Cloud Made in Germany Kritik: Realitäten und Risiken im Check

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

Cloud Made in Germany Kritik: Realitäten und Risiken im Check

Cloud Made in Germany: Klingt nach digitaler Sicherheit, Souveränität und Datenschutz wie aus dem Bilderbuch. Die Realität? Ein Flickenteppich aus Marketing-Blabla, juristischen Grauzonen und technischer Abhängigkeit von US-Giganten. Wer glaubt, mit einem „deutschen“ Cloud-Stempel sei alles rosarot, der spielt russisches Roulette mit seinen Daten – und zahlt am Ende die Rechnung. Höchste Zeit für einen harten, schonungslosen Check: Wie viel Deutschland steckt wirklich in der Cloud Made in Germany? Und wo lauern die echten Risiken?

- Was „Cloud Made in Germany“ eigentlich bedeutet – und warum der Begriff ein Minenfeld ist
- Die größten Mythen rund um deutsche Cloud-Anbieter und das vermeintliche Sicherheitsversprechen
- Reale technische, juristische und politische Risiken bei deutschen Cloud-Services
- Warum viele „deutsche Clouds“ in Wahrheit auf US-Technologie und Infrastruktur basieren
- Wie der CLOUD Act und andere US-Gesetze auch „deutsche“ Clouds angreifbar machen
- Unterschiede zwischen echten souveränen Clouds und Marketing-Produkten
- Technische Schwächen, Datenexport-Probleme und Compliance-Fallen im Alltag
- Best Practices für Unternehmen, die auf Cloud Made in Germany setzen wollen – und was sie wirklich prüfen müssen
- Ein radikales Fazit: Warum der deutsche Cloud-Traum noch weit von der Realität entfernt ist

Cloud Made in Germany – der Begriff geistert seit Jahren durch die Köpfe von Entscheidern, Datenschützern und Marketern. Wer auf deutschen Datenschutz, Infrastruktur und Rechtssicherheit setzt, fühlt sich in der Cloud Made in Germany sicher. Aber wie viel ist daran real, wie viel Wunschdenken? Die Wahrheit ist unbequem: Viele Anbieter verkaufen ein deutsches Label, liefern aber US-Software, hosten in Drittstaaten oder sind bei genauer Betrachtung nichts anderes als Reseller von Hyperscalern. Die Risiken? Sind größer als du denkst. Keine Sorge, nach diesem Artikel weißt du mehr als so mancher selbsternannte Cloud-Experte. Willkommen bei der schonungslosen Abrechnung mit der Cloud Made in Germany.

Cloud Made in Germany: Begriff, Realität und die Marketingmaschinerie

Cloud Made in Germany ist kein gesetzlich geschützter Begriff, sondern maximal ein Marketingversprechen. Jeder Anbieter kann sich dieses Label auf die Fahne schreiben, solange er irgendwie argumentieren kann, dass seine Cloud „deutsch“ ist. In der Praxis reicht das von echten deutschen Rechenzentren über Briefkastenfirmen bis hin zu White-Label-Lösungen, die irgendwo im US-Stack laufen. Wer hier auf Gütesiegel und Selbstzertifikate vertraut, läuft sehenden Auges ins offene Messer.

Technisch betrachtet ist eine Cloud Made in Germany nur dann wirklich „deutsch“, wenn Infrastruktur, Software, Datenhaltung, Management und der Betreiber selbst vollständig in Deutschland sitzen – und zwar ohne direkte oder indirekte Kontrolle durch ausländische Muttergesellschaften. Doch die Realität ist oft eine andere: Viele Anbieter betreiben zwar Rechenzentren in Frankfurt, München oder Berlin, setzen aber auf US-Software-Stacks wie

Microsoft Azure Stack, Amazon Outposts oder Google Anthos. Die Folge: Die Kontrolle über die Daten bleibt eingeschränkt, das Risiko von Datenabfluss und Fremdzugriff steigt.

Das eigentliche Problem ist die Intransparenz. Kaum ein Anbieter legt offen, auf welchen Hypervisoren, Storage-Systemen oder Netzwerkarchitekturen die Cloud tatsächlich läuft. Kunden kaufen ein Label, kein Produkt. Am Ende entscheidet nicht die Marketingbroschüre, sondern das technische und rechtliche Setup. Wer sich darauf verlässt, dass ein „deutscher“ Anbieter auch wirklich unabhängig ist, glaubt wahrscheinlich auch noch an den Weihnachtsmann.

Die Marketingmaschinerie der Cloud Made in Germany lebt von Halbwahrheiten: Ein bisschen ISO-Zertifizierung hier, ein bisschen DSGVO-Konformität da. Aber was bedeutet das in der Praxis? ISO 27001 kann auch ein US-Hyperscaler haben. DSGVO-Konformität ist ein Prozess, kein Zustand. Und ein deutsches Impressum schützt vor US-Behörden so wenig wie ein Regenschirm vor einem Meteoriteneinschlag. Wer Sicherheit will, muss tiefer bohren – und zwar technisch und juristisch.

Die Mythen der deutschen Cloud: Was wirklich dahintersteckt

Mythos 1: „Deutsche Cloud bedeutet vollständige Datensouveränität.“ Falsch. Datensouveränität ist ein komplexes Zusammenspiel aus Infrastruktur, Software, Betriebsprozessen und juristischer Kontrolle. Sobald auch nur ein Teil davon auf US-Technologie basiert, sind die Daten potenziell angreifbar. Viele Anbieter setzen auf OpenStack, VMware oder Microsoft Azure Stack – allesamt Technologien, die entweder ausländische Hersteller involvieren oder US-Patente und Support-Abhängigkeiten haben.

Mythos 2: „Deutsche Cloud schützt vor dem Zugriff ausländischer Behörden.“ Schön wär’s. Der US CLOUD Act verpflichtet US-Unternehmen, auf Anfrage Daten herauszugeben, auch wenn sie auf deutschen Servern liegen. Wer also einen Anbieter wählt, der Tochter eines US-Unternehmens ist oder US-Software einsetzt, öffnet die Tür für fremde Behörden. Der Europäische Gerichtshof hat den Privacy Shield bereits kassiert. Die Nachfolgeregelungen sind nicht besser – und das Damoklesschwert der Datenübermittlung hängt weiter über jedem Cloud-Projekt.

Mythos 3: „Cloud Made in Germany ist immer DSGVO-konform.“ Ebenfalls falsch. Die DSGVO fordert mehr als nur einen deutschen Serverstandort. Es geht um technische und organisatorische Maßnahmen, um Verschlüsselung, Zugangskontrolle, Protokollierung und Löschkonzepte. Viele Anbieter reduzieren Compliance auf das Hosting – verschweigen aber, dass Backups, Monitoring oder Support oft in Drittländern stattfinden. Die Folge: Die Cloud ist auf dem Papier „deutsch“, technisch aber löchrig wie ein Schweizer Käse.

Mythos 4: „Mit einer deutschen Cloud ist alles sicher.“ Die meisten Datenpannen in der Cloud passieren durch Fehlkonfiguration, mangelhafte Zugriffsrechte und fehlendes Monitoring – unabhängig vom Standort. Wer sich auf das Label verlässt und die eigene Cloud-Security vernachlässigt, wird früher oder später Opfer. Die Cloud ist kein Selbstläufer. Sie erfordert echtes Know-how, technische Kontrolle und permanentes Audit – egal ob in Frankfurt oder in Seattle.

Technische und juristische Risiken der Cloud Made in Germany

Die Risiken bei Cloud Made in Germany sind vielfältig – und werden oft systematisch unterschätzt. Technisch lauern die Gefahren vor allem im Bereich der Infrastruktur-Transparenz, bei API-Abhängigkeiten und in der Nutzung proprietärer US-Stacks. Viele deutsche Anbieter setzen auf VMware, Microsoft, Cisco oder NetApp – allesamt US-Unternehmen. Die Betriebssysteme, Virtualisierungsplattformen und Storage-Lösungen sind hochkomplex und selten wirklich unabhängig. Im Ernstfall entscheidet ein US-Update über die Verfügbarkeit deiner Daten. Man nennt das: digitale Fremdbestimmung.

Juristisch ist der CLOUD Act das Damoklesschwert über jeder scheinbar sicheren deutschen Cloud. US-Behörden können über den Umweg von Mutter- oder Tochterfirmen auf Daten zugreifen – völlig unabhängig vom physischen Standort. Wer glaubt, dass ein Standort in Frankfurt automatisch Immunität verleiht, hat die Funktionsweise internationaler Rechtsprechung nicht verstanden. Die Verschleierung über verschachtelte Firmenstrukturen und Subunternehmen macht die Nachverfolgung zusätzlich zur Lotterie.

Die politische Komponente kommt noch hinzu. Solange deutsche Anbieter auf US-Technologie und Support angewiesen sind, bleibt die digitale Souveränität Illusion. Sanktionen, Exportverbote oder politische Spannungen können jederzeit dazu führen, dass Updates, Support oder Security-Patches ausbleiben. Im Worst Case steht die Cloud still – und der Kunde merkt es zu spät.

Ein weiteres Risiko: Der Datenexport. Viele Anbieter speichern zwar Daten in Deutschland, aber Backups, Wartungsprotokolle oder Support-Tickets wandern regelmäßig in andere Länder. Technisch ist es schwierig, die vollständige Datenlokalität zu garantieren – schon gar nicht, wenn Monitoring, Billing oder Helpdesk in den USA oder Indien sitzen. Die Compliance-Falle ist damit programmiert.

Technische Architektur: Wie „deutsch“ ist die Cloud Made in Germany wirklich?

Wer wissen will, wie viel Deutschland in der Cloud Made in Germany steckt, muss sich die technische Architektur im Detail ansehen. Zentrale Frage: Wer betreibt die physischen Server? Wer kontrolliert die Netzwerk- und Storage-Systeme? Und wer hat Zugriff auf die Management-Interfaces? Viele Anbieter nutzen sogenannte „Colocation“-Rechenzentren, die zwar in Deutschland stehen, aber oft von internationalen Konzernen wie Equinix oder Digital Realty betrieben werden. Die Kontrolle über physische und logische Sicherheit ist damit eingeschränkt.

Die Software-Schicht ist das nächste Problemfeld. Die meisten deutschen Clouds setzen auf US-Stacks. Selbst Open Source-Lösungen wie OpenStack oder Kubernetes sind zwar quelloffen, aber ihre Entwicklung wird maßgeblich von US-Konzernen wie Red Hat, Google oder IBM gesteuert. Jeder Patch, jedes Update kann neue Schwachstellen bringen – und die Kontrolle über den Code bleibt Illusion. Wer wirklich souverän sein will, müsste auf europäische Eigenentwicklungen setzen. Die Realität? Fehlanzeige.

Auch das Thema Verschlüsselung ist ein Minenfeld. Viele Anbieter werben mit „Ende-zu-Ende-Verschlüsselung“. Doch wer hält die Schlüssel? Oft sind es die Betreiber selbst – oder sie nutzen Key-Management-Services von US-Anbietern. Eine echte Ende-zu-Ende-Verschlüsselung, bei der nur der Kunde den Schlüssel kontrolliert, ist die Ausnahme. Im Ernstfall kann jede Schwachstelle im Key-Management zum Super-GAU führen.

API-Abhängigkeit ist das nächste technische Risiko. Viele Clouds bieten Schnittstellen an, die sich an AWS, Azure oder Google orientieren. Das erleichtert die Migration – macht aber auch abhängig von den großen US-Vorbildern. Kommt es zu API-Änderungen oder Lizenzstreitigkeiten, stehen deutsche Anbieter vor massiven Problemen. Die technische Eigenständigkeit ist oft nicht mehr als ein frommer Wunsch.

Cloud Act, Datenschutz und Compliance: Die unterschätzten Gefahren

Der US CLOUD Act ist das schärfste Schwert im internationalen Cloud-Geschäft. Er verpflichtet alle US-Unternehmen – und damit auch deren Tochterfirmen – zur Herausgabe von Daten, selbst wenn diese in Deutschland liegen. Das gilt nicht nur für Google, Microsoft und Amazon, sondern auch für deutsche

Anbieter, die auf US-Software oder Support angewiesen sind. Wer also glaubt, dass seine Daten vor US-Zugriff geschützt sind, weil sie in einem Frankfurter Rechenzentrum liegen, hat die rechtliche Lage nicht verstanden.

Der Datenschutz bleibt auf der Strecke. Die DSGVO verlangt explizite Einwilligung und hohe Schutzstandards für personenbezogene Daten. Doch sobald der Anbieter Backup, Monitoring oder Support in Drittländern abwickelt, ist die Compliance dahin. Viele Unternehmen merken das erst, wenn Aufsichtsbehörden nachfragen oder ein Data Breach passiert. Die Rechtfertigung „aber unsere Cloud ist in Deutschland“ funktioniert maximal als Placebo – nicht als Schutzschild.

Compliance ist ein Dauerlauf, kein Sprint. Wer auf Cloud Made in Germany setzt, muss regelmäßig technische und organisatorische Audits durchführen, Lieferketten prüfen und Subdienstleister offenlegen. Viele Anbieter verschweigen die Komplexität ihrer Infrastruktur – und der Kunde steht am Ende juristisch im Regen. Die einzige Sicherheit ist Transparenz. Und die gibt es selten zum Nulltarif.

Die größten Datenschutzrisiken im Überblick:

- Unklare Verantwortlichkeiten beim Datenzugriff (Shared Responsibility Model wird oft ignoriert)
- Datenexporte über Backups, Ticketsysteme oder Wartung in Drittländer
- Fehlende technische Kontrolle über Verschlüsselung und Schlüsselmanagement
- Versteckte Abhängigkeiten von US-Software und -Support
- Mangelnde Auditmöglichkeiten bei verschachtelten Subunternehmen

Best Practices & Checkliste: Worauf Unternehmen bei Cloud Made in Germany wirklich achten müssen

Wer nicht in die Marketingfalle tappen will, braucht eine knallharte Cloud-Strategie. Hier die wichtigsten Punkte, die bei der Auswahl eines echten Cloud Made in Germany-Angebots geprüft werden müssen:

- Technische Infrastruktur prüfen: Wo stehen die Server? Wer betreibt die Rechenzentren? Gibt es Co-Location mit internationalen Anbietern?
- Software-Stack offenlegen: Welcher Hypervisor kommt zum Einsatz? Welche Plattform (OpenStack, VMware, Azure Stack)? Wer hat Kontrolle über Updates und Patches?
- Datenlokalität garantieren: Werden wirklich alle Daten – inklusive Backups – in Deutschland gespeichert? Was passiert mit Logs, Monitoring-Daten und Support-Tickets?
- Verschlüsselung und Schlüsselmanagement: Wer hält die Schlüssel? Gibt es

echte Ende-zu-Ende-Verschlüsselung?
- Vertragliche Absicherung: Werden Subunternehmer offen gelegt? Gibt es Exit-Strategien und Migrationssicherheit?
- Juristische Prüfung: Ist der Anbieter unabhängig von US-Unternehmen? Wie wird der CLOUD Act ausgeschlossen (Spoiler: meistens gar nicht)?
- Transparenz bei Audits: Gibt es regelmäßige technische und juristische Audits? Werden Audit-Berichte offen gelegt?
- Support und Wartung: Wo sitzt das Support-Team? Werden Wartungsarbeiten dokumentiert und nachvollziehbar protokolliert?

Ein Schritt-für-Schritt-Plan für Unternehmen:

1. Eigenen Compliance-Bedarf definieren (z.B. DSGVO, ISO-Zertifizierungen, branchenspezifische Vorgaben)
2. Cloud-Anbieter nach konkreten technischen und juristischen Kriterien befragen
3. Teststellungen anfordern und technische Audits selbst durchführen oder beauftragen
4. Verträge mit Exit- und Migrationsklauseln absichern
5. Regelmäßige Audits und Penetrationstests einplanen

Fazit: Der Traum von der deutschen Cloud – Wunschdenken oder Realität?

Cloud Made in Germany ist ein schönes Versprechen – aber eben oft nicht mehr als das. Technisch wie juristisch bleibt die echte Souveränität ein unerreichbares Ziel, solange Anbieter auf US-Technologie, internationale Rechenzentren und globale Support-Modelle setzen. Wer sich von Marketing-Labels und ISO-Zertifikaten blenden lässt, riskiert unbewusst die Kontrolle über seine sensibelsten Daten. Die Risiken reichen von Datenabfluss durch den CLOUD Act bis zu technischen Abhängigkeiten, die im Ernstfall zur digitalen Sackgasse werden.

Die einzig sinnvolle Strategie? Radikale Transparenz, schonungslose technische Prüfung und die Bereitschaft, auch unpopuläre Fragen zu stellen. Wer echte Sicherheit und Souveränität will, muss bereit sein, in Know-how, Audits und eigene Infrastruktur zu investieren – oder den Traum von der deutschen Cloud endgültig begraben. Cloud Made in Germany ist Stand heute meist ein Marketingprodukt – und bis zur echten digitalen Unabhängigkeit ist es noch ein weiter Weg.