MATERNA

Whitepaper

Wegweiser in die souveräne Cloud

Gekommen, um zu bleiben –
die souveräne Cloud in der öffentlichen Verwaltung

Zwischen Wolken und Wirklichkeit – die Verwaltung in der Multi-Cloud

Die öffentliche Verwaltung verfolgt zunehmend eine „Cloud-First"-Strategie und setzt auf Multi-Cloud-Modelle, um digitale Services effizient, flexibel und sicher bereitzustellen. Dabei müssen Chancen wie Skalierbarkeit und Modernisierung gegen Risiken wie Abhängigkeit und Herausforderungen beim Datenschutz sorgfältig abgewogen werden. Im Zentrum steht die digitale Souveränität – also die Kontrolle über Daten, Betrieb und Technologie in einer zunehmend vernetzten Cloud-Landschaft.

Inhaltsverzeichnis

„Cloud-First"-Strategie

Die Cloud ist in der öffentlichen Verwaltung angekommen. Der Einsatz von Cloud-Services ist etabliert. Häufig gibt es sogar eine „Cloud-First"-Strategie.

Beim Einsatz von Cloud-Services werden IT-Dienste, Speicherlösungen und Anwendungen nicht mehr ausschließlich auf eigenen Servern oder in lokalen Rechenzentren betrieben. Stattdessen erfolgt die Nutzung über die Infrastruktur externer Anbieter, die diese Dienste über das Internet bereitstellen. Diese Entscheidung ist häufig Ausdruck eines grundlegenden Strategiewechsels hin zu mehr Flexibilität, Skalierbarkeit und Effizienz in der IT.
In vielen Fällen existiert bereits eine sogenannte „Cloud-First"-Strategie. Das bedeutet, dass bei der Einführung neuer digitaler Lösungen oder bei der Modernisierung bestehender Systeme vorrangig geprüft wird, ob eine Umsetzung in der Cloud möglich und sinnvoll ist.

Bürgerinnen und Bürger erwarten heute schnelle, unkomplizierte und rund um die Uhr verfügbare Services – Anforderungen, die mit klassischen IT-Strukturen oft nur schwer oder sehr kostenintensiv zu erfüllen sind. Die Cloud bietet hier entscheidende Vorteile: Sie ermöglicht es, Anwendungen flexibel zu skalieren, also bei steigendem Bedarf schnell mehr Rechenleistung oder Speicher zur Verfügung zu stellen, ohne dafür neue Hardware anschaffen zu müssen. Zudem lassen sich über Cloud-Services neue digitale Angebote deutlich schneller umsetzen und aktualisieren, was der öffentlichen Verwaltung erlaubt, agiler auf gesellschaftliche und technologische Veränderungen zu reagieren.

Diese Strategie greift auch das neu geschaffene Bundesministerium für Digitales und Staatsmodernisierung auf. Zentrales Element der neuen Digitalstrategie soll künftig der sogenannte Deutschland-Stack werden, eine einheitliche digitale Infrastruktur mit Basiskomponenten wie Cloud- und IT-Diensten für die Verwaltung. Der Deutschland-Stack ist ein Konzept, das eine Reihe von digitalen Technologien und Plattformen umfasst, die als Grundlage für die digitale Transformation dienen sollen. Er soll eine Grundlage für verschiedene digitale Anwendungen und Dienste schaffen und die Zusammenarbeit zwischen verschiedenen Akteuren erleichtern.

Deutschland muss sich souverän aufstellen

Digitale Souveränität spielt in der Entscheidung der Verwaltung für eine Cloud-First-Strategie eine zentrale Rolle. Digitale Souveränität bedeutet, dass der Staat die Kontrolle über seine Daten, IT-Systeme und digitalen Infrastrukturen behält – selbst dann, wenn er Dienste externer Anbieter nutzt. Gerade dort, wo mit besonders schützenswerten Daten gearbeitet wird, ist das Vertrauen in die Integrität und Sicherheit der IT-Infrastruktur von entscheidender Bedeutung.

Bei der Umsetzung von Cloud-Strategien steht daher insbesondere die Frage im Raum, wie der technologische Fortschritt souverän gestaltet werden kann. Souveräne Cloud-Lösungen setzen die Anforderungen an Datenschutz, Datenspeicherung und Zugriffskontrolle um. Hierbei werden Daten ausschließlich in Deutschland oder zumindest innerhalb der EU gespeichert und ausländische Anbieter erhalten keinen Zugriff auf sensible Informationen.

In der Praxis bedeutet das, dass die öffentliche Verwaltung sehr genau prüft, mit welchen Cloud-Anbietern sie zusammenarbeitet, welche vertraglichen Regelungen getroffen werden und wie gewährleistet werden kann, dass die Datenverarbeitung im Einklang mit europäischen Datenschutzstandards erfolgt. Oft wird auch auf hybride oder Multi-Cloud-Modelle gesetzt, bei denen besonders sensible Daten weiterhin in staatlich kontrollierten Rechenzentren verbleiben, während weniger kritische Anwendungen in die Cloud ausgelagert werden.

Ein wichtiger Aspekt der Souveränität ist die Förderung der heimischen Cloud-Anbieter (siehe S. 10). Gleichzeitig muss die Architektur auch den Einsatz von US-amerikanischen Hyperscalern ermöglichen. Daher ist es wichtig, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits an einer Weiterentwicklung des C5-Standards arbeitet. Der Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue) spezifiziert Mindestanforderungen an sicheres Cloud Computing. Künftig wird der C5-Standard auch eine Post-Quantum-Verschlüsselung beinhalten – also Verschlüsselungsverfahren, die selbst gegenüber Angriffen mit Quantencomputern resistent sind und damit langfristig ein höheres Maß an Datensicherheit gewährleisten.

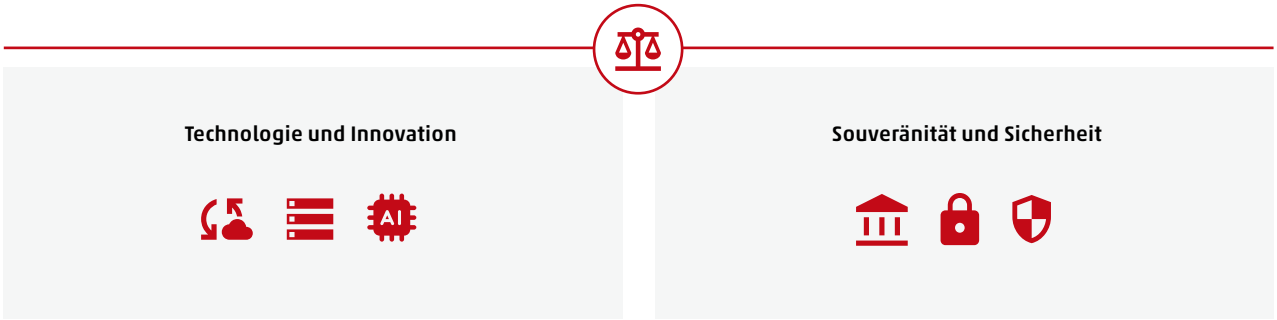

Abbildung 1: Mit den Bestrebungen zur souveränen Cloud schafft die Verwaltung eine Balance, die Innovation und Sicherheit gleichermaßen berücksichtigt.

Multi-Cloud-Lösungen in der Verwaltung

Der Trend zu Multi-Cloud-Lösungen in der Verwaltung wird getrieben durch das Bedürfnis nach Flexibilität, Unabhängigkeit und strategischer Kontrolle. Statt sich auf einen einzigen Cloud-Anbieter zu verlassen, nutzen Behörden bewusst mehrere Cloud-Plattformen parallel – etwa, um spezifische Dienste verschiedener Anbieter optimal zu kombinieren, Risiken zu streuen oder regulatorischen Anforderungen besser gerecht zu werden. Die nachfolgenden Beispiele veranschaulichen die aktuellen Entwicklungen zur Multi-Cloud.

1. Multi-Cloud-Broker über föderale Ebenen hinweg

Im Auftrag der govDigital eG entsteht ein sogenannter Multi-Cloud-Broker. Dieses technische Konzept soll es Behörden auf verschiedenen föderalen Ebenen ermöglichen, flexibel und souverän auf verschiedene Cloud-Dienste zuzugreifen – je nach Bedarf, Sicherheitsanforderung und Anwendungsszenario. Der Multi-Cloud-Broker übernimmt eine vermittelnde Rolle: Er fungiert als einheitliche Schnittstelle und Steuerungsinstrument, über das unterschiedliche Cloud-Anbieter angebunden und verwaltet werden können. Behörden können sowohl auf internationale Hyperscaler wie Amazon Web Services (AWS), Microsoft Azure und Google Cloud zugreifen als auch auf souveräne europäische Cloud-Plattformen wie IONOS und STACKIT. govDigital verfolgt einen bewusst hybriden Ansatz: Einerseits wird der Zugang zu leistungsstarken, etablierten Cloud-Diensten sichergestellt, andererseits wird die digitale Souveränität durch die gezielte Einbindung europäischer Alternativen gestärkt.

Diese Kombination erlaubt es der öffentlichen Hand, ihre IT-Strategien bedarfsorientiert umzusetzen, ohne sich auf einen einzelnen Anbieter festlegen zu müssen. Gleichzeitig können sensible Daten und kritische Anwendungen gezielt bei Anbietern betrieben werden, die höchste Anforderungen an Datenschutz, Rechtssicherheit und Datenlokalität erfüllen. Der Multi-Cloud-Broker von govDigital unterstützt darüber hinaus zentrale Verwaltungsfunktionen wie Identitätsmanagement, Abrechnungsmodelle, Monitoring und Sicherheitsrichtlinien – und ermöglicht so eine koordinierte, transparente und standardisierte Cloud-Nutzung innerhalb der öffentlichen Verwaltung.

2. Multi-Cloud-Broker für deutsche Sozialversicherungsträger

Die Bundesagentur für Arbeit, die Deutsche Rentenversicherung Bund und die Deutsche Gesetzliche Unfallversicherung – die drei größten deutschen Sozialversicherungsträger – haben sich zusammengeschlossen, um gemeinsam eine zentrale Ausschreibung für einen Multi-Cloud-Broker durchzuführen. Ziel dieses Projekts ist es, eine zukunftsfähige und zugleich souveräne IT-Infrastruktur zu schaffen, die den spezifischen Anforderungen der Sozialversicherung gerecht wird.

Der daraus hervorgegangene Rahmenvertrag ermöglicht es den beteiligten Institutionen, flexibel und bedarfsgerecht auf eine breite Palette von Cloud-Diensten zuzugreifen. Dabei stehen ihnen sowohl die leistungsstarken Angebote der führenden amerikanischen Hyperscaler zur Verfügung als auch die Dienste von vier europäischen Cloud-Anbietern: IONOS, STACKIT, OVHcloud und CloudFerro. Diese Auswahl gewährleistet einerseits den Zugang zu modernsten Technologien und globaler Skalierbarkeit und trägt andererseits dem Bedürfnis nach Datenschutz, Datenlokalität und digitaler Souveränität Rechnung. Durch den gemeinsamen Multi-Cloud-Rahmen schaffen die Träger eine Grundlage, um Digitalisierungsvorhaben effizienter, koordinierter und sicher umzusetzen – stets im Einklang mit den hohen regulatorischen und datenschutzrechtlichen Anforderungen des Sozialversicherungswesens.

3. Aufbau einer privaten Enterprise Cloud für das ITZBund

Das ITZBund, der zentrale IT-Dienstleister der Bundesverwaltung, hat den Cloud-Anbieter IONOS mit dem Aufbau einer privaten Enterprise Cloud beauftragt. Diese Cloud wird ausschließlich in den Rechenzentren des ITZBund betrieben – unter vollständiger staatlicher Kontrolle ohne Nutzung externer Infrastrukturen. Die technische Basis bildet die Public Cloud-Plattform von IONOS. Dadurch profitiert das ITZBund von laufenden Innovationen und Weiterentwicklungen, die ursprünglich für den breiten Markt entwickelt wurden. Mit diesem Projekt verfolgt der Bund das Ziel, eine leistungsfähige, skalierbare und gleichzeitig souveräne Cloud-Infrastruktur bereitzustellen, die höchsten Anforderungen an Datenschutz, Betriebssicherheit und Compliance entspricht. Die Lösung kombiniert damit die technologischen Vorteile moderner Cloud-Architekturen mit der Souveränität und Kontrolle eines staatlich betriebenen Systems. Materna steht in diesem Projekt als Cloud-Beratungspartner zur Seite, berät bei Applikationsskalierung und -betrieb sowie bei Migrations- und Integrationsfragen in die vorhandene Infrastruktur. Auch bei der Implementierung neuer Cloud-Services in die Fachlichkeit wird Materna beratend tätig.

Containern gehört die Zukunft

Moderne Cloud-Anwendungen werden heute so entwickelt, dass sie nicht mehr an eine bestimmte Cloud-Plattform oder einen bestimmten Anbieter gebunden sind. Die sogenannte Wechselfähigkeit („Portabilität") ist ein zentrales Element. Durch den konsequenten Einsatz von Containern – also abgeschlossenen, portablen Software-Einheiten, die alle nötigen Komponenten einer Anwendung enthalten – können Anwendungen unabhängig von der zugrunde liegenden Infrastruktur betrieben werden. Kubernetes, ein Open-Source-System zur Verwaltung und Orchestrierung dieser Container, sorgt dafür, dass sie automatisiert verteilt, skaliert und überwacht werden können. In Kombination ermöglichen diese Technologien, Anwendungen leichter zwischen verschiedenen Cloud-Umgebungen zu verschieben, ohne sie neu schreiben oder aufwendig anpassen zu müssen. So wird die „Portabilität" der Cloud-Plattformen und Cloud-Anwendungen realisiert – ein entscheidender Faktor für digitale Souveränität und Flexibilität in der öffentlichen IT.

Materna verfügt über umfassende Expertise im Bereich Containerisierung und Kubernetes und hat diese Technologien erfolgreich in zahlreichen Projekten implementiert. Materna unterstützt Behörden bei der Entwicklung, Einführung und dem Betrieb von containerbasierten Anwendungen. Mit dieser Kombination aus technologischem Know-how und praktischer Erfahrung positioniert sich Materna als kompetenter Partner für die Umsetzung moderner, skalierbarer und souveräner IT-Lösungen im öffentlichen Sektor.

Wege mit Materna durch den Multi-Cloud-Dschungel

Mit den Multi-Cloud-Projekten der Verwaltung entstehen vielfältige Bezugsmöglichkeit für die Cloud. Dennoch fehlt zumeist die Orientierung. Welche Anwendungsfälle bestehen in Ihrer Verwaltung? Welche sind für welchen Cloud-Anbieter geeignet? Hierfür hat Materna ein **Starter Kit Cloud** entwickelt. Darin sortieren wir für Sie die Landschaft der Anbieter. Wir zeigen die Unterschiede der Leistungsportfolios auf, ermitteln anhand Ihrer Bedürfnisse die beste Cloud und skizzieren bereits eine Architektur Ihrer Cloud-Landing-Zone – also einer vorkonfigurierten, sicheren und regelkonformen Ausgangsbasis für den Aufbau Ihrer Cloud-Umgebung. Eine Cloud-Landing Zone enthält alle notwendigen Sicherheits-, Netzwerk- und Governance-Einstellungen, um Cloud-Dienste sicher, regelkonform und effizient nutzen zu können. Als Organisation erhalten Sie damit einen strukturierten Einstieg in die Cloud für Ihre Verwaltung.

- **Klarheit:** Wir vermitteln ein eindeutiges Verständnis über die Unterschiede der Cloud-Anbieter.
- **Einfachheit:** Sie erfahren die Unterschiede des Leistungsportfolios der Anbieter anhand ausgewählter Anwendungsbeispiele aus dem Behördenalltag.
- **Flexibilität:** Sie lernen kennen, auf was Sie achten müssen, um flexibel auf zukünftige Anforderungen reagieren zu können.
- **Maßgeschneidert:** Wir erarbeiten gemeinsam die Auswahl des speziell für Ihre Behörde geeigneten Cloud-Anbieters.
- **Sicherheit:** Sie erfahren, welche Datenschutzfragen und rechtlichen Aspekte Sie beachten müssen.

Ergänzend stellen wir Ihnen gerne das **Materna Sovereign Cloud Framework** vor. Wir zeigen auf, wie Ihre Anforderungen in diesem Framework umgesetzt werden. Dabei sprechen wir über die Netzwerk-Anbindung Ihrer on-Premises Infrastruktur, die Sicherheit, Identitäts- und Zugriffsverwaltung sowie das Management und die Überwachung als zentrale Komponenten der Cloud Journey.

Materna hat langjährige Erfahrung in der Anwendungsentwicklung für die öffentliche Verwaltung und kennt die Anforderungen im Behördenalltag. Wir begleiten Sie dabei, Ihre Fachverfahren systematisch in die Cloud zu überführen: Workload-Analyse, Migration und Modernisierung (Lift-and-Shift- oder Refactoring-Migrationen), Datenmigration sowie Test und Validierung. Neben der technologischen Expertise bietet Materna auch Beratung zur Organisationsanpassung und unterstützt Sie beim Change-Management. Dies sind wichtige Grundlagen für eine gelungene Reise in die Cloud.

Als unabhängiger IT-Dienstleister sind wir Partner von zahlreichen Cloud-Anbietern und helfen Ihnen, die jeweils passende souveräne Cloud für Sie zu finden. Materna pflegt strategische Partnerschaften mit den führenden Cloud-Anbietern, darunter die internationalen Hyperscaler AWS, Microsoft Azure und Google Cloud sowie die deutschen Plattformen IONOS, STACKIT und Delos Cloud. Diese Partnerschaften ermöglichen es Materna, ein breites Spektrum an Cloud-Technologien und -Services bereitzustellen – von Public über Private bis hin zu souveränen Cloud-Lösungen. Durch die enge Zusammenarbeit mit diesen Anbietern verfügt Materna über zertifiziertes Know-how und direkten Zugang zu technischen Ressourcen, Support-Strukturen und innovativen Entwicklungen. So kann Materna maßgeschneiderte Cloud-Architekturen entwerfen, Migrationsprojekte begleiten und auch komplexe Multi-Cloud-Szenarien für öffentliche Auftraggeber sicher und effizient umsetzen.

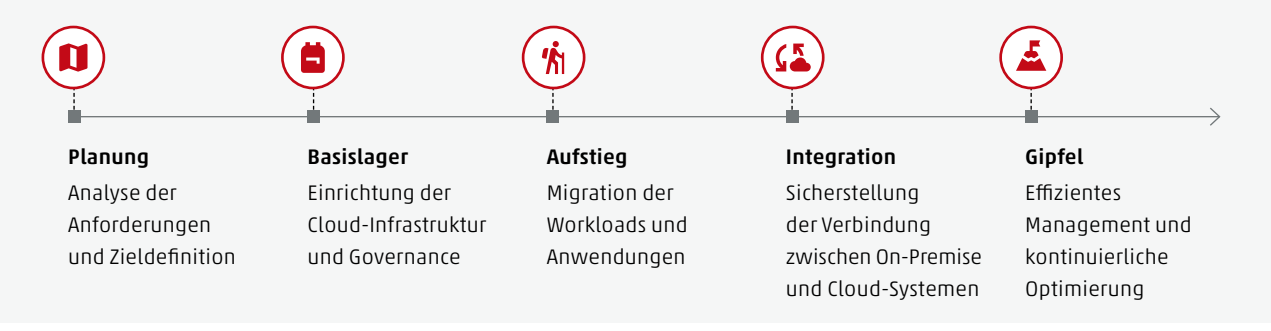

Abbildung 2: Stationen der Cloud-Reise

Wichtige deutsche und europäische Cloud-Anbieter

In Deutschland und generell im deutschsprachigen Raum gibt es eine Reihe von Cloud-Anbietern, die sich explizit auf die Bedürfnisse der öffentlichen Verwaltung und anderer sicherheitskritischer Bereiche spezialisiert haben – mit besonderem Fokus auf Datenschutz, Datensouveränität und die Einhaltung europäischer bzw. deutscher Rechtsvorgaben (z. B. DSGVO, IT-Sicherheitsgesetz, BSI-Vorgaben wie C5). Dies sind einige der wichtigsten heimischen bzw. europäischen Anbieter:

- **STACKIT (Schwarz Gruppe)**
  Ein Anbieter, unter dem Dach der Schwarz Gruppe (u. a. Lidl und Kaufland), der mit STACKIT eine eigene Cloud-Infrastruktur anbietet – vollständig betrieben in deutschen Rechenzentren. Die Plattform soll als souveräne Cloud-Alternative vor allem für öffentliche Auftraggeber und Unternehmen dienen.

- **IONOS (IONOS Cloud)**
  IONOS ist einer der größten europäischen Cloud-Anbieter mit Sitz in Deutschland. Das Unternehmen bietet eine vollwertige Public-Cloud-Plattform und positioniert sich gezielt als datensouveräne Alternative zu US-Anbietern. Die Rechenzentren befinden sich in Deutschland und IONOS betont seine DSGVO-Konformität und Unabhängigkeit von US-Recht.

- **Delos Cloud GmbH (Delos)**
  Die Delos Cloud GmbH, ein Unternehmen der SAP, wird ab Anfang 2026 eine souveräne Cloud-Infrastruktur für die öffentliche Verwaltung bereitstellen, die auf Microsoft Azure basiert. Diese Plattform ermöglicht den DSGVO-konformen Einsatz von Microsoft 365 sowie eine breite Palette von Cloud-Services innerhalb der Azure-Umgebung. Es wird hiermit eine Daten- sowie operative Souveränität erreicht.

- **Deutsche Telekom (T-Systems / Open Telekom Cloud)**
  Die Telekom bietet mit der Open Telekom Cloud (OTC) eine Public-Cloud-Plattform, die speziell auf die Anforderungen von Behörden und Unternehmen in regulierten Branchen zugeschnitten ist. Die Infrastruktur steht in Deutschland und das Unternehmen arbeitet aktiv daran, Lösungen für digitale Souveränität zu entwickeln, auch in Zusammenarbeit mit europäischen Initiativen wie Gaia-X.

- **plusserver (pluscloud)**
  Plusserver ist ein mittelständischer Anbieter aus Köln, der unter dem Label pluscloud souveräne Cloud-Dienste anbietet – zertifiziert nach ISO/IEC 27001 und konform mit dem deutschen Datenschutzrecht.
  Das Unternehmen ist besonders im Mittelstand und im öffentlichen Sektor aktiv.

- **noris network**
  noris network ist ein Anbieter aus Nürnberg, der hochsichere Rechenzentrums- und Cloud-Lösungen bereitstellt. Das Unternehmen ist besonders bekannt für individuelle, sicherheitskritische IT-Infrastrukturen und wird häufig von Banken, Versicherungen und Behörden genutzt.

- **OVHcloud (Frankreich)**
  Ein europäischer Cloud-Anbieter mit Hauptsitz in Frankreich, der auf eine eigene, weltweit betriebene Rechenzentrumsinfrastruktur zurückgreift. OVHcloud bietet skalierbare Public- und Private-Cloud-Lösungen und positioniert sich als datenschutzkonforme Alternative zu US-Hyperscalern – mit Fokus auf europäische Werte, offene Standards und digitale Souveränität.

- **CloudFerro (Polen)**
  Ein spezialisierter europäischer Cloud-Dienstleister mit Sitz in Polen, der insbesondere auf große Datenmengen und wissenschaftliche Anwendungen im Bereich Erdbeobachtung und Raumfahrt ausgerichtet ist. CloudFerro betreibt Rechenzentren in der EU und legt Wert auf offene Technologien, Transparenz und die Einhaltung europäischer Datenschutzanforderungen.

MATERNA

Digitale Souveränität als Grundlage moderner Verwaltungs-IT: Daten, Betrieb und Technologie in staatlicher Hand

Souveränität wird aus verschiedenen Blickwinkeln betrachtet. Datensouveränität, operative Souveränität und technologische Souveränität stehen für unterschiedliche, aber eng miteinander verknüpfte Aspekte der digitalen Selbstbestimmung des Staates. Jede dieser Souveränitäts-formen spielt eine entscheidende Rolle, wenn es darum geht, Cloud-Dienste oder andere digitale Infrastrukturen verantwortungsvoll und rechtssicher zu nutzen.

Datensouveränität

... bedeutet, dass der Staat jederzeit volle Kontrolle über Standort, Zugriff und Nutzung seiner Daten behält.

Operative Souveränität

... beschreibt die Fähigkeit, IT-Systeme eigenständig zu betreiben, zu steuern und bei Bedarf zu wechseln.

Technologische Souveränität

... steht für die Unabhängigkeit bei der Auswahl, Entwicklung und Nutzung digitaler Schlüsseltechnologien.

Abbildung 3: Drei Säulen der digitalen Souveränität

Hier eine Beschreibung der drei Konzepte, jeweils im Verwaltungskontext:

Datensouveränität

Datensouveränität bedeutet, dass die öffentliche Verwaltung jederzeit die Kontrolle über ihre Daten behält – darüber, wo diese gespeichert sind, wer darauf zugreifen darf und zu welchen Zwecken sie verarbeitet werden. Gerade im staatlichen Kontext, wo täglich mit personenbezogenen, sicherheitsrelevanten und vertraulichen Informationen gearbeitet wird, ist diese Form der Souveränität essenziell. Die Verwaltung muss sicherstellen können, dass ihre Daten nicht durch ausländische Gesetze oder Unternehmen kompromittiert werden und dass keine unautorisierten Zugriffe – etwa durch Drittstaaten – möglich sind. Um dies zu gewährleisten, achtet sie darauf, Cloud-Anbieter zu wählen, die ihre Dienste in europäischen Rechtsräumen betreiben, die Datenverarbeitung transparent gestalten und technologische Maßnahmen wie Verschlüsselung bieten, bei denen der Staat selbst die Schlüsselhoheit behält. Datensouveränität ist damit ein Fundament für Vertrauen in staatliches Handeln in der digitalen Welt.

Operative Souveränität

Operative Souveränität beschreibt die Fähigkeit der öffentlichen Verwaltung, ihre digitalen Infrastrukturen selbstständig zu betreiben, zu überwachen und bei Bedarf unabhängig zu steuern – auch wenn bestimmte technische Dienstleistungen ausgelagert wurden.
Es geht darum, den Überblick über sämtliche Betriebsprozesse zu behalten und jederzeit in der Lage zu sein, eigene Systeme zu warten, zu aktualisieren oder im Notfall auf einen anderen Anbieter zu migrieren, ohne in eine technologische Abhängigkeit zu geraten. Diese Unabhängigkeit setzt voraus, dass Verwaltungseinrichtungen über das notwendige Fachwissen verfügen oder dieses durch gezielten Kompetenzaufbau entwickeln. Ebenso wichtig ist eine Vertragsgestaltung, die klare Regelungen zur Datenportabilität, zu Schnittstellenstandards und zu Reaktionsmöglichkeiten in Krisensituationen beinhaltet.
Operative Souveränität ist damit ein Ausdruck digitaler Resilienz und Grundlage dafür, dass staatliche Aufgaben verlässlich erfüllt werden können – auch in einer zunehmend komplexen und vernetzten digitalen Umgebung.

Technologische Souveränität

Technologische Souveränität zielt auf die strategische Fähigkeit der öffentlichen Verwaltung, bei der Auswahl und Gestaltung ihrer technologischen Grundlagen nicht vollständig von außereuropäischen Anbietern oder proprietären Systemen abhängig zu sein. Es geht darum, den Zugang zu Schlüsseltechnologien zu sichern, Alternativen bewerten und langfristig tragfähige Entscheidungen treffen zu können – etwa bei Cloud-Infrastrukturen, Softwarelösungen oder Standards für den Datenaustausch.
In diesem Zusammenhang spielt auch die Förderung von Open-Source-Technologien eine zentrale Rolle, da diese Transparenz, Anpassungsfähigkeit und Unabhängigkeit bieten. Darüber hinaus beteiligt sich die Verwaltung an europäischen Projekten wie Gaia-X, die das Ziel verfolgen, ein digitales Ökosystem zu schaffen, das auf europäischen Werten wie Datenschutz, Sicherheit und Interoperabilität basiert. Technologische Souveränität bedeutet also, dass die öffentliche Hand aktiv an der Gestaltung ihrer digitalen Zukunft mitwirkt, statt sich ausschließlich auf den globalen Technologiemarkt verlassen zu müssen.

Alle drei Souveränitätsformen haben dasselbe Ziel:
Die öffentliche Verwaltung soll in der Lage sein, moderne digitale Technologien zu nutzen, ohne dabei ihre demokratische, rechtliche und technologische Selbstbestimmung aufzugeben. Sie will sich die Vorteile der Cloud zunutze machen – aber zu Bedingungen, die dem Gemeinwohl, dem Datenschutz und dem Rechtsstaat entsprechen.

Ihr Impulsgeber für die digitale Transformation der öffentlichen Verwaltung

Digitale Technologien sind der entscheidende Motor für eine moderne Verwaltung. Materna positioniert sich an der Schnittstelle zwischen Mensch und Technologie und begleitet Behörden bei der strategischen und IT-technischen Umsetzung staatlicher Aufgaben auf dem Weg zur digitalen Verwaltung.
Wir betreuen Sie in allen Phasen der Wertschöpfungskette: von der Beratung bis zum Betrieb mithilfe standardisierter und skalierbarer Lösungen.

Ihr Kontakt im Team Materna

Robert Knapp
robert.knapp@materna.group
Vice President Public Sector
Solutioning Journey2Cloud

Timon Schmotz
timon.schmotz@materna.group
Business Development Manager

So erreichen Sie uns:

Materna Information & Communications SE
Robert-Schuman-Straße 20, 44263 Dortmund
Tel.: +49 231 - 5599 - 00
E-Mail: sales@materna.group
www.materna.de