plusserver

Lösungsansätze für Datenhoheit in der Cloud

IT modernisieren und dabei die Daten im Griff behalten

Management Summary

Ist Cloud Computing eine Einbahnstraße? Um diese Frage näher beleuchten zu können, hat plusserver IDC mit einer Befragung von 150 IT-Entscheidern aus Deutschland beauftragt. Diese Befragung erfolgt im September 2022 und die Ergebnisse daraus wurden im von plusserver gesponserten IDC Whitepaper „Datenhoheit in der Cloud" im Januar 2023 veröffentlicht. Das Whitepaper „Datenhoheit in der Cloud – Voraussetzungen, Potenzial und Herausforderungen" zeigt, dass für ein Drittel der IT-Verantwortlichen die Datenhoheit das wichtigste Kriterium bei der Wahl eines Anbieters ist. Zugleich haben bisher nur elf Prozent aller Unternehmen eine Strategie für Datenhoheit umgesetzt, mehr als ein Viertel hat bisher noch nichts unternommen.

Diese Zusammenfassung zeigt, warum eine Strategie für Datenhoheit und die Wahl des passenden Cloud-Providers essenziell für eine nachhaltige, flexible und rechtskonforme Digitalisierungsstrategie ist.

Datenhoheit ist also der zentrale Faktor, um digitales Wachstum zu ermöglichen. Doch welche Kriterien sollten die IT-Verantwortlichen kennen, um Datenhoheit zu ermöglichen und von ihr zu profitieren?

Für wen ist Datenhoheit in der Cloud wichtig?

Für alle ...

+ ... die sich Transparenz und Kontrolle beim Umgang mit ihren Daten wünschen.

+ ... die besonderer Regulierung unterliegen (beispielsweise im Gesundheits- oder Finanzwesen).

+ ... die kritische Daten verarbeiten: Geschäftsgeheimnisse oder sensible Kundendaten sollten nicht im Zugriff von Drittstaaten liegen.

+ ... die sicherstellen möchten, dass ihre Daten den Rechtsraum nicht verlassen (beispielsweise in den Einflussbereich des CLOUD Acts).

+ ... die nicht alles auf einen Anbieter setzen möchten (für Redundanz oder zukünftige Flexibilität).

Top 5 Herausforderungen

bei der Cloud-Nutzung

IT-Sicherheit und Compliance

Nahtlose Portabilität der Daten und Workloads (On-Premises und Cloud)

Sicherstellen der Datenhoheit

Datenrückführung nach Vertragsende

Data Protection

N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt;
Quelle: IDC Whitepaper „Datenhoheit in der Cloud", gesponsert von plusserver, Januar 2023
F.: Welche Aspekte sind eine Herausforderung bei der Cloud-Nutzung?

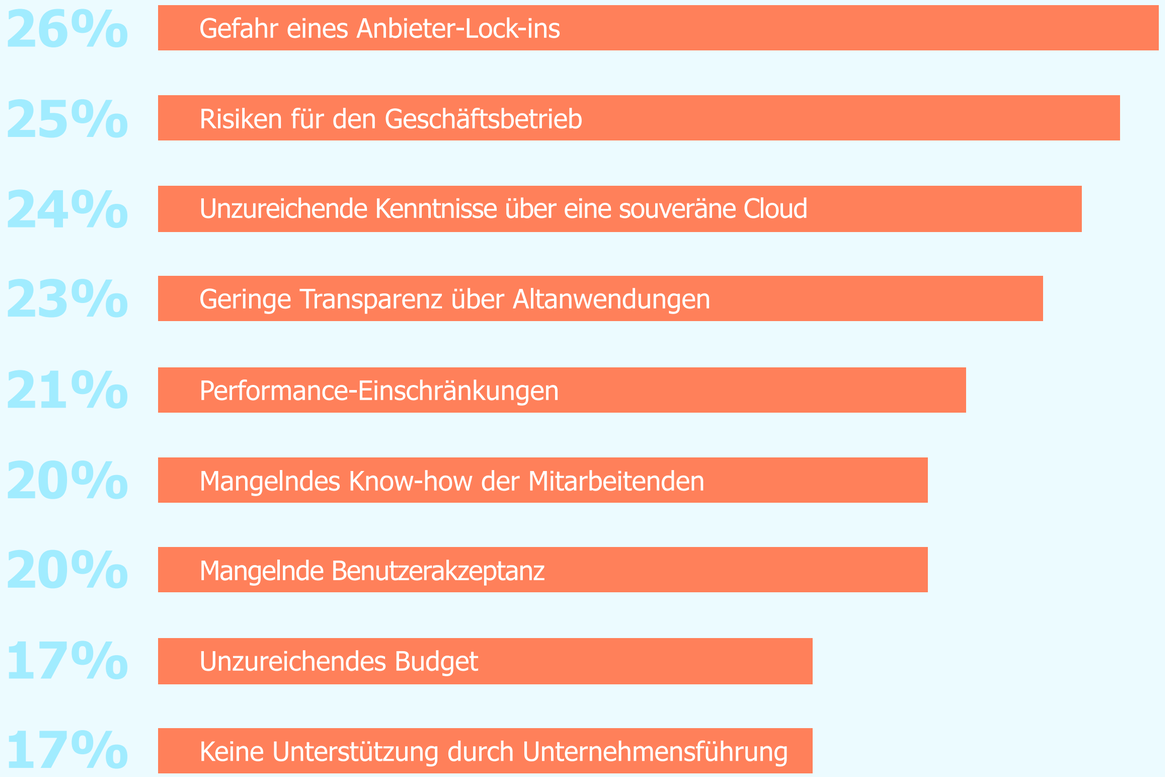
+ Ein Viertel der Befragten hat Bedenken bei der Portabilität der Daten und Workloads in die Cloud und aus der Cloud.

+ IT-Verantwortliche sorgen sich bei ihrer Cloud-Strategie besonders über den Weg aus der Cloud heraus oder zu einem anderen Anbieter.

+ Setzen sich Unternehmen nicht in einem frühen Digitalisierungsstatus mit den Themen Datenstrategie und Datenhoheit auseinander, riskieren sie einen **Vendor Lock-in**, **hohe Datentransferkosten** und einen **Digitalisierungsverzug.**

Herausforderungen

bei der Umsetzung von Datenhoheit



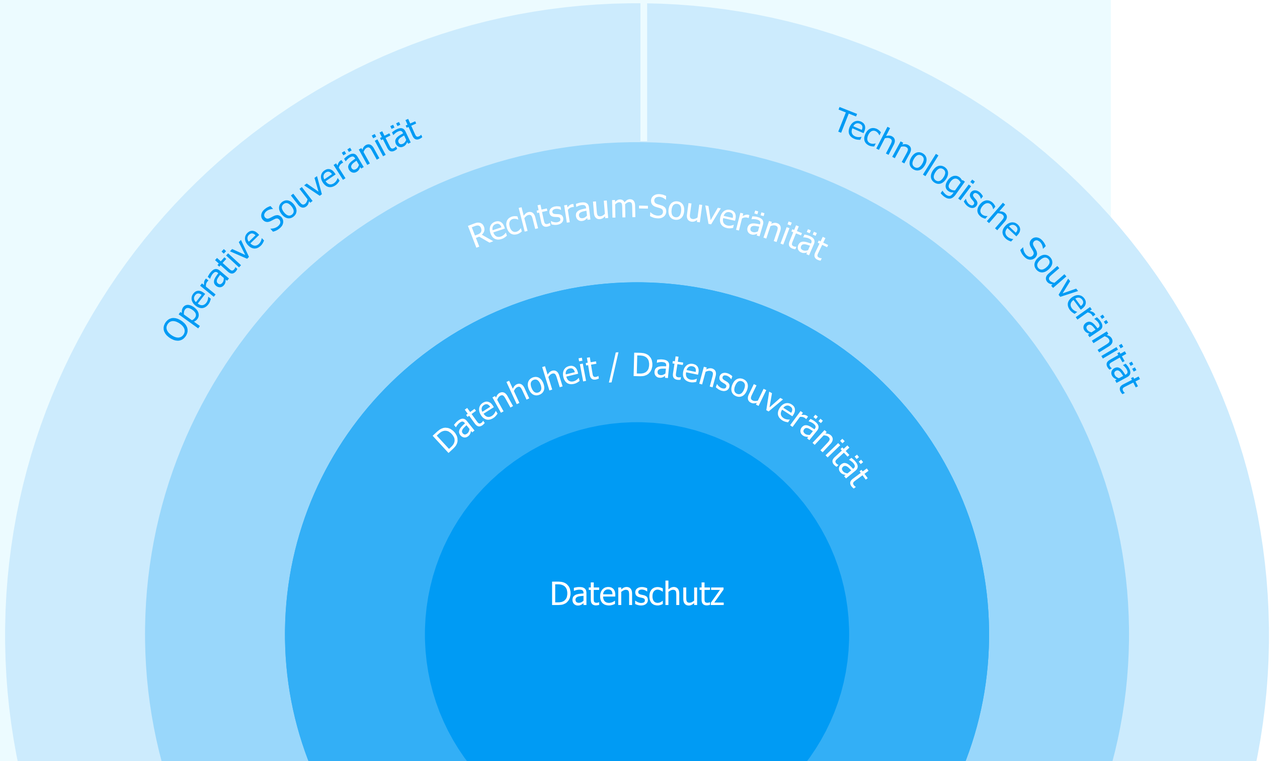
N = 150 Unternehmen, Mehrfachnennungen, Abbildung gekürzt;
Quelle: IDC Whitepaper „Datenhoheit in der Cloud", gesponsert von plusserver, Januar 2023
F.: Welche Herausforderungen sehen Sie bei der Umsetzung von Datenhoheit in einer Cloud?

Unternehmen sollten sich mit den Herausforderungen der Datenhoheit auseinandersetzen, Wissenslücken schließen und eine detaillierte Planung zur Erreichung von Datenhoheit aufbauen. Cloud-Provider können auf diese Ausrichtung hin geprüft und ausgewählt werden.

Datenhoheit ist gewünscht, der Weg dahin erscheint den Verantwortlichen nicht leicht umsetzbar zu sein.

Was ist digitale Souveränität?

Die einzelnen Facetten digitaler Souveränität ergeben in folgender Kombination ein logisches Gesamtbild:



+ Technologische Souveränität: basiert auf Open Source bzw. allgemein verfügbarer standardisierter Technologie und ermöglicht Transparenz und Nachvollziehbarkeit der Datenverarbeitung und der eingesetzten Softwarekomponenten.

+ Operative Souveränität: transparente Kontrolle der Abläufe, von der Bereitstellung und dem Management der Lösungen und Services bis hin zur Überwachung des physischen und digitalen Zugriffs auf die Infrastruktur.

+ Rechtsraum-Souveränität: beschreibt den Betrieb in einem selbstgewählten Rechtsraum ohne Durchgriffsrecht aus dritten Rechtsräumen.

+ Datensouveränität/Datenhoheit: sichert die vollständige Verfügungsgewalt bzw. selbstbestimmte Kontrolle bei der Erhebung, Speicherung, Nutzung und Verarbeitung eigener Daten.

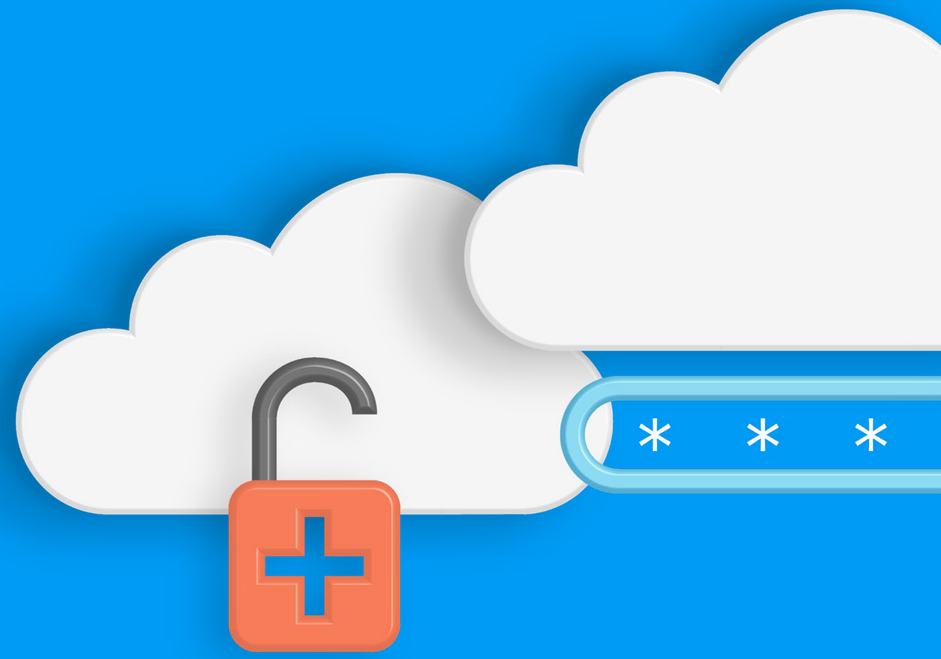
+ Datenschutz: beschreibt den Schutz vor der missbräuchlichen Verarbeitung personenbezogener Daten sowie das Recht auf informationelle Selbstbestimmung.

Datenschutz ist keine Datenhoheit

Was hat Datenhoheit mit Datensicherheit und Datenschutz zu tun?

Was gilt es für Unternehmen zu beachten?

Für Unternehmen, die ihr Tagesgeschäft in die Cloud migrieren, ist eine Strategie für Datenhoheit ein Muss. Damit Datenschutz, Datensicherheit und Datenhoheit in der Praxis richtig umgesetzt werden, müssen die IT und Fachbereiche eng zusammenarbeiten. Sie sollten gemeinsame Anforderungen definieren und die nötigen Voraussetzungen schaffen. Denn alle diese Ziele hängen unmittelbar miteinander zusammen und können nur gemeinsam existieren. Es ist eine anspruchsvolle Aufgabe, Datenschutz, Datensicherheit und Datenhoheit nachhaltig und effektiv zu implementieren, deshalb sollte dies strategisch und in gezielten Schritten umgesetzt werden.



Unternehmen kennen die Relevanz von Datenhoheit

3/4 der IT-Verantwortlichen halten Datenhoheit in der Cloud für sehr wichtig oder wichtig. Sie wissen einerseits, dass Datensicherheit und DSGVO-Konformität essenziell sind. Andererseits gibt es bereits ein Bewusstsein, dass auch Portabilität, Unabhängigkeit und Rechtssicherheit in der Cloud elementar sind. In großen Unternehmen mit über 1000 Mitarbeitenden ist das Bewusstsein besonders groß. Dort halten 39 Prozent Datenhoheit für „sehr wichtig", in kleineren Unternehmen sind es nur 19 Prozent.

Größere Unternehmen haben ein stärkeres Bewusstsein für Datenhoheit.

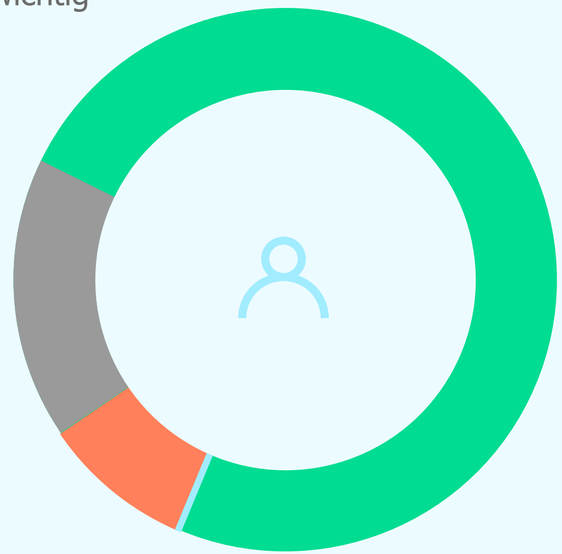
Verantwortliche sehen Datenhoheit als wichtig für die Cloud

75%
Wichtig und sehr wichtig

15%
Unentschlossen

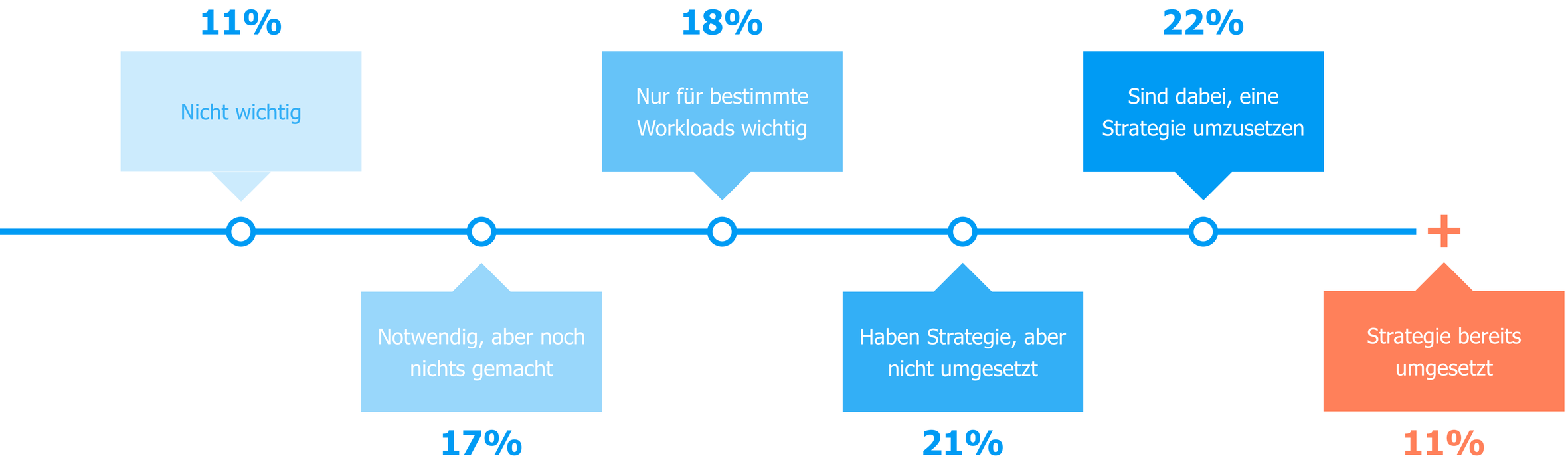
9%
Eher unwichtig

1%
Weiß nicht/keine Angabe



Umsetzung einer Strategie für Datenhoheit

Nur 11% haben derzeit bereits eine Strategie für souveräne Daten umgesetzt:



N = 150 Unternehmen; Quelle: IDC Whitepaper „Datenhoheit in der Cloud", gesponsert von plusserver, Januar 2023
F.: Welche der folgenden Aussagen beschreibt die Position Ihres Unternehmens in Bezug auf Datenhoheit am besten?

Die Wahl des Anbieters ist entscheidend

Offene Standards ermöglichen es Kunden, leicht auf eine Plattform zu migrieren und leicht wieder zu wechseln.

Alexander Wallner
CEO plusserver

Die Technologie, Datenformate und Vertragsbedingungen eines Cloud-Anbieters sind wichtige Faktoren, ob echte Datenhoheit umsetzbar ist:

+ Mit 33 Prozent ist „garantierte Datenhoheit" das wichtigste Kriterium bei der Wahl eines Cloud-Anbieters.

+ Mehr als jedes vierte Unternehmen fürchtet, wegen fehlender Datenhoheit bei einem Cloud-Anbieter festzustecken.

+ 26 Prozent sehen die Gefahr eines Vendor Lock-ins als kritischen Aspekt der Datenhoheit.

Der Standort ist entscheidend

Der Firmensitz (auch von Softwareanbietern) und Serverstandorte der PaaS- und IaaS-Anbieter sowie Service-Provider bestimmen über den Rechtsraum und damit auch über die effektive Datenhoheit.

plusserver

Matrix zur Bestimmung der digitalen Souveränität

Kriterium	Was bedeutet dies?	Public Cloud	pluscloud VMware	pluscloud open
ISO 9001	Zertifiziertes Qualitätsmanagementsystem (QMS)	+	+	+
ISO 27001	Zertifiziertes Informationssicherheitsmanagementsystem (ISMS)	+	+	+
BSI C5 Cloud Security	Testierte Informationssicherheit für Cloud-Produkte	+	+	+
IDW PH 9.860.1	Testiertes Datenschutzmanagementsystem (DSMS) nach EU-DSGVO	(+)	+	+
Rechtsraumsicherheit Rechenzentrums-Standort	Alle Rechenzentren befinden sind im selben Rechtsraum wie der Kunde (Deutschland/EU)		+	+
Rechtsraumsicherheit Betreiber	Der Firmensitz des Cloud-Providers befindet sich in Deutschland und unterliegt nicht der Gesetzgebung Dritter (CLOUD Act).		+	+
Rechtsraumsicherheit Netzwerk	Alle Netzwerkverbindungen und Routings zwischen Standorten laufen innerhalb des selben Rechtsraumes.		+	+
Rechtsraumsicherheit Support Level 1	Der Kundensupport befindet sich nicht in Drittstaaten, wodurch in Einzelfällen Kundendaten bei Anfragen den Rechtsraum verlassen könnten.		+	+
Rechtsraumsicherheit Support Level 2+	Der L2-Support befindet sich ebenfalls im selben Rechtsraum. Andernfalls könnten Mitarbeitende aus Drittstaaten Zugriff auf Kundendaten haben.		+	+
Rechtsraumsicherheit Software	Sämtliche verwendeten Softwarelayer, die Firmenstandorte der Anbieter und Nutzungsbedingungen unterliegen nicht den Rechtsräumen und der Gesetzgebung von Drittstaaten.			+
Cloud Appliance "On-Premise" für höchstsichere Kundenanforderungen	Bei Bedarf kann Cloud-Architektur auch lokal beim Kunden eingerichtet werden, um Cloud-Technologie zu nutzen, ohne, dass Daten den Standort und das eigene Netzwerk verlassen.		+	+

Wie werde ich souverän?

Die Checkliste für Ihre Strategie zur Datenhoheit

+ Habe ich meine Workloads und Daten anhand gesetzlicher oder interner Vorgaben klassifiziert und meine Cloud-Supplier entsprechend gewählt?

+ Habe ich beim Cloud-Provider nachweislich die Kontrolle und Transparenz, wie und wo meine Daten gespeichert werden?

+ Habe ich neben Zertifizierungen auch Standorte und Rechtsräume meiner Anbieter geprüft?

+ Zugriff und Portabilität – komme ich an meine Daten heran und kann ich sie zu einem anderen Anbieter migrieren?

Kommentar

„Das vorliegende IDC Whitepaper zeigt sehr detailliert, dass Sorge vor Kontrollverlust und Intransparenz im Cloud-Kontext zu den größten Bedenken und Herausforderungen von IT-Verantwortlichen zählen: In welchen proprietären Formaten werden Daten bei meinem Cloud-Anbieter gespeichert? Welche Technologien und welche Standorte kommen beim Anbieter zum Einsatz und welche rechtlichen Folgen hat dies für Unternehmensdaten? Wie kann ich Datenverarbeitungsaufträge meiner Kunden und meine Compliance-Vorgaben einhalten, wenn ich keine Transparenz über die Infrastruktur eines Anbieters habe?

In diesem Umfeld sind wir sehr stolz, mit pluscloud VMware und pluscloud open gleich zwei unterschiedliche Cloud-Modelle anzubieten, die in unseren eigenen testierten und zertifizierten deutschen Rechenzentren betrieben werden. Unsere Kunden vertrauen darauf, dass modernes Cloud Computing und Rechtssicherheit für ihre Daten Hand in Hand gehen. Nur sie entscheiden darüber, welche Daten wie lange in unseren Rechenzentren verbleiben. Es gibt keinerlei technologische oder monetäre Barrieren. Wir leben Datenhoheit.”

Alexander Wallner
CEO plusserver

Lesen Sie das gesamte IDC Whitepaper:

„Datenhoheit in der Cloud – Voraussetzungen, Potenzial und Herausforderungen” IDC, Januar 2023

+ Zum IDC Whitepaper

plusserver

Eine souveräne, zukunftsfähige und sichere Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

+ Mehr über plusserver

Mehr über die datensouveräne Cloud von plusserver:

+ pluscloud open

+ pluscloud VMware

Digitalisierung und Datenhoheit mit der pluscloud

pluscloud open ist die digital souveräne, BSI-C5-testierte Cloud auf Basis von OpenStack, made in Germany. Kontrollieren Sie die hoch verfügbare und skalierbare Cloud-Infrastruktur direkt per IaC oder GUI. Mit der pluscloud open behalten Sie jederzeit die Hoheit über Ihre Daten dank unserer DSGVO-konformen Datacenter in Deutschland. Unser einfaches Preismodell sorgt dabei für Kostentransparenz.

Mit der **pluscloud VMware** modernisieren Sie Ihre IT-Infrastruktur Schritt für Schritt und bleiben dabei gleichzeitig in Ihrer gewohnten VMware-Umgebung. Die verbrauchsbasierte Abrechnung ohne Mindestabnahmemengen und ohne Traffic-Berechnung sorgt für Planungssicherheit. Sie behalten die Hoheit über Ihre Daten dank unserer eigenen Datacenter in Deutschland sowie unser-er BSI-C5-Testierung. Mit plusserver nutzen Sie immer die für Sie passende Cloud, denn wir sind der einzige Anbieter mit einem IaaS-Angebot auf VMware-Basis, das Sie sowohl private, public als auch local aus Ihrem eigenen Rechenzentrum beziehen können.