Digitale Souveränität: Vom Schlagwort zum strategischen Imperativ für den deutschen Mittelstand

Ein praxisorientierter Leitfaden für resiliente IT-Strukturen

Vorgelegt durch den Kompetenzkreis VBKI DIGITAL

Inhalt

1. Executive Summary

Die digitale Souveränität ist für den deutschen Mittelstand (KMU) von einer strategischen Option zu einer existenziellen Notwendigkeit avanciert. Angesichts zunehmender geopolitischer Unsicherheiten, eines sich verschärfenden regulatorischen Umfelds (DSGVO, Schrems II, NIS2, DORA, EU Data Act) und einer aktuell bestehenden starken Marktabhängigkeit von außereuropäischen Hyperscalern müssen KMU ihre digitale Handlungsfähigkeit proaktiv sichern. Dieses Positionspapier analysiert die Herausforderungen und skizziert einen praxisorientierten Weg zur Stärkung der IT-/Cloud-Souveränität.

Die Analyse zeigt eine deutliche Diskrepanz zwischen dem Wunsch vieler KMU nach mehr Kontrolle und Unabhängigkeit und der tatsächlichen Umsetzung. Hemmnisse wie Vendor Lock-in, fehlende Interoperabilität, Fachkräftemangel, Ressourcenknappheit und die Komplexität der Regulatorik verhindern oft den Wandel. Digitale Souveränität bedeutet dabei nicht Autarkie, sondern die Fähigkeit zur Selbstbestimmung – die Kontrolle über Daten, operative Flexibilität und technologische Wahlfreiheit zu wahren.

Als Lösungsansätze werden hybride und Multi-Cloud-Architekturen favorisiert, die auf offenen Standards, Interoperabilität und Portabilität basieren. Der strategische Einsatz von Open-Source-Software (OSS) und die Nutzung vertrauenswürdiger europäischer Cloud-Anbieter sind zentrale Bausteine. Diese Architekturen ermöglichen es, unterschiedlich sensible Daten und Anwendungen bedarfsgerecht zu platzieren – sei es in souveränen Umgebungen oder in leistungsfähigen Public-Cloud-Diensten. Souveränität dort, wo sie notwendig ist – Usability und Skalierbarkeit dort, wo sie sinnvoll ist. Entscheidend ist dabei eine selbstbewusste, kontextbezogene Entscheidungskultur, die nicht von Technologie-„Dogmen“, sondern von den tatsächlichen Bedürfnissen der Nutzer getragen wird. Eine detaillierte Roadmap für KMU umfasst fünf Phasen: Assessment und Planung, Kompetenzaufbau und Kulturwandel, Technologie- und Partnerauswahl, schrittweise Implementierung und Migration sowie kontinuierliche Optimierung und Anpassung unter Einbeziehung eines konsequenten Change Managements.

Der Business Case für digitale Souveränität geht über reine Kostenbetrachtungen hinaus. Er umfasst nicht nur die Vermeidung hoher Compliance-Strafen und Kosten für Datenpannen, sondern auch die Minderung von Lock-in-Risiken, die Steigerung der Resilienz und die Sicherung langfristiger Innovationsfähigkeit und Wettbewerbsvorteile. Eine risikoadjustierte Lebenszyklus-Gesamtkostenbetrachtung (TCO) zeigt, dass Investitionen in Souveränität strategisch sinnvoll sind.

Die Politik ist gefordert, die Rahmenbedingungen zu verbessern: durch gezielte KMU-Förderung, die Stärkung europäischer Anbieter und offener Ökosysteme, die Förderung und

Mandatierung offener Standards, eine Reform des Vergaberechts zugunsten souveräner Lösungen und massive Investitionen in digitale Bildung und Fachkräfteentwicklung. Nur durch ein konzertiertes Vorgehen von Unternehmen, Technologiepartnern und Politik kann die digitale Zukunft des deutschen Mittelstands souverän gestaltet werden.

2. Die Notwendigkeit Digitaler Souveränität für den deutschen Mittelstand

Die Informationstechnologie (IT) bildet das Rückgrat moderner Wertschöpfungsprozesse. Für den deutschen Mittelstand, das Herz der deutschen Wirtschaft, ist die Fähigkeit, die eigene digitale Infrastruktur und Daten selbstbestimmt zu gestalten und zu kontrollieren, zu einer entscheidenden Zukunftsfrage geworden. Der Begriff „Digitale Souveränität" hat sich dabei von einem Schlagwort zu einem strategischen Imperativ entwickelt.

2.1. Begriffsbestimmung von Souveränität im digitalen Zeitalter: Mehr als nur Schlagworte

Eine tiefere Definition ist jedoch notwendig, um Missverständnisse zu vermeiden und eine klare strategische Ausrichtung zu ermöglichen. Digitale Souveränität bezeichnet die Fähigkeit von Individuen, Organisationen wie KMU und Staaten, selbstbestimmte Entscheidungen hinsichtlich ihrer digitalen Infrastrukturen, Daten und Prozesse zu treffen.[1] Souveränität (auch im digitalen Sinn) bedeutet folglich frei darüber entscheiden zu können, ob und wie und auf welche Weise digitalisiert wird, um den größtmöglichen Mehrwert zu erreichen. Souveränität ist eine wesentliche Voraussetzung für gesellschaftliche Teilhabe und Wettbewerbsfähigkeit.[2] Diese Fähigkeit umfasst mehrere Dimensionen:

1. **Datensouveränität:** Dies ist die umfassende Kontrolle und Nachvollziehbarkeit etwaiger Zugriffe über den gesamten Lebenszyklus von Daten – von der Erzeugung über Speicherung und Verarbeitung bis hin zu Zugriff und Löschung. Sie beinhaltet die Einhaltung relevanter Datenschutzbestimmungen und Sicherheitsstandards.[5] Für 95% der befragten öffentlichen Einrichtungen ist Datenhoheit ein Schlüsselmerkmal digitaler Souveränität [8], eine Einschätzung, die von sicherheitsbewussten KMU geteilt wird, für die Datenhoheit ebenfalls einen sehr hohen Stellenwert hat (79 %).[7]
2. **Betriebliche (Operative) Souveränität:** Dies beschreibt die Fähigkeit, IT-Systeme und Geschäftsprozesse flexibel zu steuern und zu betreiben, ohne in unüberwindbare Abhängigkeiten von einzelnen Anbietern zu geraten (Vendor Lock-in).[6] Hierzu gehört explizit die praktische Möglichkeit, Technologien und Anbieter wechseln zu können.[9] 76% der öffentlichen Verwaltungen sehen diese Wechselmöglichkeit als wichtig für ihre Souveränität an.[8]
3. **Technologische Souveränität:** Dies umfasst das Verständnis, die Fähigkeit zur (Mit-)Gestaltung und Anwendung sowie potenziell die eigene Herstellung von Schlüsseltechnologien.[1] Es geht darum, einseitige und irreversible Abhängigkeiten von ausländischem Know-how oder kritischen Technologieimporten zu vermeiden [11] und die *Gestaltungsfreiheit* (Wahlfreiheit) bei der Technologieentscheidung zu besitzen.[12]

Es ist entscheidend zu verstehen, dass digitale Souveränität nicht Autarkie oder Isolation bedeutet.[1] In einer global vernetzten Welt ist vollständige Unabhängigkeit unrealistisch und

oft auch nicht wünschenswert. Vielmehr geht es darum, strategische Handlungsoptionen und Kontrolle zu bewahren.[1] Ein digital souveränes Unternehmen kennt seine Abhängigkeiten und ist in der Lage, diese bewusst zu steuern, Risiken abzuwägen und bei Bedarf Alternativen zu wählen oder zu entwickeln.[6] Für KMU, die ohnehin oft keine vollständige Autarkie anstreben können, bedeutet dies, strategische Kontrolle durch informierte Entscheidungen, Diversifizierung und die Nutzung offener Technologien zu erlangen.

Für den Mittelstand übersetzt sich digitale Souveränität direkt in geschäftliche Vorteile: erhöhte Resilienz gegenüber Ausfällen und Krisen, Sicherstellung der Compliance mit europäischen und nationalen Vorschriften, Schutz sensibler Unternehmensdaten (Kundeninformationen, geistiges Eigentum), auch als Instrument der Wettbewerbsdifferenzierung und die Fähigkeit, Innovationen unabhängig von den Roadmaps großer Plattformanbieter voranzutreiben.

2.2. Warum jetzt? Die Konvergenz von geopolitischen Risiken, regulatorischem Druck und Marktabhängigkeiten

Die Dringlichkeit ergibt sich jedoch aus dem Zusammentreffen mehrerer Faktoren, die eine proaktive Auseinandersetzung mit digitaler Souveränität unumgänglich machen:

1. **Geopolitische Verschiebungen:** Zunehmende globale Spannungen, Handelskonflikte und die sich wandelnden transatlantischen Beziehungen stellen die Verlässlichkeit außereuropäischer Partner und Lieferketten in Frage, insbesondere im Hinblick auf die Dominanz US-amerikanischer Hyperscaler (AWS, Azure, Google Cloud).[11] Europäische Unternehmen müssen die Zuverlässigkeit und Preisstabilität ihrer Partner neu bewerten.[16]
2. **Regulatorische Landschaft:** Eine Welle neuer EU-Regulierungen verschärft die Anforderungen an Datensicherheit, Datenschutz und operative Resilienz erheblich:
    - **DSGVO und Schrems II:** Die Datenschutz-Grundverordnung (DSGVO) und die Urteile des Europäischen Gerichtshofs (EuGH) in den Schrems-Fällen schaffen anhaltende Rechtsunsicherheit bezüglich des Datentransfers in die USA und der Nutzung von US-Cloud-Diensten, da der Zugriff durch US-Behörden (z.B. via Cloud Act oder FISA) nicht ausgeschlossen werden kann.[5]
    - **NIS2-Richtlinie:** Die überarbeitete Richtlinie zur Netz- und Informationssicherheit (NIS2) erweitert den Anwendungsbereich auf deutlich mehr Sektoren und Unternehmen, darunter viele KMU (typischerweise ab 50 Mitarbeitern oder 10 Mio. Euro Umsatz).[19] Sie fordert verbindliche Mindeststandards für das Risikomanagement (inkl. Lieferketten-Sicherheit), strengere Sicherheitsvorkehrungen (z.B. Multi-Faktor-Authentifizierung, Verschlüsselung) und deutlich verkürzte Meldefristen für Sicherheitsvorfälle (Erstmeldung innerhalb von 24 Stunden).[19] Bei Verstößen drohen empfindliche Bußgelder (bis zu 2 % des weltweiten Jahresumsatzes) und persönliche Haftung der Geschäftsleitung.[19]

- **DORA (Digital Operational Resilience Act):** Diese Verordnung legt spezifische Anforderungen an die digitale operationale Resilienz für den Finanzsektor fest, die auch für kritische IKT-Drittanbieter, darunter potenziell KMU, gelten.[20] DORA hat Vorrang vor NIS2 für Finanzunternehmen [22] und tritt bereits im Januar 2025 vollständig in Kraft.[20]
- **EU Data Act:** Dieses Gesetz stärkt die Rechte von Nutzern (Unternehmen und Privatpersonen) auf Zugang zu Daten, die durch vernetzte Produkte und Dienste generiert werden. Es verpflichtet Anbieter zur Datenweitergabe unter fairen, angemessenen und nicht-diskriminierenden Bedingungen (FRAND), verbietet unfaire Vertragsklauseln, erleichtert den Wechsel zwischen Cloud-Anbietern (ab September 2025) und fördert die Interoperabilität durch essentielle Anforderungen.[24] Ziel ist eine fairere Verteilung des Werts von Daten.[24]

3. **Marktkonzentration und Abhängigkeiten:** Die starke Konzentration des Cloud-Marktes, insbesondere im IaaS- und PaaS-Bereich, auf wenige außereuropäische Anbieter (Hyperscaler) schafft systemische Herausforderungen, und fördert Abhängigkeiten, welche schnell zu starken Kostenrisiken werden können.[16]

Diese Entwicklungen führen dazu, dass digitale Souveränität von einem strategischen "Nice-to-have" zu einem operativen und rechtlichen "Must-have" wird. Die neuen Regulierungen wie NIS2, DORA und der Data Act fungieren als implizites Mandat für mehr digitale Souveränität. Die Erfüllung der dort festgelegten Anforderungen – etwa an nachweisbares Risikomanagement, Sicherheit der Lieferkette, spezifische technische Maßnahmen wie MFA und Verschlüsselung [19] oder die Gewährleistung von Datenzugang und Portabilität [24] – erfordert zwangsläufig eine größere Kontrolle über die eigene IT-Infrastruktur und die Datenflüsse, als dies bei der Nutzung intransparenter "Black-Box"-Dienste möglich ist.[17] Die Nichteinhaltung dieser Vorschriften birgt erhebliche finanzielle Risiken.[19] Somit treiben Compliance-Bemühungen direkt Maßnahmen voran, die die digitale Souveränität stärken, wie z.B. das Verständnis von Datenflüssen, die Bewertung der Sicherheit von Anbietern und die Sicherstellung von Interoperabilität.

3. Status Quo 2025: Marktdynamik und Realitäten im Mittelstand

Die aktuelle Situation im deutschen Mittelstand ist geprägt von einer hohen Cloud-Nutzung bei gleichzeitiger Abhängigkeit von wenigen globalen Anbietern, wachsender regulatorischer Komplexität und signifikanten Hürden bei der Umsetzung von Souveränitätsstrategien.

3.1. Das Dilemma der Cloud-Abhängigkeit

Die Cloud-Nutzung ist in der deutschen Wirtschaft etabliert: 81 % der Unternehmen nutzen Cloud Computing, weitere 14 % planen oder diskutieren den Einsatz.[30] Der Anteil der IT-Anwendungen, die aus der Cloud betrieben werden, soll in den nächsten fünf Jahren von derzeit 38 % auf 54 % steigen.[29] Insbesondere das Software-as-a-Service (SaaS)-Modell ist bei KMU beliebt, da es einen einfachen Einstieg ermöglicht, aber potenziell höhere Lock-in-Effekte birgt.[31] Die Märkte für Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS) werden von wenigen US-Hyperscalern dominiert.[18] Obwohl deutsche KMU nachweislich den Wunsch nach mehr Souveränität hegen [7], weisen über 50 % starke Abhängigkeiten von Nicht-EU-Anbietern in allen Cloud-Segmenten (IaaS, PaaS, SaaS) sowie bei KI-Anwendungen auf.[7] Selbst wenn europäische Alternativen verfügbar sind, werden oft US-Anbieter genutzt.[31] Google-Dienste beispielsweise werden von 90 % der deutschen Unternehmen eingesetzt.[34]

3.2. Navigation durch regulatorische Komplexität

KMU haben oft Schwierigkeiten, die komplexe Regulierungslandschaft zu überblicken und umzusetzen.[35]

- **DSGVO/Schrems II:** Schaffen anhaltende Rechtsunsicherheit bei der Nutzung von US-Clouds aufgrund potenzieller (ggf. unbemerkter) Datenzugriffe durch US-Behörden.[15]
- **NIS2:** Zwingt viele KMU zu erheblichen Investitionen in Cybersicherheitsmaßnahmen (Risikoanalyse, Vorfallmanagement, Lieferkettensicherheit, technische Maßnahmen wie Verschlüsselung und MFA) [21] und zur Etablierung schneller Meldeprozesse (24h) [19], was den operativen Aufwand erhöht und die Haftung der Geschäftsführung verschärft.[20]
- **DORA:** Stellt ähnliche, strenge Anforderungen an Unternehmen im Finanzsektor und deren kritische IKT-Dienstleister.[22]
- **Data Act:** Verpflichtet KMU, die vernetzte Produkte oder Dienste anbieten, dazu, Datenzugang und -portabilität "by Design" zu ermöglichen.[24] Dies kann erhebliche technische Anpassungen erfordern. Gleichzeitig erleichtert das Gesetz den Wechsel *weg* von Cloud-Anbietern.[24]

3.3. Identifizierung kritischer Hürden

Vendor-Lock-ins, proprietäre Plattformen und Fachkräftemangel sind zentrale Hürden. Aktuelle Studien erweitern das Bild um strukturelle Faktoren: fehlende Datenklassifizierung

und Portabilität, unzureichende Exit-Klauseln (Egress-Kosten), komplexe Compliance- und Audit-anforderungen, Legacy-Verflechtungen/Technische Schuld, mangelnde Interoperabilität (offene Standards) sowie fehlende FinOps-Transparenz. Auch Change-Trägheit und lückenhafte Grundlagen in IAM/PAM/MFA bremsen die Umsetzung:

- **Vendor Lock-in:** Entsteht durch proprietäre Technologien, hohe Daten-Austrittskosten, gebündelte Dienste und komplexe Migrationsprozesse.[9] Dies ist eine Hauptbarriere für Anbieterwechsel.[9]
- **Fehlende Interoperabilität und Standards:** Erschwert die flexible Kombination von Diensten und den Wechsel zwischen Anbietern.[7]
- **Fachkräftemangel:** Es fehlt an internem Know-how für Cloud-Management, Sicherheit (Cybersecurity), Kostenoptimierung (FinOps), Container-Technologien, Serverless Computing und Migration.[7] 59% der Unternehmen fehlt das Know-how für KI-Cloud-Dienste.[30] Ein Drittel der Unternehmen leidet unter Personalengpässen in der IT. [7] In Deutschland fehlen zudem IT-Fachkräfte. Bis 2040 könnten laut Prognosen etwa 660.000 IT-Fachkräfte fehlen. [144]
- **Ressourcenknappheit:** KMU verfügen oft nicht über ausreichende finanzielle Mittel und Zeit für komplexe Migrations- oder Modernisierungsprojekte und das laufende Management.[43] Kosten und Zeitmangel sind die größten Hürden.[44]
- **Fehlende IT-Kapazität / RZ-Kapazitäten:** Rund 82 % der Netzanschlusskapazitäten in deutschen Rechenzentren sind bereits ausgelastet. Dadurch entsteht ein erheblicher Wachstumsengpass durch eine strukturelle Schwäche bei Investitionen in Rechenleistung und Speicherkapazitäten.[145]
- **Komplexität:** Das Management von Hybrid- und Multi-Cloud-Umgebungen ist anspruchsvoll.[40] Das Verstehen und Umsetzen der regulatorischen Anforderungen stellt eine Herausforderung dar.[35]
- **Sicherheitsbedenken:** Trotz der Vorteile der Cloud bleibt die Sicherheit ein zentrales Anliegen (23 % äußern Bedenken [35]). Die Gewährleistung der Sicherheit über verschiedene Umgebungen hinweg ist schwierig.[7] 36% sehen sich durch zunehmende Cyberangriffe herausgefordert.[7]

3.4. Aspiration versus Aktion

Studien von Bitkom & EY, zeigen eine Diskrepanz zwischen dem Wunsch nach Souveränität und der tatsächlichen Umsetzung auf. Dies wird durch weitere Untersuchungen bestätigt.[7] Die Kontrolle über die eigenen Daten (Datenhoheit) wird sehr hoch bewertet (79 % laut IONOS-Studie [7]; 95 % im öffentlichen Sektor [8]). Ebenso wichtig ist die Vermeidung strategischer Abhängigkeiten (73 % [7]). Der Standort der Anbieter in Deutschland oder der EU spielt für viele eine Rolle (68 % [7]; öffentlicher Sektor [8]). Die tatsächliche Implementierung souveräner Strategien bleibt jedoch aufgrund der genannten Hürden oft aus. Obwohl 81% der

Unternehmen Cloud nutzen [30], widerspricht die Wahl des Cloud-Modells (oft SaaS) und des Anbieters (oft US-Hyperscaler) häufig den Souveränitätszielen.[7] Im öffentlichen Sektor haben nur 25 % eine Cloud-Strategie tatsächlich umgesetzt.[8]

3.5. Vergleichende Sichtweise: Herausforderungen aus Sicht der Stakeholder

Die Wahrnehmung der Herausforderungen und die vorgeschlagenen Lösungsansätze variieren zwischen den relevanten Akteuren:

- **Bitkom:** Betont den Fachkräftemangel und fordert weniger Regulierung sowie mehr Investitionsanreize.[46] Erkennt den Wunsch nach Souveränität an, verweist aber gleichzeitig auf die starke Nutzung von Hyperscalern.[7] Bemängelt Deutschlands nachlassende digitale Wettbewerbsfähigkeit.[47]
- **BITMi (Bundesverband IT-Mittelstand):** Fokussiert auf die Stärkung des IT-Mittelstands. Fordert eine digital getriebene Wirtschaftspolitik, gezielte Förderung des IT-Mittelstands und weniger innovationshemmende Regulierung unter dem Motto "Innovation und digitale Souveränität – made in Germany".[48]
- **BDI (Bundesverband der Deutschen Industrie):** Hebt die Notwendigkeit des Kompetenzaufbaus (digitale Fähigkeiten) und der Entwicklung eigener Schlüsseltechnologien (KI, Plattformen, Halbleiter) hervor. Warnt vor Protektionismus und plädiert für eine ganzheitliche europäische Strategie.[14]
- **ZenDiS (Zentrum Digitale Souveränität):** Definiert Souveränität durch Wahlmöglichkeit, Gestaltungsfähigkeit und Einflussnahme.[9] Sieht Open-Source-Software (OSS) und eine Reform des Vergaberechts als zentrale Hebel, insbesondere für den öffentlichen Sektor, was aber auch Auswirkungen auf die Interaktion mit KMU hat.[9]
- **PwC:** Unterstreicht die geopolitischen Risiken und die Notwendigkeit, die Verlässlichkeit außereuropäischer Anbieter kritisch zu hinterfragen.[16]
- **Fraunhofer:** Engagiert sich in der Forschung zu Schlüsseltechnologien (KI, Edge, Datenökonomie) und unterstützt KMU bei der Digitalisierung und Vernetzung (z.B. Mittelstand-Digital Zentrum Wertnetzwerke).[43]

Obwohl ein Konsens über das *Ziel* der digitalen Souveränität besteht, offenbart sich eine deutliche Spannung zwischen der Förderung heimischer bzw. europäischer Lösungen (wie von BITMi und ZenDiS favorisiert) und dem Anspruch, globale Wettbewerbsfähigkeit zu erhalten und Protektionismus zu vermeiden (wie von BDI und Bitkom betont). KMU befinden sich in diesem Spannungsfeld: Sie benötigen einerseits sichere, kontrollierbare und konforme Lösungen, andererseits aber auch Zugang zu kosteneffizienten, innovativen Technologien, die oft von globalen Marktführern angeboten werden.[7] Es entsteht ein strategisches Dilemma: Sollen KMU primär auf den schnellen Zugang zu globaler Innovation setzen (und so potenziell Abhängigkeiten vertiefen) oder mehr Aufwand und Kosten in möglicherweise weniger ausgereifte, aber souveränere europäische oder Open-Source-Alternativen investieren?

4. Vision: Architektur für souveräne und resiliente IT im Mittelstand

Eine zukunftsfähige IT-Infrastruktur für den Mittelstand muss auf Prinzipien basieren, die digitale Souveränität gewährleisten und gleichzeitig Flexibilität und Resilienz bieten. Dies erfordert durchdachte Architekturentscheidungen, die Nutzung offener Technologien und eine bewusste Auswahl von Partnern und Plattformen.

4.1. Grundlegende Prinzipien

Datenhoheit, Verschlüsselung, offene Standards, Modularität, Multi-Cloud und internes Know-how. Diese Prinzipien müssen weiter konkretisiert werden:

- **Datenkontrolle & Sicherheit:** Umfassende Kontrolle über den gesamten Datenlebenszyklus (Erzeugung, Speicherung, Verarbeitung, Zugriff, Löschung). Einsatz starker Verschlüsselung (Daten in Übertragung, im Ruhezustand und potenziell in Nutzung durch Confidential Computing [52]). Implementierung robuster Zugriffskontrollen (Identity & Access Management - IAM, Multi-Faktor-Authentifizierung - MFA [21]). Sicherstellung der Compliance "by Design" (DSGVO, NIS2). Der Standort der Datenverarbeitung und -speicherung in Deutschland oder der EU ist ein zentrales Kriterium für viele Unternehmen und den öffentlichen Sektor.[7]
- **Betriebliche Resilienz:** Gewährleistung hoher Verfügbarkeit, effektiver Notfallwiederherstellung (Disaster Recovery) und Geschäftskontinuität (Business Continuity Planning). Die Fähigkeit, Störungen durch technische Fehler, Cyberangriffe oder Anbieterprobleme zu widerstehen und schnell zu beheben.[6]
- **Flexibilität & Agilität:** Die Fähigkeit, sich schnell an veränderte Geschäftsanforderungen anzupassen, Ressourcen effizient zu skalieren und neue Technologien nahtlos zu integrieren.[5][6]
- **Offenheit & Interoperabilität:** Konsequente Nutzung offener Standards und offener Programmierschnittstellen (APIs). Aufbau modularer Architekturen, um Vendor Lock-in zu vermeiden und eine nahtlose Integration sowie den Wechsel von Komponenten oder Anbietern zu ermöglichen.[3]
- **Transparenz:** Klares Verständnis der Funktionsweise von Systemen, des Speicherorts von Daten und der bestehenden technologischen und organisatorischen Abhängigkeiten.[3]

4.2. Tragfähige Architekturentwürfe

- **Hybrid Cloud:** Kombination aus privater Infrastruktur (On-Premises oder Hosted Private Cloud) für kritische Daten und Kernanwendungen mit Public-Cloud-Diensten für weniger sensible Aufgaben, zur Skalierung oder für spezielle Funktionalitäten (z.B. KI-Dienste).[29] Dieser Ansatz erfordert eine sorgfältige Integration, einheitliches Management und klare

Sicherheitsrichtlinien über beide Umgebungen hinweg.

- **Multi-Cloud:** Nutzung von Diensten mehrerer Public-Cloud-Anbieter, um jeweils die besten Lösungen für spezifische Anforderungen auszuwählen ("Best-of-Breed"), Kosten zu optimieren, die Ausfallsicherheit zu erhöhen und die Abhängigkeit von einem einzelnen Anbieter zu reduzieren.[7] Drei Viertel der Unternehmen sehen Multi-Cloud als wichtige Maßnahme zur Stärkung der Souveränität.[7] Dies erfordert jedoch eine starke Governance, übergreifende Orchestrierung und Kompetenzen im Management verschiedener Plattformen.
- **Souveräne Cloud-Plattformen:** Einsatz dedizierter Plattformen, die speziell auf digitale Souveränität ausgelegt sind. Dazu gehören Lösungen, die auf den Prinzipien von Gaia-X oder dem Sovereign Cloud Stack (SCS) basieren, sowie spezifische Angebote europäischer Anbieter (z.B. T-Systems Open Sovereign Cloud [52], plusserver pluscloud open [69], OVHcloud Trusted Zone [71], IONOS Cloud [51]). Diese Plattformen setzen oft stark auf Open-Source-Technologien [69] und garantieren Datenresidenz und Kontrolle innerhalb der EU.[52] Jüngst entstehen auch Joint Venture Projekte zwischen SAP, Schwarz Digits u. a. mit US-Hyperscalern im EU-Betrieb. Es gelten entsprechende BSI-Cloud-Standards für den Einsatz in der Verwaltung mit dem Ziel, eine sichere, datensouveräne Cloud mit einer Kombination aus Leistungsfähigkeit und Kontrolle zu schaffen, wie z. B. die DELOS-Cloud. Dazu gehören Lösungen mit einem Technologie-Stack basierend auf Google, AWS, Microsoft Azure und getrennten Infrastrukturen durch deutsche Betreiberkonstrukte. Diese sind jedoch mit Vorsicht zu betrachten, da hier ggf. durch den Cloud Act entsprechende Zugriffsrechte für US-Behörden bestehen können.

Ein Hybrid-Architektur-Ansatz kombiniert souveräne Cloud-Infrastrukturen mit etablierten internationalen Lösungen und ermöglicht so eine flexible Multi-Cloud-Strategie. Dies erlaubt KMU, sensible Daten unter voller Kontrolle in souveränen Umgebungen zu halten, während sie gleichzeitig von der Innovationskraft und Usability globaler Dienste profitieren. Die Architektur unterstützt eine bedarfsgerechte Auslagerung und fördert zugleich Resilienz, Anpassungsfähigkeit und Skalierbarkeit.

Die Entscheidung für eine Hybrid-Architektur trägt der Ambivalenz zwischen digitaler Souveränität und Nutzerfreundlichkeit bewusst Rechnung. Im Vordergrund steht eine selbstbewusste, verantwortungsvolle Auswahl von Technologien, die sich an den konkreten Bedürfnissen der Anwender orientiert – nicht an ideologischen Extremen. So entsteht eine praxisnahe Lösung, die Sicherheit, Flexibilität und Akzeptanz vereint.

4.3. Die Säulen der Unabhängigkeit: Offene Standards, Interoperabilität (GXFS) und Datenportabilität

- **Offene Standards:** Die Verwendung breit akzeptierter, nicht-proprietärer Standards (z.B. ODF für Dokumente, SQL für Datenbanken, standardisierte APIs wie REST) erleichtert

den Austausch von Komponenten und Daten zwischen Systemen verschiedener Hersteller.[3] Die öffentliche Beschaffung sollte offene Standards verbindlich einfordern.[3]

- **Interoperabilität:** Dies ist die Fähigkeit verschiedener Systeme, nahtlos Daten auszutauschen und zusammenzuarbeiten. Initiativen wie Gaia-X mit ihren Federation Services (GXFS) zielen darauf ab, Open-Source-Bausteine (für Identität & Vertrauen, Föderierten Katalog, Datensouveränität, Compliance) bereitzustellen, um interoperable Datenräume und Föderationen zu ermöglichen.[61] GXFS liefert eine "Werkzeugkiste" für den Aufbau konformer und interoperabler Ökosysteme.[62] Sogenannte "Self-Descriptions" sind dabei zentral für die Auffindbarkeit von Diensten und Daten innerhalb einer Föderation.[63]
- **Datenportabilität:** Die Fähigkeit, Daten einfach, schnell und ohne Funktionsverlust oder übermäßige Kosten zwischen verschiedenen Systemen oder Anbietern zu übertragen. Der EU Data Act stärkt explizit die Rechte auf Datenportabilität und reduziert Hürden für den Wechsel, insbesondere bei Cloud-Diensten.[24] Systeme sollten von vornherein auf Portabilität ausgelegt sein.

Die Realität ist jedoch komplexer als einfache Dualismen wie „Open Source vs. Hyperscaler“ oder „Cloud-only vs. On-Premise“. Die Entscheidung für eine Hybrid- oder Multi-Cloud-Architektur ist Ausdruck dieser Ambivalenz – und kann bei kluger Umsetzung die Vorteile beider Welten vereinen: Innovationsgeschwindigkeit und Usability auf der einen Seite, Souveränität und Kontrolle auf der anderen.

Im Zentrum steht dabei keine ideologische Abgrenzung, sondern eine selbstbewusste, nutzerzentrierte Strategie, die sich an realen Anforderungen orientiert: Welche Daten müssen geschützt werden? Welche Systeme erfordern maximale Interoperabilität? Wo liegt der größte Mehrwert für Anwender?

Echte Hybrid- und Multi-Cloud-Strategien können ihre Vorteile wie Flexibilität und Resilienz nur dann langfristig ausspielen, wenn sie auf offenen Standards aufbauen und Interoperabilität sowie Datenportabilität gewährleisten. Andernfalls droht statt der erhofften Unabhängigkeit eine neue Form der Abhängigkeit von komplexen, fragmentierten und schwer zu managenden Insellösungen. Die Nutzung proprietärer Schnittstellen und Datenformate [37] macht den Wechsel oder die Integration von Diensten verschiedener Anbieter extrem aufwändig und teuer [37], was den ursprünglichen Zweck der Strategie – die Vermeidung von Lock-in [66] – untergräbt. Offene Standards [3] schaffen eine gemeinsame technische Sprache, Interoperabilitäts-Frameworks wie GXFS [61] liefern die technische Basis für den Datenaustausch, und gesetzliche Portabilitätsrechte [24] geben den rechtlichen Rahmen vor. KMU, die Multi- oder Hybrid-Cloud-Strategien verfolgen, müssen daher aktiv Lösungen priorisieren, die auf offenen Standards basieren und klare Wege für die Datenportabilität bieten, um die angestrebte Flexibilität und Resilienz tatsächlich zu realisieren.

Nur mit einem klaren Blick auf diese Grundlagen gelingt eine Architektur, die nicht zwischen Extremen wählen muss, sondern souverän navigiert – im Sinne der Nutzer, Unternehmen und Gesellschaft.

4.4. Strategischer Einsatz von Open Source Software (OSS)

Der strategische Wert von OSS für die digitale Souveränität liegt in mehreren Aspekten:

- **Vorteile:** Transparenz durch einsehbaren Quellcode [3], hohe Flexibilität durch Anpassbarkeit [9], Vermeidung direkter Lizenzkosten [72], Unterstützung durch aktive Communities [72] und die grundsätzliche Vermeidung proprietärer Abhängigkeiten.[9]
- **Anwendungsbeispiele:**
  - *Kollaboration & Filesharing:* Nextcloud [17], Open-Xchange (OX App Suite).[75] Nextcloud wird z.B. von der deutschen Bundesverwaltung [76] und der Landesverwaltung Schleswig-Holstein eingesetzt.[74]
  - *CRM/ERP:* Odoo, weitere spezialisierte Lösungen.
  - *Projektmanagement:* OpenProject [51], wird im Bildungssektor und öffentlichen Verwaltungen genutzt.[84]
  - *Identitäts- & Zugriffsmanagement (IAM):* Univention Corporate Server (UCS).[12] Univention ist Partner im Projekt "Souveräner Arbeitsplatz".[82]
  - *Container-Orchestrierung:* Kubernetes ist der De-facto-Standard und Open Source.
  - *Betriebssysteme:* Diverse Linux-Distributionen (z.B. SUSE [51]).
- **Überlegungen:** Der Einsatz von OSS erfordert entweder internes Know-how oder verlässliche externe Partner für Implementierung, Anpassung und Support.[99] Die Gesamtkosten (TCO) müssen sorgfältig analysiert werden (siehe Abschnitt 7). Die Sicherheit hängt von aktiver Wartung, zeitnahen Updates und der Wachsamkeit der Community bzw. des Support-Anbieters ab.[72]

4.5. Bewertung europäischer Cloud-Alternativen

Es ist wichtig, die Landschaft konkreter zu betrachten:

- **Gaia-X:** Ist keine Cloud, sondern eine Initiative zur Schaffung einer föderierten, sicheren und interoperablen Dateninfrastruktur nach europäischen Werten.[5] Ziel ist es, Anbieter über gemeinsame Standards (GXFS [61]) zu vernetzen. Gaia-X bietet KMU Potenziale für sicheren Datenaustausch, neue Geschäftsmodelle und DSGVO-Konformität.[5] Die Initiative entwickelt sich weiter, und erste Förderprojekte laufen.[95] Der Sovereign Cloud Stack (SCS) ist eine verwandte OSS-Initiative zum Aufbau Gaia-X-kompatibler Clouds.[69]
- **Anbieterlandschaft:** Mehrere europäische Anbieter positionieren sich explizit mit souveränen Angeboten:
  - **IONOS:** Deutscher Anbieter mit Fokus auf sichere, skalierbare und richtlinienkonforme Cloud-Lösungen; beteiligt an Projekten im öffentlichen Sektor.[7]

    - **OVHcloud:** Großer französischer Anbieter mit europäischer Präsenz; betont Datensouveränität und bietet eine "Trusted Zone" mit garantiertem Betrieb nur innerhalb der EU und hoher Sicherheitszertifizierung (SecNumCloud).[51]
    - **T-Systems:** Deutscher Anbieter (Telekom-Tochter); bietet verschiedene souveräne Optionen wie die Open Telekom Cloud, Future Cloud Infrastructure (FCI) und die hochsichere Open Sovereign Cloud (OSC), die auf Intel SGX basiert und für Gesundheitsdaten-IDs genutzt wird.[51]
    - **plusserver:** Deutscher Anbieter, Gaia-X Gründungsmitglied; bietet mit "pluscloud open" eine Cloud auf Basis des Sovereign Cloud Stack (SCS) an.[69]
    - **EWERK Group:** Deutscher Anbieter mit souveräner Cloud für KRITIS & öffentliche Hand; Betrieb ausschließlich in deutschen Rechenzentren, kein Zugriff durch Drittstaaten; umfangreich zertifiziert (ISO/IEC 27001, ISO/IEC 20000-1, ISO 9001, ISAE 3402)
    - **Weitere Akteure:** Anbieter wie Clever Cloud (Frankreich [51]), Secunet (Deutschland [51]), Dataport (Deutschland, öffentlicher Sektor [51]) und andere tragen ebenfalls zum Ökosystem bei.[51]
- **Evaluierungskriterien:** Neben dem Unternehmenssitz und dem Standort der Rechenzentren sind für KMU folgende Kriterien relevant: Sicherheitszertifizierungen (ISO 27001, BSI C5 [17]), Compliance-Nachweise (DSGVO, branchenspezifische Anforderungen), Qualität des Supports, Service Level Agreements (SLAs), verwendete Technologien (Anteil Open Source?), Transparenz der Architektur, garantierte Datenresidenz, vertragliche Regelungen zu Datenzugriff durch Dritte und klare Exit-Strategien bzw. Datenportabilität.

5. Die Roadmap des Mittelstands zur Digitalen Souveränität

Dieses Kapitel übersetzt das Zielbild in eine praxistaugliche 5-Phasen-Roadmap: Analyse → Quick Wins → Migration → Betrieb. Für die Realisierung im Mittelstand erweitern wir sie um drei Querschnittsstränge: Kompetenzaufbau, Partnerauswahl und konsequentes Change Management. Jede Phase definiert klare Ziele, Verantwortlichkeiten und messbare Ergebnisse – so entsteht ein nachvollziehbarer Pfad vom Start bis zum stabil stabilen Betrieb.

5.1 Roadmap in 5 Phasen

Phase 1: Standortbestimmung und Strategische Planung (Monat 0-3)

- **Aktivitäten:**
  - **Klare Zieldefinition:** Warum streben wir digitale Souveränität an? Welche spezifischen Geschäftsziele (z.B. Risikominimierung, Compliance, Innovationsfähigkeit) sollen erreicht werden?.[110]
  - **Umfassende IT-Bestandsaufnahme:** Erfassung aller Anwendungen, Datenflüsse, aktueller Anbieter, Abhängigkeiten und Vertragslaufzeiten.[107] Wo stehen wir aktuell bezüglich Cloud-Nutzung?.[113]
  - **Datenklassifizierung:** Identifikation und Priorisierung kritischer versus unkritischer Daten und Systeme basierend auf Geschäftsauswirkungen, Sensibilität und regulatorischen Anforderungen (DSGVO-Relevanz, NIS2-Anwendbarkeit prüfen).[66]
  - **Risikoanalyse:** Bewertung bestehender Abhängigkeiten (technisch, anbieterspezifisch, geopolitisch), Analyse von Lock-in-Risiken und Identifikation von Compliance-Lücken (DSGVO, NIS2 etc.).[6]
  - **Definition der Zielarchitektur:** Auswahl eines geeigneten Modells (Hybrid Cloud, Multi-Cloud, Nutzung souveräner Plattformen, OSS-Integration) basierend auf Zielen, Risiken und verfügbaren Ressourcen.[66]
  - **Entwicklung einer initialen Roadmap:** Festlegung von Prioritäten, Meilensteinen, Verantwortlichkeiten und grober Ressourcenschätzung.[110]
- **Werkzeuge/Technologien:** Assessment-Tools (z.B. von Beratungsunternehmen oder Cloud-Anbietern [114]), Software zur Abhängigkeitsanalyse, Frameworks zur Datenklassifizierung.
- **Kompetenzen:** Geschäftsanalytik, IT-Architektur, Risikomanagement, Kenntnisse regulatorischer Anforderungen (DSGVO, NIS2).
- **Partner:** Bei fehlender interner Expertise Einbindung von spezialisierten Beratern für Assessment und Strategieentwicklung.[68]

Phase 2: Kompetenzaufbau und Förderung einer Souveränitätskultur (Laufend ab Monat 1)

- **Aktivitäten:**

    - **Management-Buy-in sichern:** Die strategische Bedeutung muss von der Führungsebene getragen und das "Warum" im gesamten Unternehmen kommuniziert werden.[86] Ängste und Widerstände müssen adressiert werden.[117]
    - **Etablierung eines Kernteams:** Bildung eines funktionsübergreifenden Teams (ggf. "Cloud Champions" [117]), das die Initiative vorantreibt und als Ansprechpartner dient.
    - **Kompetenzlückenanalyse:** Identifikation fehlender Fähigkeiten bezogen auf die Zielarchitektur und die ausgewählten Technologien (Cloud-Plattformen, OSS, Security-Tools, FinOps, Automatisierung).[7]
    - **Gezielte Schulungsprogramme:** Entwicklung und Durchführung passgenauer Weiterbildungsmaßnahmen (intern/extern, Cross-Training) für IT-Personal und Anwender.[2] Förderung der digitalen Grundkompetenz und des Sicherheitsbewusstseins bei allen Mitarbeitenden.[3]
    - **Kultur des Lernens fördern:** Etablierung einer Kultur der kontinuierlichen Weiterbildung und Offenheit für technologische und prozessuale Veränderungen.[2]
- **Werkzeuge/Technologien:** Lernplattformen, externe Trainingsanbieter, interne Kommunikationsmittel (Intranet, Newsletter).
- **Kompetenzen:** Change Management, interne Kommunikation, Personalentwicklung, Trainingskonzeption.
- **Partner:** Trainingsanbieter, Change-Management-Berater, Mittelstand-Digital Zentren.[43]

Phase 3: Informierte Technologie- und Partnerauswahl (Monat 2-6)

- **Aktivitäten:**
    - **Detaillierte Anforderungsspezifikation:** Erstellung eines Lastenhefts für die Ziellösungen basierend auf den Ergebnissen aus Phase 1.
    - **Technologieevaluierung:** Bewertung potenzieller Technologien (spezifische Cloud-Plattformen, OSS-Alternativen) anhand von Kriterien wie Funktionalität, Sicherheit (Zertifizierungen), Interoperabilität, Portabilität, Gesamtkosten (TCO, siehe Abschnitt 7) und Souveränitätsaspekten.[17] Priorisierung von EU-/deutschen Anbietern, wo sinnvoll und möglich.[7]
    - **Partneridentifikation und -prüfung:** Auswahl und Bewertung potenzieller Implementierungs- oder Managed-Service-Partner. Prüfung von Expertise, Referenzen (Case Studies), kultureller Passung und Engagement für digitale Souveränität.[42]
    - **Durchführung von Proof-of-Concepts (PoCs):** Testen von Schlüsseltechnologien oder -lösungen in einer kontrollierten Umgebung (Pilotprojekte).[110] Überprüfung der Migrationsfähigkeit für kritische Anwendungen.[74]
    - **Finalisierung der Technologie- und Partnerwahl:** Abschluss von Verträgen unter Sicherstellung klarer Service Level Agreements (SLAs),

Auftragsverarbeitungsverträgen (AVV [17]), Ausstiegsklauseln und verbindlicher Sicherheitszusagen.

- **Werkzeuge/Technologien:** Bewertungsmatrizen für Anbieter/Technologien, Testumgebungen für PoCs, juristische Expertise für Vertragsgestaltung.
- **Kompetenzen:** Beschaffungswesen, Lieferantenmanagement, technische Evaluierungsfähigkeiten, Rechtskenntnisse.
- **Partner:** Potenzielle Implementierungspartner, Rechtsberater.

Phase 4: Stufenweise Implementierung und Migration (Start Monat 3-6, Dauer variabel)

- **Aktivitäten:**
  - **Priorisierung der Workloads:** Festlegung der Migrationsreihenfolge basierend auf Kritikalität, Komplexität und Potenzial für schnelle Erfolge ("Quick Wins"). Beginn oft mit weniger kritischen Systemen oder spezifischen Funktionen.[66]
  - **Vorbereitung der Zielumgebung:** Aufbau der Cloud-Umgebung (z.B. Azure Landing Zones [68]), Konfiguration von Sicherheitsmaßnahmen, Etablierung von Governance-Prozessen.[114]
  - **Durchführung der Migration:** Umsetzung in Wellen unter Nutzung geeigneter Migrationsstrategien (z.B. Rehost/"Lift & Shift", Replatform, Refactor – die "6 Rs" [116]) und etablierter Frameworks.[107] Einsatz von Automatisierung, wo möglich.[114]
  - **Implementierung ausgewählter OSS-Lösungen:** Einführung von Systemen wie Nextcloud [74] oder OpenProject.
  - **Umfassende Tests:** Durchführung von Funktions-, Performance- und Sicherheitstests nach jeder Migrationswelle.
  - **Systematische Stilllegung:** Außerbetriebnahme der Altsysteme nach erfolgreicher Migration.[107]
- **Werkzeuge/Technologien:** Migrationswerkzeuge (anbieterspezifisch oder von Drittanbietern), Automatisierungsskripte, Test-Tools, Projektmanagement-Software (z.B. OpenProject [83]).
- **Kompetenzen:** Cloud Engineering (Azure, AWS, GCP, OpenStack etc.), spezifische OSS-Kenntnisse, Testmanagement, Projektmanagement.
- **Partner:** In Phase 3 ausgewählte Implementierungspartner.

Phase 5: Verankerung des Change Managements, Betrieb & Optimierung (Laufend ab Monat 6+)

- **Aktivitäten:**
  - **Laufender Anwendersupport:** Bereitstellung von Unterstützung und gezielten Schulungen für die neuen Systeme und Prozesse.[117]
  - **Monitoring:** Überwachung der Systemleistung, der Sicherheitslage (kontinuierliches

Monitoring [64]) und der Kosten (FinOps [35]).
    - **Adoptionskontrolle:** Regelmäßige Bewertung der Nutzungsraten und der Anwenderzufriedenheit; Identifikation und Adressierung von Akzeptanzlücken.[117]
    - **Sicherheitsüberprüfungen:** Durchführung periodischer Sicherheitsaudits und Penetrationstests.
    - **Kontinuierliche Optimierung:** Laufende Anpassung der Cloud-Nutzung zur Verbesserung von Kosten und Leistung.[58]
    - **Strategie-Review:** Regelmäßige Überprüfung und Anpassung der Souveränitätsstrategie und der Roadmap basierend auf neuen Bedrohungen, Technologien, regulatorischen Änderungen und Geschäftsanforderungen.[110] Integration von Souveränitätsprüfungen in die laufende IT-Governance.
    - **Feedbackkultur pflegen:** Offene Kommunikationskanäle für Rückmeldungen aufrechterhalten.[86] Erfolge kommunizieren und feiern.[110]
- **Werkzeuge/Technologien:** Monitoring-Tools (Cloud-native oder Drittanbieter), Security Information and Event Management (SIEM)-Systeme, FinOps-Plattformen, Service-Desk-Software.
- **Kompetenzen:** Cloud Operations (CloudOps), Security Operations (SecOps), FinOps, IT Service Management (ITSM), Methoden zur kontinuierlichen Verbesserung (KVP).
- **Partner:** Optional Managed Service Provider (MSPs), externe Sicherheitsauditoren.

Diese Roadmap ist kein linearer Prozess, der mit dem Regelbetrieb endet. Gerade Phase 5 macht den Prozess **zyklisch**. Digitale Souveränität ist keine einmalige Errungenschaft, sondern eine dynamische Fähigkeit, die kontinuierliche Aufmerksamkeit erfordert. Die digitale Landschaft verändert sich ständig: Bedrohungen entwickeln sich weiter [21], Technologien schreiten rasant voran [60], Regulierungen werden angepasst und Geschäftsbedürfnisse ändern sich.[111] Ein reiner Migrations- und Betriebsmodus reicht nicht aus, um Souveränität *dauerhaft* zu sichern. Die Aktivitäten der Phase 5 – kontinuierliches Monitoring [64], Optimierung [58], regelmäßige Überprüfungen [110] und Anpassungen – sind entscheidend. Die daraus gewonnenen Erkenntnisse fließen zurück in die Strategie (Phase 1) und den Kompetenzaufbau (Phase 2), wodurch sich der Kreis schließt und eine kontinuierliche Anpassung an die Realität ermöglicht wird.

Tabelle 1: Detaillierte Roadmap zur Digitalen Souveränität für KMU

Phase	Kernaktivitäten	Zeitrahmen (indikativ)	Kompetenzen/Rollen	Werkzeuge/Technologien	KPIs (Beispiele)	Partner/Support
1. Assessment & Strategie	Ziele definieren, IT-Inventar,	0-3 Monate	Geschäftsanalyst, IT-Architekt,	Assessment-Tools, CMDB, Datenklassifizi	Klar definierte Ziele, abgeschlossen	Strategieberater, Branchen-

	Daten klassifizieren, Risiken analysieren, Zielarchitektur entwerfen, Roadmap erstellen		Risikomanager, Compliance-Beauftragter, Management	erungs-Frameworks	e Risikoanalyse, Entwurf Zielarchitektur & Roadmap	verbände
2. Kompetenz & Kultur	Management-Buy-in, Kernteam bilden, Skill-Gap-Analyse, Trainingsprogramme entwickeln/durchführen, Kommunikationsplan, Kulturwandel fördern	Laufend ab Monat 1	Change Manager, HR/Personalentwicklung, Interne Kommunikation, Management, IT-Trainer	Lernplattformen, Trainingsmaterialien, Kommunikations-Tools (Intranet, Newsletter)	Mitarbeiterzufriedenheit, Teilnahmequote an Schulungen, Verständnis der Strategie, definierte "Cloud Champions"	Trainingsanbieter, Change-Management-Berater, Mittelstand-Digital Zentren
3. Technologie- & Partnerauswahl	Anforderungen spezifizieren, Technologien evaluieren (Cloud, OSS), Partner identifizieren/prüfen, PoCs/Piloten durchführen, Verträge finalisieren (SLAs, AVVs, Exit-Klauseln)	Monat 2-6	Einkäufer, Vendor Manager, Technischer Evaluierer, Jurist, Projektleiter	Bewertungsmatrizen, Testumgebungen, Vertragsmuster	Abgeschlossene PoCs, ausgewählte Technologien & Partner, unterzeichnete Verträge	Potenzielle Implementierungspartner, Rechtsberater
4. Implementierung & Migration	Workloads priorisieren, Zielumgebung vorbereiten (Landing Zone, Security), Migration in Wellen (6R), OSS implementieren, Tests durchführen, Altsysteme	Start Monat 3-6+	Cloud Engineer, Systemadministrator, OSS-Experte, Tester, Projektmanager	Migrations-Tools, Automatisierungsskripte, Test-Tools, Projektmanagement-Software	Anzahl migrierter Workloads, Erfolgsrate der Migrationen, Testabdeckung, Einhaltung Zeitplan/Budget	Implementierungspartner

	stilllegen					
5. Betrieb, Optimierung & Anpassung	Laufender Support, Monitoring (Performance, Security, Kosten), Adoptionskontrolle, Security Audits/PenTests, Kosten-/Performance-Optimierung, Strategie-Review, Feedback einholen	Laufend ab Monat 6+	Cloud Operator, SecOps-Analyst, FinOps-Manager, ITSM-Spezialist, KVP-Beauftragter	Monitoring-Tools, SIEM, FinOps-Plattformen, Service Desk	Systemverfügbarkeit, Incident Response Time, Kosteneffizienz (Cloud Spend vs. Budget), Sicherheits-Score, Nutzerzufriedenheit, Adoptionsrate	Managed Service Provider (optional), Sicherheitsauditoren, Cloud-Provider Support

6. Illustrative Fälle: Souveränität in der Praxis

Dieses Kapitel zeigt, wie digitale Souveränität **konkret** umgesetzt wird. Drei typische Pfade adressieren unterschiedliche Anforderungen im Mittelstand und im KRITIS-/Public-Sektor:

- **Pfad A:** Open-Source-Kernsysteme (produzierender Mittelstand)
- **Pfad B: Hybrid** aus EU-kontrollierten Zonen und Hyperscalern (Dienstleister/Handel)
- **Pfad C: Souveräne EU-Cloud** für hochregulierte Umgebungen (KRITIS/öffentliche Hand)

Jeder Fall ist identisch aufgebaut: **Ausgangslage → Zielbild → Vorgehen (90/180/360 Tage) → Governance/Compliance → KPI-Raster → Risiken & Maßnahmen → Lessons Learned**. So können KMU die Ansätze vergleichen und für ihre Lage übernehmen.

6.1 Illustrative Beispiele

Beispiel A) Open-Source-Kernsysteme im produzierenden Mittelstand

Ausgangslage: Hohe Lizenzkosten, begrenzte Anpassbarkeit proprietärer Suiten, steigende Nachfrage nach schnelleren Release-Zyklen und Interoperabilität.

Zielbild: Ersatz ausgewählter proprietärer Module (z. B. Kollaboration, Filesync/Share, Projektmanagement, Identity) durch reife OSS-Alternativen; Vertrags-Support über Integrationspartner; klarer Exit-Pfad und standardisierte Schnittstellen.

Vorgehen (Meilensteine):

- T+90 Tage: Zielarchitektur, Datenklassifizierung, PoC für 1–2 OSS-Domänen; Migrations-Runbook; Change-Plan (Stakeholder, Schulungen, Champions).
- T+180 Tage: Staged Roll-out in Pilotteams; Einführung FinOps-Grundlagen für Betriebskosten; Monitoring (Verfügbarkeit, Incident-Rate).
- T+360 Tage: Produktiver Betrieb; Härtung & Audit-Trail; Vertragswerk (SLAs, Support, Exit-Klauseln) finalisiert.

Governance & Compliance. Standardisierte Rollen (IAM) und privilegierter Zugriff (PAM), Protokollierung mit revisionssicheren Logs, Backup-/Restore-Übungen, dokumentierte Lizenz-Compliance (OSS-Lizenzen, Third-Party-Notices).

KPI	Zielwert (Richtgröße)	Messmethode	Intervall	Verantwortlich

TCO über 5 Jahre	Trend ↓ ggü. Baseline	Vollkostenrechnung: Lizenzen, Integr./Betrieb (FTE), Support, Hardware/Cloud, Egress/Exit	Quartal	CFO/FinOps
Adoptionsrate	≥ 80 % aktive Nutzer nach 6 Monaten	aktive Konten/Monat	Monat	Product Owner
Incident-Rate	≤ 0,3 pro Nutzer/Monat	Tickets pro Nutzer	Monat	IT-Betrieb
Mean Time to Restore (MTTR)	≤ 4 h	Zeit Störungsbeginn→Wiederherstellung	Monat	IT-Betrieb
Anteil offener Standards	≥ 90 % der Integrationen	Architektur-Review (Protokolle/Dateiformate/APIs)	Quartal	Enterprise Arch.
Vendor-Konzentration (HHI)	Trend ↓	HHI über kritische Komponenten	Halbjahr	CISO/EA
Audit-Findings kritisch	= 0	Interne/Externe Audits	Halbjahr	Compliance

Risiken & Maßnahmen:

- Unterschätzter Integrationsaufwand → Puffer (≥ 20 %), saubere Schnittstellen-Specs, frühe End-to-End-Tests.
- Akzeptanzprobleme → Champions-Netzwerk, Onboarding-Guides, nutzernahe Roadmap.
- „Hidden“ Betriebskosten → FinOps-Transparenz (FTE-Zeit, Storage, Support), regelmäßige Review-Zyklen.

Lessons Learned:

1. Einsparungen entstehen oft erst in der 5-Jahres-TCO (Lizenz ↓, Integrations-/Betriebsaufwand initial ↑).
2. Ohne Change-Management (Training, Kommunikation, Metriken) kippt die Adoptionskurve.

Beispiel B) Hybrid: EU-kontrollierte Zonen + Hyperscaler

Ausgangslage: Daten- und Leistungsanforderungen variieren: Sensible Daten benötigen EU-Kontrolle, Innovations-Workloads profitieren von Hyperscaler-Services.

Zielbild: Daten- und Workload-Segmentierung: Schutzbedürftige Daten in EU-kontrollierten Zonen (z. B. Trusted/Shielded), elastische Workloads bei Hyperscalern; konsistentes **Identity-Fundament** und Interoperabilität.

Vorgehen (Meilensteine).

- **T+90 Tage:** Datenklassifizierung (A/B/C), CMDB/Service-Katalog, Netzwerk-Topologie (egressarm), Baseline-SLAs.
- **T+180 Tage:** Einrichtung EU-Zone (Speicher/Compute), verbindliche **Exit-Klauseln** in Verträgen, CI/CD-Pfad für portable Workloads (Container, IaC).
- **T+360 Tage:** Betriebsübergabe, FinOps-Automatisierung, regelmäßige **Failover-Drills** (RTO/RPO).

Governance & Compliance: Einheitliche Policies (DLP, KMS, Schlüsselverwaltung), getrennte Betriebs-/Schlüsselverantwortung, Drittstaatenzugriff vertraglich ausgeschlossen, Logs zentral und unveränderbar.

KPI	Zielwert (Richtgröße)	Messmethode	Intervall	Verantwortlich
Verfügbarkeit (SLA)	≥ 99,9 %	Uptime-SLA je Dienst	Monat	Provider Mgmt
RTO / RPO	RTO ≤ 4 h / RPO ≤ 1 h	Drill-Ergebnisse	Quartal	IT-Betrieb
Egress-Kostenanteil	≤ 5 % der Cloud-Kosten	Kostenreport/FinOps	Monat	FinOps

Anteil portabler Workloads	≥ 70 % containerisiert/IaC	Deployment-Statistiken	Quartal	DevOps
Schlüsselhoheit	100 % Kundenschlüssel in EU-HSM	Audit/Key-Mgmt-Report	Quartal	CISO
Datenlokalität	100 % Klasse-A in EU-Zonen	Data-Residency-Report	Monat	Data Owner

Risiken & Maßnahmen:

- **Lock-in durch proprietäre Services** → Priorität für offene Schnittstellen/OSS-Äquivalente, „Side-by-Side"-Migrationspfad.
- **Kostenexplosion durch Egress** → Data-Gravity-Design, Caching, Near-Data-Processing.
- **Komplexität** → Plattform-Team („Golden Path"), Blaupausen, Self-Service-Katalog.

Lessons Learned:

3. Der Kostentreiber ist selten Compute – **Egress und Betriebszeit** zählen.
4. **Identitäts- und Schlüsselmanagement** sind die tragenden Säulen der Souveränität, nicht das Rechenzentrumsetikett allein.

Beispiel C) Souveräne EU-Cloud für KRITIS/öffentliche Hand

Ausgangslage: Hohe regulatorische Dichte, Audits, Nachweispflichten; Bedarf an EU-bzw. DE-Betrieb und zertifizierten Prozessen.

Zielbild: Betrieb ausschließlich in **EU-Rechenzentren**, klare **Zugangskontrolle** (IAM/PAM), nachweisbare **Sicherheitszertifizierungen** (z. B. ISO/IEC 27001, BSI C5) und vollständiger Audit-Trail.

Vorgehen (Meilensteine):

- **T+90 Tage:** Regulatorische Scope-Analyse, Schutzbedarfsfeststellung, Zielarchitektur (Netz-Zonen, Härtung), Rollenmodell.
- **T+180 Tage:** Technische Härtung (Baseline-CIS/BSI), **Monitoring & SIEM**,

Notfallhandbuch, Betriebs-/Datentreuetrennung.

- **T+360 Tage:** Zertifizierungsvorbereitung, Table-Top-/Live-Übungen, Provider-Audits, Abschluss Prüfbericht.

Governance & Compliance: Dokumentierte Prozesse (Change, Incident, Access), revisionssichere Protokolle, regelmäßige interne/externe Audits, klare Verantwortlichkeiten (Rollen-RACI).

KPI	Zielwert (Richtgröße)	Messmethode	Intervall	Verantwortlich
Audit-Findings (kritisch)	= 0	Prüfberichte	Halbjahr	Compliance
SLA (kritische Dienste)	≥ 99,95 %	Uptime-Report	Monat	Provider Mgmt
MTTR (kritisch)	≤ 2 h	Störungsreport	Monat	IT-Betrieb
Patch-Compliance	≥ 98 % ≤ 30 Tage	Patch-Report	Monat	SecOps
MFA/PAM-Abdeckung	100 % privilegierte Zugriffe	IAM-Report	Monat	CISO
Backup-/Restore-Erfolg	100 % Tests bestanden	Restore-Drills	Quartal	IT-Betrieb

Risiken & Maßnahmen:

- Scheinsouveränität (Label ohne Nachweis) → Zertifikate, Prüfberichte, technische Kontrollen vertraglich fixieren; Right-to-Audit.
- Rollenunklarheit → RACI und „Segregation of Duties“ früh etablieren.
- Audit-Überraschungen → interne Pre-Audits, evidence-ready Doku (Kontroll-Nachweise, Screenshots, Log-Snippets).

Lessons Learned:

- Souveränität ist kein Logo, sondern ein prüfbares Set technischer, organisatorischer und vertraglicher Kontrollen.

- Früh geübte Notfall- und Wiederherstellungsprozesse reduzieren Audit-Risiken signifikant.

6.2. Weitere Fallstudien

Die folgenden Beispiele illustrieren verschiedene Facetten der Umsetzung digitaler Souveränität:

- **Nextcloud (Open Source Kollaboration):**
  - **Deutsche Bundesverwaltung (ITZBund):** Nach einem erfolgreichen Pilotprojekt entschied sich das ITZBund für Nextcloud als sichere Filesharing- und Kollaborationslösung für rund 300.000 Nutzer. Ausschlaggebend waren die hohen Sicherheitsanforderungen, die Skalierbarkeit und die Möglichkeit, die Lösung im eigenen, vertrauenswürdigen Rechenzentrum zu betreiben ("Private Cloud für den Bund").[76] Dies zeigt die Eignung von OSS auch für große Organisationen mit höchsten Sicherheitsansprüchen.
  - **Landesverwaltung Schleswig-Holstein:** Setzt seit Jahren strategisch auf Open Source und nutzt Nextcloud für über 40.000 Verwaltungsmitarbeiter. Die Verantwortlichen betonen die Bedeutung einer langfristigen Strategie (über 10 Jahre), starker politischer Rückendeckung, umfassenden Change Managements und – ganz entscheidend – der Unterstützung bei der Datenmigration für die Nutzerakzeptanz.[74] Dies unterstreicht, dass der Umstieg ein tiefgreifender Veränderungsprozess ist.
  - **Weitere Anwender:** Die Migration der Millionen Nutzer der Telekom MagentaCLOUD zu Nextcloud [77], der Einsatz bei Amnesty International Spanien zum Schutz vertraulicher Daten [77] oder an der Sorbonne Universität [77] belegen die breite Anwendbarkeit in verschiedenen Sektoren.
- **Univention (Open Source IAM & Infrastruktur):**
  - **Souveräner Arbeitsplatz (Öffentliche Verwaltung):** Univention ist mit seinen Lösungen (insbesondere Univention Corporate Server - UCS) ein wichtiger Baustein dieser Initiative, die einen modularen, interoperablen und souveränen digitalen Arbeitsplatz für die deutsche Verwaltung schaffen soll, oft in Kombination mit Nextcloud, Open-Xchange und Collabora.[82] Dies demonstriert das Potenzial der Integration verschiedener OSS-Komponenten.
  - **Breiter Einsatz:** Univention-Lösungen werden von über 14.000 Organisationen genutzt [94], darunter zahlreiche Bundesländer, Kommunen und Unternehmen im DACH-Raum [93], um ein zentrales Identitätsmanagement zu etablieren und die Kontrolle über die IT-Infrastruktur zu behalten.[94]
- **OpenProject (Open Source Projektmanagement):**
  - **Hochschule Coburg:** Nutzt die Cloud-Edition von OpenProject in der Lehre, um Projektmanagement-Methoden praktisch anzuwenden. Dies ersetzte mehrere

Insellösungen (Excel, Dropbox, Trello) und reduzierte den administrativen Aufwand erheblich.[84] Das Beispiel zeigt Effizienzgewinne durch integrierte OSS-Lösungen.
    - **Landratsamt Enzkreis:** Setzt OpenProject zur besseren Visualisierung von Projektzeitplänen (Gantt-Diagramme), zum erleichterten Informationsaustausch im Team und zur effizienteren Gestaltung von Besprechungen (gemeinsame Agenda/Protokollierung) ein.[85]
    - **EGS-plan (Ingenieurbüro/KMU):** Integriert OpenProject mit Nextcloud für ein effizientes Projektmanagement unter Berücksichtigung hoher Datenschutzanforderungen.[83] Dies ist ein relevantes Beispiel für die KMU-Zielgruppe.
- **Souveräne Cloud-Anbieter und KMU:**
    - **plusserver (pluscloud open / SCS):** Die Fallstudie mit dem KMU Dr. Dienst & Partner hebt die Entlastung der internen IT durch die Auslagerung des Rechenzentrumsbetriebs an plusserver hervor.[70] Auch Univention nutzt die pluscloud open und begründet dies mit dem Aspekt der Datensouveränität.[69] Dies zeigt die Marktakzeptanz SCS-basierter Clouds bei KMU und technologieorientierten Unternehmen.
    - **T-Systems (Open Sovereign Cloud):** Der Einsatz der OSC durch große deutsche Krankenkassen (BARMER, AOK) zur Verwaltung von Millionen digitaler Gesundheitsidentitäten unter strengen deutschen und europäischen Datenschutzauflagen (Sozialgesetzbuch, DSGVO) demonstriert die Fähigkeit souveräner Clouds, auch hochsensible Daten in regulierten Branchen sicher zu verarbeiten.[52]
    - **WESSLING (Labordienstleister/KMU):** Die Migration dieses Mittelständlers zu Google Cloud (begleitet durch Devoteam) [54] illustriert typische Migrationsziele (Kostenreduktion, Performance, Skalierbarkeit) und eine methodische Vorgehensweise (Analyse, schrittweise Migration über VMware Engine). Obwohl hier kein souveräner Anbieter gewählt wurde, liefert der Fall wichtige Einblicke in die Treiber und Prozesse einer KMU-Cloud-Migration, die als Vergleichsmaßstab dienen können.
    - **ServiceNow/Plat4mation Partnerschaft für den Mittelstand:** Dieser Ansatz zielt darauf ab, Mittelständlern mit potenziell geringeren Cloud-Kompetenzen den Einstieg durch gezielte, risikoarme Migration spezifischer Prozesse (z.B. Auftragsverfolgung, Bestandsmonitoring, Field Service) auf die ServiceNow-Plattform zu erleichtern. Der Fokus liegt auf einem partnergeführten Change Management, das die Unternehmenskultur berücksichtigt.[42] Dies unterstreicht die Notwendigkeit maßgeschneiderter Migrationsansätze für KMU.

6.3. Erfolgsfaktoren und Fallstricke aus der Praxis

Aus den Fallstudien lassen sich wiederkehrende Muster für Erfolg und Misserfolg ableiten:

- **Erfolgsfaktoren:**
  - **Strategische Verankerung & Führung:** Klares Bekenntnis und Rückendeckung durch die Unternehmens- oder Behördenleitung.[74]
  - **Umfassende Planung:** Eine sorgfältige Analyse der Ausgangslage und eine klare Strategie sind essenziell.[74]
  - **Effektives Change Management:** Aktive Einbindung der Nutzer, klare Kommunikation des "Warum" und der Vorteile, Adressierung von Bedenken.[74]
  - **Fokus auf Migration:** Bereitstellung technischer Unterstützung und einfacher Wege für die Datenmigration, um Nutzer nicht zu verlieren.[74]
  - **Passende Partnerwahl:** Auswahl von Dienstleistern mit nachgewiesener Expertise und Verständnis für Souveränitätsanforderungen.[42]
  - **Modularität & Interoperabilität:** Aufbau flexibler Systeme, die den Austausch von Komponenten ermöglichen.[82]
  - **Stufenweises Vorgehen:** Beginn mit Pilotprojekten oder weniger kritischen Bereichen, um Erfahrungen zu sammeln und Risiken zu minimieren.[42]
- **Fallstricke:**
  - **Unterschätzung der Komplexität:** Mangelndes Bewusstsein für den Bedarf an Fachkenntnissen und Ressourcen.[40]
  - **Vernachlässigung des Change Managements:** Fehlende Einbindung und Kommunikation führt zu Widerständen und geringer Akzeptanz.[74]
  - **Mangelhafte Migrationsplanung/-unterstützung:** Technische Hürden und Datenverlust frustrieren Nutzer und gefährden das Projekt.[74]
  - **Fokus auf kurzfristige Kosten:** Auswahl von Lösungen allein aufgrund niedriger Anschaffungs- oder Lizenzkosten ohne Berücksichtigung der TCO.[99]
  - **Ignorieren von Nutzerbedenken:** Fehlende Berücksichtigung von Ängsten und Gewohnheiten der Mitarbeiter.[117]
  - **Reines "Lift & Shift":** Übertragung alter Prozesse und Architekturen in die Cloud ohne Optimierung, wodurch Cloud-Potenziale ungenutzt bleiben.[66]

Erfolgreiche Souveränitätsinitiativen, insbesondere solche, die stark auf Open Source setzen, erfordern oft einen langen Atem. Sie sind weniger ein reines Technologieprojekt als vielmehr ein organisatorischer Transformationsprozess. Die Beispiele, wie das von Schleswig-Holstein [74], zeigen, dass ein strategisches Langzeit-Commitment notwendig ist. Die Investition muss über die reine Technologiebeschaffung hinausgehen und signifikante Mittel für Change Management, Mitarbeiterschulung und Migrationsunterstützung umfassen.[74] KMU müssen daher nicht nur die Kosten für Software und Dienstleistungen budgetieren, sondern auch die Kosten für den organisatorischen Wandel, der notwendig ist, um den Technologiewechsel erfolgreich und nachhaltig zu gestalten.

7. Der Business Case: Quantifizierung des Werts Digitaler Souveränität

Die Stärkung der digitalen Souveränität ist eine strategische Investition mit Wirkung auf Kosten, Risiko und Wertentwicklung. Treiber sind geringere Lizenzabhängigkeiten, mehr Innovationshoheit, reduzierte Compliance- und Lieferkettenrisiken sowie positive Effekte auf Unternehmensbewertung und Beschäftigung. Für eine belastbare Entscheidung im Mittelstand braucht es eine **differenzierte, quantifizierbare Bewertung**: Lebenszyklus-TCO über 3–5 Jahre (Lizenzen, Integrations-/Betriebskosten, Egress/Exit), monetarisierte Risikopositionen (Bußgelder, Ausfallzeiten, Preissteigerungen durch Lock-in) sowie nachweisbare Nutzenindikatoren (Time-to-Market, SLA-Erfüllung, Audit-Findings, Talentgewinnung).

7.1. Umfassende Kostenanalyse

Eine reine Gegenüberstellung von Lizenz- oder Abonnementkosten greift zu kurz. Notwendig ist eine Analyse der Gesamtbetriebskosten (Total Cost of Ownership - TCO) über den gesamten Lebenszyklus, die auch indirekte Kosten und Risiken berücksichtigt.

- **TCO: Cloud versus On-Premises:**
  - **Cloud (SaaS/PaaS/IaaS):** Verlagert Investitionsausgaben (Capex) zu Betriebsausgaben (Opex).[107] Die TCO umfassen Abonnements, Nutzungsgebühren (Compute, Storage, Datenübertragung), Management-Tools, Personal für Cloud-Management und -Optimierung (CloudOps, FinOps), Schulungen, Supportverträge und potenzielle Kosten für Ausfallzeiten.[38] Die Kalkulation ist aufgrund von Skalierbarkeit und Pay-as-you-go-Modellen komplex.[58] Anbieter-Tools (z.B. AWS TCO Calculator [58]) können helfen, erfordern aber eine kritische Prüfung der Annahmen.
  - **On-Premises:** Erfordert hohe Anfangsinvestitionen (Capex) in Hardware (Server, Storage, Netzwerk), Softwarelizenzen und ggf. Gebäudeinfrastruktur. Laufende Kosten (Opex) umfassen Energie, Kühlung, Wartungsverträge, Softwarepflegegebühren, umfangreiches IT-Personal (mind. 2,5 Vollzeitkräfte für vergleichbare Funktionalität laut [121]), Updates, Support und Abschreibungen.[121]
- **TCO: Open Source Software (OSS) versus Proprietäre Software:**
  - **OSS:** Vermeidet direkte Lizenzkosten.[72] Die TCO können jedoch durch andere Faktoren höher ausfallen: Bedarf an spezialisiertem Know-how (intern oder extern), Kosten für Implementierung, Anpassung, Schulung und Support, potenziell längere Entwicklungs-/Einführungszeiten und das Fehlen eines zentralen, verantwortlichen Anbieters für Support und Gewährleistung.[99]
  - **Proprietäre Software:** Beinhaltet Lizenzkosten (einmalig oder als Abo) und oft laufende Wartungs-/Supportgebühren. Dafür sind Support, Schulungen und eine definierte Produkt-Roadmap meist inkludiert.[72] Das Hauptrisiko liegt im Vendor Lock-

in und steigenden Kosten über die Zeit.[100]
    - **Fazit:** Die Wahl hängt stark von der Komplexität des Projekts, den internen Fähigkeiten, der Verfügbarkeit von Support-Partnern und der langfristigen Strategie ab.[99] Eine pauschale Aussage zur TCO-Überlegenheit einer Variante ist nicht möglich. OSS kann langfristig günstiger sein, wenn interne Kompetenzen aufgebaut werden.[100]
- **Migrations- und Exit-Kosten:**
    - Die Migration selbst verursacht Kosten für Planung, Durchführung, Tests und mögliche Betriebsunterbrechungen.[107]
    - Vendor Lock-in manifestiert sich in hohen Kosten beim Versuch, den Anbieter zu wechseln (Exit Costs): hohe Gebühren für den Datenexport [37], aufwändige Anpassung von Anwendungen an neue Plattformen (Re-Platforming) [15] oder Vertragsstrafen bei vorzeitiger Kündigung.[37]
    - Diese potenziellen Exit-Kosten müssen bei der TCO-Betrachtung von Anfang an berücksichtigt werden. Souveräne Architekturen und OSS zielen darauf ab, diese Barrieren zu senken.[17]

Eine naive TCO-Analyse, die sich nur auf sichtbare Abonnement- oder Lizenzkosten konzentriert, ist irreführend. Ein realistischer Business Case muss eine **risikoadjustierte Lebenszyklus-TCO-Perspektive** einnehmen. Diese berücksichtigt nicht nur alle direkten und indirekten Kosten über den gesamten Nutzungszeitraum (inklusive potenzieller Exit-Kosten [37]), sondern bewertet auch die finanziellen Auswirkungen von Risiken, die durch mangelnde Souveränität entstehen. Dazu gehören Compliance-Verstöße [122], Sicherheitsvorfälle [125] und die Kosten strategischer Unflexibilität durch Vendor Lock-in.[15] Die Investition in eine souveräne Lösung muss also den Gesamtkosten (Lifecycle TCO) einer nicht-souveränen Alternative gegenübergestellt werden, wobei bei letzterer die monetarisierten Risiken hinzuzurechnen sind.

7.2. Artikulation der Nutzenaspekte

Neben der Kostenbetrachtung müssen die qualitativen und quantifizierbaren Vorteile der digitalen Souveränität klar benannt werden:

- **Wert der Resilienz:** Verringertes Risiko von Geschäftsunterbrechungen durch technische Ausfälle, Cyberangriffe oder geopolitisch bedingte Anbieterprobleme, da mehr Kontrolle und Diversifizierungsmöglichkeiten bestehen.[6] Der finanzielle Wert der Geschäftskontinuität ist oft schwer direkt zu beziffern, aber existenziell.
- **Vermeidung von Compliance-Kosten:** Proaktive Erfüllung der Anforderungen von DSGVO, NIS2, DORA etc. durch kontrollierte Umgebungen hilft, hohe Bußgelder und aufwändige Nachbesserungen zu vermeiden. DSGVO-Bußgelder können erheblich sein (Meta >1,5 Mrd. € [122]), und NIS2 droht mit Strafen von bis zu 2% des globalen Jahresumsatzes.[19] Die durchschnittlichen Kosten einer Datenpanne liegen im

Millionenbereich (ältere Studie für DE: 2,41 Mio. € pro Unternehmen [125]; global 2020: 3,86 Mio. $ [126]; bei großen Vorfällen noch deutlich höher [126]).

- **Innovationskontrolle und Flexibilität:** Fähigkeit, Technologien frei zu wählen und zu kombinieren ("Best-of-Breed"), Systeme nahtlos zu integrieren, Prozesse ohne Anbieterbeschränkungen anzupassen und die eigene Innovations-Roadmap zu steuern.[3] Dies kann die Zeit bis zur Markteinführung neuer Produkte oder Dienstleistungen verkürzen.[5][6]
- **Minderung von Lock-in-Kosten:** Vermeidung zukünftiger, unkalkulierbarer Preiserhöhungen, erzwungener Upgrades oder der Unfähigkeit, zu besseren oder günstigeren Alternativen zu wechseln.[15] Erhalt der Verhandlungsmacht gegenüber Anbietern.
- **Verbessertes Vertrauen und Reputation:** Nachweisbare Kontrolle über sensible Daten (Kunden-, Mitarbeiter-, Geschäftsdaten) kann das Vertrauen von Kunden, Partnern und Investoren stärken.[17] Dies ist insbesondere im B2B-Geschäft und bei der Verarbeitung personenbezogener Daten relevant.
- **Potenzielle Auswirkung auf Unternehmensbewertung:** Ein robustes Risikoprofil, erhöhte Resilienz und die Kontrolle über geistiges Eigentum und kritische Daten könnten die Bewertung eines Unternehmens positiv beeinflussen, was insbesondere für Private-Equity-Investoren oder bei einem Unternehmensverkauf relevant sein kann.
- **Beitrag zur lokalen Wirtschaft und Arbeitsplätzen:** Die Stärkung interner Kompetenzen und die bevorzugte Nutzung lokaler oder europäischer Anbieter und Dienstleister können zur Schaffung und Sicherung von Arbeitsplätzen in Deutschland und Europa beitragen.[3][6]

Tabelle 2: TCO-Szenariovergleich für ein KMU (Illustrativ)

Kostenkategorie	Szenario 1: US-Hyperscaler (IaaS/PaaS Fokus)	Szenario 2: Hybrid (EU Private Cloud + US Public Cloud)	Szenario 3: Souveräne EU-Cloud (SCS/Gaia-X basiert)	Annahmen/ Bemerkungen
Initiale Setup-/Migrations-Kosten	Mittel	Hoch	Hoch	Abhängig von Komplexität, Rehosting vs. Refactoring; Hybrid/Souverän oft mehr Integrations-aufwand initial.
Jährliche Abonnements/Lizenzen	Hoch (variabel)	Mittel (fix + variabel)	Mittel (oft transparenter)	Hyperscaler oft Pay-as-you-go, kann bei unkontrollierter Nutzung teuer werden; Private Cloud

				oft fixere Kosten.
Jährliche Infrastrukturkosten	Gering (im Abo enthalten)	Mittel (für Private Cloud Anteil)	Gering (im Abo enthalten)	On-Prem-Anteil bei Hybrid verursacht HW/SW/Betriebskosten.
Jährliche Personal-/Supportkosten	Mittel (Cloud-Skills nötig)	Hoch (Hybrid-Management komplex)	Mittel (Spezif. Skills nötig, ggf. weniger Auswahl)	Benötigt Cloud-Architekten, Security-Spezialisten, FinOps; Hybrid erfordert Management beider Welten.
Jährliche Daten-Transferkosten	Potenziell hoch (Egress)	Mittel (Inter-Cloud/On-Prem)	Gering/Mittel (Innerhalb EU oft günstiger)	Kosten für Datenbewegung aus der Public Cloud (Egress) können erheblich sein.[37]
Geschätzte Exit-Kosten (Jahr 5)	Hoch	Mittel	Gering	Proprietäre APIs/Dienste bei Hyperscalern erhöhen Exit-Kosten; Offene Standards bei SCS/Gaia-X senken sie.[69]
TCO (5 Jahre, ohne Risiken)	**Summe 1**	**Summe 2**	**Summe 3**	Summe 1 kann initial am niedrigsten erscheinen, aber Exit-Kosten und Risiken (s. Tabelle 3) müssen betrachtet werden.

Tabelle 3: Wert der Risikominderung durch Souveränität (Illustrativ)

Risiko	**Potenzielle Kosten (€)**	**Wahrscheinlichkeit (%) - Szenario 'Geringe Souveränität' (z.B. US-Hyperscaler)**	**Erwarteter Risikowert (€) - Geringe Souveränität**	**Wahrscheinlichkeit (%) - Szenario 'Hohe Souveränität' (z.B. EU-Souverän)**	**Erwarteter Risikowert (€) - Hohe Souveränität**	**Wert der Risikominderung (€)**
Datenpanne (mittelgroß)	1.000.000	10%	100.000	5%	50.000	50.000

Compliance-Verstoß (NIS2/DSGVO, signifikant)	500.000	5%	25.000	1%	5.000	20.000
Vendor Lock-in (erzwungenes Upgrade/Preiserhöhung)	100.000 (pro Jahr)	20%	20.000	5%	5.000	15.000
Service-Ausfall (Geopolitik/Anbieterproblem)	200.000 (pro Vorfall)	2%	4.000	1%	2.000	2.000
Gesamter erwarteter Risikowert (pro Jahr)			**149.000**		**62.000**	**87.000**

Hinweis: Die Zahlen in den Tabellen sind rein illustrativ und müssen für jedes KMU individuell basierend auf dessen spezifischer Situation und Risikobewertung angepasst werden.

Diese differenzierte Betrachtung zeigt, dass der Business Case für digitale Souveränität über reine Kosteneinsparungen hinausgeht und maßgeblich durch Risikominimierung und die Sicherung strategischer Handlungsfähigkeit getrieben wird.

8. Politische Imperative: Ermöglichung eines souveränen digitalen Ökosystems

Digitale Souveränität des Mittelstands entsteht im Zusammenspiel von Wirtschaft und Staat. Unternehmen können die Aufgabe nicht allein stemmen. Souveränität braucht politische Weichen. Soll digitale Souveränität umgesetzt werden, muss die Politik dies zur Priorität machen. Bund, Länder und EU müssen verlässliche Rahmen setzen: klare und durchsetzbare Regeln, interoperable Standards, wirksame Beschaffungsleitlinien, gezielte Förderung von Kompetenzen und Infrastruktur. Ziel ist ein leistungsfähiges, europäisch kontrolliertes Ökosystem aus Anbietern, offenen Schnittstellen und zertifizierten Diensten, das Investitionen erleichtert und Abhängigkeiten reduziert.

8.1. Bestandsaufnahme: Aktuelle Initiativen und Lücken in Deutschland und der EU

Es existiert bereits eine Reihe von politischen Initiativen, die das Ziel der digitalen Souveränität verfolgen:

- **Strategien & Programme:** Die Digitalstrategie der Bundesregierung nennt explizit die Stärkung der digitalen Souveränität durch Förderung von Open Source, Kompetenzausbau und Datenräumen als Ziel.[128] Das BMBF-Rahmenprogramm FITS2030 zielt auf technologische Souveränität bis 2030.[11] Die EU verfolgt mit der "Digitalen Dekade" ambitionierte Ziele für digitale Kompetenzen und Unternehmensdigitalisierung.[128] Der Digital-Gipfel der Bundesregierung thematisiert digitale Souveränität.[130]
- **Institutionen & Fonds:** Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) fördert OSS im öffentlichen Sektor.[3] Der Sovereign Tech Fund (STF) unterstützt die Entwicklung kritischer Open-Source-Infrastruktur.[128]
- **Technologieinitiativen:** Gaia-X zielt auf eine föderierte europäische Dateninfrastruktur.[5] Der European Chips Act soll die Halbleiterproduktion in Europa stärken.[128]
- **Regulierung:** Der EU Data Act, NIS2 und DORA setzen rechtliche Rahmenbedingungen, die indirekt Souveränität fördern (siehe Abschnitt 2.2).

Trotz dieser Initiativen bestehen signifikante Lücken und Herausforderungen, denn bislang wurden weder konkrete Mittel noch nationale Strategien zur Förderung verabschiedet:

- **Umsetzung:** Die Umsetzung politischer Strategien erfolgt oft langsam und zögerlich, ohne einen politischen Plan mit Budget, Zeitrahmen und Umsetzungsdruck .[47]
- **KMU-Fokus:** Förderprogramme erreichen KMU oft nicht ausreichend oder sind zu komplex.[45] Es fehlt an spezifischer, praxisnaher Unterstützung für KMU bei der Souveränitätssteigerung.
- **Gaia-X Reifegrad:** Die praktische Nutzbarkeit und breite Adoption von Gaia-X und den

Federation Services (GXFS) steht noch am Anfang. Bürokratie, Fragmentierung und eine geringe Akzeptanz bremsen das Projekt jedoch aus.[132]

- **Vergaberecht:** Das aktuelle Vergaberecht behindert oft den Einsatz von OSS und souveränen Lösungen, da der Fokus primär auf dem niedrigsten Preis liegt und Lebenszykluskosten oder strategische Aspekte zu wenig berücksichtigt werden.[9]
- **Fachkräftemangel:** Trotz politischer Bekenntnisse bleibt der Mangel an IT-Fachkräften eine massive Hürde.[46]
- **Fragmentierung:** Politische Zuständigkeiten und Initiativen sind oft fragmentiert zwischen Bund, Ländern und EU.

8.2. Konkrete Handlungsempfehlungen für die Politik

Basierend auf der Analyse ergeben sich für uns folgende konkrete Handlungsempfehlungen:

1. **Gezielte KMU-Förderung und -Unterstützung:**
    - **Ausbau und Vereinfachung von Förderprogrammen:** Programme wie "KMU.Digital" [45] sollten aufgestockt und spezifisch auf Maßnahmen zur Stärkung der digitalen Souveränität ausgerichtet werden (z.B. für Souveränitäts-Assessments, Migration zu EU-/OSS-Lösungen, NIS2-Umsetzung). Der Zugang muss für KMU unbürokratisch gestaltet werden.
    - **Praxisnahe Beratungsangebote:** Einrichtung niederschwelliger Beratungsstellen (z.B. durch Erweiterung der Mittelstand-Digital Zentren [43]), die KMU konkret bei der Architekturauswahl, Technologiebewertung und Compliance im Kontext der Souveränität unterstützen.
    - **Finanzielle Anreize:** Schaffung von steuerlichen Vorteilen oder direkten Zuschüssen für KMU, die nachweislich in zertifizierte souveräne Cloud-Lösungen oder signifikante OSS-Migrationen investieren.
2. **Stärkung europäischer Anbieter und offener Ökosysteme:**
    - **Strategische Investitionen:** Fortgesetzte und verstärkte Investitionen in Gaia-X und verwandte Initiativen wie den Sovereign Cloud Stack (SCS), um die Entwicklung und Marktdurchdringung nutzbarer Föderationsdienste und Plattformen zu beschleunigen.[5]
    - **Gezielte Förderung:** Direkte Forschungs- und Entwicklungsförderung für europäische Cloud-Anbieter und strategisch wichtige Open-Source-Projekte (z.B. über den Sovereign Tech Fund [128], Horizon Europe). Förderprogramme sollten explizit Projekte priorisieren, die Interoperabilität und offene Standards nachweisen.[3]
    - **Förderung von EU-Repositorien:** Unterstützung des Aufbaus und der Nutzung von EU-basierten Repositorien für Open-Source-Code.[3]
3. **Förderung und Verbindlichkeit offener Standards & Interoperabilität:**
    - **Mandatierung im öffentlichen Sektor:** Gesetzliche Verankerung der Nutzung

offener Standards und APIs in der öffentlichen Beschaffung und für Betreiber kritischer Infrastrukturen.[3]
    - **Stärkung europäischer Standardisierung:** Aktive Teilnahme und Förderung europäischen Einflusses in internationalen Standardisierungsgremien.[3]
    - **Unterstützung von Gaia-X Standards:** Förderung der Entwicklung und Adoption von Gaia-X-konformen Standards (GXFS) zur Sicherstellung der Interoperabilität.[61]
4. **Reform des öffentlichen Vergaberechts:**
    - **Präferenz für Souveränität und OSS:** Einführung eines expliziten Vorrangs oder eines "Comply-or-Explain"-Prinzips für Open-Source-Software und Lösungen, die nachweislich die digitale Souveränität stärken, in öffentlichen Ausschreibungen.[9]
    - **Anpassung der Zuschlagskriterien:** Berücksichtigung von Lebenszykluskosten (TCO), Exit-Kosten und strategischen Souveränitätsaspekten bei der Angebotsbewertung, statt reiner Fokussierung auf den Anschaffungspreis.[9]
    - **Öffentliche Hand als Leitmarkt:** Strategische Nutzung der öffentlichen Beschaffung zur Förderung und Etablierung souveräner Lösungen ("Lead Market"-Funktion).[3]
5. **Klärung und Durchsetzung des regulatorischen Rahmens:**
    - **Praxisleitfäden für KMU:** Erstellung klarer, verständlicher Leitfäden und Handreichungen, insbesondere für KMU, zur Interpretation und Umsetzung der Anforderungen aus NIS2, DORA und dem Data Act im Hinblick auf Cloud-Strategien und Anbieterwahl.
    - **Konsistente Durchsetzung:** Sicherstellung einer EU-weit harmonisierten Anwendung und Durchsetzung der neuen Regulierungen.
    - **Monitoring des Data Acts:** Überwachung der Wirksamkeit der Bestimmungen zu Cloud-Wechsel und Interoperabilität und ggf. Nachschärfung.
6. **Investition in souveränitätsrelevante digitale Kompetenzen und Bildung:**
    - **Bildungsinhalte anpassen:** Integration von Konzepten der digitalen Souveränität, Cybersicherheit und Open-Source-Software in die Lehrpläne von Schulen (Informatik als Pflichtfach [3]), Berufsschulen und Hochschulen.
    - **Umfassende Weiterbildungsprogramme:** Finanzierung großangelegter Upskilling- und Reskilling-Initiativen für die bestehende Erwerbsbevölkerung mit Fokus auf Cloud-Sicherheit, OSS-Management, souveräne Technologien und Compliance (z.B. NIS2-Anforderungen).[2]
    - **Förderung von Initiativen:** Unterstützung von Plattformen wie dem KI-Campus [128] und Maßnahmen zur Erhöhung der Diversität in IT-Berufen.[128]

8.3. Markt vs. Regulierung

Angesichts der Notwendigkeit, sowohl die Handlungsfähigkeit der KMU zu stärken als auch die Wettbewerbsfähigkeit zu erhalten, erscheint ein **kombinierter Ansatz** am zielführendsten.

Dieser sollte auf **ermöglichende Maßnahmen** (Förderung, Kompetenzaufbau, Infrastruktur) setzen, diese aber durch **gezielte regulatorische Anreize und Vorgaben** (insbesondere bei offenen Standards und im öffentlichen Beschaffungswesen) ergänzen, um die Entwicklung hin zu einem souveränen digitalen Ökosystem zu beschleunigen, ohne die Flexibilität der KMU übermäßig einzuschränken.

8.4 Die Notwendigkeit Digitaler Souveränität für Startups: Vom Buzzword zur Überlebensstrategie

Für die deutsche Startup-Szene ist Digitale Souveränität – die Fähigkeit zur vollständigen Selbstbestimmung über eigene Daten, IT-Infrastrukturen und digitale Prozesse – von einer strategischen Option zu einer existenziellen Notwendigkeit geworden. Angesichts geopolitischer Unsicherheiten, eines immer strengeren regulatorischen Umfelds (DSGVO, Schrems II, NIS2, DORA, EU Data Act) und einer starken Marktabhängigkeit von außereuropäischen Hyperscalern müssen Startups ihre digitale Handlungsfähigkeit proaktiv sichern.

Souveränität bedeutet dabei nicht digitale Autarkie, sondern die Fähigkeit, informierte, strategische Entscheidungen zu treffen und die Kontrolle zu wahren. Sie umfasst:

- Datensouveränität: Volle Kontrolle über die eigenen Daten und die der Kunden.
- Betriebliche Souveränität: Flexibilität in der IT ohne einen lähmenden Vendor Lock-in.
- Technologische Souveränität: Das Verständnis und die freie Wahl der eingesetzten Technologien.

Das Startup-Dilemma: Die Verlockung der schnellen Skalierung

Viele Startups sind stark von globalen Cloud-Anbietern abhängig. Der Grund ist einleuchtend: Attraktive Startprogramme und der unmittelbare Bedarf an schneller Skalierbarkeit machen die Angebote der Hyperscaler oft zur ersten Wahl. Diese anfängliche Bequemlichkeit birgt jedoch erhebliche Risiken:

- Vendor Lock-in: Eine tiefe Integration in ein einziges Ökosystem macht einen späteren Wechsel extrem teuer und komplex.
- Kostenexplosion: Nach Auslaufen der Start-Credits können die Kosten unkontrolliert steigen und Margen auffressen.
- Mangelnde Transparenz: Unklare Datenverarbeitungswege und Abhängigkeit von den Roadmaps der Anbieter.
- Regulatorischer Druck: Die komplexe Regulierungslandschaft, insbesondere die NIS2-Richtlinie mit der persönlichen Haftung der Geschäftsführung, stellt gerade Startups mit begrenzten Ressourcen vor massive Herausforderungen.

Vision: Die „Born Sovereign“-Architektur

Eine zukunftsfähige IT-Architektur für Startups muss von Anfang an auf Kontrolle, Sicherheit, Resilienz, Flexibilität und Offenheit ausgelegt sein. Die entscheidenden Lösungsansätze dafür sind:

- Open Source Software (OSS): Der strategische Einsatz von OSS (z.B. Kubernetes, Nextcloud) ist der zentrale Hebel für Startups. Er vermeidet frühzeitig Abhängigkeiten, senkt Kosten, fördert die Interoperabilität und beschleunigt Innovationen. Ein „OSS-First-Ansatz“ ist daher fundamental.
- Lean Cloud-Strategien: Anstatt sich blind einem Anbieter hinzugeben, sollten Startups auf hybride oder Multi-Cloud-Architekturen setzen. Dies ermöglicht es, für jeden Anwendungsfall den besten – und souveränsten – Anbieter zu wählen.
- Europäische Cloud-Anbieter: Die Nutzung vertrauenswürdiger europäischer Cloud-Dienste und Gaia-X-konformer Plattformen kann die Datenresidenz und die Einhaltung europäischer Rechtsnormen sicherstellen.
- Dynamische Souveränitätsstrategie: Die Souveränitätsanforderungen eines Startups ändern sich mit dem Wachstum. Die Strategie muss daher agil sein und sich anpassen können – von einer „Minimum Viable Sovereignty“ in der Anfangsphase bis zu einer robusten Architektur in der Skalierungsphase.

Roadmap zur Digitalen Souveränität: Agil und iterativ

Ein starrer Plan funktioniert für Startups nicht. Der Weg zur digitalen Souveränität muss agil und iterativ sein:

Assessment & Strategie: Sovereignty-by-Design – Von Tag eins an Souveränitätsaspekte in Produkte und Prozesse integrieren. Das bedeutet: die eigene Kern-IP schützen und eine klare „Minimum Viable Sovereignty“ definieren.

Kultur & Kompetenz: Gründerverantwortung – In Startups wird dies durch agiles Lernen und direkte Verantwortung der Gründer getragen. Sicherheit ist kein Hindernis, sondern ein entscheidendes Feature.

Technologie- & Partnerauswahl: OSS und offene Standards bevorzugen – Eine starke Präferenz für Open Source und offene Standards ist entscheidend. Jede Technologieentscheidung muss kritisch auf ihr Lock-in-Risiko geprüft werden.

Implementierung: Iterative Entwicklung – Die Umsetzung erfolgt nicht in einem „Big Bang“, sondern iterativ im Rahmen agiler Prozesse wie Scrum oder Kanban.

Optimierung: Kontinuierliche Anpassung – Mit jeder Finanzierungsrunde, jedem Wachstumsschub und jeder Skalierung muss die Souveränitätsposition überprüft und angepasst werden.

Der Business Case: Warum Souveränität Investoren anzieht und Märkte öffnet

Digitale Souveränität ist weit mehr als eine technische Notwendigkeit – sie ist ein knallharter Business Case:

Risikominimierung: Die Vermeidung horrender Strafen (bis zu 4 % des weltweiten Jahresumsatzes bei DSGVO-Verstößen, bis zu 2 % bei NIS2) und kostspieliger Datenpannen ist für kapitalsensible Startups überlebenswichtig.

Innovationskontrolle & Agilität: Unabhängigkeit von den Roadmaps der großen Anbieter ermöglicht schnellere Entwicklungszyklen – ein entscheidender Wettbewerbsvorteil.

Minderung von Lock-in-Kosten: Langfristige Sicherung der Gewinnmargen und des unternehmerischen Handlungsspielraums.

Vertrauen & Reputation: Ein „Sovereign-by-Design"-Ansatz ist ein starkes Differenzierungsmerkmal und ein klares Signal an Kunden, dass ihre Daten sicher sind.

Investoreninteresse & Marktzugang: Eine robuste Souveränitätsstrategie erhöht die Attraktivität für Investoren erheblich, da sie Geschäftsrisiken reduziert. Gleichzeitig erleichtert sie den Zugang zu stark regulierten Märkten wie dem Finanzsektor oder dem öffentlichen Sektor. Der EU Data Act soll zudem explizit Startups einen faireren Datenzugang ermöglichen und so neue Geschäftsmodelle fördern.

Ausblick: Der „Born Sovereign"-Vorteil

Die Politik ist gefordert, die Rahmenbedingungen durch gezielte Startup-Förderung und die Stärkung offener Ökosysteme zu verbessern. Für Startups selbst gilt jedoch: Souveränität muss als strategischer Vorteil begriffen werden, der von Beginn an in die Unternehmens-DNA integriert wird. Eine „Born Sovereign"-Mentalität ist der Schlüssel, um langfristig widerstandsfähigere, innovativere und global wettbewerbsfähige Unternehmen aus Europa aufzubauen.

9. Fazit: Sicherung der digitalen Zukunft des Mittelstands

Die vorliegende Analyse hat die Dringlichkeit und Komplexität der digitalen Souveränität für den deutschen Mittelstand verdeutlicht und konkrete Handlungsfelder identifiziert.

Zentrale Erkenntnisse:

- Digitale Souveränität ist für KMU angesichts geopolitischer Risiken, regulatorischer Anforderungen (insbesondere NIS2, Data Act) und Marktkonzentrationen unerlässlich geworden. Es geht nicht um Autarkie, sondern um die Wahrung von Kontrolle und strategischer Handlungsfähigkeit.
- Es besteht eine Lücke zwischen dem Wunsch nach Souveränität und der tatsächlichen Umsetzung, bedingt durch Hürden wie Vendor Lock-in, Kompetenzmangel, Ressourcenknappheit und Komplexität.
- Souveräne Lösungen bieten bislang noch nicht immer die gleichen Kosten- und Usability-Vorteile wie globale Lösungen
- Tragfähige Lösungsansätze liegen in hybriden und Multi-Cloud-Architekturen, die konsequent auf offenen Standards, Interoperabilität und Datenportabilität basieren und risikobasiert eingesetzt werden. Der strategische Einsatz von Open-Source-Software und die Nutzung vertrauenswürdiger europäischer Cloud-Anbieter sind dabei zentrale Elemente.
- Die Umsetzung erfordert eine strukturierte Roadmap, die über die reine Technologieeinführung hinausgeht und Assessment, Kompetenzaufbau, sorgfältige Partnerwahl, schrittweise Migration und vor allem ein begleitendes Change Management umfasst. Souveränität ist ein kontinuierlicher Prozess, kein einmaliges Projekt.
- Der Business Case für digitale Souveränität muss risikoadjustiert und über den gesamten Lebenszyklus betrachtet werden. Die Vermeidung von Compliance-Strafen und Lock-in-Kosten sowie die Steigerung von Resilienz und Innovationsfähigkeit sind oft entscheidender als kurzfristige Kosteneinsparungen.

Strategische Empfehlungen:

- **Für KMU:** Beginnen Sie mit einer ehrlichen Standortbestimmung und entwickeln Sie eine klare Souveränitätsstrategie. Investieren Sie gezielt in den Aufbau interner Kompetenzen und fördern Sie eine Kultur der digitalen Offenheit und Sicherheit. Gehen Sie die Migration schrittweise an, wählen Sie Technologien und Partner sorgfältig aus und legen Sie besonderen Wert auf offene Standards und Portabilität. Betrachten Sie Change Management als integralen Bestandteil des Prozesses.

  Gleichzeitig seien Sie sich bewusst: nicht alles muss zwangsläufig auf souveräner Infrastruktur betrieben werden. Wägen Sie ab, und schätzen Sie abhängig von Ihrem Geschäftsmodell und Ihrer Datenbasis das notwendige Souveränitätslevel ein.

- **Für die Politik:** Schaffen Sie verlässliche und unterstützende Rahmenbedingungen. Vereinfachen und erweitern Sie die KMU-Förderung für Souveränitätsmaßnahmen. Stärken Sie gezielt europäische Anbieter und offene Ökosysteme. Fördern und fordern Sie offene Standards und Interoperabilität, insbesondere durch eine Reform des Vergaberechts. Investieren Sie massiv in digitale Bildung und die Ausbildung von Fachkräften mit souveränitätsrelevanten Kompetenzen.

Ein Appell zur Zusammenarbeit:

Die digitale Transformation souverän zu gestalten, ist eine Gemeinschaftsaufgabe. Sie erfordert das Engagement der KMU selbst, die Unterstützung durch innovative und vertrauenswürdige Technologiepartner (insbesondere aus Europa und dem Open-Source-Bereich), die Bündelung von Interessen durch Branchenverbände und eine proaktive Politik, die die richtigen Weichen stellt. Nur durch ein konzertiertes Vorgehen kann sichergestellt werden, dass der deutsche Mittelstand auch im digitalen Zeitalter seine Stärke, Innovationskraft und Unabhängigkeit bewahrt und ausbaut. Digitale Souveränität ist kein Selbstzweck, sondern die Grundlage für eine widerstandsfähige, wettbewerbsfähige und selbstbestimmte digitale Zukunft des Wirtschaftsstandorts Deutschland.

10. Referenzen/Quellen

- VDE Positionspapier Technologische Souveränität (2020)
- vbw Studie - Digitale Souveränität und Bildung (2018)
- OSB Alliance - Manifest für digitale Souveränität (Dezember 2021)
- Deloitte Perspectives - Digitale Souveränität im öffentlichen Sektor (undatiert, ref. Rede von der Leyen 2020)
- Mittelstand Digital WertNetzWerke - Gaia-X Vorteile für KMU (Juni 2023)
- GDV - Management der Digitalen Souveränität (Dezember 2024)
- IONOS Studie - Digitale Souveränität (März 2024)
- AKDB eReport - Vertrauen in öffentliche IT-Dienstleister (Februar 2025, ref. AKDB/EY-Studie)
- ZenDiS Positionspapier – Digitale Souveränität im Vergaberecht (Juni 2024)
- IT-Planungsrat - Strategie zur Stärkung der Digitalen Souveränität (Januar 2021)
- BMBF - Technologische Souveränität (undatiert, mit Verweis auf FITS2030)
- Acatech Publikation - Digitale Souveränität Status Quo (undatiert)
- 23 Technologies Cloud - Impuls Digitale Souveränität 12
- BDI Artikel: Europas digitale Souveränität stärken (März 2022)
- AnalyticsCreator Blog - Kosten der Cloud-Abhängigkeit (August 2024)
- PwC - Europas Cloud-Souveränität in Zeiten geopolitischer Umbrüche (April 2025)
- OpenTalk News - Digitale Souveränität durch Open Source (Januar 2025)
- Bits & Bäume Publication - An Office without GAFAM? (2023)
- NIS2-Umsetzung.com - NIS2-Richtlinie Überblick (undatiert)
- ActiveMind Magazin - NIS2 & DORA (undatiert)
- Fraunhofer IESE Blog - NIS 2 Richtlinie Zusammenfassung (November 2024)
- IT-Sicherheit Online - DORA und NIS-2 Risikomanagement (Januar 2025)

- Makonis Assessments - Azure Best Practices (undatiert)
- Europäische Kommission - Data Act Explained (Januar 2025)
- Finnegan Insights - EU Data Act Implications (undatiert, Kontext Inkrafttreten Jan 2024)
- Wilson Sonsini Alert - EU Data Act Obligations (März 2025)
- Smartcar Blog - EU Data Act (undatiert)
- IAPP Resources - EU Data Act 101 (Januar 2024)
- Bitkom Cloud Report 2024 - Charts (Juli 2024)
- Bot unable to access 29 URL
- Bitkom Pressemitteilung zum Cloud Report 2024 (Juli 2024)
- Bot unable to access 30 URL
- WIK Studie - Strategische Bedeutung von Cloud-Diensten für KMU (2022)
- Grand View Research - Cloud Computing Market Size (undatiert, ref. 2024/2025 Daten)
- Bitkom Research - Cloud Computing 2024 29
- Der Digitale Faktor - Studie zu Google-Effekten (undatiert, ref. 2023 Daten)
- Mittelstand Heute - Cloud-Anwendungen: Studie zeigt Nachholbedarf (August 2023, ref. IDC/All for One Steeb)
- Beta Systems Blog - Digitale Souveränität in der öffentlichen Verwaltung (Februar 2025)
- Cloudficient Blog - What is Vendor Lock-In (undatiert)
- MDPI Paper - Cloud Vendor Lock-in Prediction Framework (Januar 2024)
- EY Pressemitteilung - Zukunft Wirtschaftsstandort 2024 (Oktober 2024)
- IDC Blog - Ten Cloud Trends 2024 (Februar 2025)
- KfW Research - Mittelstand Publikationen (Zugriff undatiert, ref. Berichte bis März 2025)
- SITSI PAC Analyst - ServiceNow/Plat4mation Mittelstand Alliance (Februar 2024)
- Fraunhofer FIT - Mittelstand-Digital Zentrum Wertnetzwerke (Projekt 2022-2025)
- IONOS Group Pressemitteilung - KMU-Digitalisierung rückläufig (Januar 2024)

- Wirtschaftsagentur Burgenland - Anschlussförderung KMU.Digital Umsetzung 2025 (undatiert)
- Bitkom Kurzpositionen 2025 (undatiert, Kontext Wahl 2025)
- Bitkom Wahlpapier zur Bundestagswahl 2025 (November 2024)
- BITMi-Positionspapier zur Bundestagswahl 2025 (Februar 2025)
- BDI Publikationsliste (Stand April 2025)
- Fraunhofer ISST - Kurzstudie Datenwirtschaft EdgeComputing (Dezember 2024)
- LANCOM Wegweiser Digitale Souveränität (Stand Sommer 2024+)
- T-Systems Insights - The Era of Sovereign Cloud (undatiert)
- Intel Builders PDF - T-Systems Open Sovereign Cloud Case Study (undatiert)
- Devoteam Success Story - WESSLING goes into cloud (undatiert)
- PKS Whitepaper - Lünendonk Studie 2024 (undatiert, ref. Studie 2024)
- Lexware Wissen - Digitalisierung KMU (undatiert)
- Mitteldeutsche IT Ratgeber - Cloud für KMU (undatiert)
- BuzzClan Blog - Cloud TCO (undatiert)
- Cisco Blog Deutschland - IDC Studie Digitalisierung KMU (Dezember 2020)
- IONOS Blog - Cloud-Trends 2025 (undatiert)
- Gaia-X Pressemitteilung - Federation Services Implementation Phase (Dezember 2021)
- Gaia-X Hub DE - Gaia-X Explained (undatiert)
- GXFS Website - GXFS Overview (undatiert)
- GXFS Website - Set of Services (undatiert, ref. Übergabe an Eclipse Sommer 2023)
- Gaia-X Whitepaper - GXFS Executive Summary (Dezember 2021)
- Eco International - Die 10 Cloud-Gebote für Unternehmen (Juli 2017)
- CRN Asia - Gartner Hybrid Cloud Forecast (November 2024)
- ConStraight - Cloud Consulting (undatiert, ref. Ignite Nov 2024)

- plusserver Blog - pluscloud open SCS (undatiert, ref. Launch Dez 2020)
- plusserver Website - Souveräne Cloud (undatiert, ref. Case Study Dr. Dienst)
- OVHcloud Website - Trusted Zone (undatiert)
- Northwest Registered Agent - Open Source vs Proprietary (undatiert)
- LPI Blog - Open Source Myth: Higher TCO (März 2023)
- Nextcloud Help Forum - Interview Sven Thomsen (Schleswig-Holstein) (April 2025)
- MyBits Blog - Europäische Alternativen zu US-Cloud-Lösungen (undatiert)
- Nextcloud Blog - German Federal Administration relies on Nextcloud (undatiert, Kontext Tender Ende 2017)
- Nextcloud Whitepapers & Case Studies (Zugriff undatiert, ref. Studien bis Juli 2024)
- ZDNET Article - Open source's big German win: Nextcloud (April 2018)
- Bundesnetzagentur - WIK Report 31
- Econstor - WIK Report 31
- ResearchGate - WIK Report Teil 2 31
- Univention Blog - Digitale Souveränität Verwaltung (März 2023)
- EGS-plan Magazin - Wie EGS-plan mit OpenProject arbeitet (April 2024)
- OpenProject Website - Fallstudie Hochschule Coburg (undatiert)
- OpenProject Website - Case Study District Office Enzkreis (undatiert)
- Caya Magazin - Projektmanagement Software Vergleich KMU (undatiert)
- OpenProject Blog - Projektmanagement-Software aus Deutschland (März 2025)
- IZA Discussion Paper - Creative Industries Start-ups (2018)
- OSS Directory News (Zugriff April 2025)
- Wirtschaftsagentur Wien - Cloud Computing Technologiereport (undatiert, ref. Daten bis 2022)
- Eurofound Report - SMEs in Vienna (2011, ref. ältere Studien)
- Univention Presse - Digitale Souveränität beim Univention Summit (Januar 2025)

- Univention Web & Press - Digital Sovereignty Univention Summit (Januar 2025)
- Univention Website - About Us (undatiert)
- Bundesnetzagentur - Förderwettbewerb Gaia-X (undatiert, ref. Sitzung Juni 2021)
- Thomas-Krenn Magazin - Univention Summit 2020 (Februar 2020)
- Agorum Partner - Univention GmbH (undatiert)
- Slideshare - Souveräner Arbeitsplatz der Öffentlichen Verwaltung (Januar 2022)
- Astera Blog - Why Proprietary Software Can Be More Cost-Effective (Juli 2021)
- Applied CCM - Deciding Between Open and Proprietary (undatiert)
- SimScale Blog - Open Source vs Proprietary Software (undatiert)
- Digitalzentrum Bau - Glossar Gaia-X (undatiert)
- Gaia-X Pressemitteilung - Summit 2024 (undatiert, Kontext Summit 2024)
- Gaia-X News Clipping (Januar 2025)
- OVHcloud Website - Data Sovereignty (undatiert)
- OVHcloud Website - Public Sector Solutions (undatiert)
- T-Systems Website - Cloud Migration Framework (undatiert)
- Econstor - WIK Studie Teil 3 31
- Storage-24 Blog - VDI für KMU (undatiert)
- Mittelstand-Digital Zentrum Smarte Kreisläufe - Leitfaden Digi-Roadmap (undatiert, Zentrum seit März 2023)
- Kion Blog - How to Build Cloud Strategy Roadmap (August 2024)
- SMK Group Insight - IT-Strategien 2025 Leitfaden (undatiert)
- Anaptis Consulting - Cloud Strategy (undatiert)
- Accenture Website - Cloud Migration Services (undatiert)
- Intero Consulting - Best of Consulting Mittelstand 2022 (undatiert, ref. Award 2022)
- Makonis Services - Cloud Migration (undatiert)

- Naviant Blog - Cloud Change Management (Januar 2024)
- Collibra Blog - Cloud Migration Change Management (März 2024)
- CAS CRM Awards (undatiert, ref. Awards bis 2018)
- Univio Blog - TCO im Cloud Computing (undatiert)
- d.velop Blog - TCO Cloud vs On-Premises (November 2022)
- DSGVO-Portal News - Rückblick Bußgelder 2023 (undatiert)
- SocialMediaStatistik.de - DSGVO Bußgelder Deutschland (März 2022, ref. Daten bis Nov 2020)
- Datenschutz-ePrivacy.de - DSGVO Bußgelder (undatiert, ref. Daten bis 2019/2020)
- Mittelstandswiki - Was Informationsverlust kostet (undatiert, ref. ältere Studien 2008)
- Varonis Blog - Data Breach Statistics (undatiert, ref. Daten bis 2021)
- Bitkom IT-Mittelstandsbericht 2024 (Oktober 2024)
- BMDV - Digitalstrategie Deutschland (Stand April 2023)
- Wikipedia - Digitalstrategie Deutschland (Zugriff undatiert, ref. Bitkom Monitor Jan 2024)
- BMI Kurzmeldung - Digital-Gipfel 2024 (Oktober 2024)
- Digitale Verwaltung - Digital-Gipfel 2024 (Oktober 2024)
- CloudAhead Sovereign Cloud Benchmark (Oktober 2023)
- Digitalverbund Bayern - Positionspapier zur Digitalen Souveränität (April 2025)
- BDI Positionen (Stand Dezember 2024)
- EY Wealth & Asset Management (undatiert)
- Digital Austria - Leitfaden Digitale Verwaltung: KI, Ethik und Recht (Dezember 2024)
- 3CX Blog - Kosten-Nutzen-Analyse Cloud-Telefonie KMU (undatiert)
- Deepset News - Gartner Cool Vendors AI Engineering (November 2024)
- AP-Verlag - Cloud und KI im Datenbanksektor (Mai 2024, ref. HarfangLab Umfrage)
- Sopra Steria Newsroom - PAC Innovation Radar KI Services (September 2024)

- Bitkom/KPMG Cloud Monitor (2012, veraltet)
- Deloitte Studie - Mittelstand und Familienunternehmen (undatiert, ref. Pandemie-Auswirkungen)
- KfW Mittelstandspanel 2024 (undatiert, ref. Daten 2023)