Cloud Made in Germany Kritik Rant: Fakten statt Mythen

Category: Opinion
geschrieben von Tobias Hager | 16. September 2025

Cloud Made in Germany Kritik Rant: Fakten statt Mythen

Cloud Made in Germany – klingt nach digitaler Souveränität, nach sicherem Heimathafen für Daten, nach DSGVO-kompatibler Marketing-Story. Aber wie viel Substanz steckt hinter der Cloud Made in Germany, und wie viel ist heiße Luft, die clevere Vertriebler und Agenturen in PowerPoint-Präsentationen aufblasen? Hier gibt’s keine weichgespülten Phrasen, sondern eine schonungslose, technische Abrechnung mit Mythen, Märchen und Marketing-Geschwurbel rund um die angeblich so sichere, unabhängige deutsche Cloud. Fakten statt Feenstaub – Zeit für einen Reality-Check.

- Was steckt hinter dem Label Cloud Made in Germany? Buzzword oder echte Cloud-Souveränität?
- Typische Mythen und Marketing-Tricks der deutschen Cloud-Industrie im Faktencheck
- Technische Realität: Wo deutsche Clouds wirklich stehen bei Datenschutz, Compliance und Infrastruktur
- Reale Schwächen: Warum Cloud Made in Germany oft nicht mit Hyperscalern konkurrieren kann
- Was bringt das BSI-Zertifikat wirklich? Und wie sieht es mit Cloud-Act, Schrems II und Co. aus?
- Kritische Analyse: Preis, Performance, Skalierbarkeit – die harten Zahlen
- Für wen und wann eine deutsche Cloud wirklich Sinn macht (Spoiler: selten)
- Schritt-für-Schritt: So prüfst du die tatsächliche Sicherheit und Unabhängigkeit eines Anbieters
- Die besten Alternativen und Strategien für technikfokussierte Unternehmen
- Fazit: Warum Cloud Made in Germany meistens ein Placebo bleibt – und was echte Souveränität heute bedeutet

Cloud Made in Germany – das Schlagwort geistert seit Jahren durch die Flure von IT-Abteilungen, Datenschutzbeauftragten und Marketing-Managern. Das Versprechen: Total sichere, super-deutsche Cloud-Services, garantiert ohne Zugriff fremder Staaten, kompromisslos DSGVO-konform, am besten noch von "mittelständischen Familienunternehmen mit Tradition". Klingt nach digitalem Luftkurort, ist aber bei genauerem Hinsehen oft mehr Image-Kampagne als technologische Revolution. Denn Cloud Made in Germany ist kein technischer Standard, sondern ein Marketinglabel – und das wird in deutschen Pitchdecks bis zum Erbrechen ausgeschlachtet. Zeit für eine Abrechnung mit den gängigsten Mythen und eine technische Analyse, die das Label auf Herz, Nieren und TCP/IP prüft.

Cloud Made in Germany: Definition, Buzzword-Bingo und was wirklich dahinter steckt

Was ist Cloud Made in Germany? Die meisten Anbieter definieren es frei nach Schnauze: Rechenzentren stehen in Deutschland, Firma ist in Deutschland registriert, Service-Vertrag nach deutschem Recht. Klingt erstmal solide. Aber reicht das? Fakt ist: Es gibt keinen gesetzlich geschützten Begriff, kein verbindliches technisches oder rechtliches Regelwerk. Jeder Provider kann sich das Label Cloud Made in Germany aufs Banner kleben, solange er irgendeinen Server in Frankfurt oder München stehen hat und eine GmbH im Handelsregister führt. In der Praxis heißt das: Die technische Tiefe und Qualität hinter dem Label variiert zwischen "eigener VMware-Server im RZ eines Drittanbieters" und "tatsächliche Cloud-Architektur mit modernen APIs,

Kubernetes, CI/CD und Multi-Tenant-Isolation”.

Ein weiteres Problem: Viele Anbieter, die mit Cloud Made in Germany werben, sind in Wahrheit bloße Reseller oder White-Label-Partner internationaler Player. Der physische Standort der Daten ist zwar Deutschland, aber Software, Support und oft auch die Infrastruktur stammen von Drittfirmen – Stichwort “Hidden Hyperscaler”. Viele dieser Clouds sind nicht mehr als aufgemotzte Managed-Hosting-Lösungen mit einer hübschen Self-Service-Oberfläche und ein paar REST-APIs, aber weit entfernt von echter Cloud-Native-Architektur. Wer also glaubt, mit Cloud Made in Germany automatisch Zugriff auf AWS-, Azure- oder Google-Cloud-Niveau zu bekommen, lebt im Marketing-Paralleluniversum.

Besonders perfide: Das Label Cloud Made in Germany wird oft als Allheilmittel für Datenschutzängste verkauft. Doch das ist Augenwischerei. Denn selbst wenn die Server in Deutschland stehen, können Eigentumsverhältnisse, Support-Zugriffe oder Third-Party-Integrationen dazu führen, dass Daten dennoch den deutschen Rechtsraum verlassen – und damit Cloud Act, FISA oder andere “freundliche” Gesetze internationaler Behörden greifen.

Cloud Made in Germany ist technisch gesehen also meist eine Blackbox. Ohne tiefgehende Prüfung der Architektur, der Lieferkette (Supply Chain) und der Unternehmensstruktur bleibt das Label ein reines Marketingversprechen. Wer hier nicht kritisch nachfragt, fällt auf eine der ältesten Maschen der IT-Welt herein: Vertrauen statt Verifikation.

Die größten Mythen der deutschen Cloud – und was davon technisch übrig bleibt

Mythos 1: Cloud Made in Germany ist automatisch sicherer als internationale Anbieter. Das ist eine nette Fantasie, aber in der Praxis schlicht falsch. Sicherheit ist kein Standort, sondern das Ergebnis von Prozessen, Architektur und Betrieb. Viele deutsche Clouds setzen immer noch auf veraltete Virtualisierungslösungen, schwache Netzwerksegmentierung und manuelle Provisionierung. Von Zero Trust, Immutable Infrastructure oder automatisierten Security Audits fehlt bei vielen Mittelständlern jede Spur.

Mythos 2: Die Daten bleiben garantiert in Deutschland. Auch das stimmt nur halb. Viele Anbieter nutzen Subunternehmer, externe Dienstleister oder internationale Software-Stacks mit Telemetrie-Funktionen. Wer sich die AV-Verträge (Auftragsverarbeitungsvereinbarungen) genauer ansieht, findet häufig Formulierungen, die Drittzugriffe oder Notfall-Support “im Rahmen der gesetzlichen Bestimmungen” erlauben. Übersetzt: Im Zweifel entscheidet der Anbieter selbst, wo und wie auf die Daten zugegriffen wird.

Mythos 3: Deutsche Clouds sind immer DSGVO-konform. DSGVO-Konformität ist kein Zustand, sondern ein laufender Prozess. Sie hängt von technischen und organisatorischen Maßnahmen (TOM), Verschlüsselung, Schlüsselmanagement,

Löschkonzepten und vielem mehr ab. Die wenigsten Anbieter geben vollständige Auskunft über Incident-Response-Prozesse, Logfile-Aufbewahrung, Zugriffskontrollen oder Verschlüsselungsstandards. Wer glaubt, das Cloud Made in Germany-Logo auf der Startseite sei ein Freifahrtschein für Compliance, begeht einen groben Fehler.

Mythos 4: Lokale Anbieter sind unabhängiger. Viele "deutsche" Clouds gehören zu internationalen Holdings, sind auf Infrastruktur von US-Konzernen angewiesen oder nutzen Open-Source-Software mit Support aus Übersee. Die Lieferkette ist selten rein deutsch. Wer auf maximale Souveränität setzt, sollte sich die gesamte Supply Chain anschauen – inklusive Firmware, Management-Layer, Storage-Systeme und Netzwerk-Equipment. Spätestens beim Thema Backup und Geo-Redundanz wird's dann schnell international.

Technische Realität: Wie steht es wirklich um Datenschutz, Compliance und Infrastruktur?

Wer die technische Realität hinter Cloud Made in Germany beleuchten will, muss tief graben. Die zentralen Fragen: Wie sieht die Architektur aus? Welche Technologien werden verwendet? Wie werden Daten verschlüsselt? Gibt es echte Mandantenfähigkeit (Multi-Tenancy) und Isolation auf Hardware-Ebene? Verfügt der Anbieter über ein nachvollziehbares Incident-Management und ein transparentes Reporting zu Security Incidents?

Viele deutsche Clouds arbeiten nach dem klassischen Hosting-Modell: Dedizierte VMs, oft manuell provisioniert, mit eingeschränkter API-Integration und wenig Transparenz über interne Abläufe. Kubernetes, Serverless, Infrastructure as Code, automatisiertes Scaling? Fehlanzeige. Wer einmal die API-Dokumentation eines typischen deutschen Anbieters mit AWS oder Google Cloud vergleicht, merkt schnell: Vieles, was als "Cloud" verkauft wird, ist technisch Stand 2012 – hübsch verpackt, aber weit entfernt von echter Cloud-Innovation.

Datenschutz ist ein weiteres Minenfeld. Während Hyperscaler wie AWS, Azure und Google Cloud detaillierte Whitepapers zu Verschlüsselung, Zugriffsprotokollierung, Schlüsselverwaltung (KMS/HSM), Mandantenisolation und Compliance-Frameworks liefern, beschränken sich viele deutsche Anbieter auf allgemeine Floskeln. "AES-256-Verschlüsselung" klingt gut, aber wer verwaltet die Schlüssel? Wie ist Monitoring und Logging gelöst? Gibt es Security-Information- und Event-Management (SIEM)?

Compliance ist kein Vermerk auf dem Papier, sondern muss technisch im Betrieb nachgewiesen werden. ISO 27001, BSI C5 oder TISAX sind Mindeststandards, aber keine Garantie für echte Sicherheit. Viele Anbieter bestehen den Audit, weil sie ein paar Policies ins Intranet stellen, nicht weil sie ein durchdachtes Security-Konzept leben. Wer sich mit Stichproben begnügt, bekommt Compliance-Theater – aber keine echte Datensouveränität.

Cloud Act, Schrems II, BSI & Co: Was wirklich zählt – und was bloß Blendwerk ist

Ein zentrales Verkaufsargument für Cloud Made in Germany ist die angebliche Immunität gegen US-Behördenzugriffe – Stichwort Cloud Act. Aber die Realität ist komplizierter: Selbst wenn Server und Daten in Deutschland stehen, können Eigentumsverhältnisse, Wartungsverträge oder der Einsatz amerikanischer Software dazu führen, dass US-Behörden im Ernstfall Zugriff fordern. Die juristische Gemengelage ist alles andere als eindeutig – und wird von Anbietern oft verschwiegen oder schöngeredet.

Schrems II hat das Privacy Shield zwischen EU und USA gekippt. Heißt: Übermittlungen personenbezogener Daten in die USA sind hochproblematisch. Viele deutsche Clouds nutzen trotzdem US-Software, Monitoring-Lösungen, Backup-Tools oder Security-Services aus Übersee. Transparenz? Fehlanzeige. Wer wirklich wissen will, wie "sauber" die eigene Cloud ist, muss sich die gesamte Lieferkette inklusive aller Subdienstleister, Software-Komponenten und Wartungsverträge offenlegen lassen. Alles andere ist Placebo.

Und das BSI? Das "C5-Testat" (Cloud Computing Compliance Criteria Catalogue) ist mittlerweile Standard – aber kein Allheilmittel. Es gibt keine Garantie, dass ein Anbieter ohne Schwachstellen ist. Viele BSI-Audits sind punktuelle Prüfungen, keine kontinuierliche Überwachung. Wer BSI-zertifiziert ist, hat damit noch keine ausfallsichere, hochverfügbare und vor allem skalierbare Cloud gebaut. Die größten deutschen Cloud-Ausfälle der letzten Jahre fanden bei BSI-zertifizierten Anbietern statt.

Preis, Performance, Skalierbarkeit: Die harten Zahlen hinter dem Label

Wer glaubt, Cloud Made in Germany sei konkurrenzfähig mit AWS, Azure oder Google Cloud, hat nie eine größere Anwendung auf beiden Plattformen betrieben. Preislich sind deutsche Clouds oft teuer – bei schlechterer Performance. Die Gründe: Fehlende Skaleneffekte, teure Hardware, begrenzte Standorte, wenig Automatisierung und hohe Fixkosten. Während internationale Hyperscaler Ressourcen in Minuten bereitstellen, brauchen einige deutsche Anbieter Stunden oder Tage für VM-Provisionierung, Storage-Expansion oder Netzwerkkonfigurationen.

API-Funktionalität? Häufig lückenhaft. Managed Services wie Datenbanken, Analytics, KI, CDN? Mangelware. Wer hochverfügbare, elastische Cloud-

Architekturen bauen will, stößt schnell an harte Grenzen. Auto-Scaling, Self-Healing, serverlose Architekturen – in deutschen Clouds oft nur Zukunftsmusik. Die Folge: Höhere Kosten für weniger Flexibilität und Innovation.

Ein weiteres Problem: Viele deutsche Anbieter locken mit scheinbar niedrigen Einstiegspreisen, verschweigen aber Kosten für Traffic, Backups, SLA, Monitoring oder Support. Wer eine große Anwendung wirtschaftlich und performant betreiben will, muss sehr genau kalkulieren – und landet oft weit über dem Niveau internationaler Konkurrenz.

Fakt ist: Für moderne, skalierende Anwendungen sind deutsche Clouds selten die beste Wahl. Wer sich auf das Label Cloud Made in Germany verlässt, riskiert Overengineering, Budget-Explosion und Innovationsstau. Und das alles für eine Compliance-Sicherheit, die in der Praxis meistens nicht einmal solide dokumentiert ist.

Wie du Cloud-Anbieter wirklich prüfst: Schritt-für-Schritt zur Realität

Wer sich nicht von Marketing-Slides blenden lassen will, prüft Cloud-Anbieter systematisch und technisch fundiert. Hier der Ablauf, der dich von Placebo zu Fakten bringt:

1. Technische Architektur offenlegen lassen
   Fragen nach verwendeter Hardware, Virtualisierung, Netzwerksegmentierung, Storage-Systemen, API-Funktionalität. Gibt es Multi-Tenancy, Self-Service, Automatisierung?
2. Lieferkette (Supply Chain) analysieren
   Wer betreibt Rechenzentren, wer liefert Software, welche Subunternehmer sind im Spiel? Gibt es internationale Abhängigkeiten?
3. Datenschutz- und Compliance-Prozesse prüfen
   Verschlüsselung im Ruhezustand und bei Übertragung, Schlüsselverwaltung, Zugriffskontrollen, Logging. Werden Zugriffe dokumentiert? Wer kann im Notfall auf Daten zugreifen?
4. Incident-Response und Monitoring-Praxis hinterfragen
   Gibt es SIEM, automatisierte Alerts, regelmäßige Security Audits? Wie schnell werden Sicherheitsvorfälle erkannt und gemeldet?
5. Performance und Skalierbarkeit testen
   Testdeployment, Lasttests, API-Latenzen, Provisionierungszeiten. Wie schnell kann die Plattform wachsen? Gibt es Limiting-Faktoren?
6. SLAs und Preismodell kritisch prüfen
   Versteckte Kosten, Support-Levels, Verfügbarkeit, Vertragsstrafen bei Ausfällen. Was kostet echtes Enterprise-Feature-Set wirklich?
7. Backup, Geo-Redundanz, Restore-Fähigkeit prüfen
   Wie laufen Backups, wie ist die Geo-Redundanz gelöst? Gibt es regelmäßige Restore-Tests? Werden Backups außerhalb Deutschlands

gespeichert?
8. Transparenz zu Behördenanfragen verlangen
   Gibt es eine Offenlegungspflicht bei Behördenanfragen? Wie oft wurden bereits Daten herausgegeben?

Fazit: Cloud Made in Germany – Placebo oder echte Souveränität?

Cloud Made in Germany klingt nach Sicherheit und Kontrolle, ist aber in den meisten Fällen ein Marketing-Konstrukt mit wenig Substanz. Wer sich technisch und juristisch in falscher Sicherheit wiegt, zahlt am Ende drauf – mit fehlender Innovation, schlechter Skalierbarkeit und oft nur scheinbarer Compliance. Die Realität ist: Echte Souveränität entsteht durch Transparenz, technologische Exzellenz und ein tiefes Verständnis der gesamten Lieferkette – nicht durch einen Aufkleber auf der Website.

Für die Mehrheit der Unternehmen ist Cloud Made in Germany kein Heilsbringer, sondern ein Placebo. Wer wirklich Wert auf Datenschutz, Performance und Innovationskraft legt, muss sich kritisch mit der Architektur, den Prozessen und der Compliance-Praxis seines Anbieters auseinandersetzen. Der Rest ist Marketing – und der hat auf technischer Ebene noch nie ein Problem gelöst. Willkommen in der Realität. Willkommen bei 404.