Digitale Souveränität

Wechselfähigkeit am Beispiel von Cloud Service Modellen

bridging IT Gruppe

Abkürzungsverzeichnis

API	Application Programming Interface
BCM	Business Continuity Management
CaaS	Container as a Service
CI/CD	Continuous Integration / Continuous Deployment
DevOps	Development Operations
DNS	Domain Name System
DORA	Digital Operational Resilience Act
DSGVO	Datenschutz-Grundverordnung
EAM	Enterprise Architecture Management
FaaS	Function as a Service
gRPC	gRPC Remote Procedure Calls
IAM	Identity and Access Management
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
KRITIS	Kritische Infrastrukturen
MQTT	Message Queuing Telemetry Transport
OAuth 2.0	Open Authorization 2.0
OpenAPI	OpenAPI-Spezifikation
ORM	Object-Relational Mapping
PaaS	Platform as a Service
REST	Representational State Transfer
S3	Amazon Simple Storage Service
SaaS	Software as a Service
SLA	Service Level Agreement

Inhaltsverzeichnis

Executive Summary

Cloud-Wechselfähigkeit ist ein zentraler Hebel, um digitale Souveränität zu sichern, regulatorische Anforderungen zu erfüllen und technologische wie rechtliche Risiken zu reduzieren. Sie stärkt die Handlungs- und Wettbewerbsfähigkeit von Unternehmen in einer zunehmend vernetzten und dynamischen Marktumgebung.

Drei Dimensionen bilden das Fundament:

ORGANISATORISCH

Klare Governance-Strukturen, definierte Verantwortlichkeiten und eine Kultur des kontinuierlichen Lernens schaffen die Basis für Wechselfähigkeit und Resilienz.

TECHNISCH

Offene Standards, Automatisierung („Everything-as-Code“) und wiederholbare Migrationspfade ermöglichen Portabilität, Interoperabilität und Transparenz über alle Systeme hinweg.

RECHTLICH

Verträge sollten eindeutige Exit-Klauseln und kurze Kündigungsfristen enthalten sowie aktive Migrationsunterstützung sicherstellen – insbesondere im Hinblick auf den EU Data Act (ab 12. September 2025).

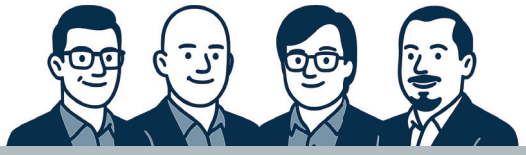
Empfohlene Maßnahmen:

- **Kritische Daten, Prozesse und Anwendungen nach Schutzbedarf priorisieren**
- **Interne und externe Fachkompetenzen gezielt aufbauen und weiterentwickeln**
- **Exit-Tests und Migrationsszenarien regelmäßig in CI/CD-Workflows prüfen**
- **Cloud-Verträge rechtzeitig an neue regulatorische Vorgaben anpassen**

Ausblick

Unternehmen, die Cloud-Wechselfähigkeit frühzeitig in ihre IT- und Unternehmensstrategie integrieren, sichern ihre Handlungsfähigkeit und Wettbewerbsfähigkeit nachhaltig. Ein regelmäßiges Reifegrad-Assessment unterstützt dabei, Abhängigkeiten zu reduzieren und Chancen in dynamischen Märkten besser zu nutzen.

Die Autoren



David Turan
david.turan@bridging-it.de

David Turan ist Senior Consultant mit juristischem Hintergrund (LL.M. IT-Recht) und bringt über zehn Jahre Erfahrung in den Bereichen Governance, Risk & Compliance, Datenschutz und Informationssicherheit mit. Mit seiner Expertise rund um DSGVO, DORA und ISO-Standards gestaltet er sichere Prozesse in Cloud- und Migrationsprojekten. So sorgt er dafür, dass Organisationen nicht nur regulatorisch auf der sicheren Seite sind, sondern auch langfristig handlungsfähig bleiben.

Martin Spörl
martin.spoerl@bridging-it.de

Martin Spörl ist Senior Cloud Solution Architekt und DevOps Coach mit umfassender Erfahrung im Aufbau hybrider Architekturen. Er verbindet klassische IT mit modernen Cloud-Lösungen und legt dabei besonderen Wert auf Portabilität und Automatisierung. Mit seinem Know-how unterstützt er DevOps-Teams dabei, resiliente Architekturen zu entwickeln und die technische Wechselfähigkeit in Projekten gezielt voranzutreiben.

Hauke Goppelt
hauke.goppelt@bridging-it.de

Hauke Goppelt ist Management Consultant mit Fokus auf IT-Infrastruktur, IT-Management und die Weiterentwicklung von IT-Organisationen. Besonders gerne begleitet er Projekte, bei denen komplexe IT-Landschaften strategisch neu ausgerichtet werden – technisch wie organisatorisch. Aktuell beschäftigt er sich intensiv mit digitaler Souveränität und deren Auswirkungen auf Cloud-Strategien sowie mit modernen Betriebskonzepten rund um Agentic AI.

Steve Gerstner
steve.gerstner@bridging-it.de

Steve Gerstner ist Senior Software- und Cloud-Architekt mit einem Schwerpunkt auf Platform Engineering. Dank seines fundierten Know-hows in Java, modernen Web-Technologien und Cloud-Infrastrukturen wie AWS und Azure steuert er komplexe Entwicklungsprozesse und setzt Prioritäten effizient. Als Lead Architect treibt er die Weiterentwicklung skalierbarer Plattformen voran und sorgt dafür, dass nachhaltige Lösungen in Cloud- und Migrationsprojekten entstehen.

1. Einleitung

In der aktuellen digitalen Welt sind Unternehmen im Rahmen ihrer verteilten Geschäftsprozesse zunehmend auf Cloud-Technologien angewiesen. Cloud-Anbieter und -Dienste flexibel wechseln zu können, wird gleichzeitig zu einer Schlüsselfähigkeit für Unternehmen im digitalen Zeitalter. Dabei ist diese Fähigkeit weit mehr als eine technische Option. Sie ist ein bedeutendes Element für digitale Souveränität und unternehmerische Resilienz.

Während globale Verflechtungen lange als Garant für Wachstum und Innovation galten, offenbaren sich zunehmend die Kehrseiten. Geopolitische Spannungen, unterbrochene Lieferketten und technologische Abhängigkeiten verdeutlichen, wie verletzlich Wertschöpfungsketten geworden sind. Gleichzeitig werden solche Abhängigkeiten derweil gezielt zur Durchsetzung politischer und wirtschaftlicher Interessen genutzt.

Durch diese Veränderung erhält die digitale Souveränität eine neue strategische Dimension. Sie steht für die Fähigkeit, kritische Daten, Prozesse und Technologien unabhängig zu steuern, regulatorische Vorgaben zuverlässig einzuhalten und wirtschaftliche Risiken gezielt zu koordinieren. Die Herausforderung, Abhängigkeiten von spezifischen Technologien, Anbietern oder sogar Architekturen zu bewältigen, ist dabei von essenzieller Bedeutung für die Wahrung der eigenen Handlungs- und Wettbewerbsfähigkeit.

Viele in Deutschland und der Europäischen Union ansässige Unternehmen stellen sich mittlerweile aktiv dieser Aufgabe. So wird gezielt gegen mögliche Auslagerungsrisiken, Lock-in-Szenarien oder einseitige Abhängigkeiten gearbeitet. Das aktuelle geopolitische und wirtschaftliche Klima fungiert als Beschleuniger. Die Wechselfähigkeit entwickelt sich somit von einem wünschenswerten Attribut („Nice-to-have“) zu einer Kernkomponente der unternehmerischen Resilienz.

Auch in Zukunft werden immer mehr kritische Workloads in die Cloud verlagert. Entsprechend wirken die drohenden Szenarien einer mangelnden Wechselfähigkeit – wie beispielsweise erzwungene Migrationen, Preiserhöhungen oder eine Verschlechterung der Servicequalität – umso signifikanter. Entsprechend zeigt die folgende Ausarbeitung, warum die Cloud-Wechselfähigkeit gerade jetzt für Unternehmen von entscheidender Bedeutung ist und wie die damit verbundenen Fähigkeiten in einer Organisation nutzbringend eingesetzt werden können.

Für strategische Entscheidungsträger, Unternehmensarchitekten und IT-Führungskräfte schafft es eine belastbare Grundlage für fundierte Entscheidungen, um die digitale Souveränität und operative Resilienz ihrer Organisationen zu stärken.

2. Grundlagen der Cloud-Wechselfähigkeit

Die Betrachtung der Wechselfähigkeit im Kontext der digitalen Souveränität ist keine einseitige Aufgabe. Vielmehr besteht sie aus drei Dimensionen, die in enger Verbundenheit zueinander stehen.

2.1 Die drei Dimensionen der Wechselfähigkeit

Die Verwirklichung der digitalen Souveränität und damit auch einer umfassenden Cloud-Wechselfähigkeit stützt sich auf drei Dimensionen - organisatorische, technische und rechtliche Ansätze:

- **Die organisatorische und kulturelle Wechselfähigkeit** betrifft die Prozesse, Fähigkeiten und Strukturen innerhalb eines Unternehmens, die einen Anbieterwechsel ermöglichen. Dazu gehören klare Verantwortlichkeiten, erprobte Wechselprozesse, das Vorhandensein notwendiger Skills und Kapazitäten sowie eine gelebte Kultur des ständigen Wandels.

- **Die technische Wechselfähigkeit** bezieht sich auf die Fähigkeit, Cloud-Dienste und -Anbieter oder bestimmte Workloads ohne unüberwindbare technische Hindernisse verlagern zu können. Sie umfasst Aspekte wie Datenportabilität, Interoperabilität von Systemen, Nutzung offener Standards und die Vermeidung von Vendor-lock-ins durch proprietäre Technologien.

- **Die rechtliche bzw. vertragliche Wechselfähigkeit** umfasst alle juristischen und kommerziellen Rahmenbedingungen, die einen Wechsel beeinflussen. Dies beinhaltet die Gestaltung von insbesondere Verträgen, Kündigungsfristen, Exit-Klauseln, Service Level Agreements sowie die Einhaltung regulatorischer Vorgaben wie beispielsweise des Datenschutzes.

2.2 Wahl der Strategie

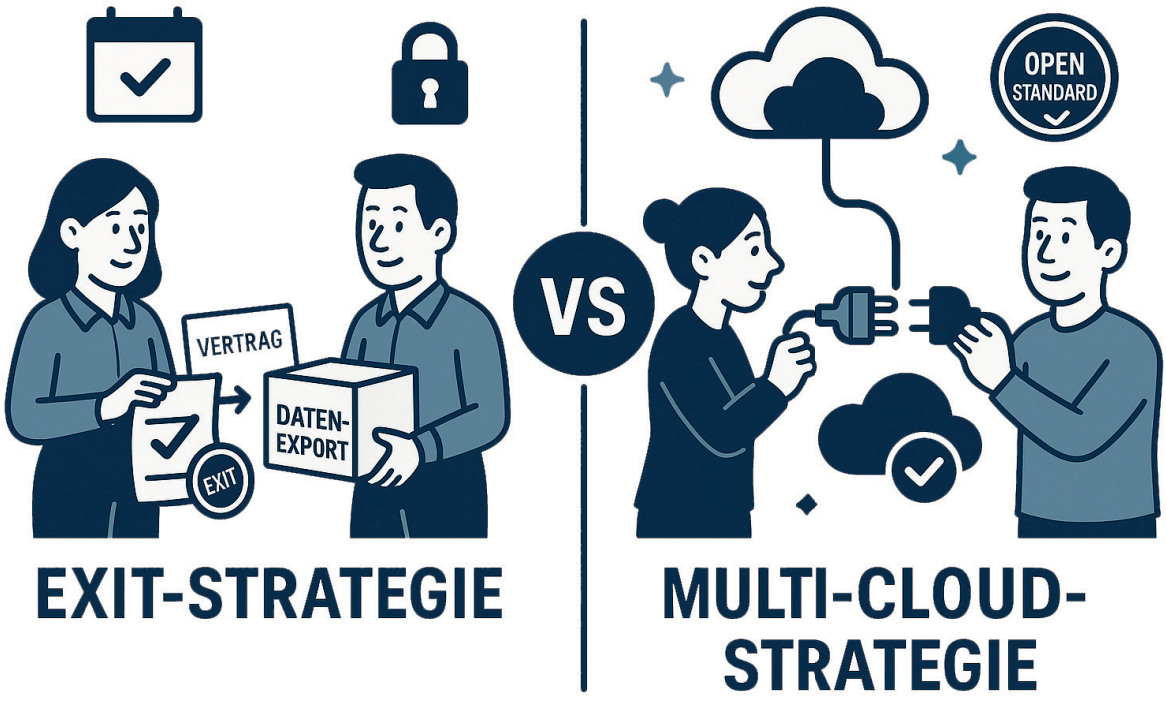
Es gibt grundsätzlich zwei Strategien zur Erreichung der Wechselfähigkeit, die miteinander verbunden sind und trotzdem separat betrachtet werden müssen, weil sie unabhängig voneinander diverse Vor- und Nachteile bieten:

Eine Exit-Strategie konzentriert sich auf den geplanten und geordneten Ausstieg aus einem spezifischen Dienst oder einer Lösung eines bestimmten Anbieters. Sie beinhaltet Überlegungen dazu, wie Daten und Anwendungen migriert, Verträge beendet und der Übergang zu einer alternativen Lösung gestaltet werden können. Ein solcher Exit kann durch verschiedene Faktoren ausgelöst werden, etwa durch Preisanpassungen, das Ende der Service-Erbringung, absinkende Service-Qualitäts-Level (SLA), Vertrauensverlust oder eine Vertragskündigung durch den Vertragspartner. In einigen Fällen erfolgt ein Exit ungeplant – umso wichtiger ist es, technisch und organisatorisch vorbereitet zu sein.

Eine Multi-Cloud-Strategie beschreibt den Ansatz, Dienste von mehreren Cloud-Anbietern gleichzeitig zu nutzen. Dies kann aus verschiedenen Gründen geschehen, etwa um die jeweils besten Dienste verschiedener Anbieter zu kombinieren (Best-of-Breed), um die Ausfallsicherheit zu erhöhen oder um Abhängigkeiten von einem einzelnen Anbieter zu reduzieren.

Im Hinblick auf die Wechselfähigkeit empfiehlt es sich, relevante Kernprozesse und -Applikationen zu schützen und diese ebenfalls in Multi-Cloud-Umgebungen zu hosten, anstatt einen vollständigen Anbieterwechsel anzustreben, der die Organisation überfordern könnte.

Während eine Exit-Strategie somit einen Plan für die Beendigung einer Beziehung zu einem Cloud-Anbieter darstellt, ist eine Multi-Cloud-Strategie eine Nutzungsstrategie, bei der mehrere Anbieter einbezogen werden. Im Kontext der Wechselfähigkeit sind die Begriffe Exit-Strategie und Multi-Cloud-Strategie nicht voneinander getrennt zu betrachten, da beide zur Erhöhung der Flexibilität und Verbesserung der Risikostreuung beitragen können. Vielmehr ist die Exit-Strategie als impliziter Bestandteil einer Multi-Cloud Strategie zu betrachten.



3. Organisatorische und kulturelle Wechselfähigkeit

Mit der Ausprägung der Wechselfähigkeit geht die Verankerung im Unternehmen einher. Ziel ist es, die Fähigkeit zu entwickeln, unabhängig von Anbietern zu wechseln, kritische Ressourcen zu erkennen und betriebliche Anforderungen zu erfüllen. In solchen wechselfähigen Organisationen sind stetige Veränderungen in Kultur und Mindset verankert - ganz nach dem Grundsatz:

3.1 Wechselfähigkeit als neuer Standard

Die Verankerung in der Organisation geht über das Mindset hinaus. Es ist wichtig, die Wechselfähigkeit in der übergeordneten Unternehmens- und IT-Strategie zu verankern. Klare Richtlinien für die Nutzung standardisierter Services, die sowohl die wirtschaftlichen Ziele als auch die auszulagernden kritischen Prozesse und Daten festlegen, sollten eindeutig definiert werden. Dies beinhaltet auch eindeutig definierte funktionale (beispielsweise angebotene Services) und nicht-funktionale (beispielsweise Performance) Anforderungen, um zukünftige Zielsysteme auszuwählen und deren Ergebnisse messen zu können.

Wechselfähigkeit kann nicht als rein Bottom-up getriebene IT-Initiative erfolgreich sein, sondern erfordert Rückendeckung und eine lenkende Strategie seitens der Unternehmensführung. Die Positionierung der organisatorischen Wechselfähigkeit als „zentrale strategische Maßnahme“ und ihre Verankerung in der Unternehmenskultur unterstreichen die Notwendigkeit dieser Ausrichtung auf höchster Unternehmensebene.

3.2 Skills und Kapazitäten

Während die Wechselfähigkeit in der Unternehmenskultur verankert wird, stellt sich gleichermaßen die Herausforderung, eine Kultur des kontinuierlichen Lernens („Change Readiness“) zu fördern. Eine Kultur des stetigen Wandels als Teil des Wechselprozesses impliziert die Notwendigkeit, die gesamte Organisation auf neue Arbeitsweisen und Denkansätze im Umgang mit möglicherweise veränderten Technologien vorzubereiten.

Gleichzeitig muss die Verfügbarkeit von Skills in Bezug auf zunehmend abstraktere Technologien, Servicemodelle und Angebote der Anbieter sichergestellt werden. Ein erfolgreicher Wechsel erfordert nicht nur technologische Fähigkeiten, sondern auch fachliche Kompetenzen in verschiedenen Bereichen. Dazu zählen technische Expertise in Cloud-Architekturen und Migrationstechnologien, strategische Planungsfähigkeiten, rechtliche Kompetenz in Datenschutz und Vertragsrecht sowie Projektmanagementfähigkeiten zur Koordination der Umstellung ohne Betriebsunterbrechung.

Die resultierende Herausforderung liegt darin, internes Wissen schnell aufzubauen und bei Bedarf externes Fachwissen zu akquirieren. Eine Abhängigkeit von einzelnen Schlüsselpersonen für kritisches Wechselfähigkeitswissen kann eine neue Form des „internen Lock-ins“ oder ein Risiko darstellen. Es muss daher sichergestellt werden, dass Wissen dokumentiert und verteilt werden kann.

Die erfolgreiche Umsetzung von Wechselfähigkeit erfordert die Identifizierung und Einbindung aller relevanten Stakeholder, die Definition klarer Rollen und Verantwortlichkeiten sowie die Etablierung von Betriebsmodellen zur Unterstützung der operativen Souveränität. Darunter versteht man die Fähigkeit, digitale Systeme im Betrieb eigenständig zu verwalten, zu überwachen und abzusichern – unabhängig von Dritten.

Der Grad der Externalisierung ist somit eine notwendige strategische Unternehmensentscheidung, die nicht zuletzt das Business Continuity Management (BCM) beeinflusst.

3.3 Business Continuity Management

Die Sicherstellung der fortlaufenden Handlungsfähigkeit ist unternehmenskritisch. Entsprechend ist die Wechselfähigkeit eng mit dem Business Continuity Management (BCM) verknüpft. Mögliche Geschäftsrisiken oder Gefahren für die eigene digitale Souveränität können durch ein entsprechend vorbereitetes BCM adressiert werden. So müssen im Hinblick auf politische Entwicklungen auch kurzfristige Backup- und Wiederherstellungsstrategien bei weiteren Hyperscalern zur Sicherstellung des Betriebs und der Datenintegrität in Betracht gezogen werden.

Ebenso sollten der Parallelbetrieb von alten und neuen Systemen für einen schrittweisen Übergang sowie kontinuierliches Monitoring und Sicherheitsprüfungen über die Grenzen eines Cloud-Anbieters hinweg berücksichtigt werden. Business-Impact-Assessments sind regelmäßig notwendig, um beispielsweise Lock-in-Gefahrenquellen frühzeitig zu erkennen und zu adressieren. Dies bedingt eine gründliche Vorbereitung, die eine Bestandsaufnahme, eine Bewertung der aktuellen Situation und eine Risikobewertung mit klar definierten Ressourcen und Verantwortlichkeiten umfasst. Diese Analyse begründet die Tiefe der Handlungsempfehlungen.

Ein effektives Business Continuity Management im Kontext der Wechselfähigkeit ist nicht nur ein wesentliches Steuerungsinstrument, sondern auch die Grundlage für regelmäßige Tests der Exit- und Multi-Cloud-Strategien einschließlich der Migrationspläne, um die Handlungsfähigkeit im Bedarfsfall sicherzustellen.

3.4 Kritikalität und Schutzbedarf

Innerhalb der Wertschöpfungskette erfahren Systeme unterschiedlichen Schutzbedarf und unterliegen unterschiedlicher Kritikalität innerhalb des Unternehmens. Daher ist es entscheidend, eine sinnvolle Priorisierung von Wechselfähigkeitsbemühungen hinsichtlich der betroffenen Daten und Prozesse auf Basis dieser beiden Faktoren vorzunehmen.

Eine vorbereitende Maßnahme hierfür ist das detaillierte Mapping von Daten, Anwendungen und Prozessen entlang dieser Faktoren, um die wertvollsten und kritischsten „digitalen Vermögenswerte“ einer Organisation zu identifizieren. Diese Transparenz ermöglicht es, zu verstehen, welche Systeme, Informationen und Abläufe für den eigenen Erfolg und die Sicherheit unverzichtbar sind und welche eine hohe Kritikalität in Bezug auf Abhängigkeiten ausweisen.

Das Konzept der „digitalen Vermögenswerte“ impliziert somit einen iterativen Ansatz für die Wechselfähigkeit. Alle relevanten Geschäftsprozesse bzw. Wertschöpfungsprozesse müssen bekannt sein und die spezifischen Fachverfahren und Anwendungen identifiziert werden, die beispielsweise von einer Cloud-Nutzung betroffen sind.

Das Verständnis der Abhängigkeiten zwischen den Prozessen und Prozessketten sowie deren Verbindungen zu IT- und Cloud-Diensten muss vorhanden sein. Besonderer Fokus sollte auf jene Assets gesetzt werden, deren Verlust an Kontrolle oder Verfügbarkeit die schwerwiegendsten geschäftlichen Auswirkungen hätte. Gleichzeitig gilt es zu beachten, dass die Verknüpfung von Wechselfähigkeit mit „Souveränität“ und „regulatorischen Anforderungen“ zudem bedeutet, dass eine Anwendung nicht nur aufgrund ihrer operativen Funktion kritisch sein kann, sondern auch aufgrund ihrer Rolle bei der Wahrung der Datenhoheit oder der Erfüllung spezifischer Compliance-Vorgaben.
Die Definition von „Kritikalität“ und „Schutzbedarf“ geht somit über rein technische oder finanzielle Aspekte hinaus und umfasst auch Reputationsrisiken, rechtliche bzw. Compliance-Risiken sowie Auswirkungen auf die Ziele der digitalen Souveränität.

Quick Check

Organisatorische Wechselfähigkeit

Zur Selbstbewertung der organisationalen Wechselfähigkeit können folgende Fragen dienen:

- **Gibt es eine klare Strategie für die Nutzung von Cloud-Diensten?**
- **Existiert ein konkretes Zielbild, das Umfang und Vorgehensweise der Cloud-Nutzung und der angestrebten Wechselfähigkeit definiert?**
- **Wurden funktionale und nicht-funktionale Anforderungen klar definiert, um zukünftige Zielsysteme auswählen und deren Ergebnisse messen zu können?**
- **Sind alle relevanten Geschäftsprozesse, Fachverfahren und Anwendungen, die von einem Wechsel betroffen wären, bekannt?**
- **Habe ich meine Prioritäten und Risiken hinsichtlich Daten, Geschäftsprozessen und Fähigkeiten nach Business-Kritikalität, Souveränitätsbedarf und Schutzgrad bewertet und dokumentiert?**
- **Besitzt mein Unternehmen die Fähigkeit, Wissen über neue Technologien und Anbieter schnell aufzubauen oder externes Fachwissen zu akquirieren?**
- **Gibt es klare Regelungen für Ersatzleistungen im Falle eines Dienstausfalls des aktuellen Anbieters?**
- **Existieren Notfallpläne oder Exit-Strategien, die den Fall eines Anbieterausfalls oder -wechsels regeln?**
- **Ist das zentrale Risikomanagement um Parameter der digitalen Souveränität erweitert worden?**

4. Technische Wechselfähigkeit

Die technische Wechselfähigkeit bildet das Fundament für die Flexibilität, Cloud-Dienste und -Anbieter bedarfsgerecht zu wechseln, ohne auf unüberwindbare technische Hürden zu stoßen. Erst mit entsprechender Expertise sowie der geeigneten Auswahl der Technologie und Datenformate kann eine technische Wechselfähigkeit erlangt werden.

4.1 Die Rolle der technischen Architektur

Die technische Architektur und die damit verbundene Lösung sind entscheidend für die Risikominimierung und die Erreichung digitaler Souveränität bei Cloud-Migrationen. Eine klare Architektur, die flexibel auf unterschiedliche Dienstleister anpassbar ist und dabei auch die Kosten berücksichtigt, vereinfacht die Verlagerung kritischer Systeme und Daten.
Maßgeblich beeinflusst wird die technische Wechselfähigkeit durch die eingesetzten Cloud-Servicemodelle – On-Premises, Infrastructure as a Service (IaaS), Container as a Service (CaaS), Platform as a Service (PaaS), Function as a Service (FaaS) und Software as a Service (SaaS). Sie bieten unterschiedliche Ausprägungen in der Abstraktion der Daten bzw. Technologien, der Eigenverantwortung gegenüber dem Anbieter und Mitbestimmung in der Architektur. Während mit jeder Ebene die Eigenverantwortung – und damit der eigene Betriebsaufwand – sinkt, steigt die Abhängigkeit vom jeweiligen Servicemodell und Anbieter gemäß dem „Everything as a Service“-Ansatz.

Everything as a Service - XaaS

Als fortlaufender Prozess und als gelebter Bestandteil der Unternehmenskultur sind die Prüfung und Weiterentwicklung der technischen Architektur zu etablieren. Bei der Einführung neuer oder bei der Modifizierung bereits bestehender Dienste muss deren Auswirkung auf die Gesamtwechselfähigkeit kontinuierlich bewertet werden. Dies spiegelt den Kern des Enterprise-Architecture-Managements (EAM) wider, das eben diese stetige Governance der Architektur impliziert. Die Entscheidung, wie weit der „Schieberegler der Wechselfähigkeit“ gestellt wird, ist dabei mit jedem Service neu zu treffen oder durch das Bereitstellen einheitlicher Entscheidungsbäume positiv zu beeinflussen.

On-Premises	Colocation	Hosting	IaaS	PaaS	SaaS
Daten	Daten	Daten	Daten	Daten	Daten
Applikation	Applikation	Applikation	Applikation	Applikation	Applikation
Datenbanken	Datenbanken	Datenbanken	Datenbanken	Datenbanken	Datenbanken
Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Physische Server	Physische Server	Physische Server	Physische Server	Physische Server	Physische Server
Netzwerk & Speicher	Netzwerk & Speicher	Netzwerk & Speicher	Netzwerk & Speicher	Netzwerk & Speicher	Netzwerk & Speicher
Rechenzentrum	Rechenzentrum	Rechenzentrum	Rechenzentrum	Rechenzentrum	Rechenzentrum

Self-Managed Provider-supplied

Tabelle 1 gibt eine vergleichende Übersicht, wie verschiedene Cloud-Servicemodelle die Wechselfähigkeit beeinflussen:

Service-modell	Key Characteris-tics	Level of Abstraction	Typische Provider-Verantwortung	Typische Kunden-Verantwortung	Wesentliche Herausforderungen für Wechselfähig-keit	Wesentliche Enabler für Wechselfähigkeit
On-Premises	Eigenes Rechenzentrum, volle Kontrolle	niedrig	Keine (außer ggf. Hard-ware-Wartung)	Alles: Infrastruktur, Plattform, Anwendun-gen, Daten, Betrieb, Sicherheit	Modernisierungsstau, gewachsene Strukturen, hohe Investitions- und Betriebskosten für Flexibilität	Volle Kontrolle über Standardisierung, Technologieauswahl, Automatisierung: keine externen Abhängiogkei-ten im Betrieb
IaaS	Virtuelle Server, Netzwek, Speicher	mittel	Physische Infra-struktur, Virtuali-sierungsschicht	Betriebssystem, Midd-leware, Anwendungen, Daten, Sicherheit der Workloads, Netzwerk-konfiguration	Unterschiedliche Hy-pervisor-Technologien, proprietäre Netzwerk- und Storage-APIs, VM-Format-Inkompati-bilitäten	Standardisierte VM-Images, Infrastruc-ture as Code (IaC), Datenmigrationstools, Nutzung offener Sto-rage-Protokolle, Abs-traktion durch eigene Netzwerk-Appliances
Caas	Container-Cluster (z.B. Kubernetes)	mittel – hoch	Container-Orches-trierungsplattform, zugrundeliegende Infrastruktur	Containerisierte An-wendungen, Container-Images, Konfiguration, Sicherheit der Anwen-dung	Unterschiedliche Kubernetes-Distribu-tionen und -Versionen proprietäre Add-ons und Management-Tools des Providers, anbieterspezi-fische Integrationen (z.B. Logging, Monitoring)	Standardisierte Con-tainer-Formate (z.B. Docker, OCI) Nutzung von Standard-Kuberne-tes-APIs, Helm-Charts für Deployment, CI/CD-Pipelines für Image Erstellung und Ver-teilung, Service Meshes für Abstraktion
PaaS	Entwicklungs- und Laufzeitum-gebungen (z.B. Datenbanken, Applikations-server)	hoch	Plattform-Soft-ware, Middleware, Betriebssystem, Infrastruktur	Anwendungen, Daten, Benutzerzugriffsmanage-ment, Konfiguration der Anwendungsdienste	Starke Bindung an providerspezifische Dienste und APIs, unter-schiedliche Feature-Sets und Versionen von Middlware/Datenban-ken, eingeschränkte Konfigurierbarkeit, Datenformat -Lock-in	Nutzun von PaaS-Diensten, die offene Standards unterstützen (z.B. SQL-Datenban-ken) Design für lose Kopplung,Abstraktions-schichten (z.B. ORM für Datenbanken), Export/Import-Funktionen für Daten und Konfigura-tionen
FaaS	Serverless Code-ausführung	sehr hoch	Ausführungsumge-bung, Skalierung, Infrastruktur	Code-Funktionen, Trigger-Konfigurationen, Abhängigkeiten (Biblio-theken)	Bindung an spezifische Function-Signaturen und Event-Quellen des Providers, unterschied-liche Laufzeitumgebun-gen und unterstützte Sprachen/Versionen, Kaltstart-Verhalten, Limits	Code-Portabilität durch gängige Programmier-sprachen, Nutzung von Frameworks (z.B. Serverless Framework) zur Abstraktion, API-Gateways zur Entkopp-lung von Triggern, klare Trennung von Code und Konfiguration
SaaS	Fertige Applika-tionen aus der Cloud (z.B. CRM, Office-Anwen-dungen)	sehr hoch	Anwendung, Platt-form, Infrastruktur	Dateninhalte, Benutzer-verwaltung, Konfigura-tion der Anwendung im Rahmen der Möglich-keiten	Starke Hersteller-bindung, proprietäre Datenformate, einge-schränkte Datenexport-/Import-Möglichkeiten, unterschiedliche Funk-tionalitäten und APIs, komplexe Migration von Berechtigungen	Nutzung von An-wendungen mit gut do-kumentieren APIs und offenen Datenformaten für Export/Import, Mög-lichkeit der Anbindung an ein zentrales IAM, klare Dokumentation der Datenstrukturen, Verfügbarkeit von Migrations-Tools oder -Services

Tabelle 1: Gegenüberstellung der Cloud-Servicemodelle hinsichtlich der Wechselfähigkeit

4.2 Abhängigkeiten, Portabilität, Automatisierung

Die Kernmechanismen zur Erreichung technischer Wechselfähigkeit umfassen die Minimierung von Abhängigkeiten, die Sicherstellung der Portabilität von Daten und Anwendungen sowie den flächendeckenden Einsatz von Automatisierung.

Die Vermeidung von Vendor-lock-ins ist eines der Ziele auf dem Weg zur technischen Wechselfähigkeit. Dies kann durch den Einsatz von Open-Source-Software, offenen Standards und APIs, Containerisierung sowie durch eine cloud-agnostische Architektur erreicht werden.

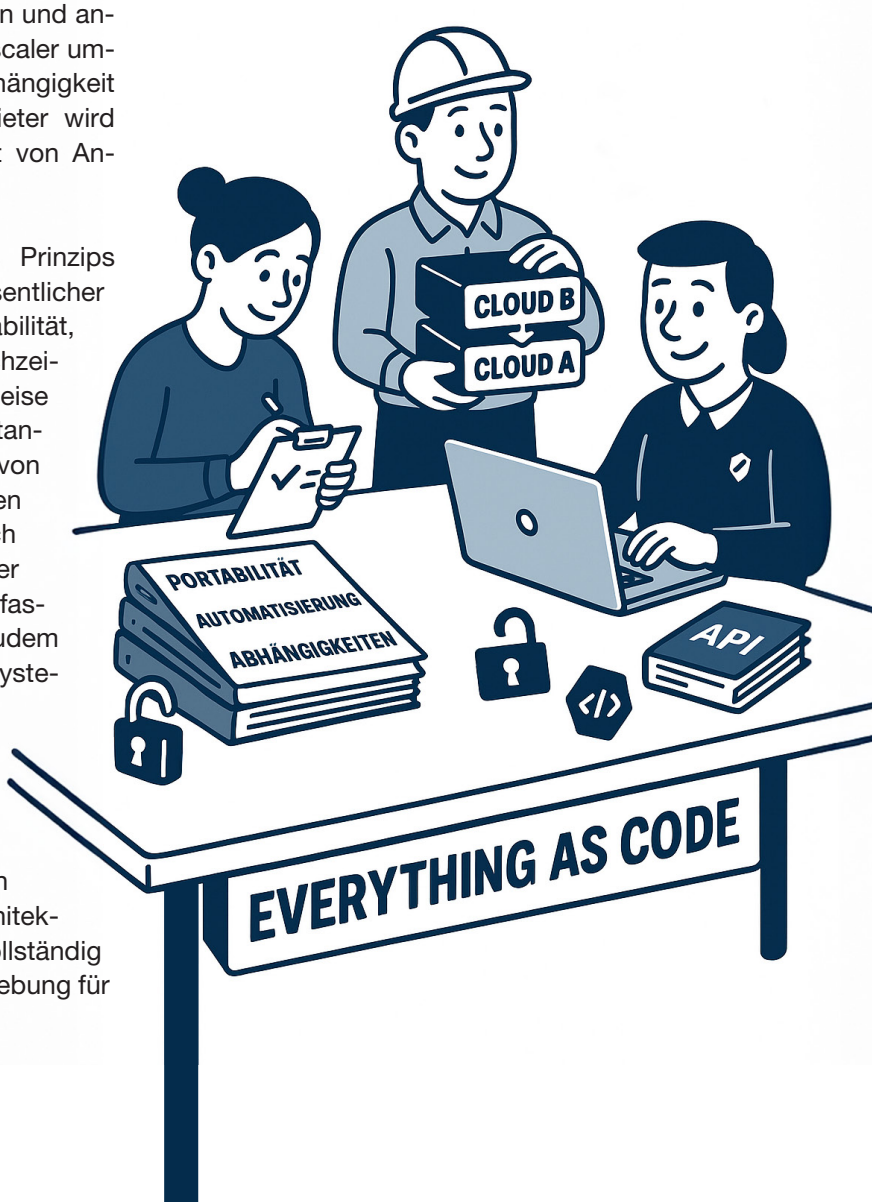
Grundsätzlich gilt, dass alle Cloud-Anwendungen so entwickelt werden sollten, dass sie flexibel und schnell auf verschiedenen Cloud-Plattformen - ob public oder private - betrieben werden können, ohne dass Änderungen an der zugrunde liegenden Technologie erforderlich sind. Beispielsweise wird die Automatisierung von Anfang an deklarativ beschrieben und anschließend für den jeweiligen Hyperscaler umgewandelt und bereitgestellt. Die Abhängigkeit von einem bestimmten Cloud-Anbieter wird somit minimiert und die Portabilität von Anwendungen sichergestellt.

Die konsequente Anwendung des Prinzips „Everything-as-Code“ ist damit wesentlicher Treiber für den Aufbau von Interoperabilität, Effizienz und Wechselfähigkeit. Gleichzeitig helfen API-Gateways, idealerweise auf Open-Source-Basis, bei der Standardisierung und Automatisierung von Schnittstellen und erhöhen somit den Reifegrad der Wechselfähigkeit durch die transparente Austauschbarkeit der angeschlossenen Systeme. Eine umfassende Dokumentation unterstützt zudem bei der Identifizierung abhängiger Systeme, was sich signifikant positiv auf die Erstellung der Wechselstrategie auswirkt. Unterstützt durch die Nutzung der Grundprinzipien der Software-Entwicklung, angewendet auf die Definition von Prozessen, Konfigurationen und Architekturbeschreibungen, entsteht eine vollständig wiederholbare und auditierbare Umgebung für Infrastruktur und Applikationen.

Dabei dient die Automatisierung nicht nur der Effizienz bei Migrationen, sondern ist auch ein Schlüsselelement für das Testen der Wechselfähigkeit. Automatisierte Deployment- und Test-Pipelines ermöglichen es Organisationen, ihre Fähigkeit zum Wechsel regelmäßig zu validieren. So wird das Vertrauen in einen Exit- oder Migrationsplan aufgebaut und kontinuierlich gestärkt.

Eine automatisierte Umgebung bildet zudem die Grundlage für die Sicherstellung einer aktiven Compliance und wirksamer Sicherheitsmechanismen. Nicht genehmigte oder manuelle Veränderungen an der Infrastruktur werden automatisiert geprüft, gemeldet und in den ursprünglichen Zustand zurückgesetzt. Etwaigen unerwarteten Problemen oder Komplikationen im Ernstfall wird somit aktiv vorgebeugt.

Ein kritischer Aspekt der operativen Souveränität und Datenhoheit ist die Fähigkeit, Daten und Anwendungen bei einem Wechsel des Cloud-Anbieters kontrolliert, sicher und effizi-



ent zu übertragen. Dies erfordert eine vorausschauende Planung und die Auswahl geeigneter technischer Strategien. Neben dem Einsatz von offenen, standardisierten Datenformaten gilt es, eine geeignete Backup-Strategie zu definieren. Eine solche Strategie beinhaltet regelmäßige, verschlüsselte Sicherungen auf unabhängigen, externen Speichern. Geeignete Wiederanlaufpläne („Disaster-Recovery"), die unabhängig von der Umgebung agieren, unterstützen die Reaktionsfähigkeit und minimieren die Auswirkungen im Ernstfall.

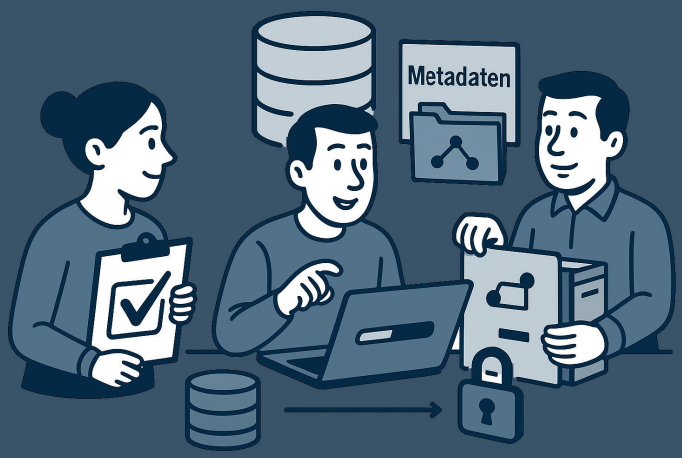
Tabelle 2 vergleicht verschiedene Datentransferstrategien, basierend auf Expertenwissen aus Cloud-Infrastrukturen unterschiedlicher Reifegrade:

Strategie	Laufende Kosten	Exit-Kosten	Implementierungs-komplexität	Hauptvorteil für Cloud-Exit	Hauptnachteil für Cloud-Exit
Backup & Restore	niedrig	mittel – hoch	mittel	niedrigste laufende Kosten, Daten sind gesichert	Langer Wiederherstellungs-prozess, potenziell hoher Datenverlust
Pilot Light	mittel	mittel	mittel – hoch	Gute Balance Kosten/Nutzen, relativ schnelle Wiederherstellung	Erfordert Aufbau/Skalierung der Infrastruktur im Ernstfall
Warm Standby	hoch	niedrig	hoch	Schnelle Umschaltung möglich, Infrastruktur großteils bereit	Höhere laufende Kosten für skalenreduzierte Umgebung
Hot Standby/ Clustering	sehr hoch	sehr niedrig	sehr hoch	Nahezu keine Ausfallzeit, sofortige Übernahme	Höchste laufende Kosten und Komplexität, oft „Overkill"

Tabelle 2: Vergleich von Datentransferstrategien für den Cloud-Exit

Datenportabilität

Wahre Datenportabilität geht über die reine Fähigkeit zur Datenextraktion hinaus. Sie umfasst auch die Nutzbarkeit und Integrität dieser Daten in einer neuen Umgebung - einschließlich zugehöriger Metadaten, Berechtigungen und relationaler Kontexte. Die Herausforderung besteht darin, dass ein einfacher Daten-Dump oft nicht ausreicht.



Quick Check

Technische Wechselfähigkeit

Zur Selbstbewertung der technischen Wechselfähigkeit können Organisationen die folgenden Fragen heranziehen:

- **Wie unabhängig sind die Virtualisierungstechnologien, die vom aktuellen Dienstleister genutzt werden?**
- **Existieren definierte Replikationsmechanismen (gegebenenfalls auch von Drittanbietern) oder ist bekannt, welche zur Verfügung stehen?**
- **Werden relevante sowie kritische Daten auf zugänglichen, unabhängigen Systemen gespeichert und archiviert?**
- **Gibt es garantierte Prozesse zur Löschung von Daten nach einem Wechsel?**
- **Werden Container-Technologien und -Orchestrierungen bereits umfangreich eingesetzt?**
- **Wird bereits umfassend auf Automatisierung (IaC, Runbooks, CI/CD-Pipelines etc.) gesetzt?**
- **Werden primär Open-Source-Middleware-Komponenten verwendet?**
- **Wurden die Abhängigkeiten zwischen den genutzten Services dokumentiert und sind den Verantwortlichen bekannt?**
- **Wird die SaaS-Anwendung bei anderen externen Anbietern angeboten und kann dort genutzt werden?**
- **Wurden mögliche Datentransferwege von und zum Dienstleister dokumentiert und sind den Verantwortlichen bekannt?**

5. Rechtliche und vertragliche Grundlagen zur Wechselfähigkeit

Die Fähigkeit eines Unternehmens, Cloud-Dienstleister zu wechseln, hängt maßgeblich von der vertraglichen und rechtlichen Ausgestaltung der bestehenden Geschäftsbeziehungen ab. Während technische Aspekte häufig im Vordergrund stehen, entscheidet die rechtliche Struktur darüber, ob ein Wechsel praktikabel, wirtschaftlich sinnvoll und rechtssicher möglich ist. Mit dem Inkrafttreten des EU Data Act (Verordnung (EU) 2023/2854 vom 12. September 2025) wird dieser Aspekt nochmals deutlich aufgewertet.

5.1 Aktuelle Anforderungen durch den EU Data Act

Diverse rechtliche und regulatorische Vorgaben stellen neue Anforderungen an vertragliche Regelungen. Dazu zählen insbesondere die Datenschutz-Grundverordnung (DSGVO), branchenspezifische Sicherheitsanforderungen – etwa für Betreiber kritischer Infrastrukturen (KRITIS) – sowie die neuen Vorgaben des Data Act.

EU Data Act:

Verpflichtet Anbieter unter anderem dazu, technische, vertragliche und organisatorische Wechselhindernisse zu beseitigen und die Migration von Daten aktiv zu unterstützen.

Im Rahmen der Vereinbarungen zwischen den Vertragspartnern nehmen Service Level Agreements (SLAs) im Kontext der Wechselfähigkeit optimalerweise eine doppelte Rolle ein: Einerseits sichern sie die Qualität und Verfügbarkeit der Cloud-Dienste, andererseits können sie bei Schlecht- bzw. Nichterfüllung als Grundlage für Sanktionen dienen. Verträge sollten daher nicht nur Mindestverfügbarkeiten definieren, sondern auch eindeutige Rahmenbedingungen für Sanktionsmöglichkeiten bei SLA-Verstößen vorsehen, etwa Vertragsstrafen oder die Möglichkeit zur außerordentlichen Kündigung. Nicht zuletzt müssen Verträge die Insolvenz der Anbieter abdecken.

Ebenso werden Exit-Klauseln vorgeschrieben, welche in diesem Kontext eine hervorgehobene Rolle einnehmen: Sie regeln die Bedingungen, unter denen ein Vertrag beendet und ein Anbieterwechsel vollzogen werden kann. Neben Kündigungsfristen und Übergangszeiträumen werden auch Unterstützungsleistungen gefordert, die in Kapitel 5.3 näher betrachtet werden.

5.2 Verbreitete Vertragsmodelle

Während technische Standards und regulatorische Anforderungen zunehmend vereinheitlicht werden, bleibt die vertragliche Gestaltung ein zentrales Instrument zur Sicherung der eigenen Interessen – insbesondere mit Blick auf Flexibilität, Datenhoheit und Exit-Möglichkeiten. Folgende Vertragsmodelle gelten hierbei als Standard:

„Click-Through-Modelle“

Standardisierte Vertragsbedingungen großer Anbieter, sogenannte „Click-Through-Modelle“, werden häufig ohne individuelle Verhandlung abgeschlossen. Aus rechtlicher Sicht handelt es sich hierbei regelmäßig um Allgemeine Geschäftsbedingungen (AGB) im Sinne der §§ 305 ff. BGB. Diese unterliegen der AGB-rechtlichen Inhaltskontrolle, insbesondere hinsichtlich überraschender oder unangemessener Klauseln (§§ 307–309 BGB). Typischerweise fehlen in diesen Modellen klare Regelungen zu Exit-Strategien, Migrationsunterstützung und Sonderkündigungsrechten. Für Unternehmen mit geschäftskritischen Anwendungen werden sie daher nur eingeschränkt empfohlen.

Individuell verhandelte Enterprise Agreements

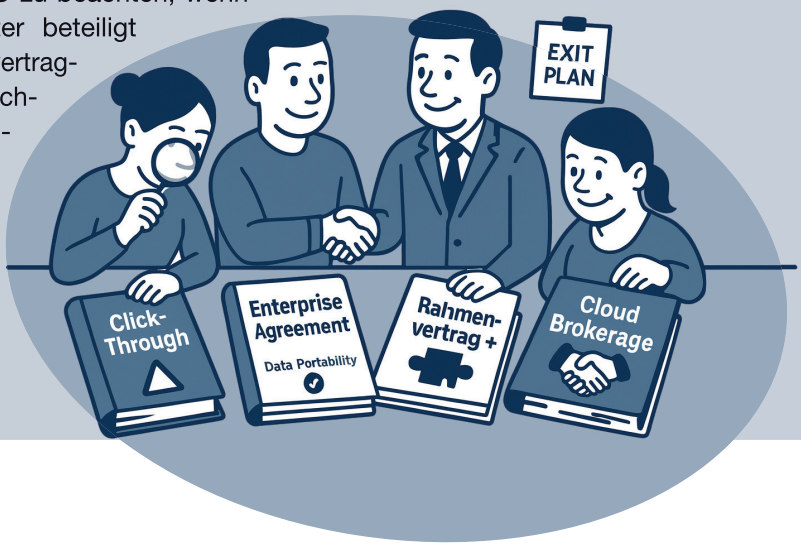
Enterprise Agreements bieten deutlich mehr Gestaltungsspielraum als „Click-Through-Modelle“. Sie ermöglichen die individuelle vertragliche Regelung zentraler Aspekte wie Datenportabilität, technischer Kompatibilität, Migrationsunterstützung und Schutz vor Drittstaatenzugriffen. Im Hinblick auf die DSGVO ist vor allem die Verantwortlichkeitsklärung nach Art. 28 DSGVO zu beachten, wenn mehrere Dienstleister beteiligt sind. Zudem sollten vertragliche Anpassungspflichten bei regulatorischen Änderungen berücksichtigt werden, etwa beim Inkrafttreten des EU Data Act.

Modulare Rahmenverträge mit Einzelabrufen

Rahmenverträge mit Einzelabrufen kombinieren eine standardisierte Grundstruktur mit der Möglichkeit, einzelne Leistungsbausteine individuell zu gestalten. Sie sind besonders im öffentlichen Sektor und in Konzernstrukturen verbreitet. Rechtlich handelt es sich um mehrstufige Vertragsverhältnisse, bei denen die Kohärenz zwischen Rahmenvertrag und Einzelabruf entscheidend ist – vor allem hinsichtlich der bereits genannten Exit-Klauseln und der Service-Level-Agreements.

Cloud-Brokerage-Modelle

Bei Cloud-Brokerage-Modellen tritt ein Intermediär als Vertragspartner auf und bündelt Leistungen verschiedener Anbieter. Dies kann die Komplexität für den Kunden reduzieren, birgt jedoch das Risiko zusätzlicher Abhängigkeiten. Rechtlich ist sicherzustellen, dass der Broker nicht nur Vermittler, sondern auch Vertragspartner ist, mit entsprechenden Pflichten zur Verfügbarkeit, Haftung und Datenverantwortung. Die DSGVO verlangt auch hier eine klare Verantwortlichkeitsklärung, insbesondere bei der Auftragsverarbeitung durch mehrere Beteiligte.



5.3 Mindestinhalte von Cloud-Verträgen zur Sicherstellung der Wechselfähigkeit

Der EU Data Act verpflichtet Anbieter und Kunden dazu, bestimmte Mindestinhalte in Cloud-Verträgen zu verankern. Diese Anforderungen gelten sowohl für neu abzuschließende als auch für bestehende Verträge, die bis zum 12. September 2025 angepasst werden müssen. Ziel ist es, einen reibungslosen, diskriminierungsfreien und technisch durchführbaren Wechsel zwischen Cloud-Dienstleistern zu ermöglichen.

Wie zu Beginn des Kapitels beschrieben, werden Kündigungsfristen und Übergangszeiträume vorgeschrieben. Als Kündigungsfrist müssen Verträge für Kunden nun maximal zwei Monate vorsehen. Diese kurze Frist soll sicherstellen, dass Kunden flexibel auf Marktveränderungen reagieren können. Daran schließt sich in der Regel ein Übergangszeitraum von 30 Tagen an, in dem die Migration der Daten abgeschlossen, der Geschäftsbetrieb ohne Unterbrechung fortgeführt und der Dienst geordnet beendet werden soll. In Ausnahmefällen kann dieser Zeitraum auf bis zu sieben Monate verlängert werden – entweder auf Antrag des Anbieters (bei technischer Undurchführbarkeit) oder des Kunden (ohne Begründungspflicht, jedoch gegen Kostentragung).

Ein weiterer verpflichtender Vertragsinhalt ist die aktive Unterstützung des Anbieters bei der Migration und Übertragung der Daten, auch an Drittanbieter. Dazu gehören die Bereitstellung von Informationen zu Datenformaten, Schnittstellen und Export-Tools, die Sicherstellung der technischen Kompatibilität mit anderen Diensten sowie die kontinuierliche Leistungserbringung während des Übergangszeitraums. Besonders hervorzuheben ist, dass der Data Act ausdrücklich verbietet, dass Anbieter Wechselhindernisse im Rahmen ihrer Verträge einbauen. Entsprechend müssen Anbieter ebenso vertraglich zusichern, dass exportierbare und nicht exportierbare Daten klar voneinander abgegrenzt und entsprechend behandelt werden. Diese Informationen müssen als Online-Register auf der Website des Anbieters veröffentlicht werden.

Nach Ablauf des Übergangszeitraums beginnt ein Abrufzeitraum von mindestens 30 Tagen, in dem Kundendaten weiterhin verfügbar sein müssen. Erst danach dürfen die Daten gelöscht werden. Diese Regelung soll sicherstellen, dass Kunden auch nach Vertragsende den Zugriff auf ihre Daten behalten, etwa zur Nachdokumentation oder zur Fehlerbehebung bei der Migration.

Der Vertrag muss zusätzlich die örtliche gerichtliche Zuständigkeit für die Datenverarbeitung sowie Maßnahmen gegen unrechtmäßige Zugriffe aus Drittstaaten dokumentieren. Diese Informationen müssen ebenfalls auf der Website des Anbieters veröffentlicht werden.

Aus finanzieller Sicht darf der Anbieter zwischen dem 12. September 2025 und dem 12. Januar 2027 nur noch ermäßigte Wechselentgelte verlangen, die sich auf die tatsächlichen Kosten der Datenextraktion beschränken. Ab dem 12. Januar 2027 sind Wechselentgelte vollständig verboten – mit Ausnahme von Multi-Cloud-Szenarien, bei denen parallele Nutzungskosten weitergegeben werden dürfen. Dabei ist zu beachten, dass bereits vor Vertragsschluss über alle potenziellen Wechselkosten durch den Anbieter aufgeklärt werden muss.

Über das geforderte Maß hinaus sollten Anforderungen an die Einhaltung von Compliance-Vorgaben im Vertrag verankert werden. Dazu zählen insbesondere Regelungen des Datenschutzes und der Informationssicherheit hinsichtlich der Datenverarbeitung, der Datenübermittlung und des Datenspeicherortes.

Letzteres kann die Auswahl alternativer Anbieter erheblich einschränken, wenn etwa gesetzlich vorgeschrieben ist, dass Daten ausschließlich innerhalb der EU gespeichert und verarbeitet werden dürfen. Auch der Schutz vor unautorisierten Zugriffen aus Drittstaaten muss vertraglich geregelt und technisch-organisatorisch abgesichert sein.

Quick Check

Vertragliche Wechselfähigkeit

Zur Einschätzung der eigenen vertraglichen Ausgangslage empfiehlt sich eine strukturierte Prüfung anhand folgender Leitfragen:

- **Wurden Kündigungsfristen und Übergangszeiträume so geregelt, dass ein geordneter Anbieterwechsel möglich ist?**
- **Ist eine vollständige Exit-Strategie dokumentiert und vertraglich abgesichert?**
- **Unterstützt der Anbieter die Migration technisch und organisatorisch, einschließlich der Schnittstellen, der Formate und der Fristen? Wurden in diesem Zusammenhang alle erforderlichen Übergangsrechte geregelt?**
- **Wurden exportierbare und nicht exportierbare Daten klar vertraglich differenziert und dokumentiert?**
- **Bestehen vertragliche Regelungen zur Datenverfügbarkeit nach Vertragsende und zur vollständigen Löschung?**
- **Welche Rahmenparameter des Service-Level-Agreements (SLA) regeln Fälle von Schlecht- oder Nichtleistung?**
- **Ist die Datenresidenz im gewünschten Rechtsraum vertraglich garantiert und vor unautorisierten Zugriffen aus Drittstaaten geschützt?**
- **Werden alle Informationspflichten (z. B. Gerichtsbarkeit, technische Maßnahmen, Wechselkosten) erfüllt?**
- **Sind anfallende Wechselentgelte transparent geregelt und entsprechen sie den Vorgaben des Data Act?**
- **Deckt der Vertrag auch Sonderfälle wie Anbieterinsolvenz oder Wechsel zu einem Wettbewerber ab?**
- **Welche spezifischen Anforderungen aus Datenschutz, Geheimschutz oder weiterführende Regularien sind für die genutzten Cloud-Dienste relevant und wie werden diese eingehalten?**

6. Reifegrad-Assessment

Um die eigene Handlungsfähigkeit in Bezug auf die Wechselfähigkeit aktuell einschätzen zu können, ist es wichtig, Stärken und Schwächen in den drei Dimensionen zu identifizieren und mögliche Chancen zu erkennen. Das Reifegrad-Assessment liefert einen systematischen Ansatz, um diesen Prozess zu optimieren. Durch regelmäßige Wiederholungen dieses Assessments wird ersichtlich, ob die sich entwickelnde Cloud-Landschaft die strategischen Ziele und Vorgaben der Organisation widerspiegelt.

6.1 Bestandsaufnahme

Der erste Schritt im Assessment des eigenen Reifegrads ist das Verständnis für die aktuelle Situation. Hierbei bilden die Fragestellungen der Quick-Checks die Basis für die Selbstkontrolle – den Self-Check.

Ferner ermöglichen weitere Fragestellungen, externe Erfahrungen sowie die Analyse entlang der drei Dimensionen eine Erweiterung der Selbstkontrolle und einen differenzierteren Blick auf die Ergebnisse.

Die Erkenntnisse der Selbstkontrolle werden genutzt, um die Schwächen und Stärken der eigenen Organisation zu identifizieren. Gleichzeitig bilden sie die Grundlage für den Aufbau einer fundierten Kommunikation innerhalb des Unternehmens und mit relevanten Stakeholdern.

Innerhalb der periodischen Wiederholung kann die beschriebene Selbstkontrolle sowohl zur Identifikation als auch zur Verifikation der Ziele und Maßnahmen herangezogen werden. Ist- und Soll-Zustand werden somit anhand derselben Fragenstellungen gegenübergestellt.

6.2 Bewertung der Erkenntnisse

Im Anschluss an den Selbstcheck müssen die Ergebnisse interpretiert werden, um spezifische Handlungsfelder zu identifizieren. Nicht alle identifizierten Schwächen erfordern sofortige, umfassende Abhilfemaßnahmen.

Kapitel 3 hat gezeigt, dass eine Priorisierung entlang von Kritikalität und Schutzbedarf erfolgen muss. Gleichermaßen gilt es, die in Kapitel 5 identifizierten Vorgaben aus regulatorischer Sicht und technischen Faktoren aus Kapitel 4 in die Priorisierung einfließen zu lassen. So können vertragliche Einschränkungen oder eine fehlende Verfügbarkeit notwendiger Skills eine mögliche Maßnahme ausschließen oder ihren Zeitpunkt in die Zukunft verschieben. Bei der Bewertung ist auch der selbst festgelegte Zielreifegrad der Wechselfähigkeit zu berücksichtigen. Maßnahmen, die diesen übertreffen oder ihm widersprechen, führen oft zu unnötigem Mehraufwand für die Organisation.

Abschließend ist zu berücksichtigen, dass die identifizierten Handlungsfelder nicht nur technische Aspekte betreffen. Möglich sind auch Änderungen von Richtlinien, Schulungsprogrammen, Strategien zur Vertragsgestaltung oder Anpassungen der Enterprise-Architecture-Roadmap, die langfristig aufgebaut und etabliert werden müssen.
Fehlende Fähigkeiten im organisatorischen Bereich können etwa ein Schulungsprogramm erforderlich machen, während ungünstige Vertragsbedingungen eine rechtliche Neuverhandlung notwendig machen.

6.3 Mögliche Maßnahmen

Die Bewertung der Ergebnisse erfordert eine differenzierte Herangehensweise und den Einsatz bewährter Methoden, um den angestrebten Reifegrad zu erreichen:

1 Etablieren Sie Wechselfähigkeit als strategisches Ziel. Wechselfähigkeit sollte innerhalb der Unternehmens- und IT-Strategie verankert sein. Eine klare Vision sowie Zielbild der Cloud-Nutzung sind dabei wesentliche Aspekte, ebenso wie wirtschaftliche Ziele, auszulagernde kritische Prozesse und Daten sowie der angestrebte Grad an Unabhängigkeit.

2 Führen Sie eine fundierte Analyse kritischer Ressourcen durch. Die digitalen Werte – also die wichtigsten Daten, Anwendungen und Prozesse – sind zu identifizieren und nach Kritikalität sowie Schutzbedarf zu priorisieren.

3 Implementieren Sie klare Wechselprozesse und eine robuste Governance. Governance-Mechanismen sollten so gestaltet sein, dass sie Risiken steuern und Compliance sicherstellen. Parallel ist ein klarer Prozess für den Anbieterwechsel zu etablieren.

4 Investieren Sie gezielt in Kompetenzentwicklung. Technische, strategische, rechtliche und Projektmanagement-Kompetenzen sind gezielt aufzubauen – intern wie extern durch Partner. Gleichzeitig sollte eine Kultur des kontinuierlichen Lernens und der Anpassungsfähigkeit gefördert werden.

5 Vermeiden Sie aktiv Vendor-lock-ins. Durch die Schaffung von Alternativen oder klaren Exit-Strategien, insbesondere für geschäftskritische Prozesse wird die Wechselfähigkeit beeinflusst. Dabei sollte auf die Auswahl an Technologien und Dienste geachtet werden, die auf offene Standards, Interoperabilität und Portabilität setzen

6 Integrieren Sie Wechselfähigkeitsüberlegungen in den gesamten Lifecycle. Aspekte der Wechselfähigkeit sollten bereits bei der ersten Evaluierung und Auswahl von Cloud-Diensten berücksichtigt werden. So fließt Wechselfähigkeit von Beginn an in Entscheidungen ein und wirkt nachhaltig.

7 Fördern Sie eine Kultur der „bewussten Abhängigkeit“. Jede Nutzung eines Cloud-Dienstes sollte das Lock-in-Risiko und die Wechseloptionen ausdrücklich bewerten. Abhängigkeiten sind bewusst zu gestalten und regelmäßig zu überprüfen, statt unkontrolliert zu wachsen.

7. Fazit

Die Fähigkeit, Cloud-Dienste und -Anbieter flexibel wechseln zu können, entwickelt sich von einer technischen Optimierung zu einer strategischen Notwendigkeit für Unternehmen, die ihre digitale Souveränität wahren und ihre Resilienz in einer dynamischen technologischen Umgebung sichern wollen. Zugleich verändern geopolitische Ereignisse das Verständnis der eigenen Wechselfähigkeit und ihrer Notwendigkeit.

Das Streben nach Wechselfähigkeit wird die Bedeutung offener Standards und interoperabler Cloud-Dienste weiter stärken – und damit auch die Roadmaps der Anbieter nachhaltig prägen. Zukünftige Fortschritte in Künstlicher Intelligenz und Automatisierung werden die technischen Komplexitäten von Cloud-Migrationen und Wechselfähigkeit voraussichtlich deutlich reduzieren. Aktuelle Automatisierungsansätze wie IaC und API-Gateways zeigen, wie Standards und klar definierte Schnittstellen der zunehmenden Komplexität wirksam begegnen. Auch Aufgaben wie Kompatibilitätsanalysen oder Code-Refactoring können zukünftig vermehrt durch KI vereinfacht werden. Damit zeigt sich, dass die Komplexität der technischen Dimension im Zuge des technologischen Fortschritts weiter abnehmen wird.

Die organisatorischen und vertraglichen Dimensionen werden jedoch auch zukünftig komplexe menschliche Aufgaben bleiben. Sie werden weiterhin strategische Entscheidungen, Prozessänderungen und Verhandlungsgeschick erfordern. Zugleich bleibt das Austarieren zwischen Mitbestimmung und Effizienz unter Berücksichtigung der Wechselfähigkeit eine zentrale Herausforderung für Unternehmen.

Die Entwicklung und Umsetzung einer umfassenden Wechselfähigkeitsstrategie erfordert tiefgreifendes Expertenwissen in technischen, organisatorischen und rechtlichen Bereichen. Die Auseinandersetzung mit Cloud-Wechselfähigkeit ist kein einmaliges Projekt, sondern ein fortlaufender Prozess der Anpassung und des Lernens. Digitale Souveränität ist ein dynamischer Zustand, der nur durch regelmäßige Überprüfung und kontinuierliche Anpassung der Strategien aufrechterhalten werden kann.

Externe Expertise ist für eine objektive Reifegradbewertung wertvoll und bringt branchenübergreifende Best Practices in die spezifischen Herausforderungen der Wechselfähigkeit ein.

Die im Dokument beschriebene Komplexität zeigt, dass viele Organisationen noch nicht über die nötige Kompetenz, aktuelles Fachwissen oder die erforderliche Objektivität für eine umfassende Bewertung verfügen. Ebenso kann es für Unternehmen herausfordernd sein, auf dieser Basis eine robuste Roadmap zur Verbesserung eigenständig zu entwickeln. Ein Beratungsengagement kann helfen, die Entwicklung und Umsetzung einer Wechselfähigkeitsstrategie zu beschleunigen – vor allem dort, wo interne Fähigkeiten oder Kapazitäten begrenzt sind.

Wir bei bridgingIT verfügen über umfangreiche Erfahrung in der Begleitung von Unternehmen bei der Gestaltung ihrer Cloud-Transformation und der Stärkung ihrer digitalen Souveränität. Zur Selbstkontrolle des Reifegrads hat bridgingIT umfangreiche Fragenkataloge zu technischer, organisatorischer und vertraglicher Wechselfähigkeit entwickelt.

Auf Basis der gewonnenen Erkenntnisse und identifizierten Schwächen entwickelt bridgingIT robuste und flexible Vorgehensmodelle, um die Wechselfähigkeit Ihres Unternehmens gezielt auszubauen und die digitale Souveränität nachhaltig zu stärken.

Über uns

Über die bridgingIT-Gruppe

Die BridgingIT GmbH wurde 2008 gegründet und bildet gemeinsam mit den Tochterunternehmen fastahead GmbH & Co. KG und CraftingIT GmbH die bridgingIT-Gruppe. Mit über 700 Mitarbeitenden an 9 Standorten in Deutschland unterstützt die Gruppe Unternehmen verschiedenster Branchen bei Veränderungs- und Digitalisierungsprojekten.

Als unabhängige Technologie- und Managementberatung bietet die bridgingIT-Gruppe ein umfassendes End-to-End-Portfolio – von der strategischen Beratung über die technologische Umsetzung bis zum Betrieb. Sie verbindet Business- und IT-Kompetenz, um digitale Transformation ganzheitlich, effizient und praxisorientiert zu gestalten. BridgingIT steht für technologische Lösungen und Prozessoptimierung, fastahead für digitale Geschäftsmodelle und craftingIT für individuelle IT-Services.

Ende 2023 fusionierte die bridgingIT-Gruppe mit der SPIE Germany Switzerland Austria GmbH, die mit 75,1 % der Stimmrechtsanteile als Mehrheitsgesellschafter einstieg. Die Dienstleistungen und Lösungen bleiben unverändert, was die anhaltende Stabilität und das Engagement für unsere Kunden bekräftigt.

Mehr zur bridgingIT-Gruppe und unseren Projekten unter: **www.bridging-it-gruppe.de**

fastahead
bridging IT
crafting IT
Technology Experience Center
SPIE ICS*

*Information & Communication Services

Schauen Sie vorbei und folgen Sie uns!

Ihr Kontakt zu uns

Felix Pille
felix.pille@bridging-it.de

Competence Lead
Security & GRC

Felix Pille ist Competence Lead für Security & GRC bei bridgingIT. Mit langjähriger Erfahrung in Sicherheitsarchitekturen, Managementsystemen und regulatorischen Anforderungen wie NIS-2 kennt er die Herausforderungen komplexer Konzernstrukturen mit Mehrfachregulierung aus erster Hand. In zahlreichen Beratungsinitiativen sorgt er dafür, dass Unternehmen auch in Cloud- und Migrationsprojekten Business Continuity, Sicherheit und Compliance zuverlässig im Blick behalten.

Tina Karbe
tina.karbe@bridging-it.de

Competence Lead
Platforms & Architectures

Tina Karbe ist Senior Consultant mit Schwerpunkt auf IT-Projektmanagement, IT-Architektur und Unternehmenstransformationen – insbesondere im Umfeld von Mergers, Carve-Outs und Rechenzentrumsverlagerungen. Darüber hinaus verantwortet sie die fachliche Weiterentwicklung unserer Portfolio-Kompetenz „Platform & Architectures“ und beschäftigt sich intensiv mit den Herausforderungen und Chancen der digitalen Souveränität.

Methodik & Quellen

Dieses Whitepaper basiert auf einer systematischen Analyse interner Projektunterlagen, strukturierten Experteninterviews mit Beraterinnen und Beratern der bridgingIT-Gruppe, ergänzenden Recherchen in fachspezifischen Datenbanken sowie auf der Praxiserfahrung der Autorinnen und Autoren aus zahlreichen Cloud-Transformationsprojekten. Zur Qualitätssicherung wurden alle Kapitel im Vier-Augen-Prinzip geprüft und mit Expertinnen und Experten aus Strategy, Technology und Legal abgestimmt. Ergänzend wurden einschlägige Leitfäden und Veröffentlichungen der Europäischen Kommission, von Bitkom e. V. und Trusted Cloud e. V. herangezogen.

Quellen:

Europäische Kommission (2025): Datengesetz | Gestaltung der digitalen Zukunft Europas.
Online: https://digital-strategy.ec.europa.eu/de/policies/data-act

Bitkom e. V. (2021): Cloud Computing – Evolution in der Technik, Revolution im Business.
Online: https://www.bitkom.org/sites/default/files/file/import/090921-BITKOM-Leitfaden-CloudComputing-Web.pdf

Bitkom e. V. (2025): Umsetzungsleitfaden zum Data Act – Hilfestellungen zur Umsetzung von (EU) 2023/2854.
Online: https://www.bitkom.org/sites/main/files/2025-09/bitkom-leitfaden-umsetzung-data-act.pdf

Trusted Cloud e. V. (2018): Leitfaden – Vertragsgestaltung beim Cloud Computing.
Online: https://www.trusted-cloud.de/sites/default/files/ap_3_vertragsleitfaden.pdf

Glossar

API-Gateways: Zentrale Verwaltung und Sicherung von APIs, einschließlich Authentifizierung, Lastverteilung und Monitoring. Praxis: Ein Kong®-Gateway bündelt Microservice-Anfragen und validiert OAuth 2.0-Tokens zur Zugriffskontrolle.

Automatisierung: Einsatz von Technologien zur automatisierten Bereitstellung, Verwaltung und Überwachung von IT-Ressourcen, z. B. mittels Infrastructure as Code (IaC) oder CI/CD-Pipelines. Praxis: Eine Jenkins®-Pipeline mit Terraform®-Skripten sorgt für reproduzierbare Infrastrukturänderungen und konsistente Deployments.

BCM (Business Continuity Management): Systematische Planung und Steuerung von Prozessen zur Sicherung des Geschäftsbetriebs bei Störungen oder Ausfällen. Praxis: Eine quartalsweise Notfallübung simuliert den Ausfall eines Cloud-Providers, um Wiederherstellungsprozesse und Disaster-Recovery-Pläne zu testen.

Cloud-Servicemodell: Bereitstellungsmodelle für Cloud-Services: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Container as a Service (CaaS), Function as a Service (FaaS) und On-Premises. Praxis: Ein Unternehmen nutzt IaaS (VMs in AWS®), PaaS (Azure® SQL) und SaaS (Salesforce®) parallel, um Flexibilität und Skalierbarkeit zu erhöhen.

Cloud-Wechselfähigkeit: Fähigkeit, Cloud-Anbieter und -Dienste mit vertretbarem Aufwand zu wechseln, um Abhängigkeiten zu reduzieren und digitale Souveränität zu sichern. Praxis: Standardisierte Datenexports und automatisierte Migrationspfade ermöglichen den Wechsel eines Cloud-Dienstes innerhalb von zwei Wochen.

Compliance: Einhaltung gesetzlicher, regulatorischer und interner Vorgaben (z. B. Datenschutz, Informationssicherheit). Praxis: Ein automatisierter Policy-as-Code-Check prüft, ob alle Sicherheitsrichtlinien einer Cloud-Umgebung eingehalten werden.

Datenportabilität: Möglichkeit, strukturierte und unstrukturierte Daten verlustfrei zwischen Systemen oder Cloud-Anbietern zu übertragen. Praxis: Ein CSV-Export und ein S3® Transfer Acceleration-Prozess mit Checksum-Validierung sichern die Integrität der übertragenen Daten.

DevOps: Verzahnung von Entwicklung und Betrieb zur schnelleren Bereitstellung von Anwendungen durch Automatisierung und agile Zusammenarbeit. Praxis: Ein GitLab®-Repository löst automatisierte Tests und Deployments in einer Multi-Cloud-Umgebung aus.

Digitale Souveränität: UFähigkeit einer Organisation, ihre digitalen Ressourcen, Daten und Prozesse eigenständig und unabhängig von externen Akteuren zu steuern. Praxis: Ein Dashboard überwacht SLA-Kennzahlen aller genutzten Cloud-Dienste in Echtzeit und sichert die Handlungsfähigkeit des Unternehmens.

EAM (Enterprise Architecture Management): Ganzheitliche Steuerung und Optimierung von Geschäftsprozessen und IT-Strukturen zur Unterstützung strategischer Ziele. Praxis: Regelmäßige Architektur-Reviews verhindern Insellösungen und fördern standardisierte, interoperable Systemlandschaften.

EU Data Act / Data Act: Europäische Verordnung (EU 2023/2854), die ab 12. September 2025 technische, vertragliche und organisatorische Wechselhindernisse für Cloud-Dienste beseitigt und Datenportabilität sicherstellt. Praxis: Ein Cloud-Vertrag wird gemäß Data Act angepasst – max. zwei Monate Kündigungsfrist, 30 Tage Übergangszeitraum, klare Auflistung exportierbarer Daten und Schnittstellen.

Exit-Strategie: Geplanter und gesteuerter Ausstieg aus einem Cloud-Dienst oder Vertrag inklusive Daten- und Prozessmigration. Praxis: Eine Exit-Checkliste mit Service-Exports, DNS®-Switchover und Validierungstests minimiert Ausfallzeiten beim Providerwechsel.

Governance, Risk & Compliance (GRC): Rahmenwerk aus Richtlinien, Prozessen und Verantwortlichkeiten, das sicherstellt, dass Unternehmens- und IT-Aktivitäten regelkonform, risikobewusst und strategisch gesteuert werden. Praxis: Ein zentrales GRC-Dashboard integriert Policy-Checks, Risikobewertungen und Audit-Nachweise, um Abweichungen in Echtzeit zu erkennen.

Hyperscaler: Globale Cloud-Anbieter mit hochskalierbarer Infrastruktur, z. B. AWS®, Azure®, Google Cloud®. Praxis: Eine Datenreplikation über zwei Hyperscaler-Regionen sichert Ausfallschutz und Datenverfügbarkeit.

Infrastructure as Code (IaC): Versionierte Bereitstellung von Infrastruktur über Code-Skripte, um Wiederholbarkeit, Transparenz und Portabilität zu erhöhen. Praxis: Änderungen an Cloud-Ressourcen werden in Git versioniert und automatisiert ausgerollt.

Interoperabilität: Nahtlose Zusammenarbeit unterschiedlicher Systeme auf Basis offener Standards und Schnittstellen. Praxis: Ein API-Gateway nutzt OpenAPI®-Standards, um Kompatibilität zwischen mehreren Cloud-Services sicherzustellen.

(Vendor-)lock-in: Abhängigkeit von einem Anbieter durch proprietäre Schnittstellen, Formate oder Tools, die den Wechsel erschweren oder verteuern. Praxis: Eine SaaS-Datenbank ohne Exportfunktion bindet Kunden langfristig an den Provider – ein klassischer Lock-in-Fall.

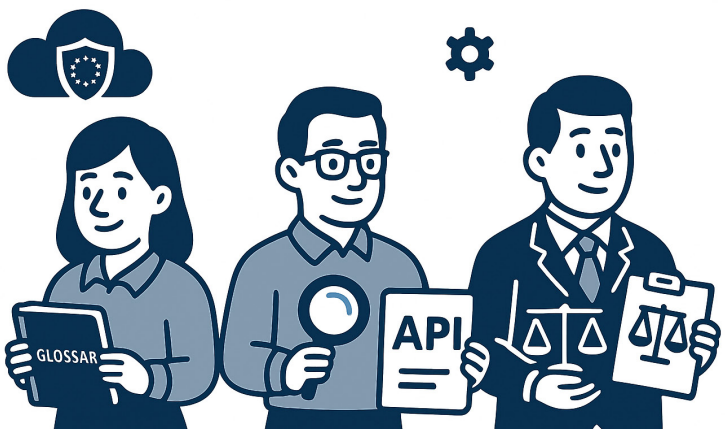
Migration: Übertragung von Daten, Anwendungen oder Prozessen zwischen Systemen oder Anbietern. Praxis: Eine CI/CD-Pipeline orchestriert eine Cloud-Migration mit Rollbacks und Canary-Releases, um Datenintegrität zu sichern.

Multi-Cloud-Strategie: Parallele Nutzung mehrerer Cloud-Anbieter, um Risiken zu minimieren und Flexibilität zu erhöhen. Praxis: Kritische Services laufen redundant in Azure® und AWS® mit DNS®-Failover, um Hochverfügbarkeit sicherzustellen.

Open Standards: Offen verfügbare, nicht proprietäre technische Spezifikationen und Protokolle, die Interoperabilität fördern und Herstellerabhängigkeiten vermeiden. Praxis: Durch den Einsatz von OpenAPI® und Kubernetes® können Services plattformübergreifend betrieben und migriert werden.

Operative Souveränität: Fähigkeit einer Organisation, digitale Systeme und Cloud-Ressourcen eigenständig zu betreiben, zu überwachen und abzusichern – unabhängig von externen Dienstleistern.

Service Level Agreements (SLAs): Vertraglich zugesicherte Leistungskennzahlen eines Anbieters, z. B. Verfügbarkeit, Latenz oder Support-Reaktionszeit. Praxis: Ein SLA garantiert 99,95 % Uptime. Ein Monitoring überprüft die Einhaltung und löst bei Abweichung automatische Gutschriften aus.



Impressum

Herausgeber
BridgingIT GmbH
N7, 5-6
68161 Mannheim
Deutschland

Geschäftsführer
Klaus Baumgärtner
Dr. Frank Wallner

Kontakt
info@bridging-it.de

Registergericht
Amtsgericht Mannheim,
HRB 703853

USt-IdNr.
DE814938761