Cloud Made in Germany Kritik Meinung: Fakten und Perspektiven

Category: Opinion
geschrieben von Tobias Hager | 15. September 2025

Cloud Made in Germany Kritik Meinung: Fakten und Perspektiven

Cloud Made in Germany – klingt nach digitaler Unabhängigkeit, nach Datenschutz-Oase, nach dem goldenen Ticket zur DSGVO-Konformität. Doch wie viel Substanz steckt wirklich hinter dem Label? Und warum kaufen so viele Unternehmen blind die deutsche Cloud-Versprechen, obwohl hinter der Fassade oft nur Marketing-Geblubber und technische Kompromisse warten? Dieser Artikel liefert die schonungslose Analyse: Fakten, Meinungen, Perspektiven. Wer nach weichgespülten Werbetexten sucht, klickt jetzt besser weg. Hier kommt die Realität – ungeschönt, kritisch und mit maximalem technischem Tiefgang.

- Was “Cloud Made in Germany” überhaupt bedeutet – und warum der Begriff technisch und rechtlich schwammig ist
- Die größten Mythen und Missverständnisse rund um deutsche Cloud-Angebote
- Datenschutz, DSGVO und Schrems II: Was deutsche Clouds wirklich besser machen (und wo sie genauso scheitern)
- Technische und wirtschaftliche Schwächen aktueller Made-in-Germany-Clouds im Vergleich zu Hyperscalern
- Vendor-Lock-in, API-Kompatibilität und Innovationsgeschwindigkeit auf dem Prüfstand
- Die wichtigsten Anbieter: Wer spielt mit – und wer blufft nur mit “German Cloud” als Feigenblatt?
- Warum “Souveränität” oft nur ein Marketing-Mythos ist und echte Cloud-Power woanders entsteht
- Schritt-für-Schritt: So prüfst du, ob ein Cloud-Anbieter wirklich deutsche Standards erfüllt
- Praxisrelevante Perspektiven für Unternehmen: Wann lohnt sich Cloud Made in Germany – und wann nicht?
- Unbequemes Fazit: Warum der Blick über den Tellerrand Pflicht ist, wenn du digital skalieren willst

“Cloud Made in Germany” ist das Buzzword, auf das deutsche Unternehmen seit Jahren abfahren wie die sprichwörtliche Lemminge – aus Angst vor bösen US-Diensten, DSGVO-Strafen und der eigenen IT-Inkompetenz. Doch wer glaubt, dass das Label automatisch für Sicherheit, Datenschutz, technische Überlegenheit und Zukunftsfähigkeit steht, ist entweder naiv oder will es nicht besser wissen. Dieser Artikel räumt auf mit den größten Irrtümern, bringt die Fakten auf den Tisch und zeigt, wie du zwischen echten Vorteilen, leeren Marketing-Versprechen und teuren Kompromissen unterscheiden kannst. Egal, ob du als CTO, Datenschutzbeauftragter oder Marketingstratege unterwegs bist: Nach diesem Artikel siehst du die deutsche Cloud-Landschaft mit anderen Augen – und triffst Entscheidungen, die wirklich zählen.

Was steckt hinter “Cloud Made in Germany”? Definition, Anspruch und Realität

Der Begriff “Cloud Made in Germany” klingt nach digitaler Souveränität, nach Datensicherheit made in Germany – und nach einer klaren Alternative zu Amazon AWS, Microsoft Azure und Google Cloud. Doch was heißt das eigentlich konkret? Fakt ist: Es gibt bis heute keine verbindliche technische oder rechtliche Definition. “Cloud Made in Germany” ist kein geschütztes Siegel, sondern in erster Linie eine Marketing-Konstruktion. Jeder Anbieter kann sich das Label aufkleben, solange die angebotenen Dienste irgendwie aus deutschen Rechenzentren stammen oder eine deutsche GmbH im Handelsregister steht.

Technisch bedeutet “Cloud Made in Germany” meistens, dass die Server-Standorte tatsächlich in Deutschland liegen – idealerweise redundant in

mehreren ISO-zertifizierten Rechenzentren. Die Betreiber unterliegen deutschem Datenschutzrecht, müssen sich an die DSGVO halten und versprechen meist, dass kein Zugriff von Dritten (insbesondere US-Behörden) möglich ist. Doch das ist nur die halbe Wahrheit: Viele Anbieter nutzen trotzdem US-Software, setzen auf US-Cloud-Stacks oder sind Tochtergesellschaften internationaler Konzerne. Wer hier nicht in die Details schaut, kauft am Ende dieselbe Blackbox wie bei den Hyperscalern – nur mit deutschem Anstrich.

Ein weiterer Punkt: "Cloud Made in Germany" wird gerne als Synonym für maximale Rechtssicherheit und Souveränität verkauft. Doch das ist Augenwischerei, solange nicht auch die gesamte Lieferkette – von der Hardware bis zum Software-Stack – unter deutscher Kontrolle steht. Die Realität: Die wenigsten Anbieter entwickeln tatsächlich eigene Cloud-Plattformen. Die meisten setzen auf Open-Source-Software (etwa OpenStack, Kubernetes, Ceph) oder lizenzieren US-Technologien. Wer souveräne Cloud will, muss tiefer bohren und hinterfragen, wo die Abhängigkeiten wirklich liegen.

Im Klartext: "Cloud Made in Germany" ist ein Label, das primär Vertrauen schaffen soll – aber technisch und rechtlich oft mehr verheißt, als es hält. Wer glaubt, dass mit einem deutschen Rechenzentrum automatisch alle Compliance-Fragen gelöst sind, hat den Schuss nicht gehört. Wirkliche Transparenz gibt es nur, wenn Architektur, Betrieb, Support und Lieferkette nachvollziehbar offengelegt werden – und das ist bis heute eher die Ausnahme als die Regel.

Datenschutz, DSGVO und Schrems II: Was deutsche Clouds wirklich bieten – und wo sie scheitern

Seit dem Schrems-II-Urteil des Europäischen Gerichtshofs ist endgültig klar: Die Übermittlung von personenbezogenen Daten in die USA ist rechtlich ein Minenfeld. US-Cloud-Anbieter unterliegen dem Cloud Act und müssen im Zweifel Daten an US-Behörden herausgeben – auch dann, wenn die Daten physisch in Europa liegen. Hier punkten deutsche Cloud-Anbieter mit einem echten Vorteil: Kein US-Mutterkonzern, keine US-Gesetzgebung, keine Extraterritorialität. Klingt nach der perfekten Lösung – aber die Sache hat Haken.

Erstens: Viele "deutsche" Cloud-Anbieter nutzen Software, Dienste oder Sub-Services, die aus den USA stammen. Selbst wenn die Server in Frankfurt stehen, läuft der Support oft über US-Ticketsysteme, werden Backups in EU-weiten Multi-Region-Clouds abgelegt oder kritische Komponenten von US-Firmen gewartet. Spätestens hier wird die Compliance zum russischen Roulette. Wer wirklich DSGVO-konform hosten will, muss die gesamte technische Lieferkette prüfen – und das ist in der Praxis meist unmöglich.

Zweitens: Datenschutz ist nicht nur eine Frage des Standorts, sondern auch der Architektur und Organisation. Wie werden Daten verschlüsselt? Gibt es Zero-Knowledge-Prinzipien? Wie werden Zugriffe geloggt, wie werden Rechte vergeben? Viele deutsche Anbieter setzen auf Standardlösungen mit wenig Innovation und noch weniger Transparenz. Wer echte Datensouveränität will, muss in die technischen Details einsteigen – und nicht nur den Marketing-Broschüren vertrauen.

Drittens: Auch deutsche Anbieter sind nicht vor Behördenzugriffen sicher. Zwar ist die Schwelle für staatliche Übergriffe höher als in den USA, doch spätestens bei Ermittlungen zu schweren Straftaten gibt es auch in Deutschland Schnittstellen zu Polizei und Geheimdiensten. Wer absolute Sicherheit sucht, sucht vergeblich – egal auf welcher Seite des Atlantiks. Im Ergebnis bleibt: Deutsche Clouds können im Datenschutz und in der DSGVO-Compliance Vorteile bieten, garantieren sie aber nicht per se. Wer sich darauf verlässt, verlässt sich oft auf Illusionen.

Technische und wirtschaftliche Perspektiven: Was deutsche Cloud-Anbieter wirklich leisten – und wo sie abgehängt werden

Cloud Made in Germany wird gerne als technisch überlegene, sicherere und leistungsfähige Alternative zu den US-Hyperscalern verkauft. Doch das halte ich für eine der größten Nebelkerzen im deutschen IT-Markt. Fakt ist: In Sachen Innovationsgeschwindigkeit, Self-Service, API-Kompatibilität, Skalierbarkeit und Preis-Leistung spielen die deutschen Anbieter in einer ganz anderen Liga – aber nicht in der, die du dir wünschst. Die Hyperscaler investieren jährlich Milliardenbeträge in Infrastruktur, Automatisierung und AI-Integration. Deutsche Anbieter können da schlicht nicht mithalten.

Das technische Kernproblem: Die meisten “German Clouds” sind klassische Managed-Hosting-Anbieter, die ihre alten Rechenzentren mit OpenStack oder Kubernetes aufgerüstet und nun als “Cloud” rebranden. Fehlende native APIs, mangelhafte Dokumentation, fragmentierte Self-Service-Portale und inkompatible Schnittstellen sind an der Tagesordnung. Wer auf AWS, Azure oder Google Cloud entwickelt, bekommt Dutzende von Managed Services, von Data Lakes bis AI-Plattformen, mit wenigen Klicks. Bei deutschen Clouds musst du dich oft noch mit Telnet-Logins, Handarbeit und manuellen Tickets rumschlagen.

Ein weiteres Problem: Vendor-Lock-in und geringe Portabilität. Viele deutsche Anbieter setzen zwar auf Open-Source-Stack, bauen aber proprietäre Zusatzschichten ein, um Kunden zu binden. Das klingt nach Sicherheit, ist

aber in Wahrheit ein Innovationskiller – und führt dazu, dass du bei jedem Wechsel Monate mit Migration, API-Refactoring und Kompatibilitätsprüfungen verbringst. Wer skaliert, wächst und digitale Produkte international launchen will, kommt mit rein deutschen Clouds schnell an die Grenzen.

Wirtschaftlich sieht es nicht besser aus: Deutsche Clouds sind oft teurer, weniger skalierbar und bieten selten echte Pay-as-you-go-Modelle. Wer auf Hochverfügbarkeit, globale Deployments und Entwicklerfreundlichkeit Wert legt, fährt mit Hyperscalern günstiger – und hat die Innovationsvorteile gleich mit im Paket. Der einzige echte Vorteil der German Clouds bleibt der Datenschutz – und der ist, wie oben beschrieben, selten so wasserdicht wie behauptet.

Die wichtigsten Anbieter: Wer liefert wirklich, wer verkauft nur Etiketten?

Die deutsche Cloud-Landschaft ist voll von Anbietern, die mit “Cloud Made in Germany” oder “souveräner Cloud” trommeln. Doch wer spielt tatsächlich vorne mit – und wer verkauft nur hübsch verpackte Managed Server? Die Platzhirsche sind Unternehmen wie IONOS, Deutsche Telekom (Open Telekom Cloud), plus kleinere Player wie Hetzner, gridscale oder noris network. Sie alle versprechen deutsche Standorte, DSGVO-Konformität, ISO-Zertifikate und Support “aus einer Hand”. Doch ein Blick unter die Haube offenbart schnell: Wirklich native Cloud-Kompetenz ist rar.

IONOS betreibt eigene Rechenzentren in Deutschland, bietet OpenStack-basierte Public-Cloud-Dienste und vermarktet aggressiv mit dem “German Cloud”-Label. Die Telekom setzt mit der Open Telekom Cloud auf ein Joint Venture mit Huawei – was angesichts aktueller geopolitischer Spannungen mindestens fragwürdig ist. Hetzner punktet mit günstigen Bare-Metal-Angeboten, aber spielt beim Thema Managed Services kaum mit. gridscale und noris network fokussieren auf Mittelstand und individuelle Projekte, doch die Skalierungsmöglichkeiten sind begrenzt.

Viele kleinere Anbieter setzen auf White-Label-Lösungen und verkaufen letztlich nur “Ressourcen im deutschen Rechenzentrum”, ohne echte Cloud-Funktionalität. Es gibt keine native Autoskalierung, keine serverlosen Funktionen, keine tief integrierten Managed Services. Wer Cloud will, bekommt oft nur Hosting im neuen Gewand – zu Preisen, die dem internationalen Wettbewerb nicht standhalten.

Wirklich souveräne Cloud-Initiativen wie Gaia-X existieren in erster Linie auf PowerPoint-Folien und Konferenz-Bühnen. Die technische Realität ist: Auch 2024/2025 gibt es keine wirklich konkurrenzfähige, vollständig deutsche Cloud-Plattform, die es mit AWS, Azure oder Google aufnehmen kann. Wer das Gegenteil behauptet, verkauft Hoffnung – oder hat einfach keine Ahnung.

Schritt-für-Schritt: So prüfst du, ob eine Cloud wirklich “Made in Germany” ist

Marketing-Versprechen sind schnell gemacht, aber technische Fakten sind (meistens) überprüfbar. Wer wirklich wissen will, ob ein Anbieter die Ansprüche von “Cloud Made in Germany” einlöst, sollte sich nicht auf Siegel und Zertifikate verlassen, sondern gezielt nachhaken:

- 1. Rechenzentrumsstandorte prüfen: Wo stehen die Server wirklich? Gibt es Nachweise für Redundanz, ISO-Zertifizierungen und Betreiberunabhängigkeit?
- 2. Rechtsform und Unternehmensstruktur analysieren: Gehören Anteile internationalen Konzernen? Gibt es US-Muttergesellschaften, die Zugriff verlangen könnten?
- 3. Lieferketten- und Software-Stack offenlegen lassen: Welche Software-Komponenten werden genutzt? Open-Source oder proprietär? Woher stammen die wichtigsten Komponenten?
- 4. Support und Administration: Findet der Kundensupport tatsächlich in Deutschland statt? Oder gibt es Ticket-Routing ins Ausland?
- 5. Vertragsbedingungen und Datenschutz prüfen: Wie werden Daten verschlüsselt? Gibt es technische und organisatorische Maßnahmen, die über das gesetzliche Minimum hinausgehen?
- 6. APIs und Schnittstellen testen: Sind die angebotenen APIs offen, dokumentiert, kompatibel mit Industriestandards? Lassen sich Workloads portieren oder ist ein Vendor-Lock-in programmiert?
- 7. Monitoring und Transparenz: Gibt es regelmäßige Audits, Penetrationstests und unabhängige Prüfberichte? Werden diese offengelegt?
- 8. Innovation und Roadmap: Welche neuen Features sind geplant? Wird in neue Technologien investiert oder stagniert der Anbieter?

Wer diese Checkliste sauber abarbeitet, erkennt schnell, ob hinter “Cloud Made in Germany” mehr als nur ein Label steckt – oder ob du nur für ein deutsches Aushängeschild zahlst, während die Technik von gestern und die Risiken von morgen kommen.

Wann lohnt sich Cloud Made in Germany aus Unternehmenssicht – und wann nicht?

Auch wenn die Kritik an deutschen Cloud-Angeboten berechtigt ist: Es gibt Szenarien, in denen “Cloud Made in Germany” tatsächlich die bessere Wahl ist.

Wer strengste Compliance-Anforderungen erfüllen muss, etwa im öffentlichen Sektor, im Gesundheitswesen oder in sicherheitskritischen Industrien, profitiert von kurzen Wegen, klaren rechtlichen Rahmenbedingungen und deutschem Support. Auch Unternehmen, die keine globalen Deployments planen und mit klassischen Workloads arbeiten, finden bei deutschen Anbietern solide Lösungen – wenn auch mit Abstrichen bei Skalierung und Innovationsgeschwindigkeit.

Für alle anderen gilt: Wer digitale Geschäftsmodelle skalieren will, auf AI, Microservices, Containerisierung und DevOps setzt, stößt mit deutschen Clouds schnell an die Decke. Die Hyperscaler sind technisch, wirtschaftlich und innovativ mindestens eine Dekade voraus. Wer sich hier einigelt, verpasst Chancen, riskiert Wettbewerbsnachteile und zahlt am Ende mehr – für weniger Leistung. Die Wahrheit ist unbequem, aber glasklar: Die deutsche Cloud ist eine Nische, keine Lösung für den digitalen Massenmarkt.

Fazit: Cloud Made in Germany – Hype, Hoffnung oder Zukunft?

Die deutsche Cloud-Branche inszeniert sich gerne als Bollwerk gegen Überwachung, Datenklau und US-Dominanz. Doch hinter den großen Versprechen steckt oft wenig Substanz. “Cloud Made in Germany” ist ein Label mit schwammiger Bedeutung, das technische Schwächen und Innovationsdefizite selten überdecken kann. Wer wirklich digitale Souveränität will, muss tiefer einsteigen, kritisch hinterfragen und die Komfortzone deutscher Marketing-Aussagen verlassen.

Für Unternehmen gilt: Nutze die deutschen Cloud-Angebote dort, wo sie Sinn machen – für Compliance, Datenschutz und spezifische Branchenanforderungen. Aber verliere niemals den Blick für den globalen Wettbewerb. Wer wachsen, skalieren und innovieren will, muss auch US-Hyperscaler, hybride Modelle und internationale Standards im Blick behalten. Die Zukunft der Cloud ist offen, dynamisch und technisch anspruchsvoll – und sie entscheidet sich nicht an Nationalflaggen, sondern an Code, APIs und echter Innovationskraft.