

DIGITALE SOUVERÄNITÄT ALS STRATEGISCHE FÜHRUNGS- AUFGABE

Wie Organisationen in DACH die Kontrolle über Daten, Betrieb und Technologie zurückgewinnen – ohne auf Innovationskraft zu verzichten.



VORWORT

Daum ein Thema wird derzeit so intensiv – und so unscharf – diskutiert wie digitale Souveränität. In Gesprächen mit Behörden und Unternehmen begegnen uns dabei immer wieder dieselbe Unsicherheit: Zwischen „Alles muss sofort in eine europäische Cloud“ und „Ohne die großen Plattformen geht es ohnehin nicht“ scheint es keine Mitte zu geben.

Genau diese Mitte existiert aber – und sie ist der Ort, an dem gute Entscheidungen getroffen werden. Digitale Souveränität entsteht nicht durch Bekenntnisse, sondern durch Architektur: durch die bewusste Entscheidung, welche Daten und Prozesse welches Maß an Kontrolle brauchen und welche Plattform dieses Maß verlässlich liefert. Dieses Whitepaper soll Ordnung in die Debatte bringen, den neuen europäischen Referenzrahmen einordnen und einen pragmatischen Weg zeigen.

Dr. Jörg Kerschbaumer
CEO Imendo GmbH

Gernot Kerschbaumer
CRO & CPO Imendo GmbH

Two handwritten signatures in blue ink. The first signature on the left is for Dr. Jörg Kerschbaumer, and the second signature on the right is for Gernot Kerschbaumer.

INHALTSVERZEICHNIS

Executive Summary	1
Souveränität wird geschäftskritisch	2
Das Problem in Zahlen	3
Was Souveränität bedeutet – und was nicht	4
Der neue europäische Referenzrahmen	5
Zwei Wege, ein Ziel: STACKIT oder Microsoft?	6
Der Weg dorthin: Kompass der digitalen Souveränität	7
Aus der Praxis	8
Fazit und nächste Schritte	9
Quellen	10

EXECUTIVE SUMMARY

Digitale Souveränität hat sich von einem politischen Schlagwort zu einer konkreten Management-Anforderung entwickelt. Regulatorische Vorgaben wie NIS2, DORA und der EU AI Act, wachsende geopolitische Spannungen und die erstmals messbare Bewertung von Cloud-Souveränität durch das EU Cloud Sovereignty Framework verändern die Spielregeln für Cloud- und KI-Entscheidungen in Wirtschaft und Verwaltung.

Zugleich gilt: Souveränität ist kein Absolutbegriff, sondern ein Spektrum – und nicht jeder Workload braucht das höchste Souveränitätsniveau. Imendo versteht digitale Souveränität deshalb als Architekturentscheidung entlang des Schutzbedarfs. Mit STACKIT und Microsoft stehen zwei leistungsfähige Wege bereit, die sich je nach Anforderung gezielt kombinieren lassen. Dieses Whitepaper zeigt, warum das Thema jetzt auf die Führungsagenda gehört, wie der neue europäische Referenzrahmen Orientierung schafft und wie ein pragmatischer Weg zu einer souveränen Zielarchitektur aussieht.

DAS WICHTIGSTE IN KÜRZE

Digitale Souveränität wird zur Management-Priorität: Neue Regulierungen wie NIS2, DORA und der EU AI Act sowie geopolitische Risiken machen sie zu einem zentralen Faktor für Cloud- und KI-Strategien.

Souveränität ist kein Entweder-oder: Der erforderliche Souveränitätsgrad hängt vom Schutzbedarf der jeweiligen Daten, Anwendungen und Geschäftsprozesse ab.

Der neue europäische Referenzrahmen schafft Orientierung: Das EU Cloud Sovereignty Framework ermöglicht erstmals eine strukturierte Bewertung und Vergleichbarkeit von Cloud-Souveränität.

Pragmatische Zielarchitekturen kombinieren Stärken: Mit STACKIT und Microsoft stehen komplementäre Lösungsansätze zur Verfügung, die je nach Anforderung flexibel und souverän eingesetzt werden können.

SOUVERÄNITÄT WIRD GESCHÄFTSKRITISCH

Drei Entwicklungen erhöhen den Handlungsdruck.

1. REGULATORIK

NIS2, DORA, der EU AI Act und der Data Act stellen wachsende Anforderungen an Kontrolle, Nachvollziehbarkeit und Resilienz digitaler Infrastrukturen. Mit dem Cloud Sovereignty Framework hat die EU-Kommission Souveränität zudem erstmals messbar gemacht. Souveränität wandelt sich damit von einer Haltung zu einem harten Vergabe- und Compliance-Kriterium.

Digitale Souveränität verbindet dabei mehrere Ebenen: anwendbares Recht, Kontrolle über Daten und Schlüssel, operative Handlungsfähigkeit, Transparenz der Lieferkette, technische Portabilität sowie Sicherheit und Compliance. Genau diese Mehrdimensionalität bildet das EU Cloud Sovereignty Framework in acht Souveränitätszielen ab (Europäische Kommission, 2025).

2. TECHNOLOGISCHE ABHÄNGIGKEIT

Technologische Abhängigkeit wird zunehmend als Geschäftsrisiko wahrgenommen. Ein europäischer Serverstandort ist ein wichtiger Baustein für Datenresidenz, beantwortet aber nicht allein Fragen zu Kontrolle, Betriebszugriffen, Schlüsselverwaltung, Lieferketten und anwendbarem Recht. Diese Dimensionen sollten für jeden Workload gemeinsam bewertet werden.

3. KÜNSTLICHE INTELLIGENZ

KI verschärft die Frage: Wer künstliche Intelligenz auf sensiblen Unternehmens- oder Verwaltungsdaten betreiben will, muss beantworten können, wo Daten und Modelle laufen, wer darauf zugreifen kann und unter welchem Recht dieser Zugriff steht.



DAS PROBLEM IN ZAHLEN

Der Handlungsdruck ist nicht nur qualitativ spürbar, sondern empirisch belegt. Die folgenden Kennzahlen stammen überwiegend aus dem Bitkom Cloud Report 2026 sowie aus Veröffentlichungen der Europäischen Kommission.

ABHÄNGIGKEIT:

85 % der deutschen Unternehmen halten Deutschland für zu abhängig von US-Cloud-Anbietern (Bitkom, 2026)

→ **Abhängigkeit wird als strategisches Risiko wahrgenommen – Tendenz steigend (Vorjahr: 78 %).**

WUNSCH VS. REALITÄT:

91 % würden Cloud-Anbieter aus Deutschland bevorzugen – 71 % nutzen US-Hyperscaler (Bitkom, 2026)

→ **Zwischen Anspruch und gelebter Architektur klafft eine strukturelle Lücke.**

HANDLUNGSDRUCK:

64 % fühlen sich durch die US-Politik unter Druck, ihre Cloud-Strategie zu überdenken (Bitkom, 2026)

→ **Souveränität ist im Management-Alltag angekommen – nicht nur in der IT.**

ALTERNATIVEN:

43 % sehen für ihre Anforderungen keine gleichwertigen europäischen Alternativen (Bitkom, 2026).

→ **Die Antwort ist selten „alles oder nichts“, sondern eine differenzierte Architektur.**

RESILIENZ:

Nur rund 12 Monate könnten Unternehmen nach eigener Einschätzung ohne US-Technologien operieren (Bitkom, 2025).

→ **Exit-Fähigkeit und Notfallszenarien gehören in jede Cloud-Strategie**

MESSBARKEIT:

180 Mio. EUR: erste EUCloud-Vergabe nach dem Cloud Sovereignty Framework mit Mindestniveau SEAL-2 (EU-Kommission, 2026).

→ **Souveränität ist erstmals ein messbares Beschaffungskriterium.**

WAS SOUVERÄNITÄT BEDEUTET UND WAS NICHT

1 Standort ist nicht Souveränität: Ein europäisches Rechenzentrum eines Nicht-EU-Anbieters löst die Jurisdiktionsfrage nicht, solange ausländisches Recht auf den Betreiber durchgreift.

2 Souveränität ist nicht Autarkie: Vollständige Unabhängigkeit über die gesamte Lieferkette – von Chips bis Software – ist auch für europäische Anbieter nicht realistisch; entscheidend ist bewusste Kontrolle über die kritischen Ebenen.

3 Es gibt nicht ein Souveränitätsniveau für alles: Workloads unterscheiden sich in Schutzbedarf, Regulierung und Geschäftskritikalität – und sollten entsprechend differenziert zugeordnet werden.

Digitale Souveränität ist zudem mehrdimensional. Sie umfasst rechtliche, technische, organisatorische und sicherheitsrelevante Aspekte, die gemeinsam bewertet werden müssen. Der Grad an Souveränität ergibt sich daher nicht aus einer einzelnen Maßnahme oder Technologie, sondern aus dem Zusammenspiel verschiedener Kontroll- und Steuerungsmechanismen. Diesem Grundgedanken folgt auch das europäische Cloud Sovereignty Framework mit seinen acht Souveränitätszielen.



DER NEUE EUROPÄISCHE REFERENZRAHMEN

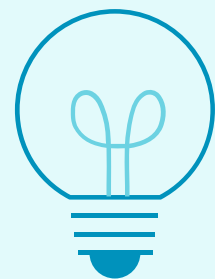
Mit dem Cloud Sovereignty Framework (CSF) hat die Generaldirektion Informatik (DG DIGIT) der Europäischen Kommission im Oktober 2025 ein einheitliches Bewertungsmodell für Cloud-Souveränität geschaffen. Es definiert fünf Sovereignty Effectiveness Assurance Levels (SEAL-0 bis SEAL-4) und ermöglicht es, Mindestanforderungen für unterschiedliche Workloads festzulegen (Europäische Kommission, 2025).

Bereits im April 2026 setzte die Europäische Kommission das Framework bei einer Cloud-Vergabe mit einem Gesamtvolumen von bis zu 180 Millionen Euro ein. Dabei erreichte STACKIT SEAL-3 („Digital Resilience“), das Konsortium um Proximus/S3NS SEAL-2 (Europäische Kommission, 2026).

Das Framework ersetzt keine individuelle Risikoanalyse, schafft aber eine gemeinsame Sprache für Architektur-, Beschaffungs- und Governance-Entscheidungen. Ergänzend hat das BSI mit C3A (Criteria enabling Cloud Computing Autonomy) einen deutschen Bewertungsrahmen veröffentlicht, der Struktur und Zielsetzung des europäischen Modells aufgreift (BSI, 2026).

Für Entscheider bedeutet das: Nicht die pauschale Bewertung eines Anbieters ist ausschlaggebend, sondern die Frage, ob dessen Kontrollen zu den Anforderungen eines konkreten Workloads passen. Das BSI empfiehlt daher eine risikokontextbezogene Bewertung der Souveränitätseigenschaften eines Cloud-Dienstes (BSI, 2026).

- 8 Souveränitätsziele als gemeinsamer Referenzrahmen
- 5 SEAL-Stufen machen Souveränität messbar
- Bereits in EU-Vergaben eingesetzt (bis zu 180 Mio. Euro Volumen)
- Schutzbedarf bestimmt das Niveau, nicht der Anbieter
- C3A überträgt die Logik nach Deutschland
- Entscheidend sind konkrete Kontrollen, nicht Herkunft oder Marketingversprechen.



ZWEI WEGE, EIN ZIEL

STACKIT ODER MICROSOFT?

Imendo ist bewusst kein Evangelist einer einzelnen Plattform. Als Partner von STACKIT und Microsoft bewerten wir vendor-agnostisch, welcher Ansatz zum Schutzbedarf, zur Regulierung und zur vorhandenen IT-Landschaft einer Organisation passt.

STACKIT bietet als europäische Cloud-Plattform höchste Jurisdiktionssicherheit und wurde in der ersten EU-Vergabe mit SEAL-3 („Digital Resilience“) bewertet (Europäische Kommission, 2026). Microsoft hat sein Souveränitätsportfolio mit Angeboten wie Sovereign Public Cloud, Sovereign Private Cloud und nationalen Partner-Clouds für regulierte Bereiche deutlich erweitert.

Entscheidend ist jedoch nicht, ob eine Plattform pauschal als „souverän“ gilt. Maßgeblich sind die konkreten Kontrollen, etwa Datenresidenz, Schlüsselverwaltung, Zugriffssteuerung, Betriebsautonomie und Portabilität. Welche Restrisiken verbleiben, hängt vom jeweiligen Betriebs-, Daten- und Rechtskontext ab. Das BSI empfiehlt daher eine risikokontextbezogene Bewertung der Souveränitätseigenschaften eines Cloud-Dienstes (BSI, 2026).

DESHALB IST DIE PLATTFORMWAHL EINE ENTSCHEIDUNG ENTLANG VON 5 KRITERIEN

- 1 Schutzbedarf und Datenklassifizierung:** Welche Daten und Prozesse brauchen welches Souveränitätsniveau?
- 2 Jurisdiktions- und Regulierungsrisiko:** Branche, kritische Infrastruktur, Vergaberecht und Aufsichtsanforderung.
- 3 Bestandslandschaft und Skills:** Vorhandene Investitionen, Integrationstiefe und verfügbare Kompetenzen im Team.
- 4 Funktionsbedarf und Innovationstempo:** Benötigte KI-Services, PaaS-Tiefe und Release-Geschwindigkeit.
- 5 Plattform ausrichten:** Exit-Fähigkeit und Betriebsmodell: Portabilität, offene Standards und realistische Notfallszenarien.

In der Praxis lautet die Antwort häufig: hybrid. Hochsensible Workloads laufen souverän auf europäischer Infrastruktur, Standard-Workloads mit souveränen Kontrollen in der Hyperscaler-Welt – verbunden durch eine gemeinsame Daten- und Sicherheitsarch.

ORIENTIERUNG STATT AKTIONISMUS

KOMPASS DER DATENSTRATEGIE

Viele Organisationen wissen, dass sie ihre Daten besser nutzen müssen. Schwieriger ist die Frage, wo der größte Hebel liegt.

Hinzu kommt: Datenstrategie betrifft nicht nur Technologie, sondern gleichermaßen Organisation, Prozesse und Verantwortlichkeiten.

Ohne klare Prioritäten drohen Initiativen zu versanden oder parallel nebeneinander zu laufen. Genau dafür haben wir den Imendo Datenstrategie-Kompass entwickelt. In einem strukturierten Vorgehen schaffen wir Transparenz über den aktuellen Reifegrad, identifizieren die wichtigsten Handlungsfelder und entwickeln ein Zielbild, das Business-Anforderungen, Organisation, Daten und Technologie miteinander verbindet.

Standortbestimmung

1

Ausgangslage, Zielbild und Prioritäten klären. Ambition und Realität

Use-Case-Workshop

2

Relevante KI Use Cases entwickeln, bewerten und fokussieren.

Daten & Plattform Check

3

Datenlage, Systemlandschaft und Governance prüfen.

Roadmap & Vision

4

Initiativen priorisieren und nächste Schritte festlegen.

KI MACHT DATENSTRATEGIE ZUR FÜHRUNGSAUFGABE



KI-Reifegradbild

Klarer Überblick über Daten, Prozesse und Technologie



Daten- & Governance-Bewertung

Transparenz über Voraussetzungen und Risiken



Priorisierte Use Cases

echter Business-Nutzen, realistische Umsetzbarkeit



Zielbild & Architekturleitplanken

Orientierung für Technologie- und Plattformentscheidungen



Umsetzungsroadmap

Konkreter Plan für die nächsten 90 bis 180 Tage



KI macht Datenstrategie zur Führungsaufgabe

AUS DER PRAXIS

Dass dieser strukturierte Weg funktioniert, zeigt eine Referenz aus dem öffentlichen Sektor. Gemeinsam mit zam Steiermark, einem Tochterunternehmen des Arbeitsmarktservice Österreich, hat Imendo die Grundlage für eine datenbasierte und souveräne Nutzung digitaler Technologien geschaffen.

Im Fokus standen die strukturierte Aufbereitung und Nutzung bestehender Datenbestände, die Schaffung transparenter Entscheidungsgrundlagen sowie der Aufbau organisatorischer Kompetenzen für die weitere Digitalisierung und den künftigen KI-Einsatz. Das Ergebnis: verbesserte Datenverfügbarkeit, effizientere Prozesse und eine belastbare Basis für datengetriebene Innovationen. Das Projekt zeigt exemplarisch, dass nachhaltige Wertschöpfung nicht mit einer Technologieentscheidung beginnt, sondern mit einer klaren Strategie, einer soliden Datenbasis und einem strukturierten Vorgehen.

„Mit Imendo stärken wir bei zam Steiermark unsere digitale Souveränität spürbar – praxisnah, datenbasiert und mit klarem Mehrwert für unsere Teilnehmer:innen.“

Mag.a Renate Frank, Geschäftsführerin zam Steiermark GmbH

WAS DAS FÜR DAS TOP-MANAGEMENT BEDEUTET

Für die Unternehmensführung ergeben sich drei klare Konsequenzen.

1. Souveränität muss vor der nächsten großen Cloud

– oder KI-Investition geklärt werden – nachträgliche Korrekturen sind teuer und langsam.

2. Die Frage lautet nicht „Hyperscaler oder Europa“,

sondern welcher Workload welches Souveränitätsniveau braucht; Lagerdenken ersetzt keine Architektur.

3. Die neue Messbarkeit sollte aktiv genutzt werden

– SEAL-Logik gehört in Lastenhefte, Verträge und Exit-Klauseln.

Für Beschaffung und Vertragsgestaltung bedeutet das: Souveränität sollte nicht nur als Standortanforderung formuliert werden. Relevant sind auch Prüf- und Auditrechte, Nachweise zur Schlüssel- und Zugriffskontrolle, Anforderungen an Subunternehmer und Lieferketten, Exit- und Migrationsszenarien sowie Mindestniveaus je Workload-Klasse. Der CSF bietet dafür eine anschlussfähige Struktur (Europäische Kommission, 2025; BSI, 2026).

Organisationen, die diesen Rahmen früh setzen, gewinnen Handlungsfähigkeit, Verhandlungsmacht gegenüber Anbietern und eine belastbare Grundlage für KI-Vorhaben. Organisationen, die darauf verzichten, riskieren regulatorische Überraschungen, ungeplante Migrationskosten und strategische Abhängigkeiten.

NÄCHSTE SCHRITTE

Die Einführung von Künstlicher Intelligenz ist heute vor allem eine strategische und organisatorische Herausforderung. Nachhaltiger Nutzen entsteht durch klare Ziele, priorisierte Anwendungsfälle sowie eine solide Daten- und Governance-Basis. Viele gescheiterte Pilotprojekte zeigen, dass reine Tool-Einführungen selten erfolgreich sind. Zugleich erhöhen Wettbewerbsdruck und Regulierung, etwa durch den EU AI Act, den Handlungsbedarf. Erfolgreiche KI-Initiativen verbinden Business Case, Datenreife, Governance und Mitarbeiterbefähigung. Ein strukturierter Ansatz wie der Imendo KI-Kompass unterstützt dabei, Potenziale zu bewerten und Prioritäten festzulegen. Ent

ÜBER IMENDO

Imendo ist ein IT-Beratungs- und Softwareunternehmen mit Standorten in Klagenfurt, Wien und Berlin. Unter dem Leitgedanken „data driven transformation“ unterstützt Imendo Unternehmen und öffentliche Verwaltungen dabei, datenbasierte Entscheidungen zu treffen, digitale Souveränität auszubauen und das Potenzial von Künstlicher Intelligenz zu nutzen. Das Leistungsspektrum umfasst Datenmanagement & KI, Prozessautomatisierung, digitale Zusammenarbeit sowie individuelle Softwareentwicklung. Imendo begleitet Kunden von der Datenstrategie über die technische Umsetzung bis zur Weiterentwicklung ihrer Lösungen und setzt dabei auf Technologien von Microsoft, Databricks, STACKIT und Peakboard. Die ISO-27001-Zertifizierung steht für hohe Standards bei Informationssicherheit und Qualität.



IHRE ANSPRECHPARTNER



Imendo Deutschland

Dr. Norman Bernhardt
Geschäftsführer
Imendo Deutschland
norman.bernhardt@imendo.com
+49 (0) 30 166360301



Imendo Österreich

Martin Zimmermann
Team Lead Sales
martin.zimmermann@imendo.com
+43 5 7076 399

Bereit für Ihre maßgeschneiderte KI-Strategie? Dann kontaktieren Sie uns gerne!

QUELLEN

Bitkom e. V. (2025): Europas Weg in die digitale Souveränität. Presseinformation, 13. November 2025. Verfügbar unter: <https://www.bitkom.org/Presse/Presseinformation/Europas-Weg-digitale-Souveraenitaet> (abgerufen am 7. August 2026).

Bitkom e. V. (2026): Cloud Report 2026. Studienbericht, 17. Juni 2026. Verfügbar unter: <https://www.bitkom.org/Bitkom/Publikationen/Cloud-Report-2026> (abgerufen am 7. August 2026).

Bundesamt für Sicherheit in der Informationstechnik – BSI (2026): C3A – Criteria enabling Cloud Computing Autonomy. 27. April 2026. Verfügbar unter: <https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A.html> (abgerufen am 7. August 2026).

Europäische Kommission (2025): Cloud Sovereignty Framework – Implementation Guidance. Directorate-General for Digital Services (DG DIGIT), Oktober 2025. Verfügbar unter: https://commission.europa.eu/documentdownload/2ad80a48-166f-4c77a513-80c53ca2a128_enfilename=Cloud%20Sovereignty%20Framework%20-%20Implementation%20guidance.pdf (abgerufen am 7. August 2026).

Europäische Kommission (2026): Commission Advances Cloud Sovereignty Through Strategic Procurement. 17. April 2026. Verfügbar unter: https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en (abgerufen am 7. August 2026).

Microsoft (2026a): What Is Microsoft Sovereign Cloud? Microsoft Learn. Verfügbar unter: <https://learn.microsoft.com/de-de/azure/azure-sovereign-clouds/microsoft-sovereign-cloud> (abgerufen am 7. August 2026).

Microsoft (2026b): Capabilities of Sovereign Public Cloud. Microsoft Learn. Verfügbar unter: <https://learn.microsoft.com/en-us/azure/azure-sovereign-clouds/public/sovereign-public-cloud-capabilities> (abgerufen am 7. August 2026).

Microsoft (2026c): What Is Microsoft 365 Local on Azure Local Infrastructure? Microsoft Learn. Verfügbar unter: <https://learn.microsoft.com/en-us/azure/azure-sovereign-clouds/private/m365-local/microsoft-365-local-overview> (abgerufen am 7. August 2026).

STACKIT (2026): EU Commission Selects STACKIT. Unternehmensmeldung. Verfügbar unter: <https://stackit.com/en/news/eu-commission-selects-stackit> (abgerufen am 7. August 2026).

imendo

datadriven transformation für Unternehmen
und öffentliche Verwaltung

Wien · Klagenfurt · Berlin