Cloud Made in Germany Kritik Check: Realität oder Mythos?

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



Cloud Made in Germany Kritik Check: Realität oder Mythos?

“Cloud Made in Germany” klingt nach digitalem Ritterschlag – Datenschutz-Helden, Souveränität und Innovation, alles in einer glänzenden Verpackung. Doch was steckt wirklich dahinter? Ist die deutsche Cloud-Initiative ein Bollwerk gegen Big Tech, oder nur ein weiteres Buzzword für PowerPoint-Folien und politische Sonntagsreden? Wir liefern den schonungslosen Check: Wer wirklich “Made in Germany” ist, wer sich nur damit schmückt – und warum echte Cloud-Souveränität vielleicht längst verloren ist. Willkommen bei der Abrechnung mit dem deutschen Cloud-Mythos.

- Was “Cloud Made in Germany” eigentlich bedeutet und warum der Begriff so dehnbar ist wie ein alter Gummiband
- Die wichtigsten Cloud-Anbieter, die mit “Made in Germany” werben – und was davon Substanz hat
- Technische und rechtliche Hintergründe: DSGVO, Datensouveränität, Schrems II und der Patriot Act im Realitätscheck
- Die größten Mythen und Marketing-Lügen rund um deutsche Cloud-Angebote
- Technische Fallstricke: Wo “deutsche Cloud” oft nur ein Label bleibt, aber US-Backends weiter alles sehen
- Warum echte Cloud-Souveränität in Deutschland technisch und wirtschaftlich kaum erreichbar ist
- Praxis-Check: Welche Szenarien tatsächlich von “Cloud Made in Germany” profitieren – und wo es vollkommen egal ist
- Schritt-für-Schritt: Wie du echte Cloud-Sicherheit und Compliance erreichst – und worauf du beim Anbieter achten musst
- Fazit: Was bleibt vom Versprechen der deutschen Wolke und wie Unternehmen jetzt wirklich handeln sollten

Cloud Made in Germany – klingt nach Digitalpatriotismus und sauberer Technik, nach Freiheit von US-Giganten und einer sicheren Zukunft für deutsche Daten. Die Wirklichkeit ist aber oft so deutsch wie ein Hamburger bei McDonalds. Zwischen EU-Mythen, DSGVO-Panik, Schrems II-Urteilen und cleveren Marketingkampagnen bleibt die Frage: Gibt es sie überhaupt, die “deutsche Cloud”? Oder ist das alles nur eine hübsche Fassade, hinter der am Ende doch wieder Microsoft, Amazon und Google das Sagen haben? Wer sich nicht auf Buzzwords, sondern auf Fakten verlassen will, muss tiefer graben. Und genau das machen wir jetzt – mit Fakten, Technik, und einer Prise Zynismus.

Begriffserklärung: Was bedeutet “Cloud Made in Germany” technisch wirklich?

Der Begriff “Cloud Made in Germany” ist so präzise wie ein Linienbus im Berliner Berufsverkehr – sprich, gar nicht. Im Marketing klingt es nach exklusiver Technik, nach lokalem Hosting, nach Unabhängigkeit von US-Recht und nach vollständiger Datensouveränität. Tatsächlich gibt es aber keine anerkannte technische oder rechtliche Definition. Jeder Anbieter versteht darunter, was ihm gerade in den Pitch passt.

Im engeren Sinn soll “Cloud Made in Germany” bedeuten, dass Daten ausschließlich in deutschen Rechenzentren liegen, von deutschen Firmen betrieben und nach deutschem (bzw. EU-)Recht verarbeitet werden. Die Realität sieht oft anders aus: Viele Anbieter nutzen US-Software, White-Label-Produkte, verwalten Schlüssel im Ausland oder lagern den Betrieb an internationale Tochtergesellschaften aus. “Made in Germany” wird so zum Etikettenschwindel: Das Frontend steht in Frankfurt, das Backend läuft auf AWS. Willkommen im DSGVO-Kosmos.

Technisch gesehen sind die wichtigsten Kriterien für eine echte “deutsche Cloud”:

- Physische Speicherung und Verarbeitung der Daten ausschließlich in deutschen Rechenzentren
- Betrieb durch ein rechtlich selbstständiges, deutsches Unternehmen ohne US-Mutterkonzern oder Einfluss von außerhalb der EU
- Verzicht auf US-Cloud-Software (Azure, AWS, Google Cloud) als Infrastruktur-Basis
- Datensouveränität: Vollständige Kontrolle über Verschlüsselung, Schlüsselmanagement und Zugriff
- Transparenz bei Subdienstleistern und Support-Teams

Wer ehrlich hinschaut, merkt schnell: Die meisten “Cloud Made in Germany”-Labels sind maximal ein Feigenblatt. Die Technik ist oft ein Mix aus Open-Source, US-Software und deutschen Hostingverträgen – und wo es unbequem wird, regelt die Marketingabteilung den Rest. Willkommen in der Welt der Cloud-Compliance, in der alles möglich ist, solange keiner nachfragt.

Das Hauptproblem: Die technischen und juristischen Details werden von Anbietern meist so verschleiert, dass nur noch Spezialisten durchblicken. Wer nur auf das Label vertraut, spielt russisches Roulette mit seinen Daten. Erst ein tiefer Blick in die Architektur, die Lieferkette und die Verträge zeigt, was wirklich “Made in Germany” ist – und was nur so aussieht.

Die größten Anbieter: Cloud Made in Germany oder nur Etikettenschwindel?

Der deutsche Cloud-Markt ist längst nicht so unabhängig, wie ihn die Hochglanzbroschüren zeichnen. Die “großen Drei” – Microsoft, Amazon und Google – dominieren auch hier, und selbst ihre “deutschen” Angebote sind oft nur Marketing-Varianten mit lokalem Hosting. Aber es gibt auch echte deutsche Anbieter, die mit “Cloud Made in Germany” werben. Die Frage ist: Wie viel Substanz steckt dahinter?

Beispiele für Anbieter mit “Cloud Made in Germany”-Versprechen:

- Ionos by 1&1: Betreibt eigene Rechenzentren in Deutschland, positioniert sich als europäische Alternative, nutzt aber für viele Services US-Software und gelegentlich auch AWS-Backends.
- Deutsche Telekom (Open Telekom Cloud): Eigene Infrastruktur in Deutschland, Kooperation mit Huawei (was wiederum in Sachen Souveränität für Stirnrunzeln sorgt), teilweise OpenStack-basiert.
- Hetzner Online: Eigene Rechenzentren, keine US-Mutter, klare Kommunikation zur Datenhaltung – aber wenig Enterprise-Cloud-Features à la AWS.
- PlusServer: Positioniert sich als “Sovereign Cloud”, deutsche

Infrastruktur, aber viele Services basieren auf OpenStack oder internationalen Partnern.
- Gaia-X und andere Initiativen: Viel Politik, viele Whitepaper, wenig echte Produkte. Gaia-X ist bislang eher ein Symbol für europäischen Cloud-Aktionismus als eine ausgereifte Plattform.

Das Problem: Kaum ein Anbieter kommt heute ohne Kooperationen, Open-Source-Komponenten oder Drittanbieter-APIs aus. Sobald US-Software, US-Provider oder internationale Subdienstleister im Spiel sind, kann der "Cloud Made in Germany"-Anspruch schnell bröckeln. Wer DSGVO, Schrems II und den Patriot Act ernst nimmt, muss tiefer bohren – und oft feststellen: Am Ende entscheidet die Lieferkette, nicht das Label auf der Website.

Anders gesagt: Wer heute eine "100% deutsche Cloud" will, zahlt entweder einen absurden Aufpreis oder bekommt maximal eine halbe Lösung. Die meisten deutschen Clouds sind Kompromisse zwischen Technik, Kosten, Compliance und Marketing. Wer ehrlich ist, spricht von "Cloud Hosted in Germany" – alles andere ist PR.

Rechtliche Realität: DSGVO, Schrems II, Patriot Act – und der Cloud-Souveränitäts-Mythos

Juristisch wird es erst richtig spannend: Spätestens seit dem Schrems II-Urteil des EuGH 2020 ist klar, dass Datentransfers in die USA (und andere Länder ohne "angemessenes Datenschutzniveau") faktisch unzulässig sind. Die DSGVO verlangt, dass personenbezogene Daten sicher und unter Kontrolle der Betroffenen verarbeitet werden. Der Cloud Act und der US Patriot Act ermöglichen US-Behörden aber Zugriff auf Daten von US-Unternehmen – egal, wo die Daten liegen. Die Folge: Selbst eine AWS-Instanz in Frankfurt unterliegt US-Recht, wenn Amazon als Provider Zugriff auf die Daten hat.

Die wichtigsten juristischen Fallstricke sind:

- Schrems II: Das Privacy Shield ist tot. Standardvertragsklauseln reichen nicht, wenn US-Unternehmen Zugriff auf die Daten haben könnten.
- Cloud Act / Patriot Act: US-Provider müssen US-Behörden auch dann Daten liefern, wenn diese in Deutschland liegen.
- Subdienstleister-Ketten: Viele "deutsche" Clouds nutzen Subunternehmer oder US-Software, wodurch Daten indirekt abfließen können.
- Datensouveränität: Wer nicht selbst die Schlüssel kontrolliert, hat keine Kontrolle. Viele Cloud-Lösungen verschleiern das Schlüsselmanagement.
- Compliance-Illusionen: Anbieter verweisen auf ISO-Zertifikate, aber die sagen nichts über reale Zugriffsmöglichkeiten oder die Wirksamkeit der Verschlüsselung aus.

Die harte Wahrheit: Eine absolute rechtliche Sicherheit gibt es in der Public

Cloud nicht, solange auch nur ein US-Unternehmen oder ein internationaler Dienstleister involviert ist. “Cloud Made in Germany” ist also bestenfalls ein Compliance-Upgrade, aber kein Allheilmittel. Wer auf Nummer sicher gehen will, muss eigene Schlüssel verwalten, Verschlüsselung “end-to-end” durchsetzen und jede Lieferkette lückenlos prüfen. Das ist technisch und organisatorisch aufwendig – und in der Praxis für die meisten Unternehmen ein Ding der Unmöglichkeit.

Und noch ein Zynismus zum Schluss: Deutsche Unternehmen, die sich über US-Zugriffe aufregen, nutzen im Alltag weiter Microsoft 365, Google Workspace oder Slack – und wundern sich, wenn der Datenschutzbeauftragte graue Haare bekommt. Willkommen im echten Leben.

Technische Fallstricke: Von US-Backends, Open-Source-Märchen und Key-Management-Katastrophen

“Cloud Made in Germany” klingt technisch sauber, ist aber oft ein Flickenteppich aus Fremdkomponenten, US-Software und undurchsichtigem Key Management. Viele Anbieter verschweigen, dass sie für zentrale Komponenten (wie Storage, Datenbanken, Monitoring oder Support) weiterhin auf US-Lösungen setzen. Das ergibt ein gefährliches Mix-&-Match: Das Frontend ist deutsch, das Backend amerikanisch, und der Schlüssel liegt irgendwo in der Cloud.

Die typischen technischen Schwachstellen:

- US-Software als Core-Komponente: Viele deutsche Clouds laufen auf OpenStack, Kubernetes oder sogar AWS-Komponenten. Wer die Kontrolle über diese Layer verliert, verliert die Souveränität.
- Key Management: Wer die Verschlüsselungsschlüssel nicht selbst generiert, speichert und verwaltet, kann keine echte Datensouveränität garantieren. Viele Anbieter bieten “Customer Managed Keys” nur als teuren Aufpreis oder gar nicht an.
- APIs und Monitoring: Oft werden für Betrieb, Monitoring oder Support US-basierte Dienste eingesetzt, die Zugriff auf Metadaten oder sogar Nutzdaten haben.
- Subdienstleister-Ketten: Jeder Subdienstleister – ob für Netzwerk, Backup oder Security – ist ein potenzielles Leck. Oft fehlen transparente Listen der eingesetzten Subunternehmen.
- “Private Cloud”-Märchen: Viele Angebote sind nur virtualisierte Server in deutschen Rechenzentren, aber keine echte Cloud mit elastischer Skalierung, Self-Service, oder API-Kontrolle. Das ist Hosting, kein Cloud Computing.

Die technische Komplexität sorgt dafür, dass nur Experten die tatsächliche

Architektur durchschauen. Für Unternehmen ohne eigene IT-Security-Teams wird “Cloud Made in Germany” damit schnell zur Black Box. Wer wirklich Souveränität will, muss mindestens folgende Punkte prüfen:

- Welche Komponenten (Hypervisor, Storage, Netzwerk, Monitoring) laufen auf welcher Software-Basis?
- Wer hat Zugriff auf die physischen Server, die Netzwerk-Infrastruktur und die Management-APIs?
- Wer kontrolliert das Schlüsselmanagement und die Verschlüsselung?
- Wie werden Supportfälle behandelt und dokumentiert?
- Welche Subdienstleister und Drittanbieter sind involviert?

Die Erkenntnis: “Cloud Made in Germany” ist oft ein Label, das technische Komplexität, internationale Verflechtungen und Kontrollverluste kaschiert. Wer auf Nummer sicher gehen will, fährt besser mit On-Premises, Private Cloud oder Hybrid-Modellen – aber das ist meist unbequemer, teurer und weniger flexibel.

Praxis-Check: Wann bringt “Cloud Made in Germany” wirklich Vorteile – und wann ist es egal?

Die Frage, ob “Cloud Made in Germany” sinnvoll ist, hängt stark vom Anwendungsfall ab. Für wen ist das Label mehr als nur Marketing? Und wer kann es sich sparen?

Typische Szenarien, in denen “Cloud Made in Germany” tatsächlich relevant sein kann:

- Branchen mit extrem hohen Datenschutzanforderungen (Gesundheit, öffentlicher Sektor, kritische Infrastrukturen)
- Unternehmen, die sensible personenbezogene Daten verarbeiten und unter ständiger Kontrolle durch Datenschutzbehörden stehen
- Organisationen, die sich explizit gegen US-Clouds positionieren wollen (politische oder strategische Gründe)
- Projekte mit spezifischen Compliance-Anforderungen, die nur durch vollständige Datenhaltung in Deutschland erfüllbar sind

In vielen anderen Fällen ist das “Made in Germany”-Label dagegen irrelevant oder sogar hinderlich:

- Wenn ohnehin mit US-Software gearbeitet wird (Microsoft 365, Google Workspace, Salesforce etc.)
- Bei Anwendungen mit niedrigen Datenschutzanforderungen (z. B. Marketing-Websites, offene Daten, nicht-personenbezogene Informationen)
- Wenn Skalierbarkeit, Innovationsgeschwindigkeit und Kosten wichtiger

sind als maximale Compliance
- Für Startups und Unternehmen, die auf globale Cloud-Ökosysteme, DevOps-Tools und APIs angewiesen sind

Die Wahrheit: Für die meisten Unternehmen ist “Cloud Made in Germany” ein nettes Argument im Vertriebsgespräch, aber kein echter Gamechanger für Sicherheit oder Compliance. Wer wirklich Datenschutz will, muss sich um Architektur, Schlüsselmanagement und Prozesse kümmern – und nicht auf das Label auf der Homepage vertrauen.

Schritt-für-Schritt: So prüfst du deinen Cloud-Anbieter auf echte Souveränität

Wer keine Lust mehr auf Marketing-Nebelkerzen hat, sollte jeden Anbieter auf Herz und Nieren prüfen. Hier ist der technische Reality-Check, der über “Cloud Made in Germany” hinausgeht:

- 1. Architektur offenlegen lassen: Lass dir detailliert erklären, welche Komponenten (Storage, Netzwerk, Management-APIs) auf wessen Technologie basieren.
- 2. Nach Subdienstleistern fragen: Verlange eine vollständige Liste aller Subunternehmer, die Zugriff auf Daten oder Infrastruktur haben.
- 3. Schlüsselmanagement prüfen: Kläre, wer Verschlüsselungsschlüssel generiert, speichert und verwaltet. Idealerweise: “Customer Managed Keys”.
- 4. API- und Monitoring-Tools analysieren: Werden US-Dienste für Betrieb, Monitoring oder Support genutzt?
- 5. Vertragsdetails durchleuchten: Prüfe, ob im Notfall Zugriff durch US-Behörden möglich ist (Patriot Act, Cloud Act etc.).
- 6. Zertifikate und Audits einfordern: ISO 27001, C5, BSI-Audits – aber nicht auf Siegel verlassen, sondern auf echte Prozesse schauen.
- 7. Support und Notfallmanagement: Wer greift wann und wie auf Systeme zu? Sind Support-Teams in Deutschland oder im Ausland?
- 8. Dokumentation und Transparenz: Lückenlose technische Dokumentation ist Pflicht – alles andere ist ein No-Go.

Wer diese Liste abarbeitet, erkennt schnell: Die meisten Anbieter, die mit “Cloud Made in Germany” werben, scheitern spätestens bei Schlüsselmanagement, Subdienstleistern oder Software-Basis. Das ist kein Zufall, sondern Ausdruck der globalen Vernetzung moderner IT – und des gnadenlosen Kostendrucks im Cloud-Geschäft.

Fazit: “Cloud Made in Germany” – Mehr Mythos als Realität?

Das Versprechen von “Cloud Made in Germany” klingt gut, verkauft sich gut – und ist technisch wie rechtlich in vielen Fällen nicht haltbar. Wer sich auf das Label verlässt, bekommt oft nur eine Illusion von Sicherheit und Souveränität, während im Hintergrund weiterhin US-Software läuft, Subdienstleister Daten sehen und Schlüssel im Ausland liegen. Die Realität ist: Absolute Datensouveränität gibt es in der Public Cloud nicht, solange internationale Anbieter, Software und Lieferketten im Spiel sind.

Für Unternehmen heißt das: Vertraue keinem Label, prüfe Technik und Verträge im Detail, setze auf eigenes Schlüsselmanagement und Transparenz in der Architektur. Und akzeptiere, dass echte Souveränität teuer, unbequem und technisch anspruchsvoll ist. Wer das nicht leisten kann oder will, sollte ehrlich sein – und sich nicht von Buzzwords blenden lassen. Die deutsche Cloud bleibt ein schönes Versprechen, aber für die meisten ein Marketing-Mythos. Willkommen in der Realität der digitalen Souveränität – made in 404.