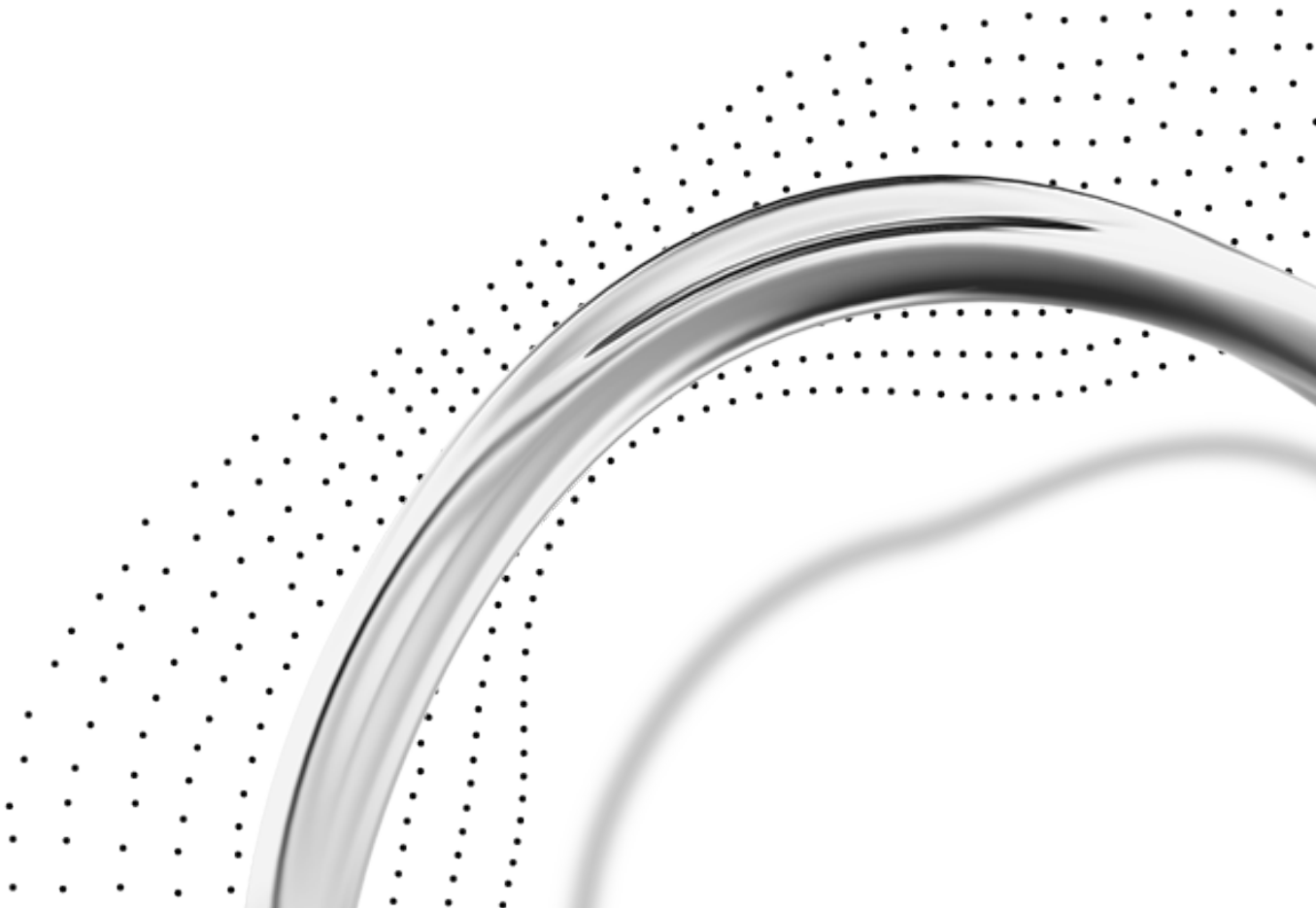
Whitepaper

Souveränitäts-Washing bei Cloud-Diensten erkennen

Warum Digitale Souveränität mehr ist als ein Standortversprechen



Inhalt

Executive Summary

Angesichts zunehmender geopolitischer Spannungen ist das Interesse an digital souveränen Lösungen zuletzt stark gestiegen. Um die Nachfrage zu bedienen, ist auch das Angebot gewachsen. Insbesondere bei Cloud-Diensten ist jedoch besondere Aufmerksamkeit geboten. Mit Verweis auf europäische Rechenzentren, „Datengrenzen“ oder Partnerschaften mit hiesigen Unternehmen versprechen Hyperscaler aus dem Nicht-EU-Ausland mitunter Digitale Souveränität, die bei genauer Betrachtung in technischer, rechtlicher und operativer Hinsicht keinen Bestand hat.

In diesen Fällen spricht man von „Souveränitäts-Washing“. Der Begriff bezeichnet Angebote, die als „souverän“ vermarktet werden, jedoch nur Teilaspekte von Digitaler Souveränität erfüllen. Für ein Höchstmaß an Digitaler Souveränität braucht es neben Datensouveränität nämlich auch Wechselfähigkeit, technologische sowie operative Souveränität und Transparenz.

1. Wenn Digitale Souveränität zur Verpackung wird

Der Begriff der Digitalen Souveränität ist in aller Munde. Verwaltungen, Unternehmen, Medien und politische Institutionen bekräftigen die Notwendigkeit, sich von digitalen Abhängigkeiten zu lösen. Auch der Koalitionsvertrag der aktuellen Bundesregierung bekennt sich offen zur Stärkung der Digitaler Souveränität und erklärt diese zum zentralen Leitmotiv der Digitalpolitik in der 21. Legislaturperiode.[1]

Konkret geht es vor allem darum, die kritischen Abhängigkeiten von großen, zumeist nicht-europäischen Software- und Cloud-Anbietern aufzulösen, deren Lösungen über die letzten Jahrzehnte fester Teil vieler staatlicher IT-Infrastrukturen geworden sind. Auch das 2022 vom Bundesministerium des Innern und für Heimat (BMI) gegründete Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) hat genau diesen Auftrag.[2]

Das Ziel ist also klar. Doch der Weg ist nicht immer leicht zu erkennen. Mit ihrer Größe und Marktmacht haben vor allem die US-amerikanischen Hyperscaler in den vergangenen Jahren faktisch ein Oligopol geschaffen. Diese Stellung versuchen die Konzerne nun mit allen Mitteln zu behaupten. Ihre Reaktion auf das europäische Streben nach mehr Digitaler Souveränität sind neue Produkte, die Souveränität versprechen – aber faktisch nicht liefern.

Was dabei entsteht, ist eine neue Form des Etikettenschwindels: Souveränitäts-Washing – also die Vermarktung von scheinbar souveränen Lösungen, die sich bei genauerer Betrachtung jedoch als neue Verpackung altbekannter Abhängigkeiten entpuppen. Hinzu kommt der Versuch von Interessenvertretern, Digitale Souveränität als nicht definiert darzustellen. Damit versuchen sie, Digitale Souveränität in ihrem Sinne umzudeuten - sie wird hierzu häufig fälschlich mit Abschottung bzw. Autarkie gleichgesetzt - und letztlich Einfluss auf staatliches Handeln zu nehmen.

Dieses Whitepaper soll helfen, Cloud-Angebote bezüglich ihres echten Souveränitätsgrades zu bewerten. Es bringt in Erinnerung, wie Politik und Verwaltung in Deutschland Digitale Souveränität definieren, gibt klare, sachliche Kriterien an die Hand und zeigt auf, warum sich Digitale Souveränität nicht allein an Rechenzentrumsstandorten oder Betriebsmodellen festmachen lässt.

[1] https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf
[2] https://www.zendis.de/unser-auftrag

2. Was ist Digitale Souveränität?

Politik und Verwaltung in Deutschland haben sich schon vor Jahren auf eine einheitliche Definition von Digitaler Souveränität verständigt. Demnach beschreibt Digitale Souveränität die Fähigkeit eines Staates oder einer Organisation, digitale Infrastrukturen und Dienste selbstständig, selbstbestimmt und sicher zu gestalten, zu betreiben und weiterzuentwickeln – ohne unkontrollierbare Abhängigkeiten von einzelnen Anbietern oder Drittstaaten. Digitale Souveränität geht damit weit über die reine Datensouveränität, die vor allem die Kontrolle über die eigenen Daten meint, hinaus und umfasst auch den Zugriff auf Quellcode, Entscheidungsstrukturen und Standards.[3]

Diese Anforderungen sind nicht optional, sie ergänzen sich. Für ein Höchstmaß an Digitaler Souveränität müssen alle Kriterien erfüllt sein. Angebote, die als „datensouverän" deklariert sind, erfüllen beispielsweise nur einen Teilaspekt: den des rechtssicheren und DSGVO-konformen Betriebs in Bezug auf die Daten. Und selbst dies muss im Einzelfall sorgfältig geprüft werden.

Ein Höchstmaß an Digitaler Souveränität bietet eine digitale Lösung dann, wenn sie:

- rechtssicher/DSGVO-konform betrieben werden kann (bspw. ohne Zugriff durch ausländische Behörden auf Daten),
- Wechselfähigkeit ermöglicht (d. h. kein Vendor-Lock-in besteht),
- Kontrolle sichert (auch bei Ausfall, Sperrung oder Wechsel von Dienstleistern),
- Transparenz bietet (z. B. durch einsehbaren Quellcode)
- und anpassbar und gestaltbar ist (z. B. durch Weiterentwicklung in der Community oder durch Dienstleister).

3. Datengrenzen, Serverstandorte & Betreibermodelle

Die politischen und gesellschaftlichen Forderungen nach Unabhängigkeit sind auch den globalen IT-Konzernen nicht verborgen geblieben. Zunehmend positionieren sich US-Hyperscaler und andere Anbieter mit vermeintlich souveränen Angeboten. Dazu gehören z. B. spezielle Rechenzentren in Europa, Kooperationen mit nationalen Unternehmen und besondere Datenschutzversprechen (bspw. „Datengrenzen"). All das soll Vertrauen schaffen und Geschäft sowie Einfluss sichern.

Ein prominentes Beispiel ist die Delos-Cloud. Dahinter steckt zwar das deutsche Unternehmen SAP, doch die Delos-Cloud baut auf proprietärer Technologie aus den USA auf – konkret Microsoft Azure und Microsoft 365.

Durch die deutsche Betreibergesellschaft bietet Delos zwar klare Vorteile in Bezug auf den Einzelaspekt der Datensouveränität. Die technologische Kontrolle – und damit auch die technologische Souveränität – wesentlicher Komponenten verbleibt jedoch bei dem US-Konzern. Das gilt auch für die Bereitstellung von Sicherheits- und Funktions-Updates. Damit werden kritische strukturelle Abhängigkeiten nicht aufgelöst. Weder Betriebssicherheit noch Operational Continuity können dauerhaft gewährleistet werden. Zudem fehlt es an der geforderten Transparenz, Gestaltungs- und Wechselfähigkeit.

[3] https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

Deep–dive

4. Warum proprietäre Cloud–Infrastruk–turen strukturell unsouverän bleiben

4.1 Update–Zyklen und Betriebsabhängigkeit

Cloud-Infrastrukturen sind komplexe, hochdynamische Systeme, die auf tägliche oder wöchentliche Software- und Sicherheitsupdates angewiesen sind. Diese Updates betreffen Hypervisor, Ressourcen-Management (Compute, Storage, Networking), Verwaltungsschnittstellen (APIs, Dashboards) sowie alle Security- und Monitoring-Dienste.

Auch die zentralen Steuerungsmechanismen (z. B. IAM-Systeme, Container-Orchestrierung, Verschlüsselungsdienste) sind integraler Bestandteil der globalen Plattformarchitektur. Bei proprietären Systemen können sie nicht unabhängig betrieben oder von Dritten gewartet werden.

Das bedeutet: Fällt die Verbindung zur zentralen Plattform des Anbieters weg – etwa durch politische Entscheidungen oder Exportrestriktionen – wird die Infrastruktur innerhalb kürzester Zeit unsicher und letzten Endes unbrauchbar. Das gilt gleichermaßen für die Public- oder Private-Cloud-Services der Anbieter selbst wie auch für Cloud-Instanzen, die in Partnerschaft mit hiesigen Anbietern oder abgeschottet in eigenen Rechenzentren (air-gapped) bereitgestellt werden.

Die großen Hyperscaler betonen selbst, dass Updates innerhalb von fünf bis sieben Tagen eingespielt werden sollten, um den sicheren Betrieb zu gewährleisten. Stünden diese Updates plötzlich nicht mehr zur Verfügung (Unterbrechung der Softwarelieferkette) – ein durchaus denkbares Druckmittel der US-Regierung, um Einfluss auf die Politik in Deutschland zu nehmen und eigene Interessen durchzusetzen –, wäre keine Zeit mehr für einen Anbieterwechsel. Nach eigenen Angaben könnte beispielsweise Delos ohne Support aus den USA seine Cloud nur einige wenige Monate weiterbetreiben.[4]

Um genau diese Problematik zu adressieren, hat das ZenDiS gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Strategie zur Absicherung von Softwarelieferketten für die Verwaltung entwickelt.[5] Im Zentrum stehen die Etablierung verbindlicher Sicherheitsstandards, Transparenz über Abhängigkeiten sowie nachvollziehbare Herkunftsnachweise für kritische Softwarekomponenten.

[4] https://www.sz-dossier.de/tiefgaenge/2025-03-25-wenn-trump-den-schalter-umlegt-wie-lange-laeuft-die-delos-cloud-83e34bce
[5] https://www.zendis.de/media/pages/newsroom/publikationen/sichere-softwarelieferketten-opencode-als-baustein-einer-souveraenen-digitalen-infrastruktur/9f4eafa96a-1746615438/2025_04_zendis_bsi_ssdlc_strategiepapier_opencode.pdf

4.2 Lock–in durch Architektur

Ein weiteres Problem liegt in der Struktur moderner Cloud-Plattformen. Zwar werben die meisten Anbieter mit der Unterstützung offener Standards (wie Kubernetes oder OpenID), doch in der Praxis sind viele zentrale Dienste proprietär erweitert oder monolithisch integriert. Die Portabilität von Daten und Workloads ist quasi nur auf dem Papier gegeben, denn der Aufwand eines Plattformwechsels ist hoch – und zwar technisch, organisatorisch sowie finanziell.

Mit Inkrafttreten des EU Data Acts[6] im September 2025 soll sich dies ändern. Er verpflichtet Cloud-Provider, ihren Kunden jederzeit mit zweimonatiger Kündigungsfrist und danach innerhalb von 30 Tagen unproblematisch einen Wechsel zu anderen Anbietern und sogar zu On-Prem-Lösungen zu ermöglichen – Stichworte Cloud-Switching und Datenportabiliät. Zudem macht der Data Act technische Vorgaben zur Interoperabilität und verpflichtet die Cloud-Anbieter, Schnittstellen für Wechsel-Tools bereitzustellen.

Die Realität sieht bislang jedoch anders aus. Bisher ist ein Wechsel zwischen proprietären Cloud-Angeboten oftmals kaum möglich, es besteht ein Plattform-Lock-in. Selbst der Digitalverband Bitkom sieht dies kritisch und weist in seiner Stellungnahme zur Digitalen Souveränität darauf hin, dass echte Wechselfähigkeit nicht nur formell, sondern auch praktisch gegeben sein muss. Alles andere sei Augenwischerei.[7]

4.3 Juristische Risiken: US–Recht kennt keine Grenzen

Spätestens seit dem NSA-Skandal ist bekannt, dass sich die USA mit Hilfe von Technologie Einfluss sichern und die Souveränität anderer Staaten untergraben. Durch Gesetze wie den CLOUD Act und FISA 702 unterliegen alle US-Cloud-Anbieter der Pflicht, Daten auch dann offenzulegen, wenn sie außerhalb der USA gespeichert sind. Dasselbe gilt für entsprechende Executive Orders des US-Präsidenten. Sie entfalten eine extraterritorialen Wirkung, selbst wenn dies mit nationalem Recht kollidiert.

Dies gilt auch für Metadaten, Betriebsprotokolle oder Systemzugriffe. Die Kontosperrungen am Internationalen Strafgerichtshof (IStGH) belegen den Einfluss der US-Regierung auf US-Unternehmen.[8] Eine Datenhoheit, wie sie europäische Datenschutzstandards fordern, ist bei der Nutzung US-amerikanischer Lösungen somit nicht gewährleistet. Dies gilt selbst dann, wenn „souveräne“ Rechenzentren in Frankfurt, München oder Amsterdam stehen oder „Datengrenzen“ eingezogen werden. Zuletzt bestätigt wurde dies im Juli 2025 durch den Chefjustiziar von Microsoft Frankreich im Rahmen einer Anhörung vor dem französischen Senat.[9]

[6] https://digital-strategy.ec.europa.eu/de/factpages/data-act-explained

[7] https://www.bitkom.org/sites/main/files/2020-01/200116_stellungnahme_digitale-souveranitat.pdf

[8] https://apnews.com/article/icc-trump-sanctions-karim-khan-court-a4b4c02751ab84c09718b1b95cbd5db3

[9] https://www.heise.de/news/Nicht-souveraen-Microsoft-kann-Sicherheit-von-EU-Daten-nicht-garantieren-10494684.html

5. Rechtliche Entwicklungen und politische Beobachtung

Die Diskussion um Digitale Souveränität bei Cloud-Diensten ist im politischen Raum allgegenwärtig. Bereits 2019 wurde im Kontext von Gaia-X das Projekt „Sovereign Cloud Stack" mit Mitteln der Bundesagentur für Sprunginnovationen (SPRIND) an- und später mit Fördergeldern des Bundesministeriums für Wirtschaft und Energie (BMWi) weiterfinanziert. Das Ziel: durch offene und einheitliche Standards und Schnittstellen ein Höchstmaß an Digitaler Souveränität beim Cloud-Betrieb ermöglichen.[10]

In 2020 befassten sich die Förderale IT-Kooperation (FITKO) und das BMI innerhalb der Deutschen Verwaltungscloud-Strategie mit der Thematik und legten die Wechselfähigkeit als Kernanforderung an einen souveränen Cloud-Betrieb fest.[11] 2023 setzte sich auch die Datenschutzkonferenz der Länder (DSK) eingehend mit Digitaler Souveränität im Kontext von Cloud-Angeboten auseinander.[12]

In einem Positionspapier definierte sie sehr detaillierte Kriterien für eine souveräne Cloud-Nutzung – darunter explizit:

- vollständige Kontrolle über den Einsatzort und Zugriff auf Daten,
- nachvollziehbare und gestaltbare technische Prozesse
- und die Möglichkeit, bei Bedarf Anbieter zu wechseln oder Dienste selbst zu betreiben.

Demnach können Cloud-Lösungen laut DSK keine rechtskonforme Alternative sein, wenn zentrale Kriterien wie die vollständige Kontrollierbarkeit und Gestaltungsfähigkeit nicht erfüllt sind.

Auch Bund und Länder haben die Digitale Souveränität weiter fest im Blick. Im Mai 2025 beschlossen die Digitalminister der Länder auf der Digitalministerkonferenz (DMK) eine Stärkung der Digitalen Souveränität in der öffentlichen Verwaltung inklusive einer Bitte an den Bund, den Einsatz von normierten und offenen Standards sowie offener Software zu gewährleisten.[13] Und auch die schwarz-rote Bundesregierung bekennt sich in ihrem Koalitionsvertrag klar dazu, die Digitale Souveränität mithilfe offener Schnittstellen und Standards sowie Open Source gezielt voranzutreiben.[14] Auf übergeordneter Ebene wiederum formuliert der EU Data Act mit dem Ziel der Stärkung von Kundenrechten klare Anforderungen an die Offenheit und Wechselfähigkeit von Cloud-Angeboten. Er tritt im September 2025 in Kraft.[15]

Quickcheck souveräne Clouds

- ☐ Bietet volle Datensouveränität (u. a. DSGVO-Konformität, kein Zugriff bspw. durch US-Behörden)
- ☐ Bietet volle technologische Souveränität (Kontrolle über Updates, Gestaltungsfähigkeit, Betriebssicherheit etc.)
- ☐ Ermöglicht Anbieterwechsel (bspw. durch offene Standards & Schnittstellen, d. h. kein Vendor-Lock-in)
- ☐ Bietet ein Höchstmaß an Transparenz (z. B. durch offenen Quellcode)

[10] https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Parlamentarische-Anfragen/2021/06/5-407.pdf?__blob=publicationFile&v=1

[11] https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/Deutsche_Verwaltungscloud_Strategie.pdf?__blob=publicationFile&v=2

[12] https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf

[13] https://www.dmk.rlp.de/fileadmin/dmk/Beschluesse_3_DMK/TOP_6.02_SH_Staerkung_digitaler_Souveraenitaet_OEV_beschluss.pdf

[14] https://www.koalitionsvertrag2025.de/sites/www.koalitionsvertrag2025.de/files/koav_2025.pdf

[15] https://digital-strategy.ec.europa.eu/de/factpages/data-act-explained

6. Das Wichtigste in Kürze

Digitale Souveränität ist in Politik und Verwaltung seit vielen Jahren klar definiert. Es geht um Handlungsfähigkeit, Selbstbestimmung und Sicherheit – allesamt Aspekte, die Kontrolle, Wechselfähigkeit und Transparenz über die eigene IT voraussetzen.

Dennoch werden zunehmend Cloud-Angebote als „souverän“ vermarktet, die diese Kriterien nicht oder nur teilweise erfüllen. Darunter fällt auch der Versuch, die Begriffe „Datensouveränität“ und „Digitale Souveränität“ de facto gleichzusetzen und somit Angebote aufzuwerten.

Um sicherzustellen, dass ein Cloud-Angebot die Anforderungen an Digitale Souveränität nicht nur auf dem Papier, sondern auch faktisch erfüllt, müssen die Marketingversprechen der Provider entsprechend kritisch entlang der in der Verwaltung festgelegten Definition von Digitaler Souveränität hinterfragt werden.

Um die Bewertung des Souveränitätsgrades von IT-Angeboten (Software, Infrastruktur, Cloud etc.) zu erleichtern, arbeitet das ZenDiS derzeit an einem Souveränitätscheck, der perspektivisch eine Analyse und Beurteilung entlang transparenter und klarer Kriterien erlauben soll. Bis dahin liefert dieses Paper eine erste gute Orientierung. Bei Beratungsbedarf steht das ZenDiS gerne zur Verfügung.

Über das ZenDiS
Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) wurde 2022 durch das Bundesministerium des Innern und für Heimat (BMI) gegründet. Als Kompetenz- und Servicezentrum unterstützt das ZenDiS die Öffentliche Verwaltung auf der Ebene von Bund, Ländern und Kommunen dabei, ihre Handlungsfähigkeit im digitalen Raum langfristig abzusichern – vor allem, indem kritische Abhängigkeiten von einzelnen Technologieanbietern aufgelöst werden. Dazu konzentriert sich das ZenDiS in der ersten Ausbaustufe darauf, den Einsatz von Open-Source-Software in der Öffentlichen Verwaltung voranzutreiben.

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung ist eine GmbH und liegt derzeit zu 100 Prozent in der Hand des Bundes. Eine Beteiligung der Länder ist in Vorbereitung. Geschäftsführer ist Alexander Pockrandt. Sitz des ZenDiS ist Bochum.

Herausgeber
Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) GmbH
Suttner-Nobel-Allee 4 | 44803 Bochum

Stand
August 2025