Cloud Made in Germany Kritik Aufschrei: Realität oder Hype?

Category: Opinion
geschrieben von Tobias Hager | 12. September 2025



Cloud Made in Germany Kritik Aufschrei: Realität oder Hype?

Du hast genug von PR-Getöse, inhaltsleeren “Digital Souveränität”-Versprechen und der nächsten “Cloud Made in Germany”-Lösung, die angeblich alles besser, sicherer und unabhängiger macht? Willkommen im Maschinenraum der Wahrheit. Wir zerlegen die deutsche Cloud-Industrie gnadenlos – von DSGVO-Mythen bis zu geopolitischen Placebo-Produkten – und zeigen, was wirklich hinter dem aktuellen Aufschrei steckt. Spoiler: Wer glaubt, Cloud Made in Germany sei automatisch die bessere Cloud, sollte dringend weiterlesen.

- Was “Cloud Made in Germany” wirklich bedeutet – Marketingbegriff,

politisches Feigenblatt oder technisches Upgrade?
- Die wichtigsten technischen und rechtlichen Anforderungen an eine deutsche Cloud
- Warum Datenstandort allein keine Sicherheit bringt: DSGVO, Schrems II & die Illusion der “digitalen Souveränität”
- Technische Herausforderungen deutscher Cloud-Anbieter: Skalierung, Infrastruktur und Innovationsdruck
- Vergleich: Deutsche Cloud-Player vs. Hyperscaler – wo liegen die echten Unterschiede?
- Die größten Mythen rund um “Cloud Made in Germany” – und was wirklich zählt
- Schritt-für-Schritt-Checkliste: Wann macht ein deutscher Cloud-Anbieter Sinn, wann nicht?
- Warum der aktuelle Aufschrei mehr mit Politik und PR zu tun hat als mit echten Innovationen
- Wie du als Unternehmen eine Cloud-Entscheidung triffst, die mehr ist als Greenwashing
- Ein kritisches Fazit: Was bleibt vom “Cloud Made in Germany”-Hype übrig?

Cloud Made in Germany – das klingt nach Sicherheit, nach Kontrolle, nach digitaler Unabhängigkeit. Nach einem Bollwerk gegen böse US-Konzerne, neugierige Staaten und undurchsichtige Datenströme. Und genau das ist die Marketing-Story, die aktuell in jedem zweiten Whitepaper, auf jeder zweiten Podiumsdiskussion und in jeder zweiten LinkedIn-Timeline rauf und runter gespielt wird. Aber wie viel Realität steckt tatsächlich hinter diesem neuen Cloud-Patriotismus? Ist “Cloud Made in Germany” ein echter Gamechanger für Datenschutz und IT-Sicherheit, oder doch nur das nächste Buzzword, das in der Praxis an der harten Realität zerbricht?

Die Wahrheit ist weniger sexy als das Versprechen. Cloud Made in Germany ist weder ein Garant für Datenschutz, noch eine technologische Revolution. Es ist zu oft ein politischer Reflex und eine Reaktion auf die Angst vor Kontrollverlust – gepaart mit der Hoffnung, endlich im globalen Cloud-Geschäft mitspielen zu können. Aber technischer Vorsprung, Innovationskraft und wirkliche Unabhängigkeit entstehen nicht durch Standortetiketten, sondern durch harte Arbeit, Investments, Skalierung und echte Souveränität auf allen Ebenen. Und genau hier trennt sich der Marketing-Nebel von der Realität.

In diesem Artikel nehmen wir die wichtigsten Aspekte auseinander: Was steckt technisch und rechtlich hinter einer deutschen Cloud? Wo liegen die echten Stärken, wo die Schwächen? Und was bleibt vom aktuellen “Cloud Made in Germany”-Aufschrei übrig, wenn man Marketing, Politik und Lobbyismus abzieht? Willkommen zur schonungslosen Analyse – ohne Filter, ohne Bullshit.

Cloud Made in Germany: Definition, Anspruch und

Realität der deutschen Cloud

Was ist “Cloud Made in Germany” eigentlich? Der Begriff klingt nach DIN-Norm, nach TÜV-Siegel und einem sicheren Hafen für Daten. Die Realität: Es gibt keine einheitliche Definition, kein offizielles Gütesiegel und keine klaren technischen Anforderungen, die diese Bezeichnung verbindlich regeln würden. Jeder Anbieter, der seine Server in Deutschland betreibt oder eine deutsche GmbH als Firmierung hat, kann sich das Label auf die Website kleben – und viele tun das auch. Doch reicht das?

Der Anspruch: Cloud Made in Germany soll Unternehmen und Behörden Schutz bieten vor ausländischem Datenzugriff, insbesondere durch US-Gesetze wie den CLOUD Act oder Patriot Act. Gleichzeitig wird suggeriert, dass deutsche Cloud-Lösungen technisch ausgereifter, sicherer und datenschutzfreundlicher seien als internationale Alternativen. Die Wahrheit ist komplexer. Denn die meisten deutschen Anbieter bauen auf denselben Technologien auf wie die internationalen Hyperscaler – von Virtualisierung über Containerisierung bis zu Infrastruktur-Automatisierung via Kubernetes.

Technisch gesehen muss eine “deutsche Cloud” mindestens folgende Merkmale erfüllen:

- Datenhaltung in deutschen Rechenzentren
- Betreiber mit Hauptsitz und juristischer Verantwortung in Deutschland
- Einhaltung der DSGVO sowie zusätzlicher deutscher Datenschutzanforderungen
- Zertifizierungen wie ISO 27001, BSI C5 oder TISAX
- Transparenz über Betriebs- und Supportstrukturen

Aber selbst wenn all diese Kriterien erfüllt sind, ist damit noch lange nicht garantiert, dass die Cloud auch wirklich “sicherer” oder “besser” ist als die Lösungen globaler Anbieter. Denn am Ende zählt nicht nur der Standort – sondern auch Architektur, Skalierbarkeit, Innovationsgeschwindigkeit und das technische Know-how der Betreiber.

Die Realität: Viele deutsche Anbieter sind im internationalen Vergleich technologisch abgehängt, müssen mit geringeren Budgets und weniger Innovationsdruck arbeiten und können die Servicebreite sowie Skalierung der Hyperscaler wie AWS, Google Cloud oder Azure nur schwerlich erreichen. Die Konsequenz: “Cloud Made in Germany” ist zu oft ein Marketingbegriff, der bei genauerer Betrachtung mehr Fragen aufwirft als beantwortet.

Datenschutz, DSGVO und Schrems II: Der Cloud Made in Germany

Mythos

Ein zentrales Verkaufsargument für die deutsche Cloud ist der Datenschutz – und hier vor allem die Einhaltung der DSGVO. Doch wer glaubt, dass eine Cloud allein durch ihren Standort in Deutschland DSGVO-konform ist, irrt gewaltig. Die DSGVO fordert nicht nur eine physische Datenhaltung in der EU, sondern auch technische und organisatorische Maßnahmen, die den Schutz der Daten gewährleisten. Und genau hier fangen die Probleme an.

Spätestens seit dem Schrems II-Urteil des EuGH ist klar: US-Anbieter – egal, ob sie Daten in Deutschland, Irland oder Timbuktu speichern – unterliegen dem US-Recht und können im Zweifel zur Herausgabe von Daten gezwungen werden. Das bedeutet: Auch, wenn Microsoft oder Google ein deutsches Rechenzentrum betreiben, ist das Risiko für einen Zugriff durch US-Behörden nicht eliminiert. Deutsche Anbieter argumentieren nun, sie seien hiervon ausgenommen – aber auch das ist zu kurz gedacht. Denn viele deutsche Clouds setzen auf Software, Services oder Supportstrukturen, die wiederum von internationalen Playern abhängen.

In der Praxis heißt das:

- Reiner Datenstandort in Deutschland garantiert keine absolute Sicherheit
- Technische Maßnahmen wie Verschlüsselung (at rest und in transit) sind Pflicht, aber selten Standard
- Organisatorische Prozesse (Zugriffsmanagement, Audits, Incident Response) entscheiden über echte Sicherheit
- Vendor Lock-in und Kompatibilität zu internationalen Standards fehlen häufig bei lokalen Anbietern

Der Mythos, dass “Cloud Made in Germany” automatisch DSGVO-konform sei, ist damit entzaubert. Nur ein ganzheitlicher Ansatz, der Technik, Prozesse und Recht verzahnt, bringt wirkliche Sicherheit. Und der ist teuer, aufwendig – und für viele Anbieter schlicht zu ambitioniert.

Die neue Lieblingsvokabel der deutschen Politik, “digitale Souveränität”, ist in Wahrheit ein Placebo. Denn solange man von US-Software, internationalen Chip-Herstellern und globalen Netzwerken abhängig ist, bleibt Souveränität eine Illusion. Wer hier mit “Cloud Made in Germany” hausieren geht, betreibt in erster Linie Symbolpolitik – aber keine echte, nachhaltige IT-Sicherheit.

Technische Herausforderungen und Limitierungen deutscher Cloud-Anbieter

Die deutsche Cloud-Branche hat in den letzten Jahren massiv aufgeholt. Aber von echter Parität mit den Hyperscalern ist sie weit entfernt. Das beginnt schon bei der Infrastruktur: Hyperscaler wie AWS, Google oder Azure

investieren jährlich Milliarden in Rechenzentren, Glasfaser, Edge-Netzwerke und eigene Hardware-Stacks. Deutsche Anbieter müssen mit einem Bruchteil dieser Budgets arbeiten – und das merkt man an Performance, Skalierbarkeit und Innovationsgeschwindigkeit.

Technische Limitierungen zeigen sich in mehreren Bereichen:

- Skalierung: Viele deutsche Clouds können große, globale Deployments nicht abbilden
- Servicebreite: Fehlende Spezialdienste wie Machine Learning, Big Data, AI und globale CDN-Netzwerke
- Automatisierung: API-Abdeckung, Self-Service-Portale und DevOps-Integrationen hinken oft hinterher
- Uptime und Redundanz: SLAs von 99,99% sind rar, Ausfälle werden zu oft verschwiegen
- Preis-Leistungs-Verhältnis: Günstige Einstiegspreise, aber schnell explodierende Kosten bei echten Enterprise-Workloads

Hinzu kommt: Viele "deutsche Clouds" sind in Wahrheit White-Label-Lösungen, Reseller-Modelle oder bauen auf den Infrastrukturen großer europäischer Player wie OVH oder Scaleway auf. Die Eigenentwicklungstiefe ist begrenzt – und damit auch die echte Kontrolle über Hardware, Netzwerk und Software.

Innovationsdruck? Fehlanzeige. Während AWS im Monatsrhythmus neue Dienste, APIs und Features launcht, dauern vergleichbare Entwicklungen bei deutschen Anbietern oft Jahre. Das liegt nicht am mangelnden Willen, sondern an strukturellen Nachteilen: kleiner Markt, wenig Kapital, Fachkräftemangel und ein regulatorisches Umfeld, das Innovation gerne im Keim erstickt.

Der vielzitierte Vorteil der "Transparenz" deutscher Anbieter ist oft ein Feigenblatt für fehlende Breite. Klar, der Support spricht deutsch, die Verträge sind verständlich, und der Datenschützer freut sich über kurze Wege. Aber Innovation, Skalierung und Integrationsfähigkeit bleiben dabei zu oft auf der Strecke. Wer als Unternehmen wirklich wachsen will, stößt mit der deutschen Cloud schnell an Grenzen.

Deutsche Clouds vs. Hyperscaler: Was sind die echten Unterschiede?

Kommen wir zum Kern der Debatte: Was unterscheidet eine "Cloud Made in Germany" tatsächlich von einem Hyperscaler wie AWS, Google Cloud oder Azure? Spoiler: Es ist nicht der Preis, nicht die Technologie und auch nicht unbedingt die Sicherheit. Es sind vor allem drei Faktoren: Standort, Kontrolle und Servicekultur.

Die wichtigsten Unterschiede auf einen Blick:

- Standort & Recht: Deutsche Clouds unterliegen rein

deutschem/europäischem Recht, Hyperscaler sind transnational – aber mit juristischen Grauzonen.
- Kontrolle & Transparenz: Lokale Anbieter bieten mehr Einblick in Betriebsprozesse, kürzere Kommunikationswege und nachvollziehbare Supportstrukturen.
- Service-Portfolio: Hyperscaler bieten tausende Dienste, von AI über IoT bis Edge Computing. Deutsche Clouds konzentrieren sich auf Kernservices wie Compute, Storage, Networking.
- Skalierung & Performance: Hyperscaler sind global, hochverfügbar und nahezu unbegrenzt skalierbar. Deutsche Clouds stoßen bei internationalen Deployments schnell an die Grenze.
- Innovationsgeschwindigkeit: Internationale Anbieter führen neue Features im Monats- oder Wochenrhythmus ein. Lokale Anbieter benötigen dafür oft Jahre.
- Preisstruktur: Einstieg meist günstiger bei deutschen Clouds, aber Skaleneffekte und Großkundenrabatte fehlen.

Die entscheidende Frage ist also nicht, "ob" die Cloud aus Deutschland kommt – sondern ob sie technisch und organisatorisch zu deinen Anforderungen passt. Wer skalieren, innovieren und international arbeiten will, fährt mit einem Hyperscaler besser. Wer maximale Kontrolle, kurze Wege und Datenschutz als oberste Priorität sieht, kann mit einer deutschen Cloud glücklich werden – sofern er mit den Limitierungen leben kann.

Der größte Fehler ist, Cloud Made in Germany als Allheilmittel zu sehen. Es ist ein Kompromiss – nie die perfekte Lösung. Die besten Architekturen kombinieren oft beide Welten: sensible Daten und Workloads lokal, skalierende, nicht-kritische Dienste global. Wer das nicht versteht, zahlt drauf – und zwar nicht zu knapp.

Mythen, Marketing und der politische Aufschrei: Was bleibt vom Cloud Made in Germany Hype?

Der aktuelle Aufschrei rund um "Cloud Made in Germany" ist so deutsch wie Weißwurst und Bürokratie. Er wird von Politikern, Lobbyisten und Beratern gleichermaßen befeuert – und das mit guten Gründen. Denn mit dem Angstnarrativ vor US-Geheimdiensten und digitalem Kontrollverlust lässt sich in Deutschland immer noch jeder Pitch gewinnen. Doch was bleibt, wenn man die Marketing-Schichten abträgt?

Mythos 1: "Cloud Made in Germany ist automatisch sicherer." Falsch. Sicherheit ist eine Frage von Architektur, Prozessen und Personal – nicht des Standorts.

Mythos 2: “Deutsche Clouds sind zu 100% DSGVO-konform.” Wunschdenken. Ohne ganzheitliche technische und organisatorische Maßnahmen bleibt DSGVO-Konformität ein frommer Wunsch.

Mythos 3: “Mit der deutschen Cloud bleibt alles unter Kontrolle.” Teilwahrheit. Kontrolle ist relativ – spätestens bei internationalen Lieferketten, Software-Stacks und Netzwerkabhängigkeiten wird’s komplex.

Mythos 4: “Die deutsche Cloud ist billiger.” Nur, solange du im Klein-Klein bleibst. Bei echten Enterprise-Workloads explodieren die Kosten oft schneller als bei Hyperscalern.

Mythos 5: “Cloud Made in Germany ist innovativ.” Der Wunsch ist der Vater des Gedankens. Die Innovationskraft ist limitiert – und das wird sich nicht ändern, solange Infrastruktur, Kapital und Mut fehlen.

Der politische Aufschrei ist vor allem eines: ein Placebo, um Handlungsfähigkeit zu beweisen. Aber echte digitale Souveränität entsteht nicht durch Gesetzestexte, sondern durch technische Exzellenz, strategische Investitionen und den Willen, wirklich konkurrenzfähig zu sein. Wer nur auf Nationalismus setzt, bleibt beim digitalen Wettrennen auf der Strecke.

Praxis-Checkliste: Wann ist Cloud Made in Germany sinnvoll – und wann nicht?

Du stehst vor der Entscheidung, ob du auf eine deutsche Cloud setzt oder doch beim Hyperscaler bleibst? Vergiss die PR und konzentriere dich auf das, was wirklich zählt. Hier die Schritt-für-Schritt-Checkliste für eine rationale Entscheidung:

- Bewerte, welche Daten und Workloads wirklich sensibel sind und zwingend in Deutschland bleiben müssen.
- Prüfe, ob der Anbieter alle relevanten Zertifikate (ISO 27001, BSI C5) und Audits vorweisen kann.
- Teste die API- und DevOps-Fähigkeiten: Wie automatisierbar sind Deployments, wie flexibel das Monitoring?
- Analysiere die Servicebreite: Fehlen dir wichtige Dienste wie KI, Big Data oder globale Netzwerke?
- Fordere SLAs und Transparenz zu Uptime, Incident Response und Supportzeiten ein.
- Vergleiche die Skalierungsmöglichkeiten: Kann der Anbieter international liefern, wenn du wächst?
- Stelle sicher, dass du im Notfall schnell (und ohne Vendor Lock-in) migrieren kannst.
- Rechne die Kosten durch – nicht nur für den Einstieg, sondern auch für künftiges Wachstum.
- Hole Feedback von anderen Kunden ein, besonders zu Ausfällen und

Support-Erfahrungen.

Erst, wenn du diese Punkte ehrlich beantwortet hast, ergibt sich ein klares Bild. “Cloud Made in Germany” macht Sinn, wenn Datenschutz, Kontrolle und lokale Nähe deine Top-Prioritäten sind – und du mit Kompromissen bei Innovation, Skalierung und Preis leben kannst. Für alle anderen ist der Griff zum Hyperscaler kein Verrat, sondern schlicht ökonomisch und technisch vernünftig.

Fazit: Cloud Made in Germany – Aufschrei, Hype oder echte Alternative?

Cloud Made in Germany ist viel Lärm um wenig Substanz – zumindest, wenn man den Marketing-Nebel beiseitewischt. Ja, es gibt Anwendungsfälle, in denen eine deutsche Cloud Sinn macht: strenge Compliance, behördliche Vorgaben, spezielle Datenschutzanforderungen. Aber für die große Mehrheit der Unternehmen bleibt die deutsche Cloud ein Kompromiss – und kein echter Ersatz für die Innovations- und Skalierungsfähigkeit der Hyperscaler.

Der aktuelle Aufschrei ist vor allem politisch und medial getrieben. Wer als Unternehmen echte digitale Souveränität will, muss tiefer gehen: in Prozesse, Technik, Architektur und Personal investieren – und sich nicht von Standortetiketten blenden lassen. Am Ende zählt nicht das Label, sondern die technische und wirtschaftliche Realität. Wer sich darauf verlässt, dass “Made in Germany” alles besser macht, verpasst die echten Chancen der Digitalisierung – und bleibt im internationalen Wettbewerb auf der Strecke.