lancon

Wir beraten Unternehmen und versorgen sie mit

- Internet & Glasfaser
- Standortvernetzung & SD-WAN
- Cloud & Rechenzentrum
- Cyber Security
- Telefonie, Mobilfunk & Kommunikation

Digitale Souveränität

Wie frei ist Ihre IT noch?

Abhängigkeiten erkennen. Wahlfreiheit erhalten. IT-Infrastrukturen so aufstellen, dass Entscheidungen auch morgen noch möglich sind.

54 %	**70 %**	**62 %**
deutsche Unternehmen nutzen kostenpflichtige Cloud-Services	des europäischen Cloud-Markts entfallen auf drei Anbieter	sagen: Ohne Cloud-Dienste stünde das Geschäft still

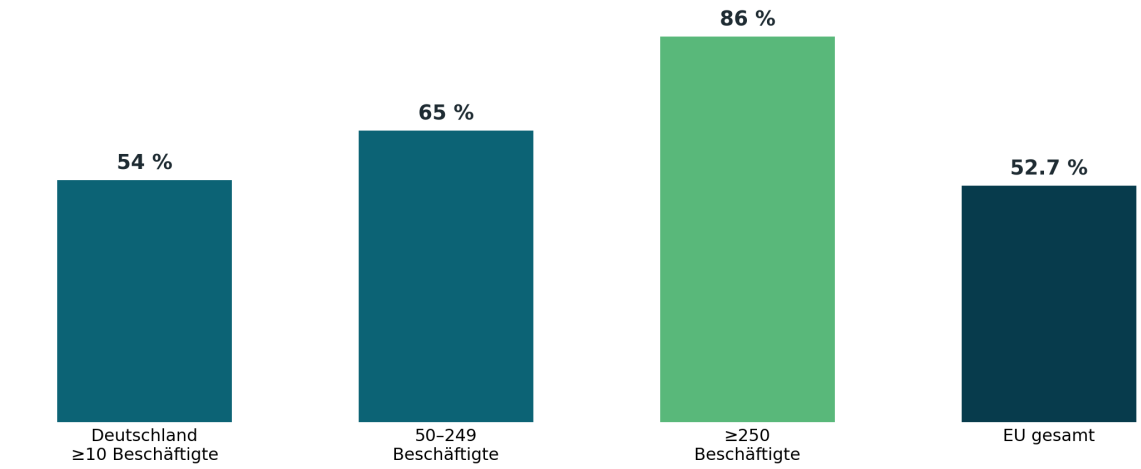
Management Summary

Cloud, Software-as-a-Service und externe IT-Dienstleister sind heute elementarer Bestandteil der Unternehmens-IT.

54 Prozent der deutschen Unternehmen mit mindestens zehn Beschäftigten nutzten 2025 kostenpflichtige Cloud-Services. Bei Großunternehmen ab 250 Beschäftigten waren es bereits 86 Prozent. Gleichzeitig entfallen rund 70 Prozent des europäischen Marktes für Cloud-Infrastruktur auf nur drei Anbieter: Amazon, Microsoft und Google.

Anteil der Unternehmen mit kostenpflichtigen Cloud-Services, 2025

Cloud-Nutzung ist im Unternehmensalltag angekommen



Quellen: Statistisches Bundesamt 2025; Eurostat 2026.

Das ist zunächst kein Problem. Leistungsfähige globale Plattformen haben Digitalisierung beschleunigt, Innovation ermöglicht und IT-Infrastrukturen flexibler gemacht.

Problematisch wird es dort, wo aus Nutzung Abhängigkeit wird.

Wenn Daten nur mit erheblichem Aufwand exportiert werden können, Anwendungen auf proprietären Diensten aufbauen, zentrale Kompetenzen ausschließlich beim Dienstleister liegen oder ein Anbieterwechsel technisch zwar möglich, wirtschaftlich aber kaum noch vertretbar ist, verliert ein Unternehmen Handlungsspielraum.

Genau darum geht es bei digitaler Souveränität.

Digitale Souveränität bedeutet nicht, alles selbst zu betreiben. Sie bedeutet auch nicht, ausschließlich deutsche oder europäische Technologien einzusetzen.

Sie beschreibt die Fähigkeit eines Unternehmens, über seine Daten, Technologien und digitalen Infrastrukturen selbstbestimmt entscheiden zu können – und getroffene Entscheidungen später auch verändern zu können.

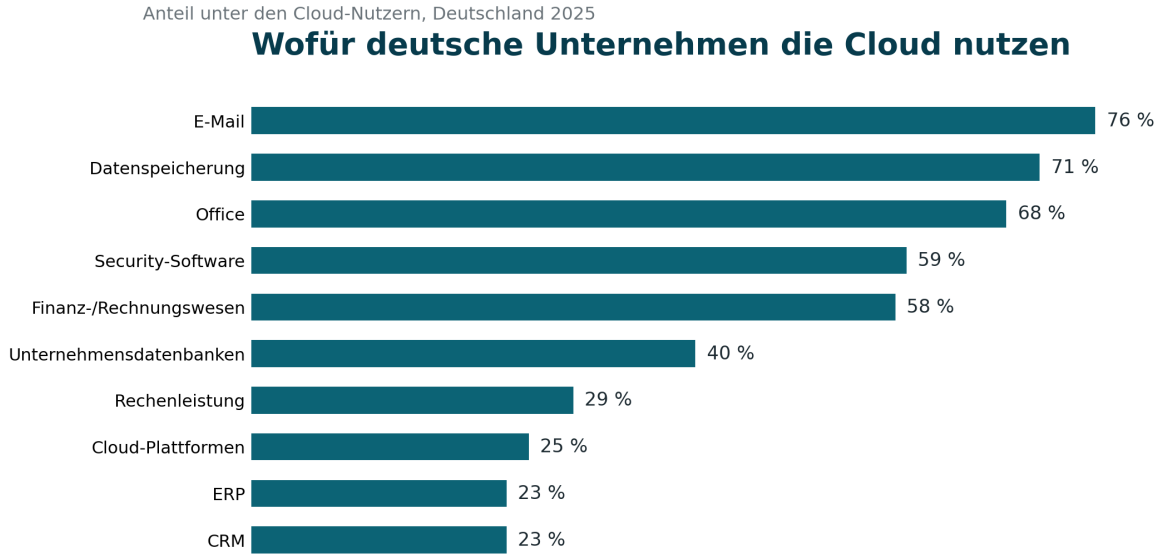
Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung, ZenDiS, stellt dabei insbesondere Wechselmöglichkeit und Gestaltungsfähigkeit in den Mittelpunkt: Organisationen müssen zwischen IT-Lösungen und Anbietern wechseln und ihre IT verstehen, bewerten und bei Bedarf mitgestalten können.

Digitale Souveränität ist damit vor allem eines: Handlungsfähigkeit.

1. Unsere IT wird leistungsfähiger – und abhängiger

Cloud Computing hat sich in wenigen Jahren von einer Alternative zum eigenen Rechenzentrum zu einer tragenden Säule moderner IT entwickelt.

2025 nutzten 54 Prozent der deutschen Unternehmen mit mindestens zehn Beschäftigten kostenpflichtige Cloud-Services. Bei Unternehmen mit 50 bis 249 Beschäftigten waren es 65 Prozent, bei Unternehmen mit mindestens 250 Beschäftigten 86 Prozent.



Quelle: Statistisches Bundesamt, Nutzung von Cloud Computing nach Beschäftigtengrößenklassen und Diensten, 2025.

EU-weit ergibt sich ein ähnliches Bild. 52,7 Prozent der Unternehmen nutzten 2025 kostenpflichtige Cloud-Dienste. 2014 waren es erst 17,8 Prozent.

Der Bitkom Cloud Report 2025 kommt zu dem Ergebnis, dass bei den dort befragten Unternehmen bereits rund 47 Prozent aller IT-Anwendungen aus der Cloud betrieben werden. 62 Prozent der befragten Unternehmen erklären, ihr Geschäft würde ohne Cloud-Dienste stillstehen.

Die Frage lautet deshalb längst nicht mehr: Cloud oder keine Cloud?

Sondern: Wie gestalten Unternehmen ihre Cloud- und IT-Infrastruktur so, dass sie leistungsfähig bleibt, ohne unnötige Abhängigkeiten aufzubauen?

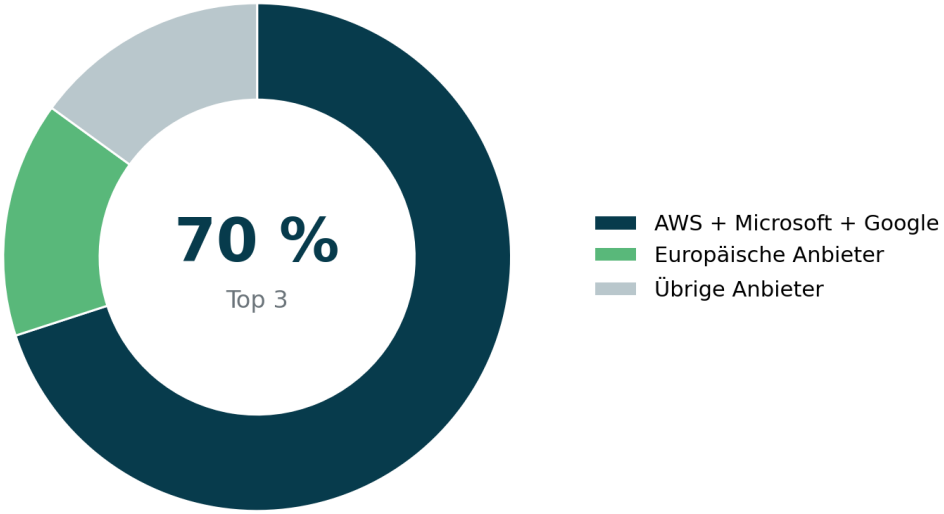
2. Drei Anbieter beherrschen rund 70 Prozent des europäischen Cloud-Marktes

Parallel zum starken Wachstum der Cloud-Nutzung hat sich der Markt erheblich konzentriert.

Der europäische Markt für Cloud-Infrastrukturdienste erreichte 2024 nach Berechnungen der Synergy Research Group rund 61 Milliarden Euro. Europäische Anbieter kamen gemeinsam auf etwa 15 Prozent Marktanteil. Amazon, Microsoft und Google vereinten dagegen rund 70 Prozent des europäischen Marktes auf sich.

Marktanteile Cloud-Infrastruktur in Europa, 2024

Europas Cloud-Infrastruktur ist stark konzentriert



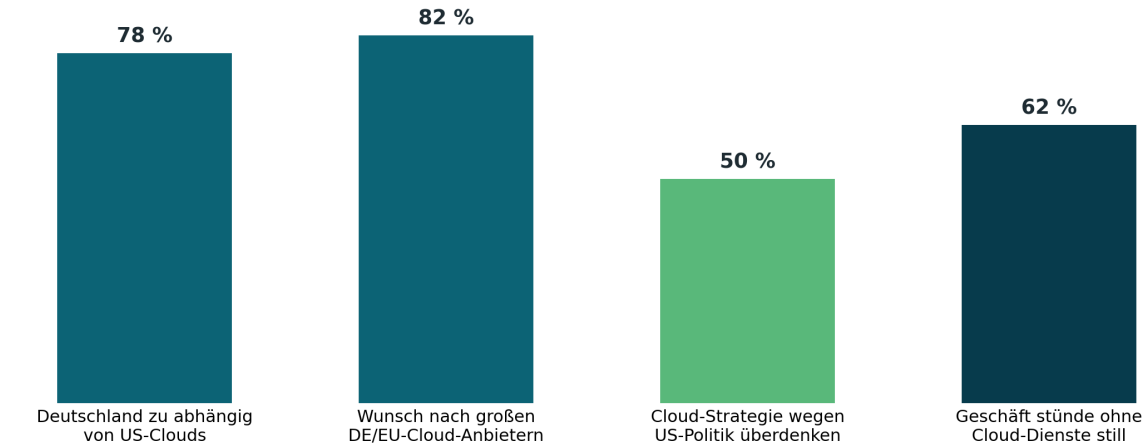
Quelle: Synergy Research Group, European Cloud Providers' Local Market Share Now Holds Steady at 15%, 24.07.2025.

Die Umsätze europäischer Cloud-Anbieter sind nicht eingebrochen. Sie haben sich zwischen 2017 und 2024 sogar mehr als verdreifacht. Der Gesamtmarkt ist allerdings ungefähr um den Faktor sechs gewachsen.

Europas Problem ist damit nicht das Fehlen leistungsfähiger Anbieter. Es ist vor allem ein Größen- und Konzentrationsproblem.

Ergebnisse des Bitkom Cloud Report 2025

Unternehmen sehen die Abhängigkeit selbst



Quelle: Bitkom Cloud Report 2025.

78 Prozent der vom Bitkom befragten Unternehmen halten Deutschland für zu abhängig von US-amerikanischen Cloud-Anbietern. 82 Prozent wünschen sich große Cloud-Anbieter aus Deutschland oder Europa. Die Hälfte der Cloud-Nutzer erklärte 2025, aufgrund der politischen Entwicklung in den USA die eigene Cloud-Strategie überdenken zu müssen.

3. Digitale Abhängigkeit reicht weit über die Cloud hinaus

Cloud ist nur ein Teil des Problems.

Eine 2025 von der Bertelsmann Stiftung veröffentlichte EuroStack-Analyse kommt zu dem Ergebnis, dass mehr als 80 Prozent der in Europa eingesetzten digitalen Technologien und Infrastrukturen importiert werden. Rund 70 Prozent der weltweit verwendeten grundlegenden KI-Modelle stammen aus den USA. Europäische Unternehmen verantworten lediglich etwa sieben Prozent der globalen Forschungsaufwendungen für Software und Internet.

Digitale Abhängigkeit reicht weit über die Cloud hinaus

EuroStack-Analyse / Bertelsmann Stiftung, 2025

>80 %	70 %	7 %
der in Europa eingesetzten digitalen Technologien und Infrastrukturen werden importiert	der weltweit eingesetzten grundlegenden KI-Modelle stammen aus den USA	Anteil europäischer Unternehmen an den globalen F&E-Aufwendungen für Software und Internet

Quelle: Bertelsmann Stiftung, EuroStack – A European Alternative for Digital Sovereignty, 2025.

Abhängigkeiten entstehen deshalb auf zahlreichen Ebenen gleichzeitig:

Halbleiter → Hardware → Rechenzentrum → Virtualisierung → Betriebssystem → Netzwerk → Cloud → Plattform → Software → Identität → Security → KI → Daten

Eine Organisation kann auf einer Ebene sehr souverän und auf einer anderen vollständig abhängig sein. Digitale Souveränität lässt sich deshalb nicht anhand eines einzelnen Produktmerkmals beurteilen. Sie muss über die gesamte Liefer- und Technologiekette betrachtet werden.

4. Ein Server in Frankfurt macht noch keine souveräne Cloud

Bei Cloud-Angeboten wird häufig mit dem Speicherort der Daten argumentiert: „Ihre Daten liegen in Deutschland.“ Das ist wichtig. Für eine Bewertung digitaler Souveränität reicht diese Information jedoch nicht aus.

- Wem gehört der Anbieter und welchen Rechtsordnungen unterliegt er?

- Wer betreibt und administriert die Systeme?
- Wer verfügt über privilegierte Zugänge und kryptographische Schlüssel?
- Wo befinden sich Support- und Administrationsorganisationen?
- Welche Unterauftragnehmer und Technologie-Stacks werden eingesetzt?
- Lassen sich Daten vollständig exportieren und Anwendungen übertragen?
- Wie lange würde ein Wechsel dauern – und was würde er kosten?

Die Europäische Kommission verfolgt inzwischen genau diesen breiteren Ansatz. Ihr 2026 vorgestelltes Cloud Sovereignty Framework bewertet Cloud-Souveränität anhand von 48 Kriterien in acht Bereichen.

48	8	SEAL 0–4
Kriterien im EU Cloud Sovereignty Framework	Souveränitätsdimensionen	Bewertungsstufen für Souveränität

Die Bereiche umfassen strategische, rechtliche und jurisdiktionelle, Daten- und KI-bezogene, operative, Lieferketten- und technologische Souveränität sowie Sicherheit/Compliance und ökologische Nachhaltigkeit.

Damit wird klar: Der Standort der Daten ist ein Kriterium. Nicht das Kriterium.

5. Souveränität wird messbar

Mit dem Cloud Sovereignty Framework hat die EU-Kommission sogenannte Sovereignty Effectiveness Assurance Levels – SEAL – eingeführt. Die Skala reicht von SEAL-0 bis SEAL-4. SEAL-2 steht für ein definiertes Niveau der Datensouveränität; SEAL-4 beschreibt die höchste Stufe mit einer vollständigen europäischen Lieferkette von Chips bis zur Software.

Interessant ist daran weniger die konkrete Bewertung einzelner Anbieter. Entscheidend ist der methodische Wechsel: Digitale Souveränität wird nicht mehr nur als politisches Ziel behandelt, sondern anhand überprüfbarer Kriterien.

6. Sieben Ebenen digitaler Souveränität

6.1 Datenhoheit

Wo liegen die Daten? Wer kann technisch darauf zugreifen? Wer verfügt über Schlüssel und privilegierte Berechtigungen? Können Daten vollständig exportiert und nach Vertragsende nachweisbar gelöscht werden?

6.2 Rechtliche und jurisdiktionelle Souveränität

Ein physischer Serverstandort und der Rechtsraum eines Anbieters sind nicht zwangsläufig identisch. Für personenbezogene Daten erlaubt die DSGVO internationale Datenübermittlungen unter definierten Voraussetzungen. Datenschutzkonformität und digitale Souveränität bleiben jedoch unterschiedliche Fragen.

6.3 Technologische Souveränität

Wie stark hängt eine Anwendung von proprietären Funktionen eines bestimmten Herstellers ab? Ein virtueller Server mit standardisiertem Betriebssystem ist meist leichter zu migrieren als eine Anwendung, die tief in

proprietäre Datenbanken, Identity-Dienste, Serverless-Funktionen oder herstellerspezifische APIs integriert ist.

6.4 Operative Souveränität

Wer kann das System tatsächlich betreiben? Fehlendes internes Know-how, nur beim Anbieter vorhandene Administrationsrechte und unzureichende Dokumentation können operative Abhängigkeit erzeugen – auch wenn die Daten dem Unternehmen gehören.

6.5 Lieferketten-Souveränität

Unter einem sichtbaren Cloud-, Netzwerk- oder Security-Anbieter können Rechenzentrumsbetreiber, Carrier, Hardwarehersteller, Plattformen und Managed-Service-Provider stehen. Zwei Vertragspartner bedeuten deshalb nicht automatisch zwei unabhängige Lieferketten.

6.6 Wechselfähigkeit

Kann das Unternehmen einen Anbieter tatsächlich innerhalb eines wirtschaftlich und operativ vertretbaren Zeitraums wechseln? Zu prüfen sind Datenformate, APIs, Dokumentation, Identitäten, proprietäre Plattformdienste, Kündigungsregeln und verfügbare Alternativen.

6.7 Wirtschaftliche Souveränität

Technische Portabilität allein reicht nicht. Eine Migration kann technisch möglich und wirtschaftlich trotzdem unrealistisch sein. Preisänderungsrechte, Lizenzkosten, Mindestabnahmen, Laufzeiten und Migrationsaufwand gehören daher in die Bewertung.

Der europäische Data Act stärkt die Wechselfähigkeit ausdrücklich. Ab 12. Januar 2027 werden Switching Charges einschließlich Data-Egress-Gebühren im Anwendungsbereich der Regelungen vollständig abgeschafft.

12.01.2027

Abschaffung von Switching-/Data-Egress-Gebühren im Data Act

7. Multi-Cloud ist nicht automatisch souverän

41 Prozent der im Bitkom Cloud Report 2025 befragten Unternehmen setzen bereits auf Multi-Cloud, 29 Prozent auf Hybrid-Cloud-Modelle.

Anteil der befragten Unternehmen, Bitkom Cloud Report 2025

Mehrere Clouds sind noch keine Exit-Strategie



Quelle: Bitkom Cloud Report 2025.

Das kann Risiken reduzieren, muss es aber nicht. Wer kritische Dienste gleichzeitig tief in AWS und Microsoft Azure integriert, besitzt möglicherweise nicht weniger Abhängigkeiten, sondern zwei unterschiedliche.

Mehr Anbieter sind noch keine Exit-Strategie.

8. Auch eine Private Cloud kann abhängig sein

Auch eine Private Cloud oder eine eigene Infrastruktur ist nicht automatisch souverän. Abhängigkeiten können in Virtualisierung, Betriebssystem, Datenbank, Storage, Backup, Netzwerk, Security, Hardware und Lizenzmodellen stecken.

Digitale Souveränität ist deshalb keine Entscheidung zwischen Public und Private Cloud. Sie ist eine Architektur- und Beschaffungsfrage.

9. Souveränität ist auch Resilienz

Abhängigkeiten werden besonders dann sichtbar, wenn etwas ausfällt. Die ENISA Threat Landscape 2026 stellt fest, dass digitale Abhängigkeiten die Angriffsfläche erweitern und die Auswirkungen von Cybervorfällen vergrößern können.

Cyberrisiko macht Abhängigkeiten sichtbar

Bitkom Wirtschaftsschutz 2025

289,2 Mrd. €

geschätzter Schaden durch Datendiebstahl, Industriespionage und Sabotage in Deutschland 2025

70 %

des Schadens laut Bitkom unmittelbar auf Cyberangriffe zurückzuführen

Quelle: Bitkom Wirtschaftsschutz 2025. Ergänzend: ENISA Threat Landscape 2026.

Souveränität und Cybersecurity sind nicht dasselbe. Sie beeinflussen sich aber unmittelbar. Eine resiliente Architektur sollte nicht nur gegen Angriffe schützen, sondern auch vermeiden, dass der Ausfall eines einzelnen Dienstes, Providers oder Technologiebausteins das gesamte Unternehmen handlungsunfähig macht.

10. Regulierung rückt Abhängigkeiten in den Fokus

NIS2

Mit Inkrafttreten des deutschen NIS-2-Umsetzungsgesetzes am 6. Dezember 2025 gelten für betroffene Unternehmen unter anderem Registrierungs- und Meldepflichten. NIS2 stärkt zugleich Anforderungen an Risikomanagement, Business Continuity, Incident Management und Lieferkettensicherheit.

DORA

Für Finanzunternehmen geht der Digital Operational Resilience Act weiter. Die Verordnung gilt seit 17. Januar 2025 und harmonisiert Anforderungen an ICT-Risikomanagement, Incident Reporting, Resilienztests und Third-Party-Risk-Management. DORA verlangt bei kritischen oder wichtigen Funktionen eine Bewertung von ICT-Konzentrationsrisiken, insbesondere wenn Dienstleister nicht einfach substituierbar sind.

06.12.2025	17.01.2025
NIS2-Umsetzungsgesetz in Deutschland in Kraft	DORA gilt in der EU

11. Europa reagiert

Im April 2026 vergab die Europäische Kommission einen Rahmenvertrag über souveräne Cloud-Dienste mit einem Volumen von bis zu 180 Millionen Euro über sechs Jahre. Die Vergabe an mehrere Anbieter wurde ausdrücklich auch mit Diversifizierung, Resilienz und der Vermeidung von Lock-in begründet.

180 Mio. €	6 Jahre	4
maximales Volumen des EU-Rahmenvertrags	Laufzeit	Anbieter bzw. Konsortien

Die Kommission hält dabei auch nicht-europäische Technologie unter geeigneten organisatorischen und technischen Rahmenbedingungen für vereinbar mit definierten Souveränitätsniveaus. Digitale Souveränität ist damit keine Herkunftsideologie. Es geht um kontrollierbare Abhängigkeiten.

12. Vier typische Situationen aus der Praxis

Microsoft 365

Ein europäischer Datenstandort beantwortet noch nicht die Frage, wie stark Mail, Office, Teams, SharePoint, OneDrive, Identity, Security und Geräteverwaltung miteinander verzahnt sind. Entscheidend ist, welche Funktionen mit vertretbarem Aufwand ersetzt werden könnten.

Hyperscale Cloud

Mit Managed Databases, Serverless, proprietären Storage-Diensten, Identity, Monitoring und KI steigt der Komfort – aber häufig auch der Migrationsaufwand. Architekturentscheidungen sollten deshalb bewusst zwischen plattformspezifischer Effizienz und Portabilität abwägen.

Backup

Liegt das Backup beim selben Provider und hängt vom selben Identity- oder Administrationsmodell ab wie die Produktion, ist Datenredundanz vorhanden – aber nicht zwingend Redundanz der Abhängigkeit.

Connectivity

Zwei Internetzugänge verschiedener Vertragspartner können im Hintergrund dieselbe Glasfasertrasse oder denselben Vorlieferanten nutzen. Anbieterdiversität und technische Diversität sind zwei verschiedene Dinge.

13. Der lancon Souveränitäts-Check

Die folgende Kurzbewertung ist keine Zertifizierung und ersetzt keine technische oder rechtliche Prüfung. Sie hilft jedoch, kritische Abhängigkeiten systematisch sichtbar zu machen.

Bereich	Prüffrage	Punkte
Daten	Wissen wir, wo kritische Daten gespeichert, verarbeitet und gesichert werden?	/5
Zugriff	Wissen wir, wer technisch und administrativ auf diese Daten zugreifen kann?	/5
Schlüssel	Haben wir angemessene Kontrolle über Verschlüsselung und Schlüsselmanagement?	/5
Rechtsraum	Kennen und bewerten wir die Jurisdiktionen unserer kritischen Anbieter?	/5
Technologie	Können wir zentrale Anwendungen ohne vollständige Neuentwicklung übertragen?	/5
Betrieb	Besitzen wir intern oder über alternative Partner ausreichendes Know-how?	/5
Lieferkette	Kennen wir wesentliche Subunternehmer, Vorleister und technische Abhängigkeiten?	/5
Redundanz	Sind Backup, Leitungen und Ausweichsysteme technisch wirklich unabhängig?	/5
Vertrag	Enthalten Verträge klare Regelungen zu Datenexport, Exit, Unterstützung und Löschung?	/5
Exit	Existiert für kritische Services ein realistisches, getestetes Exit-Szenario?	/5

Maximal 50 Punkte. Der Gesamtwert ist weniger wichtig als die Verteilung: Ein einziges kritisches System kann trotz gutem Gesamtergebnis die Handlungsfähigkeit des Unternehmens bestimmen.

14. Fünf Schritte zu mehr digitaler Souveränität

1. Abhängigkeiten sichtbar machen

Welche Anwendungen, Daten, Leitungen, Cloud-Dienste und Security-Systeme sind geschäftskritisch? Welche Hersteller und Vorleister stecken dahinter?

2. Kritikalität bewerten

Nicht jeder Dienst benötigt maximale Souveränität. Souveränität sollte risikobasiert nach Daten, Funktion und Ausfallwirkung bewertet werden.

3. Exit vor dem Einstieg planen

Datenexport, Formate, Schnittstellen, Kündigungsfristen, Migrationsunterstützung, Löschung, Kosten und technische Alternativen gehören in die Beschaffung.

4. Architektur und Beschaffung gemeinsam betrachten

Ein günstiger Vertrag kann langfristig teuer werden, wenn er technologische Abhängigkeit erzeugt. Technik, Providerstruktur, Betrieb und Markt müssen gemeinsam betrachtet werden.

5. Souveränität regelmäßig überprüfen

Anbieter, Preise, Produkte, Regulierung und technische Alternativen verändern sich. Souveränität ist deshalb Teil kontinuierlicher IT- und Risikosteuerung.

15. Nicht alles selbst machen. Aber selbst entscheiden können.

Die Diskussion um digitale Souveränität wird schnell grundsätzlich: Europa gegen USA, Open Source gegen proprietäre Software, Private Cloud gegen Public Cloud, Eigenbetrieb gegen Outsourcing.

Für Unternehmen helfen solche Gegensätze wenig. AWS, Azure oder Microsoft 365 können für eine konkrete Anforderung genau die richtige Lösung sein. Ein regionales Rechenzentrum kann für eine andere Anwendung besser passen. Manche Systeme gehören möglicherweise in eine souveräne europäische Cloud, andere in eine Public Cloud, wieder andere in eine lokale Infrastruktur.

Entscheidend ist nicht, welcher Anbieter grundsätzlich der richtige ist. Entscheidend ist, welcher Anbieter, welche Architektur und welches Betriebsmodell zur jeweiligen Anforderung und zum akzeptierten Risiko passen – und wie einfach diese Entscheidung später verändert werden kann.

Digitale Souveränität bedeutet nicht Unabhängigkeit von allem. Sie bedeutet Kontrolle über die eigenen Abhängigkeiten.

lancon

Anbieterneutral beraten. Marktgerecht beschaffen.

Digitale Souveränität beginnt mit Transparenz über bestehende Abhängigkeiten.

lancon betrachtet nicht nur einzelne Produkte, sondern das Zusammenspiel von Connectivity, Rechenzentrum, Cloud, Security, Kommunikation und Betrieb.

Wir analysieren bestehende Strukturen, vergleichen technische und wirtschaftliche Alternativen und prüfen, welche Provider- und Betriebsmodelle zur jeweiligen Anforderung passen.

Damit entsteht keine IT-Landschaft nach Ideologie. Sondern eine Infrastruktur, bei der Unternehmen wissen, wovon sie abhängig sind, warum sie es sind – und welche Alternativen sie haben.

Quellen und weiterführende Literatur

Statistisches Bundesamt (Destatis), 24.11.2025: Jedes zweite Unternehmen nutzt kostenpflichtige Cloud-Services; Nutzung von Cloud Computing nach Beschäftigtengrößenklassen.
https://www.destatis.de/DE/Presse/Pressemitteilungen/2025/11/PD25_416_52911.html

Eurostat, 03.02.2026: 53% EU enterprises used paid cloud services in 2025.
https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260203-1

Bitkom, 11.06.2025: Cloud Report 2025 / Wirtschaft ruft nach einer deutschen Cloud.
https://www.bitkom.org/Presse/Presseinformation/Wirtschaft-ruft-nach-deutscher-Cloud

Synergy Research Group, 24.07.2025: European Cloud Providers' Local Market Share Now Holds Steady at 15%. https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15

Bertelsmann Stiftung, 2025: EuroStack – A European Alternative for Digital Sovereignty.
https://www.bertelsmann-stiftung.de/doi/10.11586/2025006

Europäische Kommission, 01.06.2026: Sovereign Cloud Framework explained / Implementation Guidance.
https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

Europäische Kommission, 17.04.2026: Commission advances cloud sovereignty through strategic procurement. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en

Europäische Kommission: Data Act explained – Switching, Interoperabilität und Egress-Gebühren.
https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

Europäische Kommission: Angemessenheitsbeschlüsse / EU-US Data Privacy Framework.
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

U.S. Department of Justice: Clarifying Lawful Overseas Use of Data Act – CLOUD Act.
https://www.justice.gov/archives/opa/pr/justice-department-announces-publication-white-paper-cloud-act

BSI: Informationen zur Umsetzung von NIS2 in Deutschland. https://mip2.bsi.bund.de/de/info-nis2-registrierung/

ESMA: Digital Operational Resilience Act – DORA. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora

ENISA, 22.09.2026: ENISA Threat Landscape 2026. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

Bitkom: Wirtschaftsschutz 2025 – Schäden durch Datendiebstahl, Industriespionage, Sabotage und Cyberattacken. https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf

ZenDiS: Unser Auftrag – Digitale Souveränität, Wechselmöglichkeit und Gestaltungsfähigkeit.
https://www.zendis.de/unser-auftrag

Stand der Recherche: Oktober 2026. Dieses Whitepaper dient der allgemeinen Information und stellt keine Rechtsberatung dar.