Connecting your world.

Cloud-Strategie und Datensouveränität:

Handlungsempfehlungen für sichere Cloud-Nutzung

Datensouveränität bedeutet die Kontrolle über die eigenen Daten, ohne dass diese anderweitig eingesehen, verarbeitet, manipuliert oder gelöscht werden können. Wird sie verletzt, drohen hohe Strafen, Reputationsverluste und der Abfluss von Know-how.

Was bedeutet das für Ihre Daten- und Cloud-Strategie in geopolitisch herausfordernden Zeiten?

Datenhoheit ist nicht überall gegeben

Unsere nationale und die europäische Rechtsgebung stellt hohe Anforderungen an Datenlokalität, Datenschutz und Datensicherheit, die nationale und europäische Cloud-Anbieter erfüllen müssen. Das Problem ist: Clouds außereuropäischer Anbieter unterliegen anderen Rechtsordnungen und Zugriffsbestimmungen, beispielsweise dem US Cloud Act. Nutzen Unternehmen außereuropäische Cloud-Lösungen, besteht also je nach Rechtslage das Risiko unerwarteter Datenzugriffe. Die geopolitischen Entwicklungen führen dazu, dass immer mehr Unternehmen dies als kritisch einschätzen und versuchen, unabhängiger von außereuropäischen Cloud-Anbietern zu werden.

US Cloud Act

Der US Cloud Act von 2018 verpflichtet US-Cloud-Anbieter, gespeicherte Daten auf Anfrage an US-Behörden herauszugeben – unabhängig vom Speicherort. Befinden Cloud-Server sich unter der Kontrolle von US-Unternehmen oder deren Tochtergesellschaften, unterliegen sie also der US-amerikanischen Rechtsordnung, auch wenn die Rechenzentren in Europa liegen.

Warum ist Datensouveränität so wichtig?

Rechtliche Risiken: Bei der Nutzung externer Cloud-Dienste müssen Unternehmen diverse rechtliche Anforderungen in Bezug auf Datensicherheit erfüllen. Je nach Branche und Unternehmensgröße gilt es, die Bestimmungen der DSGVO, NIS-2, DORA, KRITIS und weiterer Verordnungen zu berücksichtigen. Diese betreffen etwa die Transparenz über Datenflüsse, die Erfüllung von Auskunfts- und Löschpflichten sowie Anforderungen an die Verfügbarkeit, Integrität und Sicherheit von IT-Systemen und Daten.

Ohne vertraglich geregelte Datenhoheit können Unternehmen diese Auflagen und Rechenschaftspflichten nicht erfüllen. Bei der Nutzung US-amerikanischer Anbieter entsteht zudem ein internationaler Rechtskonflikt, da diese dazu verpflichtet sind, Daten auf Anfrage an Regierungsbehörden weiterzugeben. Ein weiteres rechtliches Risiko besteht in unklaren Verantwortlichkeiten. Bei der Nutzung externer Cloud-Dienste ist oft nicht geklärt, wer im Schadensfall haftet. Es drohen empfindliche Geldstrafen, für die Unternehmen haften und für die auch die Geschäftsführung persönlich haftbar gemacht werden kann.

Strafen bei Verletzung der Datensicherheit

(Beispiele)

NIS-2: Geldbuße mit einem Betrag von mind. **10 Mio. €** oder **2 % des weltweiten Konzernumsatzes** des Vorjahres (je nachdem, was höher ist)

DSGVO: Für die im Gesetz unter Art. 83 Abs. 5 DSGVO aufgelisteten, besonders gravierenden Verstöße beträgt der Bußgeldrahmen bis zu **20 Millionen €** oder im Fall eines Unternehmens bis zu **4% des gesamten weltweit erzielten Jahresumsatzes** im vorangegangenen Geschäftsjahr (je nachdem, was höher ist).

Wichtig: Verletzt die Geschäftsführung die Sorgfaltspflicht, können **Vorstände und Geschäftsführer*innen** verantwortlicher Unternehmen auch **persönlich** mit ihrem **Privatvermögen** haften[1].

[1] Siehe Haftungsnormen Art. 82, 83 Abs. 4 DSGVO

Wirtschaftliche Risiken: Doch nicht nur Geldstrafen drohen bei geringer Datensouveränität. Wenn sensible Daten wie Produktentwicklungen oder Kundenanalysen unkontrolliert verarbeitet oder weitergegeben werden, führt dies auch zum Abfluss von Know-how. Auf diese Weise werden Wettbewerbsvorteile aufs Spiel gesetzt und die souveräne Weiterentwicklung datenbasierter Geschäftsmodelle behindert.

Zusätzliche Kosten können zudem durch Rechtsstreitigkeiten entstehen. Auch Reputationsschäden bei Geschäftspartnern und Kunden können sich negativ auf den wirtschaftliche Erfolg auswirken. Folgemaßnahmen wie nachträgliche Compliance-Maßnahmen oder Datenmigrationen verursachen darüber hinaus zusätzlichen Aufwand. Auch durch den Wechsel des Dienstleisters können Ablösekosten oder Strafgebühren entstehen (Vendor-Lock-in-Effekte).

Alles On-Prem? Maximale Souveränität erreicht man natürlich, wenn man alles lokal betreibt, idealerweise mit Hardware aus verschiedenen geopolitischen Regionen. Das bietet die höchste Flexibilität und Kontrolle, ist aber hinsichtlich Kosten, Personalaufwand, Komplexität und Fehleranfälligkeit suboptimal. Der intelligente Kompromiss besteht darin, einen vertrauenswürdigen Anbieter (oder mehrere) zu wählen, der das gleiche Wertegerüst teilt und im gleichen Rechtsraum agiert (z. B. EU/Deutschland). Der Ansatz ermöglicht es, ganz kritische Geschäftsprozesse (und deren Daten) lokal zu halten und alles andere auszulagern. Dadurch reduziert man Abhängigkeit und nutzt gleichzeitig die Skalierungsvorteile der Cloud.

Bild KI-generiert

Sechs Schritte zur Stärkung der Datensouveränität

Was also tun, um den aktuellen Unsicherheiten zu begegnen? Diese sechs Empfehlungen zeigen auf, wie Unternehmen die Kontrolle über wichtige Daten behalten können, ohne an Handlungsfähigkeit und Innovationskraft zu verlieren.

1 Governance stärken und europäische Cloud integrieren

Zunächst sollte eine **Data-Governance-Richtlinie** eingeführt oder aktualisiert werden, die klar regelt, welche Daten wo unter welchen Bedingungen gespeichert werden dürfen. In diesem Zusammenhang ist es auch wichtig, die Cloud-Dienste hinsichtlich ihres Speicherorts, der Zugriffsmöglichkeiten, der Verschlüsselungstechniken und etwaiger Exit-Strategien zu bewerten. Durch das **Zulassen mehrerer Technologien und Anbieter** werden Abhängigkeiten vermieden, was direkt zu einer Steigerung der **Flexibilität und Sicherheit** führt. Darüber hinaus ist es sinnvoll, europäische Cloud-Angebote, zu prüfen, da diese oft höhere Standards in Bezug auf vertragliche Sicherheit, Datenschutz und Datensicherheit bieten.

2 Verträge prüfen und Datenhoheit sichern

Ein wichtiger Aspekt der Datensouveränität ist die Prüfung und gegebenenfalls Nachbesserung von **Auftragsverarbeitungsverträgen (AVV)** gemäß der DS-GVO. Diese Maßnahme ist sinnvoll, da sie sicherstellt, dass die vertraglichen Regelungen den aktuellen rechtlichen Anforderungen entsprechen und die Kontrolle über die Datenverarbeitung gewährleistet ist.

3 Daten klassifizieren und anforderungsgerecht speichern

Datenschutzklassen sind Kategorien, die Daten nach ihrer Sensibilität und Schutzbedürftigkeit einordnen. Sie legen fest, welche **Sicherheitsmaßnahmen und Zugriffsrechte für unterschiedliche Datentypen** erforderlich sind. Diese Regeln gelten unabhängig vom physischen Speicherort der Daten, was besonders wichtig ist, wenn Daten auch in ausländischen Clouds gespeichert werden. Durch die Klassifizierung kann genau festgelegt werden, welche Art von Daten in welcher Cloud mit welchen Sicherheitsmaßnahmen gespeichert werden darf.

4 Offene Technologien nutzen und Vendor Lock-in vermeiden

Die Nutzung von offenen Standards und Open-Source-Software ermöglicht es, Daten leichter zu einem anderen Anbieter zu migrieren. So bleiben Sie **unabhängig von einzelnen Anbietern** und verhindern ein Vendor Lock-in.

5 Ende-zu Ende verschlüsseln

Die **Datensouveränität** kann in den Cloud-Angeboten großer Anbieter durch **technische Maßnahmen** gestärkt werden. Eine zentrale Rolle spielt dabei die **Ende-zu-Ende-Verschlüsselung**, bei der die **Schlüsselverwaltung** entweder direkt beim Unternehmen oder bei einer vertrauenswürdigen dritten Partei liegt. Dadurch wird sichergestellt, dass **ausschließlich autorisierte Personen** auf die in der Cloud gespeicherten Daten zugreifen können. Diese Technik gewährleistet zudem die **Vertraulichkeit und Integrität** der Daten über ihren gesamten Lebenszyklus hinweg.

6 Clouds dediziert anbinden

Dedizierte Datenverbindungen wie **private Leitungen** oder **direkte Cloud-Anbindungen** stärken die **Datensouveränität**, indem sie die Abhängigkeit vom öffentlichen Internet reduzieren. Diese Verbindungen schaffen eine **isolierte, kontrollierte Umgebung** für den Datentransfer zwischen dem Unternehmen und der Cloud. Das ermöglicht eine **konsistentere Performance** und **eine durchgängige Kontrollierbarkeit** des gesamten Übertragungsweges. So sinkt das Risiko von Abhörversuchen oder unbefugtem Zugriff durch Dritte auf dem Weg zum Cloud-Anbieter.

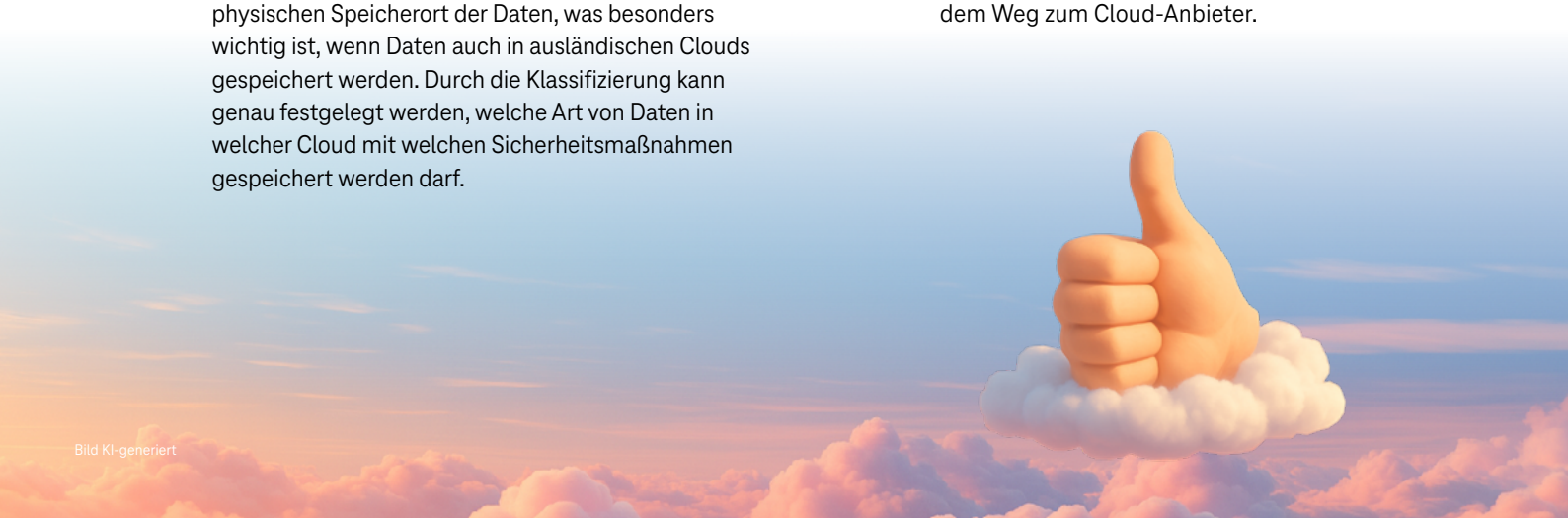

Bild KI-generiert

T Cloud:
Digitale Souveränität made in Europe

Sie möchten die Kontrolle über Ihre digitalen Infrastrukturen, Daten und Technologien eigenständig und nachhaltig ausüben – ohne abhängig von Dritten zu sein, die Ihre Entscheidungs- und Handlungsfähigkeit einschränken? Mit T Cloud bieten wir Cloud-Lösungen aus Deutschland und Europa, die Ihnen volle Souveränität garantieren.

Ihre Daten sind in Sicherheit

- **DSGVO-konforme** Infrastruktur
- **Zero-Trust**-Architektur
- **24/7 Monitoring im Telekom SOC** (Security Operations Center)
- **Einhaltung internationaler Standards** wie ISO, TISAX und HIPAA
- **Exit-Strategien** und **Auditierbarkeit**
- Zertifizierte **europäische Rechenzentren**

Wir sind offen und flexibel

Wir zeigen, wie Daten verarbeitet und geschützt werden – nachvollziehbar und dokumentiert. Dank offener Technologien und europäischer Standards bietet T Cloud volle Gestaltungsfreiheit: Sie können jederzeit den Anbieter wechseln und Daten einfach migrieren. Auch einem Hybrid-Cloud-Ansatz steht nichts im Wege – führende Hyperscaler-Plattformen und Cloud-Infrastrukturen der Telekom können in einem integrierten Ökosystem vereint werden.

T Cloud

T Cloud bündelt alle Cloud-Kompetenzen der Telekom individuell kombinierbar – für digitale Gestaltungsfreiheit, Sicherheit und wirtschaftliche Transformation.

Mehr zum Thema Cloud-Strategie und digitale Souveränität Jetzt herunterladen und nachlesen!

Behalten Sie die Kontrolle!

Jetzt Beratung anfordern

Kontakt
Persönlicher Kundenberater
https://geschaeftskunden.telekom.de

Herausgeber
Deutsche Telekom Geschäftskunden GmbH
Landgrabenweg 149
53227 Bonn

Connecting your world.