Digitale Souveränität in der Verwaltungscloud: Anforderungen, Architektur und Praxisbeispiele aus dem AAA-Bereich

Digital Sovereignty in the Administrative Cloud: Requirements, Architecture and Practical Examples from the AAA Sector

Elmar Happ | Sören Matthies | Michael Müller | Markus Reuter

Zusammenfassung

Die Vermessungs- und Katasterverwaltungen in Deutschland haben digitale Verfahren schon früh in ihre Fachprozesse integriert. Mit der in den letzten Jahren bereits etablierten Nutzung cloudbasierter Betriebsmodelle ergibt sich die Notwendigkeit, diese Strukturen gezielt weiterzuentwickeln, um die langfristige Handlungs- und Leistungsfähigkeit zu sichern. Digitale Souveränität bildet dabei die Grundlage für einen sicheren, unabhängigen und regelkonformen Betrieb von Geobasisdaten und Fachverfahren im AAA-Umfeld. Der Beitrag beschreibt die Anforderungen an cloudbasierte Betriebsmodelle unter Berücksichtigung der NIS-2-Richtlinie (NIS-2) und des KRITIS-Dachgesetzes (KRITIS). Im Fokus stehen Multi-Cloud-Ansätze, Containerisierung, offene Standards sowie moderne Entwicklungs- und Betriebsansätze. Anhand praxisnaher Beispiele wird aufgezeigt, wie bestehende Anwendungen schrittweise modernisiert und stabil betrieben werden können. Ergänzend wird ein kooperativer Ansatz zur Weiterentwicklung cloudbasierter Lösungen im Zusammenspiel von Verwaltung und Wirtschaft skizziert.

Schlüsselwörter: Cloud-Transformation, Digitale Souveränität, AAA-Fachverfahren, IT-Sicherheit, Cloud-Architektur, VertiGIS LM Co-Innovation HUB

Summary

Cadastral and surveying administrations in Germany have long integrated digital procedures into their domain-specific processes. With the growing adoption of cloud-based operating models, there is a need to further develop these structures to ensure long-term operational capability and performance. Digital sovereignty provides the basis for a secure, independent and compliant operation of geospatial base data and AAA systems. This paper outlines the requirements for cloud-based operating models considering regulatory frameworks such as the NIS-2 Directive (NIS-2) and the German KRITIS Act (KRITIS). It focuses on multi-cloud approaches, containerisation, open standards and modern development and operational practices. Using practical examples, the paper demonstrates how existing applications can be incrementally modernised and reliably operated. In addition, a cooperative approach for the structured evolution of cloud-based solutions through collaboration between public administration and industry is outlined.

Keywords: *cloud transformation, digital sovereignty, AAA systems, cybersecurity, cloud architecture, VertiGIS LM Co-Innovation HUB*

1 Cloud-Strategien in der Vermessungs- und Katasterverwaltung

1.1 Die Cloud als Treiber der Verwaltungsdigitalisierung

Die weitere Digitalisierung der Vermessungs- und Katasterverwaltung ist eine zentrale Voraussetzung für die Modernisierung staatlicher Strukturen und die Sicherstellung ihrer Leistungsfähigkeit in einer zunehmend vernetzten Welt. Cloud-Technologien stellen einen wichtigen Baustein zur Bewältigung der Herausforderungen des digitalen Wandels dar. Sie ermöglichen flexible, skalierbare und innovative Anwendungen, die Effizienzsteigerungen fördern sowie neue Formen der Zusammenarbeit und der Bereitstellung von Geobasisinformationen ermöglichen. Während hierbei Staaten wie Estland oder Finnland als digitale Vorreiter gelten, sieht sich Deutschland weiterhin mit strukturellen und bürokratischen Hürden konfrontiert, die eine umfassende Cloud-Transformation erschweren (EY 2025).

1.2 Nutzung von Cloud-Diensten in der öffentlichen Verwaltung

Der Einsatz von Cloud-Diensten ist auch in der Vermessungs- und Katasterverwaltung bereits etabliert. Laut der aktuellen Lünendonk-Studie (Lünendonk & Hossenfelder 2025) messen rund 80 % der öffentlichen Verwaltungen der Cloud-Transformation eine hohe Priorität bei. Jedoch setzen bislang lediglich 18 % Cloud-Services umfassend ein und verfügen über eine explizite Cloud-Strategie. Weitere

DOI 10.12902/zfv-0558-2026
© DVW e.V.

71 % nutzen bereits erste Cloud-Services und arbeiten an einer Cloud-Strategie, um deren Einsatz künftig systematisch auszubauen.

Um den Behörden die strukturierte und sichere Nutzung von Cloud-Technologie zu erleichtern, hat der IT-Planungsrat mit der Deutschen Verwaltungscloud (DVC) ein verbindliches Rahmenangebot geschaffen. Die DVC ist ein Angebot der Bundesregierung bzw. des IT-Planungsrates und bildet einen wichtigen Baustein in der Verwaltungsdigitalisierung. Sie verfolgt das Ziel, eine interoperable, modulare und föderale Cloud-Infrastruktur zu implementieren. Seit April 2025 ist die DVC produktiv und stellt Bund, Ländern und Kommunen einen einheitlichen Zugang zu zertifizierten Cloud-Diensten bereit (CIO Bund 2024).

Der Aufbau cloudbasierter fachlicher und technischer Strukturen der Vermessungs- und Katasterverwaltung folgt dem Leitbild der digitalen Souveränität. Digitale Souveränität bedeutet, technologische und wirtschaftliche Abhängigkeiten von einzelnen Anbietern gezielt zu reduzieren, die Kontrolle über kritische Daten und Infrastrukturen zu sichern und die eigene Handlungsfähigkeit dauerhaft sicherzustellen. Die Bundesregierung setzt dabei auf eine Multi-Cloud-Strategie mit offenen Schnittstellen sowie strikten Sicherheits- und Transparenzanforderungen (CIO Bund 2024). Eine Multi-Cloud-Strategie bedeutet, Cloud-Dienste verschiedener Anbieter parallel zu nutzen, um Abhängigkeiten zu vermeiden und flexibel die jeweils beste Lösung einzusetzen.

Die Beweggründe für die Nutzung von Cloud-Technologien sind vielfältig. Neben Effizienz- und Flexibilitätsgewinnen stehen insbesondere Aspekte der digitalen Souveränität sowie die Kontrolle über Daten und Prozesse im Vordergrund. Aktuell werden vor allem Private-Cloud- und Verwaltungscloud-Lösungen bevorzugt, während Public-Cloud-Angebote und souveräne Clouds eine geringere Nachfrage erfahren (BMDS 2024).

Private Clouds sind dedizierte IT-Umgebungen, die für eine einzelne Organisation betrieben werden, häufig im eigenen oder in einem behördlichen Rechenzentrum. Verwaltungscloud-Lösungen bezeichnen hingegen speziell für die öffentliche Verwaltung konzipierte Infrastrukturen, wie sie etwa im Kontext der Deutschen Verwaltungscloud entwickelt werden, und ermöglichen eine organisationsübergreifende, standardisierte Nutzung bei gleichzeitiger Einhaltung regulatorischer Anforderungen. Public Clouds sind gemeinsam genutzte Dienste großer Anbieter, die mandantenfähig betrieben werden. Souveräne Clouds stellen eine besondere Ausprägung dar, bei der Anforderungen an Datenhoheit, Compliance und staatliche Kontrolle im Vordergrund stehen.

1.3 Herausforderungen der Cloud-Transformation

Geobasisdaten sind unverzichtbar für zahlreiche Prozesse der Vermessungs- und Katasterverwaltung sowie für weiterführende Verwaltungs- und Wirtschaftsprozesse. Ein Ausfall dieser Prozesse, etwa durch die Nichtverfügbarkeit der Basisdaten, hätte gravierende Konsequenzen. Zu den wichtigsten Geobasisdaten zählen ALKIS-Liegenschaftsdaten und ATKIS-Topographiedaten sowie digitale Gelände- und Höhenmodelle. Sie dienen als Grundlage für Planungs-, Genehmigungs-, Bau-, Infrastruktur- und Katasterprozesse. Die komplexen Anforderungen sowohl an die Daten als auch an die Prozesse erfordern ein umfassendes Sicherheitskonzept, denn ohne Informationssicherheit kann die Aufgabenerfüllung der Vermessungs- und Katasterverwaltung als Bestandteil der öffentlichen Daseinsvorsorge nicht gewährleistet werden.

1.3.1 Sicherheit und Compliance

Mit der zunehmenden Nutzung von Cloud-Lösungen und dem wachsenden Risiko hybrider Bedrohungen steigen auch die Anforderungen an IT-Sicherheit und Compliance. Die EU-NIS-2-Richtlinie (EU-Richtlinie zur Netz- und Informationssicherheit) sowie das deutsche KRITIS-Dachgesetz (Gesetz zur Stärkung der Resilienz kritischer Infrastrukturen) definieren neue Standards für Cybersicherheit und die Resilienz kritischer Infrastrukturen (BSI 2025).

Ziel beider Regelwerke ist es, ein durchgehend hohes Sicherheitsniveau in Europa sicherzustellen und die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen. Die NIS-2-Richtlinie richtet sich nicht nur an Unternehmen, sondern auch an öffentliche Einrichtungen auf allen Verwaltungsebenen, einschließlich der Vermessungs- und Katasterverwaltung, sofern sie essenzielle oder wichtige Dienste bereitstellen (BSI 2025).

Zu den zentralen Pflichten zählen unter anderem:

- Einführung eines Risikomanagements für Netz- und Informationssysteme, das technische und organisatorische Maßnahmen umfasst (z. B. Zugriffskontrolle, Verschlüsselung, Notfallmanagement).
- Meldepflichten: Sicherheitsvorfälle müssen innerhalb von 24 Stunden an die zuständige Behörde gemeldet werden.
- Verantwortung der Behördenleitung: Die Leitung der Behörde ist verpflichtet, sich regelmäßig über Cybersicherheitsrisiken zu informieren und entsprechende Schulungen zu absolvieren.
- Sicherheitsstrategien und Nachweispflichten: Es müssen strukturierte Sicherheitskonzepte vorliegen und deren Umsetzung dokumentiert werden.

Das KRITIS-Dachgesetz setzt die EU-CER-Richtlinie (EU-Critical Entities Resilience Directive/EU-Richtlinie zur Resilienz Kritischer Einrichtungen) in nationales Recht um und erweitert den Schutz kritischer Infrastrukturen. Dabei werden neben klassischen Versorgungsunternehmen auch Software- und IT-Dienstleister einbezogen, sofern deren Leistungen von kritischer Bedeutung sind (BMI 2025).

 © DVW e.V.

Bei KRITIS-Relevanz gelten u. a.:

- Einführung und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) nach BSI-Grundschutz (BSI: Bundesamt für Sicherheit in der Informationstechnik).
- Nachweise zur IT-Sicherheit und regelmäßige Prüfungen durch unabhängige Stellen.
- Meldepflichten bei Sicherheitsvorfällen und Einrichtung einer 24/7-Kontaktstelle.
- Erstellung eines Resilienzplans mit Risikoanalyse, Bewertung und Umsetzung technischer und organisatorischer Maßnahmen, um im Störungsfall handlungsfähig zu bleiben.

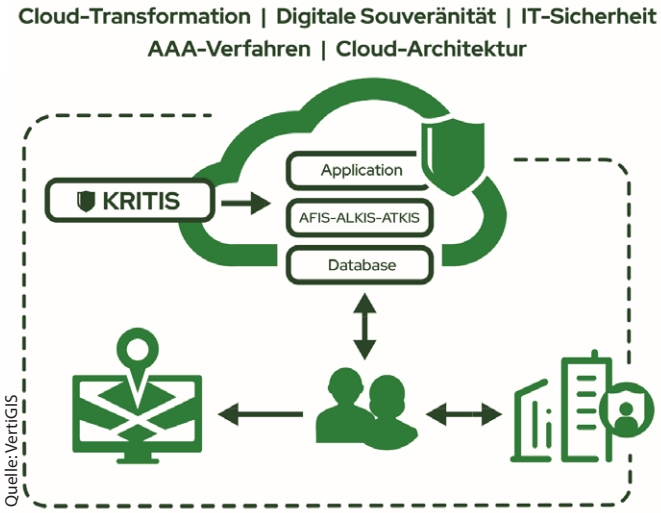


Abb. 1: KRITIS-orientierte Sicherheitsanforderungen und digitale Souveränität als Basis robuster Verwaltungs- und Geodateninfrastrukturen

In diesem Kontext rückt die digitale Transformation von Geobasisdaten in das Zentrum vieler staatlicher Aktivitäten und steigert damit nicht nur deren Relevanz, sondern auch die Anforderungen an Schutz, Verfügbarkeit und Resilienz. Geobasisdaten sind entscheidend für Planung, Genehmigung und operative Abläufe und nehmen, wie Abb. 1 anhand einer cloudbasierten AAA-Architektur mit KRITIS-Bezug verdeutlicht, eine zentrale Rolle innerhalb sicherheitskritischer Verwaltungsprozesse ein. Sie sind integraler Bestandteil digitaler Wertschöpfungsketten und damit unmittelbar mit Fragen der digitalen Souveränität, IT-Sicherheit und regulatorischen Compliance verknüpft. Der Schutz dieser Daten ist folglich nicht allein eine technische, sondern in hohem Maße auch eine organisatorische und strategische Aufgabe. Die Risiken reichen von Datenverlust und Manipulation über unautorisierte Zugriffe bis hin zu Ausfällen kritischer Infrastrukturen, die vollständige Verwaltungsprozesse beeinträchtigen können und damit sowohl Behörden als auch die Gesellschaft insgesamt betreffen (Heise Online 2025).

Um die Anforderungen von NIS-2 und KRITIS zu erfüllen, müssen staatliche Stellen und Betreiber kritischer Infrastrukturen ein ganzheitliches Sicherheitsmanagement etablieren. Die Verantwortung für die Cybersicherheit liegt dabei beim Führungspersonal: Management und Geschäftsleitung sind persönlich für die Einhaltung der Sicherheitsanforderungen und Meldepflichten verantwortlich. Zu den zentralen Aufgaben gehören die Auswahl und die laufende Kontrolle von Cloud-Anbietern. Dazu zählt auch die Prüfung relevanter Zertifizierungen, etwa BSI C5 (Cloud Computing Compliance Controls Catalogue des BSI) und ISO/IEC 27001 (internationaler Standard für Informationssicherheits-Managementsysteme). Ergänzend werden technische und organisatorische Maßnahmen umgesetzt sowie Resilienzpläne erstellt, um die Handlungsfähigkeit bei Störungen sicherzustellen (IHK Rhein-Neckar 2025).

1.3.2 Digitale Souveränität und Abhängigkeiten

Die Stärkung der digitalen Souveränität zählt zu den zentralen Zielen der deutschen Cloud-Strategie. Sie bezeichnet die Fähigkeit, IT-Infrastruktur, Daten und Prozesse unabhängig von externen Dienstleistern eigenständig sowie sicher zu steuern. Die Abhängigkeit von großen, überwiegend nichteuropäischen Cloud-Anbietern birgt Risiken für die Kontrolle sensibler Daten. Zudem kann die Einhaltung der DSGVO (Datenschutz-Grundverordnung der Europäischen Union zum Schutz personenbezogener Daten) erschwert werden (BMDS 2024, Security Insider 2025).

Aktuell bestehende gesetzliche Regelungen, wie etwa der CLOUD Act (Clarifying Lawful Overseas Use of Data Act), ermöglichen unter bestimmten Voraussetzungen den Zugriff staatlicher Stellen auf Daten von Anbietern, auch wenn diese außerhalb des eigenen Staatsgebiets gespeichert sind. Vor diesem Hintergrund wird dem Aufbau souveräner Cloud-Infrastrukturen in Europa eine besondere Bedeutung beigemessen. Bund und EU setzen dabei auf offene Standards, Verschlüsselung sowie geeignete Rahmenbedingungen, um Anforderungen an Datenschutz, Sicherheit und digitale Souveränität langfristig zu unterstützen (BMDS 2024, Security Insider 2025).

1.3.3 Organisatorische und personelle Herausforderungen

Zusätzlich zu den bereits genannten technischen und regulatorischen Anforderungen stellen der zunehmende Fachkräftemangel sowie die steigende Komplexität von Compliance-Vorgaben erhebliche Herausforderungen dar. Cloud-Strategien beschränken sich daher nicht allein auf Infrastruktur- oder Betriebsmodelle, sondern müssen auch die Art und Weise adressieren, wie cloudbasierte Fachverfahren entwickelt, betrieben und kontinuierlich weiterentwickelt werden.

Insbesondere bei der Nutzung von Cloud-Services verändern sich Entwicklungs- und Betriebsprozesse grundlegend: Software wird häufiger aktualisiert, stärker automatisiert bereitgestellt und enger mit dem laufenden Betrieb verzahnt. Vor diesem Hintergrund sind kontinuierliche Weiterbildungen, die Etablierung einer nachhaltigen Sicherheitskultur sowie die konsequente Integration von

© DVW e.V.

Sicherheitsaspekten in allen Phasen der Softwareentwicklung und des Betriebs unerlässlich.

Ein ganzheitlicher DevSecOps-Ansatz, der Entwicklung, Bereitstellung und Betrieb integriert betrachtet, ist daher ein zentrales Element moderner Cloud-Strategien. Er stellt sicher, dass Sicherheit nicht nachträglich ergänzt, sondern von Beginn an systematisch berücksichtigt wird. DevSecOps bedeutet, dass Sicherheitsmechanismen und -prüfungen nicht isoliert am Ende des Entwicklungsprozesses erfolgen, sondern als fester Bestandteil in jede Phase integriert werden – von der Planung über die Entwicklung bis hin zum Betrieb. Dies umfasst automatisierte Sicherheitstests, kontinuierliche Überwachung und die enge Zusammenarbeit von Entwicklung, Betrieb und Sicherheitsteams, um Schwachstellen frühzeitig zu erkennen und zu beheben (NCCoE 2026).

Sicherheitsrelevante Anforderungen werden so bereits während der Softwareentwicklung durch sicherheitsorientiertes Denken und unter Berücksichtigung der späteren Inbetriebnahme sowie der betrieblichen Prozessabläufe adressiert.

2 Technische Grundlagen und Architektur

2.1 Einsatz von Cloud-Anbietern und Vermeidung von Anbieterabhängigkeiten

Cloud-Anbieter aus den USA wie Amazon Web Services, Microsoft Azure und Google Cloud Platform sowie Anbieter mit Sitz in Europa wie T-Systems (T Cloud Public, ehemals Open Telekom Cloud), STACKIT oder IONOS Cloud bieten ein breites Spektrum an skalierbaren Diensten, die für den Betrieb von Verwaltungssoftware genutzt werden können. Ergänzend gewinnen regionale Rechenzentren und spezialisierte Cloud-Dienstleister an Bedeutung, insbesondere wenn spezifische Anforderungen an Datenschutz und Datenlokalität bestehen.

Zur Vermeidung eines Vendor Lock-in empfiehlt sich eine Multi-Cloud-Strategie. Unter einem Vendor Lock-in wird eine starke technische und organisatorische Abhängigkeit von einem einzelnen Cloud-Anbieter verstanden, die entsteht, wenn Anwendungen, Daten oder Betriebsprozesse auf anbieterspezifische Dienste und Schnittstellen zugeschnitten sind. Die parallele und – wo sinnvoll – integrierte Nutzung mehrerer Cloud-Anbieter ermöglicht es, spezifische Stärken zu kombinieren, Abhängigkeiten zu reduzieren und die langfristige Handlungs- und Entscheidungsfähigkeit zu sichern.

Solche Abhängigkeiten treten insbesondere dann auf, wenn proprietäre Lösungen eingesetzt werden, die von anderen Anbietern nicht oder nur eingeschränkt unterstützt werden. Dem kann durch eine konsequente Portabilität von Anwendungen und Daten begegnet werden. Diese wird durch den Einsatz offener Standards und klar definierter Schnittstellen erreicht. Ergänzend kommen Cloud-native Technologien zum Einsatz. Der Begriff »Cloud-nativ« bezeichnet dabei Architekturen und Anwendungen, die von Grund auf für den Betrieb in Cloud-Umgebungen konzipiert sind und Eigenschaften wie Skalierbarkeit, Automatisierung und lose Kopplung unterstützen. Ein zentrales Beispiel hierfür sind Container, bei denen Anwendungen gemeinsam mit ihrer Laufzeitumgebung standardisiert verpackt und unabhängig von der zugrunde liegenden Infrastruktur betrieben werden können. Werden diese Prinzipien bereits in der Architektur berücksichtigt, bleibt die Flexibilität erhalten, auf technologische Weiterentwicklungen sowie veränderte regulatorische Anforderungen angemessen zu reagieren.

2.2 Offene Schnittstellen und modulare Infrastruktur

Eine moderne Cloud-Architektur für die Vermessungs- und Katasterverwaltung basiert auf offenen Schnittstellen und einer modularen Infrastruktur. Offene Programmierschnittstellen, sogenannte Application Programming Interfaces (APIs), ermöglichen einen standardisierten und kontrollierten Austausch von Daten und Funktionen zwischen Systemen. In der Praxis kommen dabei häufig webbasierte Schnittstellen zum Einsatz, die auf etablierten Prinzipien wie Representational State Transfer (REST) oder auf abfrageorientierten Ansätzen wie Graph Query Language (GraphQL) beruhen. Die formale Beschreibung solcher Schnittstellen erfolgt üblicherweise über offen dokumentierte Schnittstellenbeschreibungen wie die OpenAPI-Spezifikation.

Ergänzt werden diese Schnittstellen durch standardisierte Protokolle und etablierte Datenformate, etwa die Standards des Open Geospatial Consortium (OGC) für den Austausch von Geodaten. Diese Kombination ist essenziell, um die Interoperabilität zwischen unterschiedlichen Fachverfahren, IT-Systemen und Cloud-Diensten sicherzustellen.

Die Modularisierung der Anwendungen erfolgt durch eine Architektur aus sogenannten Microservices, bei der eine Anwendung aus fachlich klar abgegrenzten, eigenständig betreibbaren Diensten besteht. Dadurch können einzelne Komponenten unabhängig voneinander entwickelt, skaliert und gewartet werden, ohne das Gesamtsystem zu beeinträchtigen.

Die Bereitstellung und der Betrieb komplexer Cloud-Umgebungen werden durch das Konzept der Infrastruktur als Code (IaC) unterstützt. IaC beschreibt den Ansatz, bei dem IT-Infrastruktur wie Server, Netzwerke oder Plattformdienste nicht manuell, sondern über maschinenlesbare Konfigurationsbeschreibungen definiert, versioniert und automatisiert bereitgestellt wird. Dadurch lassen sich Umgebungen reproduzierbar aufbauen, konsistent betreiben und nachvollziehbar ändern.

Ergänzend kommen Automatisierungslösungen zum Einsatz, deren Aufgabe es ist, wiederkehrende Betriebs- und Verwaltungsaufgaben zuverlässig und ohne manuelle

 © DVW e.V.

Eingriffe auszuführen. Dazu zählen insbesondere die automatische Bereitstellung von Ressourcen, die Konfiguration von Systemen, die Durchführung von Updates sowie die kontrollierte Skalierung von Anwendungen. Solche Automatisierungslösungen sorgen dafür, dass definierte Zustände dauerhaft eingehalten werden und reduzieren zugleich Fehlerquellen im Betrieb.

Für einen sicheren und regelkonformen Cloud-Betrieb ist zudem die Integration zentraler Sicherheits- und Betriebsfunktionen unerlässlich. Dazu gehört das Identitätsmanagement, das die eindeutige Zuordnung und Steuerung von Benutzer- und Systemzugriffen ermöglicht, sowie die Verschlüsselung zum Schutz sensibler Daten und das Monitoring zur kontinuierlichen Überwachung von Systemzuständen und Betriebskennzahlen. Diese technischen Maßnahmen müssen stets im Einklang mit geltenden Compliance-Anforderungen umgesetzt werden.

Die konsequente Nutzung offener Schnittstellen und modularer Architekturen trägt wesentlich zu einer nachhaltigen, wartbaren und flexibel anpassbaren IT-Infrastruktur bei.

2.3 Standardisierungsbedarf bei Fachverfahren und Prozessen

Trotz bundeseinheitlicher Standards wie dem AFIS-ALKIS-ATKIS-Modell (AAA-Modell) sowie dem normbasierten Austauschformat NAS bestehen weiterhin landesspezifische Ausprägungen in den fachlichen Geschäftsprozessen. Diese sind Ausdruck der föderalen Struktur sowie der historisch gewachsenen fachlichen und organisatorischen Rahmenbedingungen.

In der praktischen Umsetzung führt dies dazu, dass Fachverfahren vielfach in unterschiedlichen Ausprägungen betrieben werden. Die Potenziale cloudbasierter Architekturen, insbesondere im Hinblick auf gemeinsame Nutzung, Skalierbarkeit und einen einheitlichen Betrieb, können dadurch bislang nur eingeschränkt genutzt werden.

Mit der zunehmenden Etablierung cloudbasierter Infrastrukturen rückt die Ausgestaltung geeigneter Betriebsmodelle stärker in den Fokus. Perspektivisch erscheint ein plattformorientierter Ansatz sinnvoll, bei dem fachliche Verfahren auf einer gemeinsamen technischen Grundlage betrieben und weiterentwickelt werden, während spezifische Anforderungen in strukturierter Form berücksichtigt werden.

Voraussetzung hierfür ist eine weitergehende Annäherung der fachlichen Prozesse sowie eine klare Differenzierung zwischen standardisierbaren Plattformdiensten und fachlichen Ausprägungen. Ergänzend gewinnen übergreifende Anforderungen an Interoperabilität, Informationssicherheit und Governance an Bedeutung. Nationale und internationale Standards für den Datenaustausch sowie etablierte Sicherheitsanforderungen, etwa im Kontext der ISO 27001, bilden hierfür einen geeigneten Rahmen. Klare Zuständigkeiten, nachvollziehbare Entscheidungsstrukturen und eine konsistente Dokumentation sind wesentliche Voraussetzungen für einen nachhaltigen und sicheren Betrieb entsprechender Plattformlösungen.

3 Beispiel LM Cloud

VertiGIS verfolgt mit der LM Cloud einen strukturierten Modernisierungsansatz zur technischen Weiterentwicklung und Bereitstellung der AAA-Fachverfahren. Die in Kapitel 2 beschriebenen Anforderungen – insbesondere hinsichtlich Portabilität, Vermeidung von Anbieterabhängigkeiten, Sicherheit sowie digitaler Souveränität – werden dabei gezielt in der Architektur und im Betriebsmodell der LM Cloud umgesetzt. Wie in Abb. 2 dargestellt, werden bestehende Anwendungen schrittweise auf eine cloudfähige Zielarchitektur überführt, die auf Standardisierung, Modularität und automatisierten Betriebsprozessen basiert.

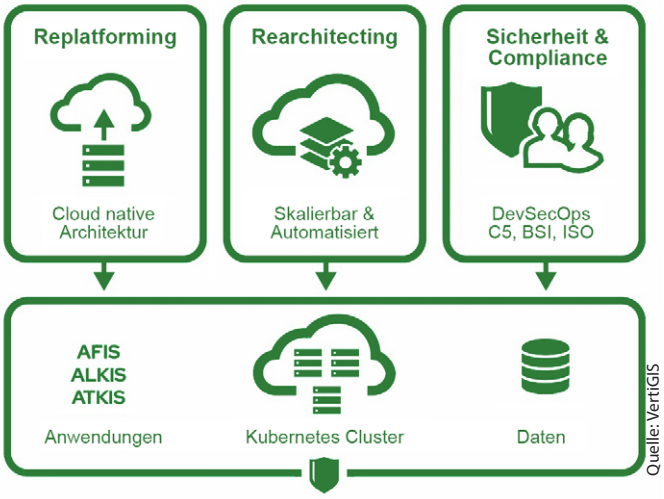


Abb. 2: Cloud-Modernisierung der AAA-Verfahren: Ein Zusammenspiel aus Replatforming, Rearchitecting sowie Compliance-Maßnahmen für eine skalierbare, souveräne Betriebsarchitektur

Im Zuge dieses sogenannten Replatformings werden bestehende Anwendungen auf standardisierte Plattformdienste umgestellt. Während in klassischen Architekturen Betriebssystem, Laufzeitumgebung und Anwendung eng miteinander verknüpft und überwiegend manuell betrieben werden, übernehmen Plattformdienste zentrale Aufgaben des technischen Betriebs automatisiert. Dazu zählen insbesondere die Bereitstellung einheitlicher Laufzeitumgebungen, die Überwachung des Systemzustands sowie die dynamische Anpassung von Ressourcen an die tatsächliche Auslastung. Dadurch werden Anwendungen portabler, stabiler und reproduzierbarer betreibbar als mit der bisherigen, überwiegend serverbasierten Technik.

Programme, die bislang ausschließlich auf voll ausgestatteten Windows-Server-Systemen installiert werden konnten, werden hierfür auf das Linux-Betriebssystem

© DVW e.V.

portiert und in leichtgewichtigere Container überführt. Leichtgewichtig bedeutet, dass der Container nur die für den Betrieb notwendigen Komponenten enthält. Dies reduziert den Ressourcenbedarf und unterstützt zugleich sicherheitsrelevante Anforderungen durch eine geringere Angriffsfläche.

Ergänzend dazu werden im Rahmen des Rearchitectings ausgewählte Komponenten gezielt neu entwickelt, um eine Cloud-native Architektur zu erreichen, die Skalierbarkeit und Flexibilität von Beginn an unterstützt. Ein Beispiel dafür ist die Integration eines zentralen Identitätsmanagements, das die verschiedenen, historisch gewachsenen Anmeldesysteme ablöst. Anwender müssen sich nur noch einmal authentifizieren und benötigen keine separaten Zugangsdaten für unterschiedliche Anwendungen. Insbesondere der Aufwand, der durch das Zurücksetzen und Verwalten von Zugangsdaten entsteht, wird dadurch reduziert.

Die technische Basis der LM Cloud bildet Kubernetes, eine Plattformarchitektur, die den Betrieb der containerisierten Anwendungen weitgehend automatisiert und damit die in Kapitel 2 beschriebenen Anforderungen an Standardisierung und Portabilität unterstützt. Das automatische Skalieren stellt sicher, dass Anwendungen auch bei Lastspitzen leistungsfähig bleiben. Durch den modularen Aufbau können einzelne Komponenten unabhängig angepasst oder weiterentwickelt werden, ohne den Betrieb des Gesamtsystems zu beeinträchtigen. Konzepte für Hochverfügbarkeit und Ausfallsicherheit sind dabei von Beginn an berücksichtigt und gewährleisten einen stabilen Betrieb mit minimalen Unterbrechungen.

Sicherheit und Compliance sind integraler Bestandteil der Architektur und adressieren die in Kapitel 2 dargestellten regulatorischen Anforderungen. Definierte Sicherheitsvorgaben werden bereits während der Bereitstellung und Aktualisierung der Anwendungen technisch überprüft und durchgesetzt. Ergänzt wird dies durch eine kontinuierliche Überwachung des Systembetriebs sowie durch regelmäßige Prüfungen, die die Einhaltung regulatorischer und datenschutzrechtlicher Anforderungen sicherstellen. Auf diese Weise entsteht eine nachhaltige, wartbare und zukunftsfähige Cloud-Plattform für den Betrieb von AAA-Fachverfahren.

4 Praxisbeispiele und Umsetzung

4.1 Cloud-Betrieb der AAA-Verfahren im Land Berlin

Ein Beispiel für die erfolgreiche Überführung geodätischer Fachverfahren in eine Cloud-Umgebung ist die AAA-Lösung der Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen in Berlin. Diese Verfahren wurden zunächst zentral im IT-Dienstleistungszentrum Berlin (ITDZ Berlin) betrieben. Im Jahr 2019 begann die schrittweise Verlagerung in eine Cloud-Infrastruktur der Open Telekom Cloud (heute: T Cloud Public). Ziel war es, Betrieb, Datenhaltung und fachliche Betreuung in einer einheitlichen und skalierbaren Umgebung zusammenzuführen und damit die Grundlage für einen sicheren und langfristig stabilen Betrieb zu schaffen.

Die Umsetzung erfolgte in drei Schritten: Zunächst wurde eine Testumgebung aufgebaut, um Sicherheits- und Leistungsanforderungen zu prüfen. Anschließend wurden vollständige Test- und Produktivsysteme eingerichtet, die Daten übernommen und das Datenbanksystem auf PostgreSQL umgestellt. Abschließend ging das System in den Regelbetrieb über, der durch klar definierte Servicevereinbarungen abgesichert ist. Grundlage hierfür waren umfassende Sicherheits- und Betriebskonzepte nach BSI-Grundschutz, ergänzt um Regelungen für Migration, Notfälle und fachliche Abläufe.

Seit 2021 wird das AAA-Verfahren vollständig in der Cloud betrieben. Die Architektur ist so aufgebaut, dass sensible Daten besonders geschützt sind, etwa durch getrennte Sicherheitsbereiche und unterschiedliche Datenbanken für operative Nutzung und Auskunft. Ergänzend kommen etablierte Sicherheits- und Zugriffsmechanismen zum Einsatz, beispielsweise Zertifikatslösungen zur Authentifizierung (PKI), gesicherte Datenaustauschplattformen sowie virtuelle Arbeitsumgebungen (VDI). Der Betrieb wird zentral gesteuert und überwacht, was die Stabilität und Effizienz deutlich erhöht.

Im Jahr 2025 wurde die Migration in die neue VertiGIS LM Cloud initiiert. Ziel ist sowohl die technische Überführung der bestehenden Cloud-Umgebung in ein konsolidiertes Zielbetriebsmodell als auch die Einführung der neuen Produktgeneration VertiGIS LM.

Die Umstellung auf die VertiGIS LM Cloud erfolgt parallel zum laufenden operativen Betrieb der bestehenden Lösung, der somit uneingeschränkt während der gesamten Übergangsphase gewährleistet bleibt. Die vollständige Migration soll bis 2027 abgeschlossen sein.

Für VertiGIS ist das Land Berlin in diesem Kontext ein qualifiziertes Referenzprojekt. Anhand dieses Anwendungsfalls wird deutlich, wie AAA-Verfahren strukturiert, revisionssicher und skalierbar in eine cloudbasierte Infrastruktur überführt werden können. Zentrale Erfolgsfaktoren sind:

- ein standardisiertes Migrationsvorgehen mit klar definierten Phasenmodellen,
- die konsequente Trennung von Datenmigration, Applikationsmodernisierung und Betriebsüberführung,
- ein definiertes Sicherheits- und Berechtigungskonzept im Einklang mit geltenden IT-Sicherheitsanforderungen (u. a. BSI-Grundschutz) sowie
- die Etablierung eines nachhaltigen Managed-Service-Betriebsmodells, bei dem Betrieb, Wartung, Monitoring und Weiterentwicklung der Fachverfahren auf einer zentralen Plattform gebündelt und durch den Betreiber in klar definierten Verantwortungs- und Service-Strukturen übernommen werden.

© DVW e.V.

Die Erfahrungen aus Berlin zeigen, dass die Migration von AAA-Fachverfahren in eine Cloud-Infrastruktur keine rein technische Aufgabe darstellt. Während sich die Migration im engeren Sinne auf die Überführung von Daten, Anwendungen und Infrastruktur bezieht, umfasst die Transformation das gesamte Vorhaben zur Neuausrichtung eines bestehenden Fachverfahrens in eine zukunftsfähige Gesamtarchitektur.

Aus Sicht der Vermessungs- und Katasterverwaltung betrifft dies nicht nur die technische Umsetzung, sondern insbesondere auch die Anpassung von Prozessen, Rollen und Verantwortlichkeiten sowie die Sicherstellung der fachlichen Kontinuität und Nachvollziehbarkeit. Die Überführung in eine Cloud-Umgebung ist damit als organisatorisches Transformationsvorhaben zu verstehen, bei dem Standardisierung, Governance und Sicherheit eine zentrale Rolle für Zuverlässigkeit und Langfriststabilität einnehmen.

4.2 Cloud-Betrieb der AAA-Verfahren in Bremen und Hamburg

Ein weiteres Praxisbeispiel für die Modernisierung geodätischer Fachverfahren durch Cloud-Technologien ist die länderübergreifende Zusammenarbeit zwischen der Freien und Hansestadt Hamburg und der Freien Hansestadt Bremen. Beide Länder sind für die Führung und Bereitstellung der amtlichen Geobasisdaten verantwortlich und betreiben hierfür das AFIS-ALKIS-ATKIS-Verfahren (AAA-Verfahren) mit den Komponenten Amtliches Festpunktinformationssystem (AFIS), Amtliches Liegenschaftskatasterinformationssystem (ALKIS) und Amtliches Topographisch-Kartographisches Informationssystem (ATKIS).

Steigende Anforderungen an Informationssicherheit und technische Weiterentwicklung sowie Fachkräftemangel machten eine grundlegende Neubewertung des bisherigen Betriebsmodells erforderlich. Spätestens mit der von der Arbeitsgemeinschaft der Vermessungsverwaltungen der Länder der Bundesrepublik Deutschland (AdV) beschlossenen Einführung der GeoInfoDok 7.1 bis Ende 2023 ergab sich zusätzlicher Handlungsbedarf zur technologischen Erneuerung der bestehenden Betriebsumgebung.

Vor diesem Hintergrund entschieden sich die Länder Bremen und Hamburg für eine gemeinsame Neuausrichtung des AAA-Betriebs und schrieben diesen länderübergreifend als cloudbasierten Betrieb auf Basis von Managed Cloud Services aus. Ziel war eine moderne, skalierbare und sichere Betriebsplattform, die zukünftige Digitalisierungsschritte unterstützt, personelle Engpässe kompensiert und zugleich wirtschaftliche Synergien durch eine gemeinsame Betriebsumgebung schafft.

Der Aufbau der Produktionsumgebung erfolgte in der ersten Hälfte des Jahres 2024. Der cloudbasierte Betrieb der AAA-Verfahren wurde im weiteren Verlauf des Jahres 2024 aufgenommen. Mit der neuen Betriebsform verbinden die beiden Länder insbesondere die Erwartung, den zuverlässigen Produktionsbetrieb langfristig sicherzustellen, ortsflexibles Arbeiten zu ermöglichen und Softwareaktualisierungen ohne Produktionsunterbrechungen durchzuführen. Gemeinsame Test- und Produktivumgebungen sowie der Abbau redundanter Infrastrukturen tragen darüber hinaus zu Effizienzgewinnen und einer nachhaltigen Nutzung vorhandener Ressourcen bei.

Die Kooperation der Länder Hamburg und Bremen ergänzt die Berliner Lösung um die Perspektive einer länderübergreifenden Cloud-Strategie. Damit wird deutlich, dass neben der rein technischen Modernisierung organisatorische Kooperationen für die zukunftsfähige, sichere und wirtschaftliche Weiterentwicklung von AAA-Fachverfahren an Bedeutung gewinnen.

5 Public-Private-Partnership und digitale Souveränität: Der VertiGIS LM Co-Innovation HUB

Eine nachhaltige Stärkung der digitalen Souveränität von Behörden kann unter anderem durch gezielte Public-Private-Partnerships (PPP) erreicht werden, wenn diese so ausgestaltet sind, dass die öffentliche Hand die Kontrolle über Daten, Architekturentscheidungen und Betriebsmodelle behält. Sie ermöglichen es, externes technologisches Know-how und Innovationspotenzial einzubinden, ohne die eigene Handlungsfähigkeit aufzugeben. Dies gelingt, indem offene Standards genutzt, eigene Kompetenzen aufgebaut und Abhängigkeiten von Anbietern reduziert werden.

Der VertiGIS LM Co-Innovation HUB bildet eine webbasierte Kooperationsplattform, in der Vermessungs- und Katasterverwaltungen gemeinsam mit VertiGIS und weiteren beteiligten Akteuren Anforderungen, Konzepte und prototypische Weiterentwicklungen für cloudbasierte AAA-Fachverfahren erarbeiten und bewerten. Die Teilnahme erfolgt in der Regel im Rahmen bestehender Projekt- oder Kundenbeziehungen; die inhaltliche Ausgestaltung wird dabei maßgeblich durch die beteiligten Verwaltungen geprägt.

Ausgangspunkt der Zusammenarbeit ist die Identifikation relevanter fachlicher und technischer Handlungsfelder durch die beteiligten Verwaltungen, beispielsweise im Kontext neuer gesetzlicher Anforderungen oder veränderter Prozessanforderungen. Darauf aufbauend werden in iterativen, eng abgestimmten Entwicklungszyklen prototypische Lösungen entwickelt, erprobt und hinsichtlich ihrer Praxistauglichkeit bewertet. Diese Vorgehensweise ermöglicht es, neue Funktionalitäten schrittweise zu entwickeln und frühzeitig unter realen Bedingungen zu validieren.

Synergien entstehen insbesondere dadurch, dass einmal entwickelte Lösungen oder konzeptionelle Ansätze auf andere Verwaltungen übertragbar sind und dort mit geringem Anpassungsaufwand genutzt werden können.

© DVW e.V.

Gleichzeitig fließen Erfahrungen aus unterschiedlichen organisatorischen und fachlichen Kontexten in die Weiterentwicklung ein, wodurch ein breiterer Anwendungsbezug sichergestellt wird.

Der VertiGIS LM Co-Innovation HUB adressiert zentrale technologische Handlungsfelder wie die Standardisierung von Schnittstellen, die Weiterentwicklung cloudbasierter Betriebsmodelle, die Integration von Sicherheitsanforderungen sowie die Unterstützung moderner Entwicklungs- und Betriebsprozesse. Innovation entsteht dabei nicht isoliert, sondern im Zusammenspiel fachlicher Anforderungen der Verwaltungen und der technischen Umsetzungskompetenz auf der gemeinsam genutzten Kollaborationsplattform.

Der Wissenstransfer erfolgt zwischen den beteiligten Vermessungs- und Katasterverwaltungen sowie dem Lösungsanbieter und trägt dazu bei, fachliche und technische Kompetenzen auf beiden Seiten weiterzuentwickeln. Auf diese Weise unterstützt der VertiGIS LM Co-Innovation HUB die strukturierte Weiterentwicklung von AAA-Fachverfahren und zeigt, wie sektorübergreifende Zusammenarbeit organisatorisch ausgestaltet werden kann, ohne die digitale Souveränität der öffentlichen Hand zu beeinträchtigen.

6 Zusammenfassung

Die Transformation hin zu cloudbasierten Lösungen in der Vermessungs- und Katasterverwaltung ist ein anspruchsvoller Prozess, um digitale Souveränität, IT-Sicherheit und Innovationsfähigkeit nachhaltig zu sichern. Die Deutsche Verwaltungscloud, die konsequente Umsetzung von Sicherheitsstandards sowie der gezielte Einsatz souveräner Cloud-Architekturen setzen dabei wesentliche Impulse für eine moderne und zukunftsfähige Verwaltung.

Ergänzend dazu leistet der VertiGIS LM Co-Innovation HUB als Public-Private-Partnership-Modell einen zusätzlichen Beitrag, indem er Innovation, Praxisnähe und Kompetenzaufbau strukturiert verbindet und damit die nachhaltige Weiterentwicklung cloudbasierter AAA-Fachverfahren unterstützt. Gemeinsam mit innovativen Technologien entsteht so eine Basis für einen sicheren, souveränen und zukunftsfähigen Verwaltungsbetrieb.

Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2025): NIS-2-Richtlinie. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/NIS-2-Richtlinie/nis-2-richtlinie_node.html, letzter Zugriff 04/2026.

Bundesministerium des Innern und für Heimat (BMI) (2025): Bundeskabinett beschließt Gesetzentwurf zum KRITIS-Dachgesetz. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2025/09/kritis-dg-kabinett.html, letzter Zugriff 04/2026.

Bundesministerium für Digitales und Staatsmodernisierung (BMDS) (2024): Digitale Souveränität in der öffentlichen Verwaltung. https://bmds.bund.de/themen/digitale-souveraenitaet/digitale-souveraenitaet-in-der-oeffentlichen-verwaltung, letzter Zugriff 04/2026.

CIO Bund (2024): Deutsche Verwaltungscloud-Strategie. https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html, letzter Zugriff 04/2026.

EY (2025): Der digitale Wandel in der öffentlichen Verwaltung. https://www.ey.com/de_de/insights/consulting/der-digitale-wandel-in-der-offentlichen-verwaltung, letzter Zugriff 04/2026.

Heise Online (2025): Kritische Infrastruktur: Bundestag verabschiedet NIS-2-Gesetz. https://www.heise.de/news/Kritische-Infrastruktur-Bundestag-verabschiedet-NIS2-Gesetz-11077959.html, letzter Zugriff 04/2026.

IHK Rhein-Neckar (2025): KRITIS & NIS2: Neue gesetzliche Anforderungen zur IT-Sicherheit. https://www.ihk.de/rhein-neckar/innovation/digitale-wirtschaft/netz-und-informationssicherheit/kritis-nis2-it-sicherheit-6234750, letzter Zugriff 04/2026.

Lünendonk & Hossenfelder (2025): Cloud-Transformation im öffentlichen Sektor. https://www.luenendonk.de/oeffentlicher-sektor-forciert-die-cloud-transformation-souveraenitaet-wird-zum-erfolgsfaktor, letzter Zugriff 04/2026.

National Cybersecurity Center of Excellence (NCCoE) (2026): Software Development, Security, and Operations (DevSecOps) Practices. https://pages.nist.gov/nccoe-devsecops, letzter Zugriff 03/2026.

Security Insider (2025): Europäischer Gipfel zur Digitalen Souveränität. https://www.security-insider.de/europaeischer-gipfel-digitale-souveraenitaet-unabhaengigkeit-us-cloud-a-dcbea8ba0041933a7b3706645038488e, letzter Zugriff 04/2026.

Kontakt

Elmar Happ
VertiGIS GmbH
Mallwitzstraße 1-3, 53177 Bonn
elmar.happ@vertigis.com

Sören Matthies
VertiGIS GmbH
Wendenstraße 8-12, 20097 Hamburg
soeren.matthies@vertigis.com

Michael Müller
VertiGIS GmbH
Carl-Wery-Straße 22, 81739 München
michael.mueller@vertigis.com

Markus Reuter
VertiGIS GmbH
Mallwitzstraße 1-3, 53177 Bonn
markus.reuter@vertigis.com

Dieser Beitrag ist auch digital verfügbar unter https://geodaesie.info.

 © DVW e.V.