GovImpact
Policy Paper

Souveräne Cloud: Handlungsfähigkeit der Verwaltung stärken

Digital Service

NExT

Dieses Projekt wird gefördert durch

STIFTUNG MERCATOR

EXECUTIVE SUMMARY

Der Cloud-Bedarf der Verwaltung steigt stark an, doch der Markt wird von außereuropäischen Anbietern dominiert. Geopolitische Risiken wie Datenzugriffe oder Accountsperren durch Drittstaaten-Sanktionen bedrohen die staatliche Handlungsfähigkeit. Der Umstieg auf souveräne Alternativen ist in der Praxis jedoch erschwert: Europäische Anbieter können aufgrund fehlender Skaleneffekte oft nicht die funktionale Tiefe der Marktführer bieten. Zudem fehlen in den Behörden IT-Spezialist:innen, um den dadurch entstehenden Mehraufwand zu bewältigen. Produktbündelungen und andere Barrieren erschweren zusätzlich den Anbieterwechsel.

Mangels zentraler Steuerung führen unkoordinierte Einzelbeschaffungen zu strategischen Unsicherheiten, während eine ausgeprägte Risikoaversion in der Verwaltung die Transformation blockiert.

Das im April 2026 eingeführte C3A-Framework des Bundesamts für Sicherheit in der Informationstechnik (BSI) ermöglicht zwar erstmals die strategische, rechtliche und technologische Prüfung von Cloud-Souveränität in sechs Dimensionen, kann die bestehenden strukturellen Herausforderungen und Zielkonflikte jedoch nicht allein auflösen.

Daher empfiehlt dieses Papier Maßnahmen auf vier Ebenen:

- **Transparenz & Messung:** Die Bundesverwaltung benötigt ein klares Lagebild von Abhängigkeiten. Dafür müssen die geplanten Beschaffungsvorgänge des IT-Zustimmungsvorbehalts genutzt werden, um Abhängigkeiten ressortübergreifend und systematisch zu erfassen. Ein Risiko-Stufenmodell priorisiert anstehende Migrationen nach Reichweite und Schutzbedarf, zum Beispiel mit Fokus auf Arbeitsplätze und KI.

- **Finanzierung & Unterstützung:** Zur praktischen Umsetzung sollte ein zweckgebundener Souveränitätsfonds nach dem Vorbild des Effizienzfonds aufgebaut werden. Um den Fachkräftemangel in lokalen Behörden auszugleichen, unterstützen Roll-in-Teams die Umsetzung und fördern den Kompetenzaufbau.

- **Marktsteuerung:** Der IT-Zustimmungsvorbehalt muss als Steuerungsinstrument genutzt werden, um den Staat als Ankerkunden für souveräne Anbieter zu positionieren. Sollte eine Vergabe an Hyperscaler unvermeidbar sein, müssen technisch geprüfte Exit-Strategien vorgelegt werden. Offene Standards wie die Deutsche Verwaltungscloud (DVC) und der Sovereign Cloud Stack (SCS) müssen verbindlich durchgesetzt werden.

- **Kulturwandel:** Die Förderung offener Ökosysteme muss strukturell als Erfolg gewertet und der Wechsel zu souveränen Lösungen belohnt werden. Dafür ist die konsequente Umkehr der Begründungspflicht notwendig: Nicht der Einsatz souveräner Lösungen, sondern das Eingehen neuer Abhängigkeiten braucht eine zwingende Rechtfertigung.

Souveränität ist kein statischer Zustand, sondern ein ständiger Prozess des Risikomanagements. Sie kann operativ nur umgesetzt werden, wenn die Regierungsspitze durch ein klares politisches Mandat die notwendigen Ressourcen sichert.

Dieses Papier ist Teil der Reihe GovImpact, einer Kollaboration zwischen NExT e. V. und DigitalService des Bundes, die durch die Stiftung Mercator gefördert wird. Die Inhalte wurden in Workshops, Umfragen und semistrukturierten Interviews erhoben, die beide Kollaborationspartner zum Teil gemeinsam durchgeführt haben.

Ein herzlicher Dank gilt den Expert:innen beim Accenture Kompetenzzentrum für Digitale Souveränität, beim Bundesamt für Soziale Sicherung, beim Bundesamt für Sicherheit in der Informationstechnik, der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, dem Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend und der Kommunalen Gemeinschaftsstelle für Verwaltungsmanagement. Ebenso bedanken wir uns bei Dr. h.c. Marit Hansen (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein), Mark Neufurth, Paul Rosenthal, Sofie Schönborn (Schwarz Digits), Friederike Zelke (VanillaCore) sowie insbesondere Anke Domscheit-Berg. Ihre wertvollen Umsetzungserfahrungen sind maßgeblich in die Erkenntnisse dieses Papiers eingeflossen.

1. EINLEITUNG: SOUVERÄNE CLOUD FÜR VERTRAUENSWÜRDIGE STAATLICHE LEISTUNGEN

Die Handlungsfähigkeit, Agilität und Vertrauenswürdigkeit der deutschen Verwaltung hängen maßgeblich von verlässlichen IT-Infrastrukturen ab. Vor diesem Hintergrund steigt der Bedarf an Cloud-Kapazitäten. Ob für die flexible Skalierung von Software, die Anpassung an Lastspitzen oder die Integration von Künstlicher Intelligenz (KI) in Behördenprozesse – 53 Prozent der öffentlichen IT-Dienstleister planen den Ausbau ihrer Cloud-Angebote.[1] Gleichzeitig entsteht eine kritische Asymmetrie: Während die Verwaltung auf Cloud-Lösungen angewiesen ist, fehlt die Kontrolle über die zugrunde liegende Infrastruktur – häufig verschärft durch den Fachkräftemangel.

Digitale Souveränität ist vor diesem Hintergrund kein Selbstzweck, sondern eine zentrale Daueraufgabe des Risikomanagements. Jede Cloud-Strategie beinhaltet letztlich die Abwägung, welchen Akteuren der Staat den Zugriff auf sensible Daten überlässt. Laut dem Souveränitätsbarometer von next:public schätzen 65 Prozent der befragten Verwaltungsmitarbeitenden die Abhängigkeit ihrer Organisation von außereuropäischen IT-Anbietern als stark oder sehr stark ein.[2] Solche Abhängigkeiten und die damit einhergehenden Risiken wie unautorisierte Datenzugriffe oder politische Einflussnahme gefährden nicht nur die Akzeptanz von Services in der Bevölkerung, sondern bedrohen auch die staatliche Handlungsfähigkeit.[3]

---

1 next:public (2025) Souveränitätsbarometer der öffentlichen IT Eine Studie zur digitalen Souveränität in der Verwaltung. https://nextpublic.de/wp-content/uploads/2025/12/Souveraenitaetsbarometer_der_oeffentlichen_IT.pdf, S. 31.

2 next:public (2025), S. 12.

3 Wachsmann, D.; Goldacker, G.; Hartmann, H.; Opiela, N.; Schmitz, C.; Weber, M.; Weidner, C. (2025) Digitale Souveränität und grosse Sprachmodelle in der Bundesverwaltung. Kompetenzzentrum Öffentliche IT, Fraunhofer Fokus. https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet-und-grosse-sprachmodelle-in-der-bundesverwaltung/Digitale%20Souver%c3%a4nit%c3%a4t%20und%20grosse%20Sprachmodelle%20in%20der%20Bundesverwaltung.pdf, S. 25.

Die Politik hat dieses Risiko erkannt. Die Digitalministerkonferenz bezeichnete die digitale Souveränität als „eine grundlegende Voraussetzung für die technologische und wirtschaftliche Wettbewerbsfähigkeit und Sicherheit Deutschlands und Europas“.[4] Auch im Koalitionsvertrag ist sie verankert.[5] Souveränität bedeutet, dass die Verwaltung in der Lage sein muss, „ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.[6] 46 Prozent der Verwaltungen planen, digitale Souveränität durch Einführung eigener Cloud-Infrastruktur oder die Nutzung von souveränen Cloud-Angeboten zu erhöhen.[7] Zwar nutzen 64 Prozent der öffentlichen IT-Dienstleister zumindest teilweise europäische Anbieter,[8] doch die Abhängigkeit von außereuropäischen Anbietern bleibt hoch.

Das liegt auch daran, dass das Risikomanagement der deutschen Verwaltung lange Zeit einem technischen Fokus folgte: der Informationssicherheit. Die Sicherheitsanforderungen für Clouds sind – zumindest für Bundesbehörden – durch den IT-Grundschutz-Baustein OPS.2.2[9] und den Mindeststandard des Bundesamts für Sicherheit in der Informationstechnik (BSI)[10] klar definiert und verbindlich. Der C5-Kriterienkatalog des BSI,[11] der Mindestanforderungen an die Informationssicherheit festlegt,[12] hat sich auf europäischer Ebene als zentraler Standard etabliert. Da die Clouds der Hyperscaler die C5-Anforderungen oder relevante ISO-Normen, wie etwa ISO/IEC 27001, meist erfüllen, blieben geopolitische Abhängigkeiten hingegen weitgehend unberücksichtigt. Die Datenschutzkonferenz (DSK) setzte bereits 2023 mit eigenen Kriterien einen wichtigen Impuls.[13] Als primär rechtlicher Prüfrahmen entfalteten die DSK-Kriterien jedoch wenig Wirkung in der Beschaffung und Marktsteuerung.

Mit dem im April 2026 vorgestellten C3A-Framework (Criteria enabling Cloud Computing Autonomy)[14] schließt das BSI diese Lücke. Es liefert konkrete Ansatzpunkte, um Souveränität über effektive Kontrolle, operative Unabhängigkeit und Lieferketten zu prüfen und bietet somit den Rahmen, um Souveränität in der Praxis umzusetzen.[15]

---

4 Konferenz der Regierungschefinnen und Regierungschefs der Länder am 12. März 2025 in Berlin (2025) https://www.ministerpraesident.sachsen.de/ministerpraesident/07_TOP2_Beschluss_MPK_RS.pdf, S. 2.

5 CDU, CSU und SPD (2025) Verantwortung für Deutschland. Koalitionsvertrag. https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf, S. 67.

6 ÖFIT (2017) Digitale Souveränität, https://www.oeffentliche-it.de/publikationen/digitale-souveraenitaet/Digitale%20Souver%C3%A4nit%C3%A4t.pdf, S. 3. Diese Definition wurde auch vom IT-Planungsrat genutzt. Das BMDS überarbeitet jedoch momentan die Definition, um einen stärkeren Fokus auf Wechselfähigkeit zu legen.

7 next:public (2025), S. 35.

8 next:public (2025), S. 11.

9 BSI (2023) OPS.2.2 Cloud-Nutzung. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/04_OPS_Betrieb/OPS_2_2_Cloud-Nutzung_Edition_2023.pdf?__blob=publicationFile&v=3

10 BSI (2022) Mindeststandard des BSI zur Nutzung externer Cloud-Dienste https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html.

11 BSI (2026) C5:2026. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_2025/C5_2025_node.html.

12 Ein C5-Testat erhalten Cloud-Anbieter durch eine externe Prüfung. Eine formelle Zertifizierung durch das BSI erfolgt nicht und ist aufgrund des hohen personellen Aufwands auch nicht wahrscheinlich.

13 DSK (2023) Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf.

14 BSI (2026) C3A - Criteria enabling Cloud Computing Autonomy https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A_node.html.

15 Dennoch ist die konkrete Operationalisierung, etwa bei der Frage einer Unternehmenszentrale, noch nicht bei allen Kriterien abschließend geklärt.

BSI C3A – Kriterien für Cloud-Autonomie

Die Kriterien sind modular aufgebaut und können somit an die Schutzbedarfe und Risikokontexte der Anwender:innen angepasst werden.

1. **Strategisch (SOV-1):** Fokus auf Gerichtsstand (EU/DE), Hauptsitz und effektive Unternehmenskontrolle.
2. **Rechtlich (SOV-2):** Regelung von Audit-Rechten für Behörden und Möglichkeiten zur Übernahme des Betriebs im Verteidigungsfall.
3. **Daten (SOV-3):** Kontrolle über Speicherorte, Verschlüsselung (z. B. externes Key-Management) und Identitätsmanagement.
4. **Operativ (SOV-4):** Anforderungen an Betriebspersonal, Standorte von Security Operations Centers und die Fähigkeit zur Trennung von Netzwerken.
5. **Lieferkette (SOV-5):** Transparenz über Abhängigkeiten bei Software, Hardware und externen Dienstleistern.
6. **Technologisch (SOV-6):** Verfügbarkeit des Quellcodes und Sicherstellung der kontinuierlichen Dienstleistung bei Ausfall Dritter, wie etwa externer Softwarehersteller.

Unsicherheit lähmt Handlungsfähigkeit

Trotz der politischen Ambitionen für digitale Souveränität klafft in der Umsetzung eine Lücke, die auch die neue Prüfbarkeit nicht allein schließen kann. Denn der politische Wille zur Souveränität kollidiert mit strukturellen Gegebenheiten und einer gewachsenen Entscheidungskultur, die durch Verantwortungsdiffusion geprägt ist. In den von uns geführten Interviews beschreiben Verwaltungsmitarbeitende eine strukturelle Lähmung: Da die bestehenden Vorgaben – einschließlich der C3A-Kriterien – nicht vollumfänglich verbindlich sind, verbleibt die Last der Risikoabwägung bei den Mitarbeitenden auf Umsetzungsebene.

Die Interviews zeigen, dass dieser Druck defensive Entscheidungen begünstigt, die primär auf die eigene Absicherung abzielen. Mitarbeitende ziehen sich entweder komplett auf vermeintlich sicherere On-Premises-Strukturen zurück oder greifen zum global etablierten Produkt. Die Angst vor individuellen Fehlentscheidungen konserviert somit den Status quo oder verfestigt die Abhängigkeiten der Gesamtorganisation. Drei Hürden verschärfen diese Problematik weiter:

I. Fehlende technologische Reife und zusätzlicher Integrationsbedarf bei europäischen Alternativen

Ein zentrales Hindernis für den Umstieg auf europäische Alternativen ist deren oft geringere funktionale Tiefe im Vergleich zu globalen Marktführern. US-Hyperscaler sind oft schon viele Jahre am Markt, profitieren von Skaleneffekten[16] und können auf hochqualifiziertes Personal und umfassende finanzielle Mittel zurückgreifen. Im Gegensatz dazu zeigen unsere Interviews, dass der Einsatz souveräner Lösungen derzeit mit einem höheren Integrations- und Personalaufwand einhergeht, der häufig nicht aufzubringen ist.

16 Manganelli, A. (2026) Gatekeeper in der Cloud, Konrad-Adenauer-Stiftung https://www.kas.de/de/einzeltitel/-/content/gatekeeper-in-der-cloud.

Der Fachkräftemangel verschärft das Problem: Er drängt viele Organisationen in die Cloud, da Kapazitäten für den Eigenbetrieb fehlen. Gleichzeitig mangelt es oft an spezialisierter Expertise, um die damit verbundenen, langfristigen Risiken fundiert abzuwägen. Da zudem unterstützende Strukturen wie gewachsene Support-Communities oder geteiltes Wissen in diesem Bereich noch im Aufbau sind, erscheinen die Komplettpakete globaler Hyperscaler als die einfachere und risikoärmere Lösung.

Wie der DigitalService zusätzliche Integrationsbedarfe durch eine Plattformpauschale abbildet

Als Dienstleister für Bundesministerien spielt Souveränität auch für den DigitalService eine zentrale Rolle. Die Wahl eines souveränen Cloud-Anbieters führte in der Praxis jedoch zu einem erhöhten Integrations- und Personalaufwand, da bestimmte Cloud-Features etablierter Anbieter eigenhändig nachgebaut werden müssen. Um diesen zusätzlichen Bedarf strukturiert und finanziell planbar zu lösen, wurden Anpassungen der sogenannten Plattformpauschale durchgeführt. Sie soll die Betriebskosten der Plattform fair auf die verschiedenen Projekte verteilen. Mit dem Wechsel des Cloud-Anbieters wurde die Pauschale erhöht, um den gestiegenen Aufwand abzubilden:

- **Personalaufwand**: Um den personellen Mehraufwand zu decken, wird pro Projekt pauschal der Aufwand von ca. 0,3 FTE (Full-Time Equivalent) eines Plattform-Engineers veranschlagt. Diese Kosten werden direkt in die jeweiligen Projektbudgets eingepreist.

- **Ausnahmeregelung für Prototypen:** Für kleine Teams und kurze Projekte (< 3 Monate) stellte die Pauschale eine zu hohe Barriere dar. Hier greift eine Sonderregelung: Obwohl die Vorhaltekosten der Plattform gleich bleiben, werden diese Barrieren bewusst gesenkt, um innovative Projekte zu ermöglichen.

II. Zersplitterung im Status quo

Als Reaktion auf frühere Kapazitätsengpässe der ursprünglichen Bundescloud setzt der Bund heute bewusst auf eine Multi-Cloud-Umgebung. Damit soll eine zu starke Abhängigkeit von einzelnen Anbietern (Vendor-Lock-in) vermieden werden. Doch wo souveräne Gesamtlösungen nicht die Featuretiefe der Marktführer erreichen, weichen Behörden unter hohem Handlungsdruck zum Teil ohne strategische Abstimmung auf globale Hyperscaler aus.

Gleichzeitig verschärft sich die Situation durch die Struktur der Aufgabenverteilung: Von 30 befragten Institutionen des Bundes geben 57 Prozent an, den Betrieb ihrer IT-Infrastruktur an öffentliche IT-Dienstleister auszulagern.[17] Doch die Bundescloud des ITZBund steht diesen externen Dienstleistern nicht zur Verfügung.

17 msg (2025) IT-Konsolidierung in der öffentlichen Verwaltung, https://s3.msg.systems/Publications/Studie_IT-Konsolidierung_2025.pdf, S. 18.

Dies erhöht die strukturelle Komplexität für die Anwender:innen: Private Clouds des ITZBund, souveräne Speziallösungen (wie Delos oder nearcloud), Public-Cloud-Angebote globaler Großkonzerne sowie europäische Alternativen, wie STACKIT, IONOS oder OVHcloud, existieren parallel und können über Broker-Plattformen wie govdigital beschafft werden. Die Deutsche Verwaltungscloud (DVC) entwickelt gemeinsame Standards, um Interoperabilität zu gewährleisten, und bietet über den Marktplatz Deutschland Digital DVC-konforme Cloud-Services für Kommunen, Länder und Behörden an. Trotz dieser Standardisierungsansätze bleibt die Belastung auf Umsetzungsebene hoch: 80 Prozent identifizieren den Koordinationsaufwand zwischen Behörden und IT-Dienstleistern als Hemmnis für die digitale Transformation.[18]

III. Zentrale Unschärfe in der politischen Rahmensetzung

Die beschriebene Zersplitterung der Cloud-Infrastruktur resultiert auch aus einer langjährigen Unschärfe auf politischer Ebene. Weil eine operationalisierbare Definition von digitaler Souveränität bis zur Einführung der C3A-Kriterien fehlte, entwickelten globale Hyperscaler eigene, oft rein geografische Konzepte wie lokales Hosting oder europäische Support-Teams. Das Zentrum für digitale Souveränität (ZenDiS) warnte hier vor „Souveränitäts-Washing“:[19] Solange die Kernsteuerung und wesentliche Komponenten bei außereuropäischen Großkonzernen verbleiben, bleibt Souveränität ein Marketingslogan, der Abhängigkeiten verschleiert, statt sie aufzulösen.

Außerdem leiden die aktuellen Souveränitätsambitionen unter einer Glaubwürdigkeitskrise. Während einerseits die Abkehr von Abhängigkeiten gefordert wird, zementieren milliardenschwere Verträge mit US-Anbietern den Status quo. Auch zur Zusammenarbeit des BSI mit der AWS European Sovereign Cloud[20] und zur Delos-Cloud von SAP und Microsoft[21] gab es kritische Stimmen wegen fehlender Souveränität. Widersprüchliche Signale verunsichern sowohl Verwaltungsmitarbeitende als auch europäische Anbieter.

18 msg (2025), S. 18.

19 ZenDis (2025) Souveränitäts-Washing bei Cloud-Diensten erkennen, https://www.zendis.de/media/pages/newsroom/publikationen/souveraenitaets-washing/b977c6748e-1755243871/zendis-whitepaper-souveraenitaets-washing.pdf.

20 Staudacher, M. (2026) Ein kritischer Blick auf die Partnerschaft zwischen BSI und AWS, Security Insider, 21.01.2026, https://www.security-insider.de/kritik-aws-european-sovereign-cloud-bsi-kooperation-a-0b20d6be7bc3a6c99668c0dc876cd99c/.

21 Breukel, P. (2025) Baden-Württemberg zweifelt an Souveränität der Delos Cloud, Security Insider, 27.10.2025, https://www.security-insider.de/delos-verwaltungscloud-soveranitatsdebatte-drittstaatenzugriffe-a-8077fff80fed537183f6f70ad99c1824/.

2. HINTERGRUND: MARKTDOMINANZ UND GEOPOLITISCHE HERAUSFORDERUNGEN

Ein effektives Risikomanagement setzt voraus, dass die Verwaltung bestehende Bedrohungen und Abhängigkeiten systematisch analysiert und versteht. Die größte Gefahr resultiert heute aus einer verschärften geopolitischen Lage, in der digitale Infrastrukturen zunehmend als Machtinstrumente eingesetzt werden. Die Folge ist eine kritische Verwundbarkeit: Seit 2017 hat sich der Anteil europäischer Anbieter auf etwa 15 Prozent fast halbiert,[22] während in Deutschland 2023 allein AWS und Microsoft 66 Prozent des Marktes ausmachten.[23] Aus dieser Abhängigkeit entsteht ein dringender Handlungsbedarf.

Infrastruktur als politischer Hebel

Mit der Aushöhlung rechtsstaatlicher Prinzipien in den USA steigt das Risiko, dass digitale Infrastruktur gezielt als politischer Hebel eingesetzt wird. So steigt etwa die Sorge vor möglichen „Kill-Switches“,[24] dem verminderten Zugang zu kritischer Infrastruktur oder politisch gesteuerten Updates.

Diese Vulnerabilität zeigte sich in den letzten Wochen besonders deutlich, als die USA per Exportkontrolle die Abschaltung der leistungsstarken Anthropic-Modelle Fable 5 und Mythos 5 für Personen ohne US-Staatsbürgerschaft durchsetzten, was zu einer weltweiten Abschaltung führte.[25] Bereits im vergangenen Jahr gab es einen ähnlichen Vorfall als der Chefankläger des Internationalen Strafgerichtshofs (IStGH), Karim Khan,[26] sowie weitere Mitarbeitende[27] mit US-Sanktionen belegt wurden und Khan den Zugriff auf sein Microsoft-Konto verlor. Zwar dementierte Microsoft, den Zugang bewusst gesperrt zu haben, doch verdeutlicht der Vorfall ein strukturelles Risiko: US-Unternehmen sind gezwungen, nationale Sanktionen umzusetzen, um zivil- und strafrechtliche Konsequenzen zu vermeiden.[28] Der IStGH wechselte daraufhin zur deutschen Open-Source-Alternative openDesk des ZenDiS.

Dass Sanktionen gegen europäische Akteur:innen genutzt werden, um politische Konflikte auszutragen, zeigen auch Maßnahmen wie Einreisesperren gegen Personen, die sich für die Regulierung von Tech-Unternehmen und die Umsetzung europäischer Digitalpolitik einsetzen.[29]

---

22 European Commission (2026) Proposal for a Cloud and AI development Act, COM(2026) 502 final, 2026/0138 (COD) https://ec.europa.eu/newsroom/dae/redirection/document/129111, S. 1.

23 Hillebrand, A.; Stuck, J. (2024) Cloud-Lösungen für die öffentliche Verwaltung, WIK Diskussionsbeitrag, No. 529, https://www.econstor.eu/bitstream/10419/308076/1/1913296369.pdf, S. 12.

24 Rudolph, T. H. (2025) A ‘Kill Switch’ Could Shutter Europe’s Access to US Tech. Here’s How. Tech Policy Press, 28.08. https://www.techpolicy.press/washington-could-activate-a-kill-switch-to-terminate-european-access-to-us-tech-heres-how-it-could-work/.

25 Connors, M. (2026) Why the US government shut down Anthropic’s latest Claude AI model, The Conversation, 15. Juni, https://theconversation.com/why-the-us-government-shut-down-anthropics-latest-claude-ai-model-285223.

26 Kerkmann, C. (2025) Strafgerichtshof ersetzt Microsoft durch deutsche Lösung, Handelsblatt, 30.10. https://www.handelsblatt.com/technik/it-internet/software-strafgerichtshof-ersetzt-microsoft-durch-deutsche-loesung/100166382.html.

27 US Department of State (2025) Imposing Further Sanctions in Response to the ICC’s Ongoing Threat to Americans and Israelis, https://www.state.gov/releases/2025/08/imposing-further-sanctions-in-response-to-the-iccs-ongoing-threat-to-americans-and-israelis.

28 Thorne, B. (2025) Artificial Sanctions: Potential Implications of US Sanctions on the ICC’s use of AI and Digital Evidence, Opinio Juris, https://opiniojuris.org/2025/02/25/artificial-sanctions-potential-implications-of-us-sanctions-on-the-iccs-use-of-ai-and-digital-evidence/.

29 Tagesschau (2025) Scharfe Kritik an „inakzeptablen“ US-Sanktionen, 24.12. https://www.tagesschau.de/inland/innenpolitik/reaktionen-einreiseverbot-hateaid-usa-100.html.

Rechtliche Unsicherheit durch Cloud Act und Co.

In Europa dominiert neben der Sorge um die Marktmacht der derzeit „dominanten“ Cloud-Anbieter vor allem die Angst vor unbefugten Datenzugriffen.[30] Dies betrifft vor allem den Clarifying Lawful Overseas Use of Data Act (CLOUD Act). Das Gesetz erlaubt US-Strafverfolgungsbehörden Zugriff auf Daten, die bei US-amerikanischen Firmen gespeichert sind – auch wenn sich diese außerhalb der USA befinden. Das oft beworbene europäische Hosting bietet daher keinen wirksamen Schutz. Bereits eine Niederlassung in den USA oder das Anbieten von Dienstleistungen könnte für US-Behörden ausreichend sein, um Zugriffe auszuüben.[31] Um diese Risiken zu erfassen, fordern die C3A-Kriterien eine jährliche Offenlegung betreffender Drittstaaten-Gesetze.

Im Gegensatz zu Maßnahmen wie dem Foreign Intelligence Surveillance Act (FISA), die es US-Behörden erlauben, Datenzugriffe unter strengster Geheimhaltung anzuordnen, setzt der CLOUD Act einen Gerichtsbeschluss oder ähnliche Maßnahmen voraus. Doch obwohl Transparenzberichte aus dem Jahr 2025 darauf hindeuten, dass direkte Zugriffe auf Enterprise-Daten über den CLOUD Act selten sind,[32] räumte 2025 sogar der Chefjustiziar von Microsoft die Möglichkeit von US-Zugriffen ein.[33]

Das Kernproblem bleibt dabei der dauerhafte Konflikt mit der Europäischen Datenschutz-Grundverordnung (DSGVO) und dem Data Act, die Datenübermittlungen ins Ausland streng begrenzen. Seit 2018 ist kein Fall bekannt, in dem Anbieter eine Herausgabe mit Verweis auf europäisches Recht erfolgreich abgewehrt haben. Für Behörden und öffentliche Dienstleister bedeutet dies ein dauerhaftes Restrisiko. Die Risikoabwägung kann nicht auf der operativen Referent:innenebene geleistet werden, sondern ist eine zentrale Gestaltungsaufgabe der Leitungsebene.

---

30 In der Antwort auf eine kleine Anfrage bestätigte die Bundesregierung, dass sie „grundsätzlich Risiken durch unberechtigte Zugriffe beim Einsatz cloudbasierter Kommunikations- und Kollaborationsdiensten [sic] aus Drittstaaten“, siehe Bundesregierung (2026) Antwort – Sicherheitsrisiken staatlicher Überwachungssysteme und Cloud-basierter IT Lösungen, Drucksache 21/5573, https://dserver.bundestag.de/btd/21/058/2105844.pdf, S.2.

31 Universität Köln (2025) Rechtsgutachten zur US-Rechtslage zum weltweiten Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten, 21.03. https://fragdenstaat.de/dokumente/273689-rechtsgutachten-zur-us-rechtslage-zum-weltweiten-datenzugriff-durch-us-behoerden-bei-nutzung-von-cloud-diensten/ S. 5.

32 AWS gibt an, dass es in keinem Fall zur Herausgabe von Daten aus dem Enterprise-Kontext oder einer Regierung betreffend von Nicht-US Kunden kam. Microsoft meldete zwischen Januar und Juni 2025 nur 5 von mehr als 28000 Anfragen in Ermittlungen.

33 Senat (2025) Audition de MM. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France https://www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html.

Fehlende systemische Resilienz

Neben geopolitischen Risiken verringert die Abhängigkeit von wenigen Anbietern auch die Resilienz. Sie schafft Single Points of Failure, deren Ausfall die staatliche Handlungsfähigkeit gefährden kann. 2024 verursachte etwa ein Update der Cybersicherheitsfirma CrowdStrike Ausfälle bei mehr als acht Millionen Windows-Geräten weltweit und betraf sowohl Cloud-Umgebungen als auch lokale Systeme.[34]

Ein Rückzug auf lokale Systeme löst dieses Abhängigkeitsproblem also nicht und garantiert keine Sicherheit: On-Premises-Lösungen ermöglichen zwar eine höhere Kontrolle über Daten, doch laut einem Bericht des Bundesrechnungshofs erfüllt ein Großteil der Rechenzentren des Bundes die Mindeststandards des BSI nicht.[35] Lokale Systeme, die keine ausreichende Redundanz bieten, und fehlende regelmäßige Sicherheitsupdates bergen oft größere Risiken als professionell verwaltete Cloud-Umgebungen.

Preissteigerungen und fehlende Wechselfähigkeit

Die Relevanz von Cloud-Ausgaben im Bundeshaushalt wächst.[36] Gleichzeitig bergen die Monopolstrukturen im Cloud-Ökosystem dabei deutliche haushaltspolitische Risiken. Durch die Abhängigkeit von außereuropäischen Hyperscalern verliert der Staat die Kontrolle über langfristige Kostenentwicklungen. So betragen die erwarteten Kostensteigerungen wegen der erhöhten Preise von Microsoft-Office-Lizenzen beispielsweise bis zu 41,7 Prozent.[37] Während AWS[38] oder Google Cloud[39] im Jahr 2025 Rekordgewinne erzielten, bedeuten die steigende Kostenlast und fehlende Planbarkeit eine Herausforderung für die Haushalte des öffentlichen Sektors.

Diese Kostensteigerungen resultieren unter anderem aus gezielten Produktbündelungen. Hyperscaler wie Microsoft Azure nutzen ihre Marktmacht im Software-Bereich, um Verwaltungen über All-in-One-Pakete (vom Betriebssystem bis zur KI) in ihr gesamtes Ökosystem zu ziehen. Da einzelne Komponenten im Vergleich zu den Paketen deutlich teurer sind, kaufen viele Behörden oft nur noch Produkte innerhalb bestehender Abonnements statt der funktional besten Lösung. Das schränkt den Wettbewerb ein, erhöht Barrieren für neue Anbieter[40] und erhöht die Exit-Kosten beim Anbieterwechsel.

Dominante Anbieter verschlechtern diese Exit-Optionen,[41] etwa durch proprietäre Dienste oder Funktionen oder geringe Interoperabilität. Verwaltungen verlieren dadurch die Fähigkeit, flexibel auf Preiserhöhungen oder Marktveränderungen zu reagieren.

---

34 vdi Nachrichten (2024) Crowdstrike-Fehler löst weltweite Computer-Probleme aus, 19.07. https://www.vdi-nachrichten.com/technik/informationstechnik/crowdstrike-fehler-loest-weltweite-computer-probleme-aus/.

35 Bundesrechnungshof (2025), Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit, https://www.politico.eu/wp-content/uploads/2025/07/02/88-Absatz-2-BHO-zur-Cybersicherheit.pdf, S. 10.

36 Bundesregierung (2025) Antwort – Digitale Souveränität und Nutzung von Open Source bei Clouds der Bundesverwaltung und der Status der Deutschen Verwaltungscloud-Strategie, Drucksache 20/15036, https://dserver.bundestag.de/btd/20/151/2015138.pdf. Die tatsächlichen Kosten sind vermutlich deutlich höher, da hier nicht alle Organisationen berücksichtigt wurden.

37 Bundesregierung (2026) Antwort – Lizenzkosten der Bundesverwaltung für Produkte von Microsoft und anderen US-amerikanischen Techkonzernen, Drucksache 21/5006, https://dserver.bundestag.de/btd/21/054/2105413.pdf.

38 Amazon (2026) Amazon.com Announces Fourth Quarter Results, 05.02., https://ir.aboutamazon.com/news-release/news-release-details/2026/Amazon-com-Announces-Fourth-Quarter-Results/.

39 Bylund, A. (2026) Google Cloud Revenue Just Surged 48%. Is Alphabet the Best AI Stock to Buy Now? https://www.aol.com/finance/google-cloud-revenue-just-surged-185300739.html.

40 Manganelli, A. (2026)

41 Competition and Markets Authority (2026) CMA announces package of actions on business software and cloud services, 31.03., https://www.gov.uk/government/news/cma-announces-package-of-actions-on-business-software-and-cloud-services.

3. SOUVERÄNE CLOUD ALS INDUSTRIEPOLITISCHER SCHWERPUNKT AUF EU-EBENE

Ein erfolgreiches Risikomanagement der Bundesverwaltung funktioniert nicht isoliert, sondern muss auch die EU-Ebene berücksichtigen. Diese reagiert auf die Marktdominanz der Hyperscaler, indem sie digitale Souveränität zum industriepolitischen Schwerpunktthema macht, um die europäische Wettbewerbsfähigkeit und geopolitische Resilienz zu sichern.[42] Da nur ein gemeinsamer europäischer Markt die notwendige Skalierung bieten kann, um echte Alternativen zu den US-Hyperscalern zu schaffen, darf Souveränität nicht auf nationale Maßnahmen oder Anbieter verengt werden. Die Bundesverwaltung sollte daher auf den konkreten Instrumenten aufbauen, die die EU bereits für eine Marktsteuerung bereitstellt. Nationale Initiativen müssen von Beginn an so konzipiert werden, dass sie anschlussfähig an europäische Standards sind und grenzüberschreitende Synergien nutzen, um das europäische Ökosystem zu stärken.

EU Cloud Sovereignty Framework und der Cloud and AI Development Act

Das von der EU-Kommission im Oktober 2025 veröffentlichte EU Cloud Sovereignty Framework steuert EU-Ausschreibungen nach Souveränitätskriterien[43] und diente auch als Vorbild für die C3A-Kriterien des BSI. Sovereignty Effectiveness Assurance Levels (SEAL) beschreiben ein Spektrum von SEAL 0 (exklusive Kontrolle durch außereuropäische Akteure) bis SEAL 4 (volle digitale Souveränität). Wer den Mindeststandard nicht erfüllen kann, wird nicht zugelassen. Ein detaillierter Souveränitätsscore bewertet zudem insgesamt acht strategische Kriterien.

Der im Juni 2026 von der EU-Kommission vorgeschlagene Cloud and AI Development Act (CADA)[44] würde nun dessen Übersetzung in verbindliches Recht bedeuten. Die Verordnung verankert gesetzliche Union Assurance Levels (Stufen 1 bis 4) und verpflichtet Behörden, ihre IT-Infrastruktur mit Risikoanalysen zu bewerten. Für staatliche Prozesse, die die öffentliche Ordnung betreffen, sind ausnahmslos Cloud-Angebote der souveränen Stufen 2 bis 4 vorgesehen. Bei der konkreten Ausgestaltung, etwa der Beteiligung von US-Unternehmen als Technologielieferanten, bleiben die Vorgaben jedoch ungenau. Dennoch setzt der CADA industriepolitische Impulse, um europäische Cloud-Infrastrukturen für die nächste Generation der KI-Entwicklung zu optimieren und die Abhängigkeit von US-Rechenkapazitäten zu verringern.

---

42 Draghi, M. (2024) The future of European competitiveness, https://commission.europa.eu/topics/competitiveness/draghi-report_en. S. 24–30.

43 European Commission (2025) Cloud Sovereignty Framework, Version 1.2.1 – Oct. 2025, https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en.

44 European Commission (2026).

Flankierende regulatorische Instrumente

Flankiert werden diese Maßnahmen durch eine Reihe regulatorischer Instrumente, um die Macht dominanter Cloud-Anbieter einzuschränken. Der Data Act senkt die Barrieren für den Anbieterwechsel, etwa durch ein Verbot von Gebühren, die bei der Übertragung von Daten aus dem System anfallen (Egress-Gebühren), während der Digital Markets Act (DMA) konkrete Vorgaben für Gatekeeper macht und zukünftig auch Cloud-Anbieter verstärkt in die Pflicht nimmt.[45] Ein geplantes Cybersicherheitszertifizierungsschema für Cloud-Dienste scheitert bisher am Streit über Souveränitätsregeln: Frankreich fordert in Anlehnung an SecNumCloud strenge Auflagen (z. B. Joint-Venture-Pflichten für Nicht-EU-Anbieter), andere Staaten lehnen sie ab.

Dass ein strategischer Kurswechsel in der Praxis möglich ist, zeigen jedoch auch Beispiele aus anderen europäischen Nachbarländern. Finnland entschied kürzlich, einen geplanten Wechsel der Wahlplattform zu AWS zunächst zu stoppen. In den Niederlanden forderte das Parlament die Regierung im März 2026 auf, sich von US-amerikanischen Firmen zu entflechten und eine niederländisch kontrollierte Cloud aufzusetzen.

Infrastruktur: IPCEI-CIS als Gegenentwurf

Auf Infrastrukturebene treibt die EU alternative Strukturen wie das Important Project of Common European Interest – Next Generation Cloud Infrastructure and Services (IPCEI-CIS) voran, in dessen Rahmen ein dezentrales Cloud-Edge-Kontinuum aufgebaut werden soll. Im Gegensatz zu Gaia-X, das immer wieder zu Kritik führte, weil auch chinesische und US-amerikanische Anbieter beteiligt waren,[46] werden hier strengere Souveränitätsstandards angelegt. Deutschland fördert das Projekt 2026 mit 250 Millionen Euro.

45 European Commission (2026) Review highlights Digital Markets Act remains fit for purpose and has positive impact, 28.04. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_914. Für eine detaillierte Analyse zur Konzentration im Cloudmarkt und möglichen Lösungsansätzen, insbesondere zu Eingriffsmöglichkeiten unter dem DMA, siehe von Thun und Colville (2026) sowie Manganelli (2026).

46 Goujard, C. & Cerulus, L. (2021) Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project, Politico, 26.10., https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/.

4. LÖSUNGSANSÄTZE FÜR MEHR CLOUD-SOUVERÄNITÄT

Um die staatliche Handlungsfähigkeit dauerhaft abzusichern, muss die Verwaltung von der reinen Risikoanalyse in die gezielte Gestaltung übergehen. Dies erfordert ein koordiniertes Vorgehen auf vier strategischen Ebenen: Transparenz und Priorisierung, (finanzielle) Befähigung, aktive Marktsteuerung sowie ein tiefgreifender Kulturwandel.

I. Transparenz und Priorisierung

Digitale Souveränität braucht konsequente Messung

Um Risiken zu steuern, müssen wir sie verstehen. Bisher waren souveräne Lösungen oft im Nachteil: Während die funktionale Tiefe der US-Anbieter unmittelbar sichtbar ist, bleiben die Risiken fehlender Souveränität abstrakt. Daher müssen wir Abhängigkeiten bewusster operationalisieren, messen und navigieren. Die Herausforderung besteht nicht in einem Mangel an Kriterien, sondern in deren systematischer Zusammenführung und Anwendung:

- **Risikoanalyse und Evaluation:** Instrumente wie der Souveränitätsscore der Stadt München,[47] die Souveränitätskriterien des ZenDiS,[48] das Software Sovereignty Framework von Schwarz Digits[49] oder der Digital Dependence Index der Universität Bonn[50] übersetzen digitale Souveränität in messbare Kriterien und machen strategische Risiken sichtbar.

- **Leitplanken und Anforderungen:** Das C3A-Framework des BSI bildet seit April 2026 den zentralen Rahmen, um sowohl für Unternehmen als auch für den öffentlichen Sektor Anforderungen an Souveränität zu etablieren. Sie ergänzen die bereits 2023 entwickelten Vorgaben der DSK.[51] Die ergänzenden Vertragsbedingungen (EVB-IT) Cloud dienen schließlich als Kriterienkataloge, um solche Standards auch in der IT-Beschaffung abzubilden. Die allgemeinen EVB-IT setzen bereits standardmäßig auf Open Source; die EVB-IT Cloud werden noch in diesem Jahr überarbeitet.

47 Stadt München (2026) Digitale Souveränität, https://muenchen.digital/projekte/digitale-souver%C3%A4nit%C3%A4t.html.
48 ZenDiS (2026) Kriterien zur Bewertung von Digitaler Souveränität, https://www.zendis.de/newsroom/presse/pressemeldung-konsultationsprozess.
49 Schwarz Digits (2026) Cyber Security Report, https://schwarz-digits.de/publikationen/cyber-security-report/cyber-security-report-herunterladen.
50 Universität Bonn (2025) Vermessung der digitalen Dependenz, https://digitaldependence.eu/.
51 DSK (2023).

Klares Lagebild mit systematischer Erfassung von Risiken

Um langfristige Risiken zu minimieren und Sparpotenziale zu identifizieren, benötigt die Verwaltung ein klares Lagebild über Cloud-Abhängigkeiten und Alternativen. Aktuell fehlt eine solche Übersicht; laut einer kleinen Anfrage Anfang 2026 ist sie auch nicht geplant.[52] Ohne Transparenz über die genutzte Infrastruktur und die damit verbundenen Kosten bleibt digitale Souveränität ein vages Versprechen. Ein solches Lagebild braucht drei zentrale Elemente:

- Erfassung von Abhängigkeiten: Die bestehende Datenbank des IT-Zustimmungsvorbehalts mit bereits über 2.000 erfassten Beschaffungsvorgängen muss systematisch genutzt und erweitert werden, um Cloud-Ausgaben und Risikoprofile ressortübergreifend zu erfassen.

- Analyse von Lock-in-Effekten: Erst die konsequente Berücksichtigung von Exit-Kosten und Datenportabilität macht die Betriebskosten wirklich vergleichbar und macht deutlich, wo strategische Wechselmöglichkeiten liegen.

- Risiken erkennen: Das Lagebild muss Single Points of Failure und Engpässe in Lieferketten bis auf Hardware- und Chip-Ebene identifizieren, die bei einem Ausfall die staatliche Handlungsfähigkeit gefährden können. Besondere Relevanz hat dies für KI-Anwendungen, deren enormer Rechenleistungsbedarf bestehende Abhängigkeiten weiter zu verschärfen droht.

Risiko-Stufenmodell und Roadmap zur Priorisierung

Nicht jede administrative Anwendung benötigt maximale Souveränität. Um die operative Umsetzung zu erleichtern und Ressourcen zielführend einzusetzen, sollte die Verwaltung ein Risiko-Stufenmodell nach Reichweite (Scale) und Schutzbedarf (Scope) etablieren und als Basis für eine ambitionierte Roadmap mit konkreten und verbindlichen Zielvorgaben nutzen. So können zunächst Bereiche mit hoher Hebelwirkung priorisiert werden, wie etwa Arbeitsplätze, Cloud-Infrastruktur und KI-Anwendungen, um die Handlungsfähigkeit zu stärken und Kompetenzen aufzubauen. Das Modell kann als methodische Grundlage für die im CADA (Art. 29) verankerten Sovereignty Risk Assessments zum Schutz der öffentlichen Ordnung dienen.

52 Bundesregierung (2025) Antwort – Neuordnung der Digitalpolitik – Struktur und Zuständigkeiten im Bundesministerium für Digitales und Staatsmodernisierung, Drucksache 21/853, https://dserver.bundestag.de/btd/21/010/2101041.pdf.

Reichweite (system-relevante Bereiche und Betroffene)	Schutzbedarf (Vertraulichkeit von Daten und System)	Beispiele
Hoch: Flächendeckend, kritische Infrastruktur, staatliche Kernprozesse	**Hoch:** VS-Daten, hoch-vertrauliche Finanz-/ Bürger:innendaten	Rentenversicherung, Daseinsvorsorge
Mittel bis hoch: Ressortübergreifende Nutzung, allgemeine Anwendung in der Verwaltung	**Mittel:** Personen-bezogene Daten, KI-gestützte Workflows, allgemeiner Schrift-verkehr	Arbeitsplätze, behördeninterne KI-Assistenzsysteme
Niedrig bis mittel: Isolierte Fachanwen-dungen, punktuelle Tool-Nutzung	**Niedrig:** Öffentlich zugängliche Daten, unkritische administra-tive Prozesse	Lokale Informations-portale, Veranstaltungs-management

Tabelle 1: Einstufung des Souveränitätsbedarfs nach Reichweite und Schutzbedarf

II. Finanzielle Befähigung und operative Unterstützung

Souveränitätsfonds für wirkungsorientierte Finanzierung
Souveräne Lösungen scheitern oft an einer kurzfristigen oder einseitigen Budgetlogik, da globale Anbieter durch Skaleneffekte kurzfristig kostengünstiger sind. Um digitale Souveränität zu stärken, sollte der Bund daher einen Souveränitätsfonds nach dem Vorbild des Effizienzfonds der Modernisierungsagenda einrichten. Dieser fördert Effizienzprojekte in der Verwaltung und setzt „positive Anreize zur Effizienzsteigerung".[53]

Das entscheidende Leitprinzip des Souveränitätsfonds ist eine strikte Wirkungsorientierung: Die Mittel dürfen nicht für beliebige IT-Projekte genutzt werden, sondern sind fest an messbare Meilensteine gekoppelt. Nur Organisationen, die sich an den C3A-Kriterien orientieren, Abhängigkeiten nachweislich reduzieren und die europäische Wertschöpfungskette stärken, erhalten Gelder. Durch einen klaren Fokus auf Open Source und Nachnutzbarkeit werden Entwicklungs- und Integrationsaufwände langfristig reduziert.

53 BMDS (2025) Modernisierungsagenda — für Staat und Verwaltung (Bund), Oktober, https://bmds.bund.de/fileadmin/BMDS/Dokumente/Modernisierungsagenda_barrierefrei.pdf, S. 33.

Souveräne Roll-in-Teams für dauerhaften Kompetenzaufbau in der Verwaltung

Der Mangel an IT-Fachkräften in den Vergabestellen und IT-Referaten ist eine zentrale Herausforderung für die Umsetzung digitaler Souveränität. Auch in Interviews wurde deutlich, dass gerade kleinere Behörden die technische Migration und Integration von souveränen Alternativen oft personell nicht leisten können. Das ZenDiS bietet mit dem Souveränitätscheck[54] bereits Unterstützung bei der Analyse von Abhängigkeiten. Dennoch fehlen Kapazitäten für die praktische Umsetzung.

Um über Pilotprojekte Praxiserfahrungen zu sammeln und die Umsetzung zu fördern, ist der Einsatz bundesfinanzierter, souveräner Roll-in-Teams notwendig. Erfolgreiche Vorbilder existieren bereits in Hessen und Bayern zur Umsetzung des Onlinezugangsgesetzes. Dieses Modell lässt sich auch auf die Cloud-Transformation von Standard-Infrastrukturen, wie etwa Office- und Arbeitsplatzsystemen, übertragen:

- **Standardisierung:** Die Roll-in-Teams etablieren standardisierte Migrationsprozesse und bauen vor Ort das notwendige Wissen für den eigenständigen Betrieb auf.

- **Interdisziplinarität:** Die Einheiten nutzen Expertise von IT-Architekt:innen, Migrations-Expert:innen, Change Manager:innen und agilen Coaches, um die Umsetzung bestmöglich zu unterstützen.

- **Wissenstransfer:** Über strukturierte Austauschräume vernetzen die Teams Behörden, Kommunen und Länder, um Praxiserfahrungen aus Pilotprojekten direkt zu teilen.

III. Aktive Marktsteuerung und Vergabeprozesse

IT-Zustimmungsvorbehalt als Steuerungsinstrument für souveräne Beschaffung

Ein souveränes Ökosystem entsteht nur, wenn die Beschaffung den Markt gezielt gestaltet. Während der Gründer von OVHcloud eine Quote von 15 Prozent des staatlichen Vergabevolumens für einen kompetitiven Cloud-Markt fordert,[55] empfiehlt der CADA, 25 Prozent der Cloud- und KI-Projekte an innovative KMU zu vergeben (Art. 33(4)). Um diese Ziele wirksam umzusetzen, muss die Steuerung ressortübergreifend greifen: Da auch in Zukunft ca. 40 Prozent der IT-Ausgaben außerhalb des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) verwaltet werden,[56] ist der IT-Zustimmungsvorbehalt ein zentrales Instrument, um den Staat als „Ankerkunden der Wirtschaft zu stärken und ihn digital souverän und bürgernah auszurichten".[57]

- **Transparente Kriterien:** Das BMDS muss verbindliche, klare Kriterien entwickeln, nach denen IT-Beschaffungen bewertet werden. Während die Einhaltung der IT-Richtlinien des Bundes, etwa die Architekturvorgabe AV-09 Digitale Souveränität, bereits formal geprüft werden, fehlt es an Verbindlichkeit und

54 ZenDiS (2026) Souveränitätscheck, https://www.zendis.de/unser-angebot#beratung.
55 Hosan, B. (2026) „Ich will keine Subventionen. Ich will Umsatz." Tagesspiegel, 20.03., https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/ich-will-keine-subventionen-ich-will-umsatz.
56 Heumann, S. (2026) Der erhoffte Schub? Analyse der Digitalausgaben 2025 im Lichte von Sondervermögen, BMDS-Gründung und Souveränitätsdebatte https://agoradigital.de/wp-content/uploads/2026/04/ADT_Policy-Paper_Digitalausgaben_2025.pdf, S. 6.
57 BMDS (2025) Starkes Instrument für IT-Steuerung des Bundes, https://bmds.bund.de/aktuelles/pressemitteilungen/detail/starkes-instrument-fuer-it-steuerung-des-bundes.

Transparenz. Ein transparentes Regelwerk erlaubt eine verlässliche Planung für Ministerien und Unternehmen, welche Mindeststandards (z. B. Interoperabilität und offene Schnittstellen) erfüllt sein müssen.

- **Schnelle Prüfung:** Um die Handlungsfähigkeit der Ressorts zu bewahren, müssen Prüfverfahren innerhalb weniger Wochen abgeschlossen sein. Daher muss sich das BMDS auf wesentliche Prioritäten fokussieren, etwa Arbeitsplatzsoftware, Cloud-Infrastruktur sowie KI.

- **Verbindliche Exit-Strategien:** Sind Vergaben an globale Hyperscaler unvermeidbar, müssen Behörden eine technisch geprüfte Exit-Strategie inklusive langfristiger Kosten vorlegen. Vorbild ist etwa Frankreich, das seine Ministerien bis Herbst 2026 zu konkreten Plänen für den Wechsel von Microsoft Windows zu Linux verpflichtet.[58]

Eine souveräne Beschaffungsstrategie stärkt dabei nicht nur staatliche Autonomie, sondern auch kleinere und mittlere Unternehmen. Laut einer Bitkom-Studie wünschen sich 84 Prozent der Befragten die priorisierte Umsetzung digitaler Souveränität durch die Bundesregierung.[59] Aktive Marktgestaltung senkt die Barrieren für europäische Anbieter und baut Vertrauen in das lokale Ökosystem auf. Dieser Effekt lässt sich bereits in Schleswig-Holstein beobachten, das als Vorreiter auf Länderebene konsequent auf eine Open-Source-Ausrichtung setzt.

Interdisziplinärer Kompetenzmix für verbesserte Vergabeprozesse

Im Rahmen der Vergaberechtsreform hat der Gesetzgeber die digitale Souveränität erstmals explizit im Gesetz gegen Wettbewerbsbeschränkungen (GWB) verankert.[60] Diese Änderungen müssen schnellstmöglich umgesetzt werden, um Organisationen die rechtssichere Beschaffung zu ermöglichen. Aus den Interviews ging hervor, dass rein juristische Prüfungen hier zu kurz greifen. Stattdessen ist ein interdisziplinärer Kompetenzmix in Vergabestellen erforderlich, der Expertise aus den Bereichen Vergabe- und Wirtschaftsrecht, Verwaltungswissenschaft sowie IT-Architektur bündelt. Konkrete Unterstützungsangebote, standardisierte Textbausteine und Leitfäden erleichtern eine rechtssichere Auftragsvergabe und fördern transparente Verfahren. Zusätzlich müssen Vergabestellen befähigt werden, die im CADA (Art. 32) vorgeschlagenen Kriterien für einen EU-Mehrwert in Ausschreibungen operativ umzusetzen.

Souveräne Clouds im Rahmen des Deutschland-Stacks

Der Deutschland-Stack bietet immenses Potenzial, um das Cloud-Ökosystem langfristig zu steuern und Basisinfrastrukturen souverän zu gestalten. Ein entscheidender Erfolgsindikator ist der Open-Source-Anteil, der neue proprietäre Abhängigkeiten verhindert, eine unabhängige Sicherheitsprüfung ermöglicht und die europäische Anschlussfähigkeit offener Standards sichert. Dieser ist in vielen Bereichen jedoch zu gering, um digitale Souveränität effektiv zu fördern. Verbindliche Standards und eine transparente Offenlegung bilden hier wirksame Hebel.

---

58 Schuler, M. (2026) France Orders Government-Wide Exit From Windows to Linux, Ministry Plans Due by Fall, Implicator AI, 10.04. https://www.implicator.ai/france-orders-government-wide-exit-from-windows-to-linux-ministry-plans-due-by-fall/.

59 Bitkom (2025) Digitale Souveränität: Wie abhängig ist unsere Wirtschaft? https://doi.org/10.64022/2025-digitale-souveraenitaet.

60 Bundestag (2025) Entwurf eines Gesetzes zur Beschleunigung der Vergabe öffentlicher Aufträge, Drucksache 21/1934, https://dserver.bundestag.de/btd/21/019/2101934.pdf, S.12.

Ein zentraler Baustein ist die verbindliche Integration der DVC und des Sovereign Cloud Stacks (SCS).[61] Der SCS definiert zertifizierbare, offene Cloud- und Container-Infrastrukturen, basiert auf Open Source und sichert durch die Kompatibilität mit der DVC Wechselfähigkeit und Interoperabilität. Um die Einhaltung der Standards zu sichern, sind eine konsequente Durchsetzung der Vorgaben sowie die Befähigung der Akteure erforderlich.

IV. Kulturwandel

Von Risikoaversion zu echtem Risikomanagement

Um langfristig Handlungsfähigkeit zu sichern, bedarf es neben technologischen Werkzeugen und einer strategischen Marktgestaltung vor allem eines grundlegenden Wandels in der Entscheidungskultur. Um eine Lähmung zu verhindern, muss die Begründungspflicht umgekehrt werden: Wer sich für eine abhängige Lösung entscheidet, muss das damit verbundene Risiko rechtfertigen, nicht umgekehrt. Für eine fundierte, evidenzbasierte Risikoabwägung benötigen Verwaltungsmitarbeitende praxisnahe Leitlinien und Best Practices, wie die BSI-Leitlinien für den Umgang mit VS-Daten[62], strategische Formate, wie den Cloud-Nutzungsstrategie-Workshop,[63] sowie eine einheitliche Umsetzung.

Gleichzeitig muss dieser kulturelle Wandel auch strukturell verankert werden, etwa in internen Zielvereinbarungen. Die Förderung souveräner und offener Ökosysteme muss als Erfolg gewertet werden, auch wenn dies initial mit einem höheren Koordinationsaufwand verbunden ist. Denn dieser Aufwand resultiert langfristig im Aufbau eigener digitaler Kompetenzen.

Ohne Rückendeckung von ganz oben stoßen solche Bemühungen jedoch schnell an ihre Grenzen. Der Blick auf europäische Nachbarländer zeigt deutlich: Digitale Souveränität erfordert ein klares politisches Mandat der Regierungsspitze.

---

61 Sovereign Cloud Stack (2026) Deutschland-Stack setzt auf Sovereign Cloud Stack als Standard, https://sovereigncloudstack.org/deutschland-stack-setzt-auf-sovereign-cloud-stack-als-standard/.

62 BSI (2026) Leitfaden für den Einsatz von Cloud-Lösungen im VS-Kontext der Bundesverwaltung, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Geheimschutz/Leitfaden_Cloud-Loesungen_Bundesverwaltung.html.

63 BSI (2025) Cloud-Nutzungsstrategie - Workshop, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_Cloud_Strategie.pdf?__blob=publicationFile&v=4.

5. FAZIT: SOUVERÄNITÄT ALS STRATEGISCHE GESTALTUNGSAUFGABE

Digitale Souveränität ist eine zentrale Antwort auf veränderte geopolitische Realitäten. Denn die Abhängigkeit von außereuropäischen Cloud-Ökosystemen stellt ein Risiko für die staatliche Handlungsfähigkeit dar.

Die Analyse zeigt deutlich: Es fehlt nicht an Instrumenten, um Abhängigkeiten zu verringern. Mit dem C3A-Framework des BSI und dem EU Cloud Sovereignty Framework liegen Kriterien und Standards vor, die Orientierung bieten. Mit dem IT-Zustimmungsvorbehalt und dem Deutschland-Stack kann das BMDS Hebel nutzen, um das Ökosystem zu verändern. Die Reform des Vergaberechts schafft ab Juli 2026 zusätzlich Rechtssicherheit.

Der entscheidende Hebel liegt jedoch in einem bewussten Risikomanagement. Souveränität muss zum Standardkriterium jeder Wirtschaftlichkeitsuntersuchung werden, um Abhängigkeiten bewusst zu steuern und Exit-Optionen vorzubereiten. Als Ankerkunde hat der Staat die Kraft, das europäische Ökosystem durch gezielte Beschaffung zu stärken. Um dies auch in der Umsetzungsebene zu verankern, ist es wichtig, die Verantwortung für Risikoabwägungen nicht auf die operative Ebene zu verlagern, sondern durch die politische Führung aktiv zu unterstützen. Dafür müssen wir die Begründungspflichten konsequent umkehren: Weg von der Rechtfertigung souveräner Alternativen, hin zur zwingenden Begründung strategischer Abhängigkeiten.

Autorin: Anke Obendiek, PhD
Mitwirkende: Erik Dörnenburg, Melike Geyik, Joshua Pacheco,
Ann Cathrin Riedel, Magdalena Zadara

IMPRESSUM

Co-Herausgeber

NExT e. V.
Prinzessinnenstr. 8, 10969 Berlin
info@next-netz.de
www.next-netz.de
Vereinsregisternummer: VR 36904 B
Registergericht: Amtsgericht Charlottenburg

DigitalService GmbH des Bundes
Prinzessinnenstr. 8, 10969 Berlin
hallo@digitalservice.bund.de
www.digitalservice.bund.de
Handelsregister-Nummer: HRB 212879 B
Registergericht: Berlin Charlottenburg
Umsatzsteueridentifikationsnummer: DE327075535

Autorin
Anke Obendiek, PhD

Mitwirkende

Erik Dörnenburg
Melike Geyik
Joshua Pacheco
Ann Cathrin Riedel
Magdalena Zadara

Stand
Juni 2026

Layout
TAU GmbH