

SOUVERÄNITÄT UND RESILIENZ IN DER CLOUD:

Herausforderungen, Lösungen & Best Practices

Cloud-Strategien neu denken: Souveränität & Resilienz im Fokus

Einer aktuellen [Bitkom-Studie](#) zur digitalen Souveränität zufolge fühlen sich deutsche Unternehmen extrem stark von Diensten und Technologien aus dem Ausland abhängig (96 %). Gleichzeitig ist ihr Vertrauen in die USA „erheblich geschwächt“ (37 %). Zusätzlich zwingen regulatorische Vorgaben wie NIS 2 oder die DSGVO sie dazu, ihre Daten besser zu kontrollieren und ihre Cloud-Strategie zu hinterfragen. Es besteht also Handlungsbedarf. Dieses Whitepaper hilft Ihnen, in einer polarisierten und emotional geführten Debatte den Überblick zu behalten und Ihr Unternehmen sicher und zukunftsorientiert durch die Klippen der Extrempositionen zu steuern.

Die Cloud ist heute unverzichtbar für Unternehmen, die innovativ und flexibel bleiben wollen. Doch mit der steigenden Abhängigkeit von großen internationalen Anbietern wachsen die Bedenken: Wer kontrolliert eigentlich die Daten? Wie sicher sind sie vor fremdem Zugriff? Und was passiert bei geopolitischen Spannungen? Diese Fragen beschäftigen IT-Entscheider zunehmend. Digitale Souveränität ist inzwischen kein theoretisches Konzept mehr, sondern harte Notwendigkeit. Dabei geht es längst nicht nur um Datenschutz, sondern um die grundsätzliche Fähigkeit, selbstbestimmt zu agieren und die Kontrolle über die eigene digitale Infrastruktur zu behalten.





Dimensionen digitaler Souveränität

Wer über digitale Souveränität spricht, muss drei zentrale Aspekte berücksichtigen.

Technologische Souveränität: Hier steht Ihre Unabhängigkeit bei der Technologiewahl im Vordergrund. Auf Software-Ebene bedeutet dies die Freiheit, über Anwendungen, Betriebssysteme und Entwicklungsumgebungen selbstbestimmt zu entscheiden, diese nach Bedarf weiterzuentwickeln oder zu migrieren. Bei der Hardware umfasst die Souveränität die unabhängige Auswahl von Prozessoren, Speicherlösungen und Netzwerkkomponenten ohne herstellerseitige Einschränkungen. Auf Infrastrukturebene sichert sie die Kontrolle über Rechenzentren, Netzwerke und Übertragungswege.

Operative Souveränität: Dieser Aspekt zielt darauf ab, dass Ihr Unternehmen kritische Betriebsabläufe jederzeit eigenständig durchführen kann – unabhängig von externen Dienstleistern oder Cloud-Anbietern. Im Kern geht es darum, die notwendigen Kapazitäten und Fähigkeiten aufzubauen, die jederzeit selbstbestimmtes Handeln ermöglichen.

Datensoeveränität: Hier steht die Kontrolle über Ihre Daten in der Cloud im Mittelpunkt. Sie bestimmen, wo die Daten liegen, wer auf sie zugreifen darf und was mit ihnen geschieht. Vom Speicherort bis zur Löschung – Sie behalten die volle Kontrolle.



Im Fokus:

Europäische Regularien zur Datensouveränität

Die EU-Datenschutz-Grundverordnung (DSGVO) gilt für alle Firmen, die in der EU personenbezogene Daten verarbeiten, sowie für Unternehmen außerhalb der EU, sofern sie Daten von Personen in der EU verarbeiten oder Dienstleistungen für diese anbieten.

Daten dürfen grundsätzlich nur auf Basis einer rechtlichen Grundlage verarbeitet werden – etwa durch Einwilligung, zur Vertragserfüllung, aufgrund rechtlicher Verpflichtungen oder zum Schutz lebenswichtiger Interessen. Für die Übermittlung ins Ausland muss die Datenverarbeitung – unabhängig vom Ort – auch den DSGVO-Anforderungen entsprechen.

Eine Datenverarbeitung außerhalb der EU ist dann erlaubt, wenn ein angemessenes Datenschutzniveau nach EU-Standards im Empfängerland gewährleistet ist. Das entscheidet die EU-Kommission per sogenanntem Angemessenheitsbeschluss. Für unsichere Drittländer gibt es zusätzliche Anforderungen wie Standardvertragsklauseln oder Binding Corporate Rules.

Bei einem Angemessenheitsbeschluss handelt es sich um eine formelle Feststellung der EU-Kommission, dass in einem Drittland oder innerhalb eines spezifischen Sektors ein „der Sache nach gleichwertiges“ Datenschutzniveau wie in der EU besteht. Die Grundlage dafür bildet **Artikel 45 DSGVO**, der Anforderungen an Verfahren und Schutzmaßnahmen im Vergleich zur EU festlegt. Der Beschluss fällt nach einer umfassenden Bewertung, zu der auch Stellungnahmen des Europäischen Datenschutzausschusses gehören.

Zu den zentralen Elementen für die Bewertung des US-Datenschutzniveaus im Rahmen von EU-Angemessenheitsbeschlüssen zählen die

US-amerikanische **Presidential Policy Directive 28** (PPD-28) sowie die **Executive Order 14086**, die die Überwachung durch US-Dienste auf „notwendige und verhältnismäßige“ Zwecke begrenzen sollen. Darüber hinaus schaffen sie einen zweistufigen Rechtsbehelf (Redress Mechanism), der einen speziellen, unabhängigen Data Protection Review Court für EU-Bürger einschließt.

Sollten US-Behörden durch den **Foreign Intelligence Surveillance Act** (FISA) oder den **CLOUD Act** Zugriff auf personenbezogene Daten aus Europa erhalten, stellt dies eine unzulässige Datenübermittlung in ein Drittland dar. Unternehmen laufen Gefahr, bei einer Prüfung durch Datenschutzbehörden (etwa DSB oder BfDI) nicht nachweisen zu können, dass ihre Datensouveränität gewahrt bleibt.

Auch das aktuelle **EU-US Data Privacy Framework** (DPF) bietet nur bedingt Sicherheit – der EuGH hat seine Vorgänger (**Safe Harbor** und **Privacy Shield**) bereits für ungültig erklärt (Schrems-Urteile).

Diese Rechtslage bringt für Unternehmen verschiedene Herausforderungen mit sich. Verstöße gegen die DSGVO können hohe Bußgelder und Reputationsschäden verursachen. Aber auch abseits der DSGVO entstehen mitunter operative Risiken im Hinblick auf die Legitimität und Sicherheit grenzüberschreitender Datenflüsse.

IT- und Unternehmensverantwortliche sollten die weiteren Entwicklungen aufmerksam verfolgen, individuelle Risikoabwägungen treffen und die Resilienz ihrer Organisation proaktiv durch transparente, innovative und flexible IT-Konzepte stärken.

US Public Clouds: Werkzeuge und Grenzen im Kontext der digitalen Souveränität

Die großen Hyperscaler reagieren auf den Souveränitätsdruck mit neuen Angeboten: Sie gründen EU-Gesellschaften oder kooperieren mit europäischen Partnern, um Cloud-Dienste unter europäischer Gerichtsbarkeit anzubieten. Diese Maßnahmen sollen Kunden vor Datenzugriffen durch US-Gesetze wie FISA oder den CLOUD Act schützen.

Aktuelle Beispiele:

- AWS lässt über Tochtergesellschaften eine eigenständige europäische Sovereign Cloud betreiben.
- Microsoft strebt hingegen die Partnerschaft mit rechtlich unabhängigen Unternehmen an, die Clouds mit seiner Technik anbieten. Ein Beispiel dafür ist die SAP-Tochter Delos, für die die deutsche Firma Arvato den Betrieb der Cloud übernimmt.
- Google setzt auf Partnerschaften mit S3NS (Thales) und eine von T-Systems gehostete Air-Gapped-Cloud.

Einschränkungen: Die Angebote sind auf den öffentlichen Sektor zugeschnitten und nur zum Teil zugänglich für die Privatwirtschaft. Darüber hinaus sind die Konstrukte teilweise primär juristischer Natur – die Hyperscaler haben technisch potenziell weiterhin Zugriffsmöglichkeiten auf die Daten. Uneingeschränkte technische Souveränität bieten hier in bestimmten Settings Verfahren wie Confidential Computing, die durch kryptografische Methoden den Fremdzugriff auf Firmendaten technisch unterbinden.

Zusätzlich zu den Bestrebungen, US-Technik so anzubieten, dass Unternehmen sie EU-konform nutzen können, stellen die Hyperscaler bereits jetzt zahlreiche Dienste und Werkzeuge bereit. Diese unterstützen Unternehmen dabei, die Kontrolle über ihre Daten und Systeme zu behalten und regulatorische Anforderungen zu erfüllen:

Data Residency Controls: Damit legen Sie fest, wo Ihre Daten gespeichert und verarbeitet werden sollen.

Zugriffskontrollen: Mit detailliertem Identitäts- und Zugriffsmanagement, Multi-Faktor-Authentifizierung und geografischen Zugangsbeschränkungen bestimmen Sie präzise, wer welche Daten sehen und nutzen darf.

Verschlüsselung: Eine starke Verschlüsselung schützt Ihre Daten bei der Übertragung und Speicherung. Durch die Nutzung eigener Kryptoschlüssel (BYOK-Modell) behalten Sie dabei die Kontrolle.

Monitoring: Dienste wie AWS CloudTrail oder VPC Flow Logs dokumentieren alle Zugriffe und Aktivitäten, wodurch sie sich ideal für Audits und Sicherheitsanalysen eignen.

Zertifizierungen: AWS, Microsoft und Google lassen sich nach internationalen Standards wie ISO 27001/17/18 zertifizieren und unterziehen sich regelmäßigen SOC-Audits.

Neben den US-Anbietern mit EU-Ablegern positionieren sich auch originär europäische Cloud-Provider als Alternative. Ihr Portfolio kann bislang aber noch nicht mit dem der großen Anbieter aus Übersee mithalten. Sie bieten zwar in der Regel die Basisfunktionalitäten wie Computing, Storage, Datenbanken, Managed Kubernetes und virtuelle Netzwerke, es fehlt aber die breite Palette an aufeinander abgestimmten Angeboten. Die US-Hyperscaler glänzen hier mit einem reichhaltigen Ökosystem, das auch die Bereiche KI, Machine Learning, Big Data, IoT oder High-Performance-Computing abdeckt.



Handlungsoptionen im Spannungsfeld digitaler Souveränität

Die Datensouveränität ist durch die gesetzlichen Vorgaben und die mediale Aufmerksamkeit der vergangenen Monate scheinbar der Aspekt mit dem größten Stellenwert. Es empfiehlt sich jedoch, den Blick zu weiten und alle Dimensionen der digitalen Souveränität zu betrachten. Nur so erreicht Ihr Unternehmen die Fähigkeit, unabhängig zu denken, zu entscheiden und zu handeln. Souveränität – oder vielmehr der differenzierte Umgang mit all ihren Facetten – ist kein statischer Zustand, sondern ein Prozess, der zwischen Abhängigkeit und völliger Autarkie verläuft.

Wer bei der Suche nach einem pragmatischen Mittelweg Resilienz als Ziel anstrebt, findet leichter den richtigen Kurs. Es geht also nicht um absolute Unabhängigkeit, sondern um die Fähigkeit, bei Störungen oder Veränderungen handlungsfähig zu bleiben und Alternativen zu haben. So können Sie sich gegen Disruptionen wie Embargos oder Zölle wappnen und eine souveräne Haltung entwickeln. Das hilft dabei, die individuelle Balance zwischen Leistungsfähigkeit und Wettbewerbsfähigkeit auf der einen Seite sowie Kontrolle auf der anderen Seite zu finden.

Mehrere Herausforderungen erschweren diese Abwägung. Organisationen müssen sich zunächst einen Überblick über ihre Abhängigkeiten verschaffen, die oft vielschichtig und unerwartet sind. Um tatsächlich souveräne Entscheidungen treffen zu können, brauchen sie zudem echte Alternativen – und das nicht nur in Form eines Vergleichs zwischen verschiedenen großen Cloud-Anbietern, sondern durch die Berücksichtigung einer breiteren Palette an technologischen, organisatorischen und rechtlichen Optionen.

Ein wesentlicher Faktor bei der Entscheidungsfindung sind die Kosten. Denn die Maßnahmen für mehr Souveränität verursachen zunächst höhere Ausgaben, ohne unmittelbar mehr Umsatz zu generieren. Sie müssen deshalb abwägen, wie wahrscheinlich bestimmte Risikoszenarien eintreten, die diese Investitionen rechtfertigen könnten. Diese Betrachtung sollte für jede einzelne Technologieentscheidung separat erfolgen.

Im Folgenden stellen wir Ihnen Optionen und Best-Practice-Lösungen vor, die Unternehmen dabei helfen, im Cloud-Kontext selbstbestimmt und wirtschaftlich erfolgreich zu agieren.



Empfehlung 1: Nutzen Sie strategisch mehrere Anbieter

Ein Multi-Vendor-Ansatz stärkt Ihre digitale Souveränität am wirksamsten. Sie können sensible Daten gezielt in einer privaten oder europäischen Cloud verarbeiten und unkritischere Workloads flexibel verteilen. Doch Vorsicht vor der Best-of-Breed-Falle: Der Einsatz der jeweils besten Spezialdienste mag verlockend erscheinen, schafft jedoch ein kaum zu beherrschendes Komplexitätsmonster. Die wenigsten Firmen können es sich leisten, das Know-how für mehrere Cloud-Ökosysteme aufzubauen und aktuell zu halten. Der Einsatz der jeweils besten Spezialdienste kann zwar kurzfristige Vorteile bringen, wird sich langfristig aber in den meisten Fällen rächen.

Praxistauglicher ist der Balanced-Multi-Vendor-Ansatz, bei dem Sie Workloads strategisch auf mehrere Anbieter verteilen, dabei aber vergleichbare Standarddienste für Container, Speicher oder Datenbanken nutzen. So entstehen echte Ausweichmöglichkeiten bei Störungen oder Preis-

erhöhungen. Cloud-agnostische Managementlösungen ermöglichen eine konsistente Steuerung unterschiedlicher Umgebungen, wenn Sie mehrere Clouds nutzen. Gleichzeitig gewährleisten sie eine einheitliche Verwaltung – ohne Anbindung an einen einzelnen Anbieter.

Natürlich hat dieser Multi-Vendor-Ansatz seinen Preis: Sie verzichten auf einige Spezialfunktionen und nehmen durch parallele Strukturen höhere Kosten in Kauf. Die gewonnene Unabhängigkeit und Verhandlungsmacht rechtfertigen diese Investition jedoch in den meisten Fällen. Selbst mit nur einem Hyperscaler können Sie übrigens mehr Souveränität erlangen: Setzen Sie auf ein Vendor-Agnostic-Design mit portablen Anwendungen, etwa durch Open-Source-Datenbanken oder Kubernetes-Container. So halten Sie sich Ihre Optionen offen, wenn Sie den Anbieter wechseln müssen. Es erleichtert auch den Umstieg auf die Multi-Cloud deutlich.

Exkurs: Confidential Computing

In der Cloud sind Daten bei der Übertragung und Speicherung generell verschlüsselt und damit gut gegen unberechtigten Zugriff geschützt. Unternehmen haben hier also volle Kontrolle darüber, wer auf schützenswerte Daten Zugriff erhält und wer nicht. Anders sieht das jedoch während der Verarbeitung aus: Hier liegen die Informationen im Arbeitsspeicher im Klartext vor und sind somit angreifbar für Insider, bösartige Software oder kompromittierte Infrastruktur.

Um die Lücke zu schließen, wurde Confidential Computing eingeführt. Diese Technik sorgt für den Schutz der Daten „in use“, und zwar durch die Verschlüsselung und Isolation von Prozessen. Confiden-

tial Computing nutzt Hardware-Funktionen moderner Prozessoren, um abgegrenzte, kryptografisch gesicherte Bereiche für jede Anwendung mit ihren Daten zu schaffen. Diese isolierten Bereiche heißen „Trusted Execution Environments“ (TEE) oder „Enklaven“.

Die großen Hyperscaler bieten die Technik zwar auch an, allerdings als proprietäre Lösungen, die die Abhängigkeit vom jeweiligen Anbieter vergrößern und einen Wechsel erschweren. Gegen dieses Problem hilft es, die Lösung eines unabhängigen Multi-Cloud-Confidential-Computing-Brokers einzusetzen.



Empfehlung 2: Exit-Strategien vorsehen

Sie müssen präzise festlegen, unter welchen Umständen Sie einen Cloud-Anbieter verlassen wollen. Dies umfasst nicht nur offensichtliche Trigger wie Preiserhöhungen oder Sicherheitsvorfälle, sondern auch schleichende Entwicklungen wie nachlassende Servicequalität oder strategische Neuausrichtungen des Anbieters. Eine detaillierte Dokumentation dieser Ausstiegsszenarien schafft Handlungssicherheit im Ernstfall.

Die Steuerung verschiedener Cloud-Provider gelingt nur mit klaren Governance-Strukturen. Standardisierte Prozesse für das Vertragsmanagement, die Leistungsüberwachung und das Eskalationsmanagement bilden das Fundament für einen kontrollierten Ausstieg. Diese Strukturen müssen regelmäßig überprüft und angepasst werden, damit sie ihre Wirksamkeit behalten.

Cloud-Anbieter locken häufig mit Rabatten für langfristige Verpflichtungen. Dies sollten Sie jedoch kritisch prüfen und auf die tatsächlichen Anforderungen abstimmen. Ein kontinuierliches Management der Verpflichtungen verhindert

überhöhte Kosten und erleichtert den späteren Wechsel. Besonders wichtig: Reservierungen und Mindestabnahmemengen müssen flexibel bleiben.

Die vertragliche Absicherung des Cloud-Ausstiegs entscheidet über den Erfolg oder Misserfolg der Migration. Essenzielle Vertragsbestandteile umfassen detaillierte Regelungen zur vollständigen Datenherausgabe, technische Unterstützungsleistungen während der Migration sowie klar definierte Übergangsfristen. Auch die Kündigungsmodalitäten müssen präzise festgelegt werden, um rechtliche Fallstricke zu vermeiden.

Doch theoretische Planung allein reicht nicht aus – Sie sollten auch regelmäßig Testmigrationen durchführen, um die Machbarkeit des Exit-Plans in der Praxis zu verifizieren. Diese Tests decken technische Hürden, Datentransferprobleme und Kompatibilitätsfragen auf, bevor sie sich im Ernstfall als kritische Probleme erweisen. Eine lückenlose Dokumentation dieser Testläufe bildet die Basis für kontinuierliche Verbesserungen der Exit-Strategie.





Empfehlung 3: **Kubernetes als Schlüsseltechnik zur Portabilität verwenden**

Kubernetes hat sich zu einem entscheidenden Faktor für die digitale Souveränität entwickelt. Diese Container-Orchestrierungstechnologie ermöglicht es, komplexe Anwendungen zuverlässig über verschiedene Infrastrukturen hinweg zu betreiben – von AWS über Azure bis zur eigenen Private Cloud. Der entscheidende Vorteil: Sie machen damit Ihre Workloads portabel. Wenn ein Cloud-Anbieter die Preise erhöht, problematische Geschäftsbedingungen einführt oder schlicht nicht mehr Ihren Anforderungen entspricht, ziehen Sie einfach um – ohne aufwendige Neuentwicklung.

Die Entkoppelung von Infrastruktur und Workload stellt einen fundamentalen Paradigmenwechsel dar. Kubernetes geht aber weit über eine reine Container-Orchestrierungslösung hinaus. Es funktioniert vielmehr als umfassendes Framework und Suite an Technologien, die den Aufbau

komplexer Plattformen ermöglicht. Während zu den Hauptvorteilen der Public Cloud das reiche Ökosystem an Lösungen und deren enge Integration zählt, lässt sich mit Kubernetes als Plattformlösung ein ähnliches Niveau anstreben – mit dem entscheidenden Unterschied der Portabilität.

Als Open-Source-Projekt profitiert Kubernetes von einer riesigen Community und ständiger Weiterentwicklung. Es fungiert als Meta-Plattform für zahllose Zusatzfunktionen – von KI-Integration über Entwicklungsumgebungen bis hin zu Sicherheitsfeatures. Besonders wertvoll: Mit Kubernetes umgehen Sie den Lock-in-Effekt serverloser Architekturen wie Function as a Service (FaaS). Statt proprietäre FaaS-Dienste zu nutzen, kapseln Sie Ihre Funktionen in Containern und können so bei Bedarf leicht die Plattform wechseln. Das stärkt die Unabhängigkeit und Entscheidungsfreiheit nachhaltig.



Empfehlung 4: **Inhouse Know-how aufbauen und durch Partner verstärken**

Der Weg zur digitalen Souveränität erfordert Kompetenzen, die viele Unternehmen erst aufbauen müssen. Oft haben sie diese Fähigkeiten über Jahre ausgelagert – jetzt müssen sie sie zurück ins Haus holen. Bei diesem Kraftakt helfen spezialisierte Dienstleister.

Langfristig sollten Sie den Aufbau interner Expertise anstreben, doch die Realität zeigt: Cloud-Spezialisten sind rar und teuer. Ohne externe Unterstützung scheitern viele Souveränitätsprojekte bereits in der Anfangsphase. Starten Sie mit gezielter Beratung, um eine realistische Strategie

zu entwickeln. Für den laufenden Betrieb eignet sich ein Co-Management-Modell: Interne und externe Teams verwalten die Cloud-Workloads gemeinsam – vergleichbar mit Pair-Programming in der Software-Entwicklung.

Der Clou bei dieser Zusammenarbeit: Beide Teams nutzen identische Tools und Prozesse, entwickeln eine gemeinsame Sprache und letztlich ein einheitliches Mindset. So fließt das externe Know-how kontinuierlich in Ihr Unternehmen, während Sie gleichzeitig von der Erfahrung und Schlagkraft des Dienstleisters profitieren.



Fazit

Digitale Souveränität in der Cloud ist kein absoluter Zustand, den Unternehmen einmalig erreichen können. Vielmehr handelt es sich um einen kontinuierlichen Prozess, der ständige Abwägungen erfordert. Weder ein vollständiger Rückzug aus den Hyperscaler-Welten noch eine einseitige Abhängigkeit von ihnen sind realistische Optionen. Der Königsweg liegt in einer ausgewogenen Strategie, die Kontrolle, Resilienz und Flexibilität gleichermaßen berücksichtigt. Dazu gehört es, die Vorteile der Hyperscaler bewusst zu nutzen, gleichzeitig aber durch Maßnahmen wie Multi-Vendor-Modelle, cloud-agnostische Architekturen und klare Exit-Strategien die eigene Unabhängigkeit zu wahren.

Diese Maßnahmen kosten Geld und Ressourcen, doch die Investition zahlt sich mehrfach aus: Sie erhöhen Ihre Sicherheit und Compliance, verringern Abhängigkeiten und bleiben gleichzeitig innovativ und widerstandsfähig gegenüber künftigen Markt- und Regulierungsänderungen. Am Ende geht es nicht um technologische Autarkie um jeden Preis, sondern um ein strategisches Gleichgewicht zwischen Leistungsfähigkeit, Kontrolle und Zukunftssicherheit. Wer diesen Balanceakt meistert, erreicht Schritt für Schritt mehr digitale Souveränität in der Cloud.

Experten-Call: Jetzt durchstarten!

- **Persönlicher Austausch:**

Wir nehmen uns Zeit für Ihre aktuelle Ist-Situation, Ziele und Herausforderungen.

- **Fokus auf digitale Souveränität & Resilienz:**

Erfahren Sie, wie Ihr Unternehmen unabhängig, widerstandsfähig und wettbewerbsfähig bleibt.

- **Ihre Fragen im Mittelpunkt:**

Sie bestimmen die Agenda – wir liefern konkrete Antworten, Impulse und Praxistipps.

- **Mehrwert für Ihr Unternehmen:**

Erhalten Sie individuelle Empfehlungen, wie Sie Ihre Cloud-Infrastruktur und Betriebsprozesse nachhaltig optimieren oder neu aufstellen können.



Starten Sie jetzt – unverbindlich & kostenfrei

Sichern Sie sich Ihr 60-minütiges, cloud-neutrales Beratungsgespräch und erkunden Sie neue Wege zu mehr digitaler Souveränität und Resilienz!

[Hier mehr erfahren >](#)

Checkliste: Der Fahrplan zu digitaler Souveränität & Resilienz

Eine Checkliste für Unternehmen, die konsequent mehr digitale Souveränität für ihre Cloud-Workloads aufbauen wollen:



Bestandsaufnahme durchführen

- Alle bestehenden Cloud-Dienste, Datenflüsse und Abhängigkeiten inventarisieren.
- Klassifizierung der Daten (zum Beispiel personenbezogen, geschäftskritisch, sensibel).
- Einschätzung der aktuellen regulatorischen Anforderungen (DSGVO, NIS 2, branchenspezifische Vorgaben).

Strategie definieren

- Klare Souveränitätsziele (technologisch, operativ, datenbezogen) festlegen.
- Risikobewertung vornehmen: Welche Daten und Prozesse dürfen in die Public Cloud – und welche nicht?
- Governance-Modell für die Cloud-Nutzung entwickeln.

Architektur und Technologieauswahl

- Multi-Vendor- oder Balanced-Multi-Vendor-Strategie planen, um Abhängigkeiten zu minimieren.
- Cloud-agnostische Technologien wie Kubernetes oder Open-Source-Datenbanken einführen, um Portabilität sicherzustellen.
- Exit-Strategien für jeden kritischen Workload bedenken.
- Confidential Computing, Verschlüsselung und striktes IAM nutzen.

Sicherheit und Compliance sicherstellen

- Schutzmaßnahmen für Data Residency (Datenstandorte in der EU) überprüfen.
- Rollen- und Zugriffskontrollen (IAM, MFA, Geo-Restrictions) konsequent umsetzen.
- Monitoring und Auditing einführen (zum Beispiel CloudTrail, Security Logs).
- Regelmäßige Audits und Zertifizierungen der Anbieter berücksichtigen (ISO 27001/17/18, SOC).

Organisation und Kompetenzen

- Inhouse-Expertise aufbauen (Cloud-Architekten, Security Engineers, Compliance-Fachkräfte).
- Externe Dienstleister für Beratung und Co-Management einbinden, falls nötig.
- Parallelstrukturen für Wissensaufbau schaffen: enge Verzahnung von internen Teams und Partnern.

Prozesse etablieren

- Standardisierung und Dokumentation der Cloud-Prozesse.
- Klare Verantwortlichkeiten im Betrieb: Wer entscheidet? Wer kontrolliert?
- Notfall- und Wiederanlaufpläne erstellen (Resilienz erhöhen).

Über Claranet

Claranet ist ein globaler Managed Service Provider mit Kompetenzen in den Bereichen Cloud, Cyber Security, SAP, Workplace, Netzwerke, Data & AI sowie IT-Trainings. Wir begleiten Unternehmen bei der IT-Modernisierung mit flexiblen, skalierbaren Technologielösungen, lokalem Service und globaler Umsetzungsstärke. Dabei unterstützen wir unsere Kunden genau dort, wo sie stehen, in ihrer Region und in ihrem Tempo.

Claranet GmbH

Hanauer Landstraße 196
60314 Frankfurt am Main
Tel.: +49 69 40 80 18 0

de-info@claranet.com
www.claranet.com/de

