Cloud Made in Germany Kritik Review: Sicher oder Show?

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

Cloud Made in Germany Kritik Review: Sicher oder Show?

Cloud Made in Germany – klingt nach digitaler Sicherheit mit Bundesadler-Gütesiegel, oder? Doch was steckt wirklich hinter dem Marketing-Gewitter der deutschen Cloud-Anbieter? In diesem Artikel zerlegen wir das Versprechen "Sicherheit und Datenschutz aus Deutschland" bis auf den letzten Bit und prüfen, ob du deiner "Cloud Made in Germany" wirklich trauen kannst – oder ob du am Ende nur für schicke Siegel und patriotische Phrasen bezahlst. Achtung: Es wird kritisch, technisch und garantiert weniger PR-beschönigt als in den Hochglanzbroschüren der Anbieter.

- Was “Cloud Made in Germany” überhaupt bedeutet – und was nicht
- Die wichtigsten technischen und rechtlichen Kriterien deutscher Cloud-Dienste
- Sicherheitsversprechen: Realität, Marketing oder Placebo?
- Vergleich der führenden deutschen Cloud-Plattformen
- Unbequeme Wahrheiten: Backdoors, Datentransfer und Compliance-Lücken
- Technische Architektur: Wie sicher sind die Infrastrukturen wirklich?
- DSGVO, Schrems II & Co.: Welchen Schutz bietet “deutsche Cloud” tatsächlich?
- Checkliste: So prüfst du, ob dein Anbieter mehr als nur eine Deutschland-Flagge hat
- Warum Cloud-Souveränität 2025 mehr als ein Marketinggag sein muss

Cloud Made in Germany – das klingt nach dem digitalen Schutzwall gegen US-Geheimdienste, nach DSGVO auf Steroiden und nach maximaler Souveränität. Doch zwischen Hochglanz-Marketing und technischer Wirklichkeit klafft oft eine gewaltige Lücke. Wer 2025 noch glaubt, dass ein Standort in Frankfurt automatisch höchste Sicherheit bedeutet, hat die Spielregeln der Cloud-Industrie nicht verstanden. Denn: “Made in Germany” ist kein technisches Konzept, sondern ein Label, das mehr Fragen aufwirft als es beantwortet. Dieser Artikel räumt auf mit Mythen, Buzzwords und deutschen PR-Märchen – und zeigt, worauf es bei echter Cloud-Sicherheit wirklich ankommt.

Die Cloud ist längst das Rückgrat der digitalen Wirtschaft. Doch während US-Giganten wie AWS, Google Cloud und Azure den Markt dominieren, versuchen deutsche Anbieter mit “Cloud Made in Germany” zu punkten. Klingt nach Datenschutz und Unabhängigkeit – doch was ist dran? Sind die deutschen Clouds wirklich sicherer, oder ist das nur cleveres Storytelling? Und wie sieht es technisch, regulatorisch und praktisch tatsächlich aus? Zeit für eine kritische Review, die keine Marketingphrase unkommentiert lässt.

Cloud Made in Germany: Definition, Anspruch und Wirklichkeit

Beginnen wir mit der wichtigsten Frage: Was bedeutet “Cloud Made in Germany” überhaupt? Die meisten Anbieter definieren das Label so: Rechenzentren in Deutschland, Betrieb nach deutschem Recht, DSGVO-Konformität und Support aus Deutschland. Klingt solide, ist aber in der Praxis oft ein Flickenteppich. Denn es gibt keinen einheitlich geschützten Begriff, kein verbindliches Zertifikat und keine objektiven Prüfkriterien, die diesen Anspruch wirklich absichern. Jeder Anbieter kann seine Services so labeln – unabhängig davon, ob die Cloud-Architektur tatsächlich “deutsch” ist oder nur ein Mietvertrag mit einem Frankfurter Colocation-Anbieter besteht.

Technisch betrachtet heißt “Cloud Made in Germany” meistens: Die Daten werden in einem deutschen Rechenzentrum gehalten, betrieben von einem in Deutschland registrierten Unternehmen. Aber: Die eingesetzte Software stammt oft von

internationalen Herstellern (Stichwort: VMware, Microsoft, OpenStack), das Support-Team sitzt vielleicht in Deutschland, aber der Code wird weltweit entwickelt – inklusive US-Komponenten und Libraries. Wer hier echte Souveränität sucht, sollte sehr genau hinschauen, wo die Abhängigkeiten liegen.

Außerdem: Selbst wenn die Hardware und der Betrieb "deutsch" sind, heißt das nicht automatisch, dass die Daten vor Zugriff durch Dritte geschützt sind. Cloud-Provider müssen auch in Deutschland unter bestimmten Umständen Daten herausgeben – etwa bei Ermittlungen. Und spätestens bei internationalen Support-Vorfällen wird es kritisch: Werden Tickets über globale Systeme bearbeitet, landen Metadaten und Logs schnell außerhalb Deutschlands. "Made in Germany" ist damit eher ein Marketing-Claim als ein echter technischer Sicherheitsgarant.

Auch beim Thema Compliance trennt sich schnell die Spreu vom Weizen. Nur weil ein Anbieter auf seiner Website mit ISO 27001, BSI C5 oder TISAX wedelt, heißt das noch lange nicht, dass die gesamte Architektur wirklich durchgehend auditierbar, transparent und konform ist. Viele Zertifikate gelten nur für Teilbereiche oder einzelne Services – und was "cloudfähig" ist, steht oft im Kleingedruckten. Wer auf echte Compliance Wert legt, muss jedes Detail prüfen – und nicht auf das große Siegel am Seitenanfang vertrauen.

Sicherheitstechnische Architektur: Was steckt wirklich hinter deutschen Clouds?

Die zentrale Frage bleibt: Wie sicher sind die deutschen Cloud-Infrastrukturen 2025 wirklich? Technisch unterscheiden sich viele deutsche Anbieter kaum von ihren internationalen Konkurrenten. Die meisten setzen auf Virtualisierungstechnologien wie KVM, VMware oder OpenStack, nutzen Standard-Netzwerk-Stack (oft mit Linux-Firewalls und SDN-Komponenten) und lagern Storage auf SAN- oder Ceph-Cluster aus. Wer hier Exotik oder "deutsche Spezialtechnik" erwartet, wird enttäuscht – die Basistechnologien sind global identisch. Der Unterschied liegt höchstens im Betriebsmodell und im Support.

Eine große Schwachstelle vieler "Cloud Made in Germany"-Angebote bleibt die fehlende End-to-End-Verschlüsselung auf Anwenderseite. Während US-Anbieter wie Google Cloud oder AWS mit clientseitiger Verschlüsselung und dedizierten Key Management Services (KMS) punkten, bieten viele deutsche Clouds nur eine ruhige Verschlüsselung der Daten im Storage (at rest), nicht aber während der Übertragung (in transit) oder auf Anwendungsebene (end-to-end). Das heißt: Wer wirklich sicher sein will, muss eigene Verschlüsselungslösungen implementieren – und kann sich nicht auf die Infrastruktur verlassen.

Auch das Thema Multi-Tenancy – also die saubere Trennung von Kundendaten auf gemeinsam genutzten Ressourcen – ist technisch anspruchsvoll. Viele deutsche Clouds setzen auf klassische Virtualisierung oder Containerisierung, aber die Isolation ist nicht immer so wasserdicht, wie es die Marketingfolien suggerieren. Sogenannte “Noisy Neighbor”-Effekte, Side-Channel-Angriffe oder fehlerhafte Netzwerksegmentierung sind auch in deutschen Infrastrukturen kein Fremdwort. Ohne regelmäßige externe Penetrationstests und detaillierte Audits bleibt die “Trennung” oft ein frommer Wunsch.

Und dann wäre da noch das Backdoor-Problem. Deutsche Anbieter betonen zwar, keine absichtlichen Hintertüren einzubauen – aber sie nutzen fast immer Open-Source- oder US-Software-Komponenten mit eigenem Patch- und Update-Management. Wer garantiert, dass nicht doch ein Zero-Day oder eine fest verdrahtete Remote-Access-Lücke im Stack schlummert? Die technische Transparenz endet oft beim Provider – und für den Kunden bleibt nur Hoffnung, dass Security-Versprechen und Realität übereinstimmen.

DSGVO, Schrems II und Compliance: Deutsche Cloud als Rettungsanker?

Spätestens seit dem Schrems II-Urteil des EuGH sind international betriebene Clouds regulatorisch ein Pulverfass. Datenübertragungen in die USA oder andere “unsichere Drittländer” sind ohne spezielle Garantien praktisch unmöglich. Hier setzen deutsche Anbieter an: Keine Daten außerhalb Deutschlands, keine US-Muttergesellschaft, kein Patriot Act – so zumindest der Claim. Doch wie sieht die Praxis aus?

Viele “Cloud Made in Germany”-Provider werben offensiv mit DSGVO-Konformität, BSI-Zertifikaten und sogar mit “Schrems II-Sicherheit”. Doch der Teufel steckt im Detail. Ein deutsches Rechenzentrum reicht nicht, wenn der Betreiber Tochter einer US-Firma ist oder die Betriebssoftware aus den USA stammt. Im Zweifel kann auch ein Gericht in den USA Zugriffsrechte erzwingen – und deutsche Anbieter müssen sich entscheiden, ob sie Geschäftsgeheimnisse oder Compliance opfern. Die vollständige Cloud-Souveränität ist in einer globalen Lieferkette fast unmöglich.

Außerdem bleibt das Thema Joint Controller und Auftragsverarbeitung kritisch. Die meisten deutschen Anbieter bieten Standard-AV-Verträge, aber die technische Umsetzung der datenschutzrechtlichen Vorgaben ist oft lückenhaft. Wer etwa wissen will, ob Logs, Snapshots und Metadaten wirklich nicht ins Ausland wandern, muss sehr tief in die technischen Prozesse einsteigen – und bekommt selbst dann meist nur vage Antworten.

Ein weiteres Problem ist die “Schatten-IT” durch Third-Party-Integrationen. Viele deutsche Clouds bieten Marketplace-Lösungen, API-Anbindungen und externe Add-ons – und öffnen so doch wieder das Tor zu internationalen Datenströmen. DSGVO-Sicherheit ist deshalb nur so stark wie das schwächste

Glied im Service-Stack. Wer echte Compliance will, braucht vollständige Transparenz – nicht nur beim Hosting, sondern in jedem Layer der Architektur.

Last but not least: Die Behördenfreundlichkeit. Auch in Deutschland gibt es gesetzliche Zugriffsmöglichkeiten (Stichwort: TKÜV, BKA-Gesetz, BSI-Gesetz), die im Zweifel Vorrang vor Datenschutz haben. Wer also glaubt, mit einer "deutschen Cloud" sei er vor allen Zugriffen geschützt, verkennt die Realität. Die Frage ist nicht, ob Behörden zugreifen können – sondern wie transparent und nachvollziehbar der Prozess für den Kunden ist.

Technik vs. Marketing: Wie erkennst du echte Sicherheit?

Wie also prüfst du als Unternehmen, ob deine "Cloud Made in Germany" wirklich hält, was sie verspricht? Die meisten Anbieter werfen mit Zertifikaten, Compliance-Versprechen und Support-Garantie um sich. Doch was zählt wirklich? Hier eine Schritt-für-Schritt-Checkliste, mit der du technische und organisatorische Sicherheit unabhängig vom Marketing prüfen kannst:

- Standortprüfung: Liegen alle primären und sekundären Rechenzentren tatsächlich in Deutschland? Gibt es Ausweichstandorte im Ausland?
- Rechtsstruktur: Ist der Anbieter selbständig oder Teil eines internationalen Konzerns? Gibt es Mutter- oder Tochtergesellschaften im Ausland?
- Technologiestack: Welche Software- und Hardware-Komponenten werden eingesetzt? Gibt es US- oder Drittland-Komponenten im Stack?
- Datenflüsse und Integrationen: Werden Metadaten, Logs oder Supportdaten ins Ausland übertragen? Welche APIs sind offen und an wen?
- Verschlüsselung: Welche Verschlüsselungsmechanismen sind aktiv? Gibt es clientseitige, Ende-zu-Ende- oder nur Storage-Verschlüsselung?
- Isolation und Multi-Tenancy: Wie wird die Trennung der Kundendaten technisch umgesetzt? Gibt es regelmäßige Penetrationstests und Audits?
- Transparenz und Auditierbarkeit: Gibt es vollständigen Einblick in die technischen Prozesse? Werden externe Prüfberichte bereitgestellt?
- Notfall- und Zugriffsszenarien: Wie wird mit Behördenanfragen umgegangen? Gibt es klare Prozesse und dokumentierte Transparenzberichte?

Wer diese Punkte konsequent prüft, trennt schnell die echten Sicherheitsanbieter von den Marketingkünstlern. "Cloud Made in Germany" ist kein Selbstzweck, sondern muss technisch, organisatorisch und rechtlich durchdekliniert werden – sonst bleibt es bei schönen Worten und leeren Versprechen.

Die großen deutschen Cloud-

Provider im harten Vergleich

Natürlich gibt es in Deutschland nicht “die eine” Cloud. Die wichtigsten Anbieter heißen IONOS, Deutsche Telekom (Open Telekom Cloud), PlusServer, noris network und Hetzner. Jeder verspricht maximale Sicherheit und Compliance – aber die Unterschiede liegen im Detail. Während IONOS und Telekom mit eigenen Rechenzentren und starker Compliance punkten, bauen viele kleinere Anbieter auf gemietete Infrastruktur und Standardsysteme. Bei den großen Playern kommt oft OpenStack als Cloud-Engine zum Einsatz – mit allen Vor- und Nachteilen der Open-Source-Basis.

Ein besonders kritischer Punkt ist das Thema Support und SLAs. Wer Service auf Enterprise-Niveau will, muss bei deutschen Providern oft tiefer in die Tasche greifen als bei US-Wettbewerbern. Gleichzeitig ist die technische Flexibilität oft eingeschränkt – viele Features wie serverlose Architektur, Big Data Services oder KI-Integrationen fehlen oder hinken der internationalen Konkurrenz Jahre hinterher. Wer also nur auf den Standort setzt, zahlt oft einen hohen Preis beim Innovationsgrad.

Und dann ist da noch die Performance-Frage. Während US-Clouds mit globalen Backbone-Netzen und Edge-Locations glänzen, sind die meisten deutschen Clouds auf nationale Infrastruktur beschränkt. Das reicht für viele klassische Enterprise-Workloads, aber bei globalen Anwendungen, Latenz oder Skalierung stoßen viele deutsche Clouds schnell an ihre Grenzen – spätestens wenn Traffic-Spitzen oder internationale User ins Spiel kommen.

Auch bei der API-Kompatibilität gibt es Unterschiede. Während AWS und Azure de-facto-Standards bei Automatisierung und DevOps setzen, kochen viele deutsche Clouds ihr eigenes Süppchen. Das macht Migrationen, Hybrid-Cloud-Modelle und Multi-Cloud-Ansätze oft zum Albtraum für Entwickler. Wer auf “Cloud Made in Germany” setzt, muss also genau prüfen, wie offen und standardkonform die Schnittstellen wirklich sind.

Abschließend: Die Sicherheitsversprechen der deutschen Cloud-Anbieter sind nicht per se falsch – aber sie sind kein pauschaler Freifahrtschein. Wer echte Sicherheit will, muss sich mit Architektur, Compliance und Betriebsprozessen im Detail auseinandersetzen – und nicht auf das Label “Made in Germany” vertrauen.

Fazit: Cloud Made in Germany – Sicher, aber nie absolut

Cloud Made in Germany ist mehr als nur ein Aufkleber – aber eben auch nicht das digitale Schutzschild, als das es vermarktet wird. Wer echte Sicherheit und Compliance braucht, muss tiefer graben als bis zum Standort der Server. Die technische Architektur, die Verschlüsselung, die Organisationsstruktur und die komplette Lieferkette entscheiden darüber, wie sicher deine Daten wirklich sind. Ein deutsches Rechenzentrum ist ein guter Anfang – aber kein

Garant.

Am Ende bleibt: Cloud Made in Germany kann eine sinnvolle Antwort auf regulatorische Anforderungen und digitale Souveränität sein – wenn der Anbieter transparent, technisch versiert und konsequent auditierbar ist. Für viele Unternehmen ist das Label ein Pluspunkt im Compliance-Check – aber niemals eine Ausrede, das eigene Risiko- und Sicherheitsmanagement zu vernachlässigen. Wer 2025 noch glaubt, Marketing-Siegel ersetzen technische Exzellenz, wird irgendwann böse aufwachen. Sicherheit ist keine Frage des Herkunftslabels, sondern des technischen und organisatorischen Gesamtpakets.