service Provider GISA.