Cloud Made in Germany Kritik Fragezeichen: Realität oder Mythos?

Category: Opinion
geschrieben von Tobias Hager | 14. September 2025

Cloud Made in Germany Kritik Fragezeichen: Realität oder Mythos?

“Cloud Made in Germany” – klingt nach Datensicherheit, Rechtstreue und digitaler Souveränität vom Feinsten. Die Wahrheit? Zwischen cleverem Marketing, juristischer Nebelkerze und technischer Realität klafft ein Abgrund, in den so manche deutsche IT-Strategie schon kopfüber gestürzt ist. Dieser Artikel zerlegt die Wolke in ihre Einzelteile, entlarvt Mythen und zeigt, warum “Cloud Made in Germany” oft mehr Fragezeichen als Antworten liefert. Wer jetzt noch glaubt, mit deutschem Hosting sei alles geregelt, bekommt hier die schonungslose Abrechnung – garantiert ohne Filterblase.

- Was “Cloud Made in Germany” wirklich bedeutet – und warum der Begriff rechtlich fragwürdig ist
- Die wichtigsten technischen und juristischen Anforderungen an eine deutsche Cloud
- Warum Datenstandort Deutschland nicht gleichbedeutend mit Datenschutz ist
- Die größten Mythen und Marketing-Tricks deutscher Cloud-Anbieter
- Wie US-Clouds, DSGVO, Schrems II und der CLOUD Act die Karten neu mischen
- Technische Realitäten: Infrastruktur, Zertifikate, Compliance und Security
- Step-by-Step: Was bei der Auswahl einer “deutschen Cloud” wirklich zählt
- Worauf Unternehmen achten müssen, um nicht auf die Marketingmasche hereinzufallen
- Fazit: Warum “Cloud Made in Germany” selten das hält, was das Label verspricht

“Cloud Made in Germany” ist längst zum Feigenblatt der deutschen Digitalwirtschaft geworden. Aber hält das Label, was es verspricht? Wer nur auf den Datenstandort Deutschland schielt und sich von schwarz-rot-goldenen Logos blenden lässt, hat die Rechnung ohne die technologische und juristische Wirklichkeit gemacht. Denn: Die Cloud ist kein Ort, sondern ein komplexes Konstrukt aus Infrastruktur, Verträgen, Compliance und internationalen Abhängigkeiten. Wer wirklich souverän agieren will, braucht mehr als einen Marketing-Slogan auf dem Briefkopf.

Die Debatte um “Cloud Made in Germany” ist dabei alles andere als neu. Seit den Snowden-Enthüllungen, dem Schrems-II-Urteil und der zunehmenden Dominanz amerikanischer Hyperscaler hallt der Ruf nach einer deutschen Cloud durch die Flure von Politik, Verwaltung und Wirtschaft. Doch was steckt hinter den Versprechen? Was bedeutet es technisch und organisatorisch, eine Cloud “Made in Germany” zu betreiben? Und warum genügt es eben nicht, einfach einen Server in Frankfurt zu mieten, um alle Datenschutzprobleme elegant aus der Welt zu schaffen?

Dieser Artikel nimmt die Buzzwords auseinander, benennt die wunden Punkte und zeigt, warum sich die meisten Unternehmen mit dem Label “Cloud Made in Germany” in falscher Sicherheit wiegen. Wer tatsächlich Wert auf echte Datenhoheit und Compliance legt, muss tiefer graben – und sich mit den harten technischen, rechtlichen und organisatorischen Fakten auseinandersetzen. Willkommen in der Realität. Willkommen bei 404.

Cloud Made in Germany: Begriff, Ursprung und

juristische Grauzonen

Fangen wir bei den Basics an: “Cloud Made in Germany” ist kein geschützter Begriff. Jeder kann seine Infrastruktur, Software oder Dienstleistung als solche vermarkten, solange der Begriff nicht irreführend im Sinne des Gesetzes gegen den unlauteren Wettbewerb (UWG) verwendet wird. Das eigentliche Problem: Es gibt keinen verbindlichen Standard, keine gesetzliche Definition und keine unabhängige Zertifizierungsstelle, die dieses Label vergibt oder überprüft.

Der Begriff wurde in den späten 2010ern von einer Reihe mittelständischer IT-Provider und Lobbyverbände in die Welt gesetzt, um sich vom wachsenden Einfluss amerikanischer Hyperscaler wie AWS, Microsoft Azure und Google Cloud abzugrenzen. Die Botschaft war (und ist): Wer bei uns hostet, ist “sicher”, “DSGVO-konform” und vor ausländischem Zugriff geschützt. Die harte Realität: Das ist juristisch wie technisch ein Trugschluss.

Das zentrale Verkaufsargument lautet: “Deutsche Cloud = deutsches Recht = maximaler Datenschutz.” Doch genau hier liegt der Hund begraben. Denn das Hosting in Deutschland garantiert weder automatisch die Einhaltung der DSGVO, noch schützt es vor dem Zugriff ausländischer Behörden – insbesondere dann nicht, wenn der Anbieter Mutterkonzerne oder technische Abhängigkeiten im Ausland hat. Die Realität ist komplexer, und genau das nutzen viele Anbieter für ihre Marketingstrategie aus.

Juristisch gesehen ist die Frage, wer als “Auftragsverarbeiter” agiert, welche Subdienstleister beteiligt sind und wer tatsächlich Zugriff auf die Daten hat, entscheidend. Ein deutsches Rechenzentrum mit US-amerikanischer Konzernmutter bleibt ein Compliance-Risiko. Und auch die beste ISAE 3402 oder ISO 27001-Zertifizierung ersetzt keine saubere Vertrags- und Risikoanalyse. Wer hier auf “Cloud Made in Germany”-Siegel vertraut, handelt bestenfalls naiv, schlimmstenfalls grob fahrlässig.

Technische Anforderungen: Was eine echte “deutsche Cloud” leisten muss

Technisch betrachtet reicht ein Serverstandort in Deutschland nicht einmal ansatzweise, um die Ansprüche an eine “Cloud Made in Germany” zu erfüllen. Wer sich auf das Label verlässt, sollte sich folgende Fragen stellen (und beantworten lassen): Wer ist Eigentümer und Betreiber der Infrastruktur? Wie tief geht die technische Kontrolle – von der Hardware über Firmware, Hypervisor, Netzwerk bis zum Management-Stack? Wer liefert Updates, Support und Monitoring?

Viele Anbieter setzen auf Colocation in deutschen Rechenzentren, nutzen aber US-Software, US-Support oder internationale Subdienstleister. Das technische

Ownership liegt damit oft nicht in Deutschland. Für echte Datensouveränität braucht es aber eine vollständige Kontrolle der gesamten Wertschöpfungskette: von der physischen Infrastruktur über das Netzwerk bis zur Software-Schicht. Jede Abhängigkeit – etwa in Form von "White-Label-Clouds" oder Managed Services aus dem Ausland – ist ein potenzielles Risiko.

Ein weiteres Problem: Die wenigsten deutschen Anbieter können mit der Skalierbarkeit, Verfügbarkeit und Innovationsgeschwindigkeit der Hyperscaler mithalten. Während AWS, Azure & Co. mit Multi-Region-Replikation, automatischer Skalierung, globalem CDN, KI-Diensten und APIs aufwarten, sind viele "deutsche Clouds" funktional und infrastrukturell Jahre zurück. Wer auf "Cloud Made in Germany" setzt, muss oft Einbußen bei Resilienz, Features und Preis-Leistung akzeptieren.

Worauf es ankommt, sind unter anderem:

- Eigentümerschaft und Betrieb der Infrastruktur (keine Abhängigkeit von US-Konzernen)
- Transparente Subdienstleister-Listen und klare Vertragsverhältnisse
- Technische und organisatorische Maßnahmen zur Datenisolation und -verschlüsselung
- Nachweisbare Compliance mit ISO 27001, BSI C5 oder vergleichbaren Standards
- Souveränität bei Wartung, Updates und Incident Response

Kurz: Wer Cloud Made in Germany ernst meint, muss liefern – und zwar technisch, organisatorisch und juristisch. Alles andere ist Etikettenschwindel.

Datenstandort Deutschland: Warum der Mythos nicht reicht

Der größte Irrglaube beim Thema "Cloud Made in Germany" ist die Gleichsetzung von Datenstandort mit Datenschutz. Die Realität: Der physische Speicherort ist nur ein kleiner Baustein im Gesamtkonstrukt Datensicherheit und Compliance. Entscheidend ist vielmehr, wer Zugriff auf die Systeme hat, wer als Datenverarbeiter auftritt und ob technische wie organisatorische Schutzmaßnahmen tatsächlich greifen.

Spätestens seit dem Schrems-II-Urteil des EuGH (Juli 2020) ist klar: Selbst wenn Daten ausschließlich in Deutschland gespeichert werden, kann ein Zugriff durch US-Behörden nach dem CLOUD Act nicht ausgeschlossen werden, sofern der Anbieter einer US-Jurisdiktion unterliegt. Das betrifft so ziemlich jeden "europäischen" Cloud-Service, der zu einem US-Konzern gehört – unabhängig davon, wie viele deutsche Flaggen auf der Website prangen.

Der Datenstandort alleine schützt weder vor Datenabfluss noch vor Überwachung. Was zählt, ist die gesamte Lieferkette: Transparenz bei Subdienstleistern, technische Maßnahmen wie Ende-zu-Ende-Verschlüsselung, echte Mandantentrennung (Multi-Tenancy), Zugriffsprotokollierung und ein

klarer Vertrag nach Art. 28 DSGVO. Wer sich hier auf Lippenbekenntnisse verlässt, kann schnell vor dem Datenschutzbeauftragten oder der Aufsichtsbehörde alt aussehen.

Ein weiteres Problem: Viele Anbieter verschweigen, dass sie US-Software (z. B. VMware, Microsoft, Oracle) einsetzen oder kritische Betriebsprozesse (Monitoring, Patching, Backups) von ausländischen Dienstleistern durchführen lassen. Das öffnet – auch bei deutschem Hosting – Einfallstore für Datenzugriffe, die mit "Cloud Made in Germany" nichts zu tun haben.

Marketing, Mythen und die Realität: Was deutsche Cloud-Anbieter (nicht) erzählen

Wer sich durch die Websites deutscher Cloud-Anbieter klickt, stößt auf ein Feuerwerk aus Buzzwords: "100% DSGVO-konform", "Hosting in deutschen Rechenzentren", "zertifizierte Sicherheit", "keine US-Zugriffe möglich" – die Liste ist endlos. Die wenigsten Claims halten, was sie versprechen. Denn: Die Marketingabteilungen verkaufen oft eine Wunschwelt, die technisch und juristisch kaum abbildbar ist.

Besonders beliebt: Siegel wie "Cloud Made in Germany", "Hosted in Germany", "TÜV-zertifiziert" oder "Trusted Cloud". Die meisten davon sind Eigenkreationen von Anbieterverbänden oder Marketinginitiativen – keine staatlichen oder unabhängigen Zertifikate. Sie sagen wenig bis nichts über die tatsächliche Sicherheit, Souveränität oder Compliance eines Dienstes aus. Wer sich darauf verlässt, handelt blauäugig.

Ein weiteres beliebtes Märchen: "Wir speichern alles ausschließlich in Deutschland, also sind Sie sicher." Das greift zu kurz. Entscheidend ist nicht, wo die Daten physisch liegen, sondern wer sie technisch, organisatorisch und juristisch kontrolliert. US-Cloud-Anbieter können trotz deutschem Datenstandort verpflichtet werden, Daten an US-Behörden herauszugeben. Und auch "deutsche" Anbieter mit internationalen Subunternehmern sind davon nicht ausgenommen.

Viele Anbieter verschweigen zudem, dass sie zentrale Komponenten wie Storage, Netzwerk, Virtualisierung oder Security aus dem Ausland beziehen. Wer wirklich Wert auf Souveränität legt, muss die gesamte Supply Chain prüfen – und bekommt dabei oft unangenehme Antworten.

US-Clouds, DSGVO, Schrems II,

CLOUD Act: Die Karten werden neu gemischt

Seit dem Schrems-II-Urteil sind Datentransfers in die USA praktisch illegal – zumindest dann, wenn nicht zusätzliche Schutzmaßnahmen greifen. Der CLOUD Act macht es US-Behörden zudem möglich, auf Daten von US-Unternehmen weltweit zuzugreifen – unabhängig davon, wo die Server stehen. Das stellt die gesamte "Cloud Made in Germany"-Idee auf den Kopf, denn viele deutsche Cloud-Dienste basieren auf US-Infrastruktur, -Software oder -Eigentümerstruktur.

Die DSGVO verlangt, dass personenbezogene Daten nur dann in "Drittstaaten" (wie die USA) übermittelt werden dürfen, wenn ein angemessenes Schutzniveau gewährleistet ist. Ohne ein gültiges Angemessenheitsabkommen (wie das gescheiterte Privacy Shield) ist das praktisch unmöglich. Einzige Auswege: Standardvertragsklauseln, zusätzliche Schutzmaßnahmen (z. B. Verschlüsselung, Anonymisierung) und eine lückenlose Dokumentation. Doch auch diese Konstrukte bieten keinen 100%igen Schutz vor dem Zugriff ausländischer Behörden.

Für Unternehmen bedeutet das: Wer auf eine echte "Cloud Made in Germany" setzt, muss nicht nur auf den physischen Standort achten, sondern auf die gesamte Ownership- und Verarbeitungsstruktur. Wer blind auf US-Software, US-Support oder internationale Subdienstleister setzt, riskiert Abmahnungen, Bußgelder und den Verlust der Datenhoheit. Die Zeiten, in denen ein Serverstandort in Frankfurt als Allheilmittel galt, sind endgültig vorbei.

Wer jetzt immer noch glaubt, mit einer "deutschen Cloud" sei alles geregelt, sollte dringend das Kleingedruckte lesen. Denn viele Anbieter sind entweder Teil internationaler Konzerne, nutzen US-Technologie oder haben kritische Betriebsprozesse ausgelagert. Die Karten werden neu gemischt – und das Spielfeld ist härter als je zuvor.

Step-by-Step: Worauf Unternehmen bei der Auswahl einer "Cloud Made in Germany" achten müssen

Die Wahl eines Cloud-Anbieters ist heute weniger eine Frage des Marketings als knallharte Due Diligence. Wer nicht in die Falle laufen will, sollte systematisch vorgehen – und zwar so:

- Detaillierte Anbieteranalyse: Wer steht hinter dem Anbieter? Ist er unabhängig oder Teil eines internationalen Konzerns?
- Transparente Subdienstleister prüfen: Gibt es eine vollständige Liste aller Subdienstleister? Welche Rolle spielen sie im Betrieb?

- Technische Kontrolle: Wer betreibt die Infrastruktur? Wer liefert Software, Updates und Support? Gibt es Abhängigkeiten von US-Unternehmen?
- Vertragliche Absicherung: Sind AV-Verträge nach Art. 28 DSGVO vorhanden und sauber gestaltet? Wie sind Haftung und Verantwortlichkeiten geregelt?
- Compliance und Zertifikate: Liegen relevante Zertifikate (ISO 27001, BSI C5, ISAE 3402) vor? Werden sie regelmäßig erneuert?
- Datenisolation und Verschlüsselung: Gibt es echte Mandantentrennung? Werden Daten wirklich Ende-zu-Ende verschlüsselt?
- Zugriffsprotokollierung und Monitoring: Wie werden Zugriffe dokumentiert? Gibt es ein transparentes Incident-Management?
- Reaktionsfähigkeit bei Datenpannen: Wie läuft das Notfallmanagement ab? Gibt es klar definierte Prozesse?
- Regelmäßige Audits und Penetrationstests: Werden technische und organisatorische Maßnahmen regelmäßig überprüft?
- Juristische Beratung einholen: Wer juristisch auf der sicheren Seite sein will, braucht eine fundierte Rechtsberatung – Marketingversprechen reichen nicht.

Nur wer diese Punkte sauber abarbeitet, kann Risiken minimieren und eine informierte Entscheidung treffen. Alles andere ist digitales Wunschdenken.

Fazit: Realitätsschock für die deutsche Cloud – und was wirklich zählt

Das Label “Cloud Made in Germany” ist im Jahr 2024 mehr Marketing als Substanz. Wer wirklich Wert auf Souveränität, Datenschutz und Compliance legt, muss tiefer schauen – und hinter die Fassaden der Anbieter blicken. Der physische Standort ist nur ein Mosaikstein im komplexen Puzzle der Cloud-Sicherheit. Was zählt, ist die Kontrolle über Infrastruktur, Software, Personal und Prozesse. Und die ist bei vielen vermeintlich “deutschen Clouds” alles andere als garantiert.

Die digitale Souveränität bleibt eine Herausforderung – technisch, juristisch und organisatorisch. Wer glaubt, mit einem hübschen Siegel und ein paar Servern in Frankfurt sei alles in Butter, spielt mit dem Feuer. Die Zukunft gehört denen, die kritisch hinterfragen, technische Ownership verlangen und sich nicht mit Buzzword-Bingo abspeisen lassen. Die Wolke bleibt grau – höchste Zeit, genauer hinzusehen.