Whitepaper

In die Cloud?
Aber souverän!

Cloud never felt more solid.

value – inspired by people

.msg

Datensouveränität in der Cloud

Behalten Sie die Kontrolle über Ihre Daten

Was es braucht, um souverän mit Daten in der Cloud umzugehen

Die Cloud ermöglicht auf vielen Ebenen neue Business-Potenziale und Synergieeffekte. Dennoch steht der Einsatz der Cloud vor einer entscheidenden Herausforderung: der Wahrung der Datensouveränität.

Datensouveränität bedeutet, dass ein Unternehmen jederzeit die vollständige Kontrolle und Hoheit über seine Daten behält – unabhängig davon, wo diese gespeichert oder verarbeitet werden. Doch insbesondere bei sensiblen Daten wird genau diese Kontrolle häufig in Frage gestellt, wenn die Verantwortung für den Betrieb und die Datenhaltung teilweise oder ganz an einen Cloud Provider übertragen wird.

Was können Unternehmen tun, um sicherzustellen, dass sie die volle Kontrolle über ihre Daten in der Cloud behalten? Dieses Whitepaper gibt Antworten darauf und zeigt, warum Datensouveränität in der Cloud so wichtig ist und wie Sie diese erfolgreich in Ihrem Unternehmen umsetzen können.

Inhalt:

Darum ist Datensouveränität in der Cloud so wichtig

Definition:
Datensouveränität, oder auch Datenhoheit, ist ein Teilaspekt der digitalen Souveränität. Sie bezieht sich auf die Fähigkeit von Einzelpersonen, Unternehmen und Organisationen, selbstbestimmt über die eigenen Daten zu verfügen. Im Kern geht es darum, durchgängig Kontrolle und Transparenz über die eigenen Daten zu haben.

Als Voraussetzung für einen souveränen Umgang mit Daten in der Cloud müssen Unternehmen jederzeit auf die Daten zugreifen, sie überwachen sowie bestimmen können, wer Zugang zu den Daten hat und wie sie genutzt werden.

Regulatorische Konformität

Datensouveränität ist entscheidend für die Einhaltung regulatorischer Pflichten, Branchenstandards und ethischer Verpflichtungen. Sie ermöglicht Unternehmen, sich rechtskonform und verantwortungsbewusst im Umgang mit Daten zu verhalten.

Voraussetzung für neue Geschäftsmodelle

Die Fähigkeit, Daten sicher und souverän in unternehmensübergreifenden Ökosystemen auszutauschen, ist die Grundlage für die Entwicklung neuer datenbasierter Geschäftsmodelle, Produkte und Dienstleistungen.

Potenzial von KI nutzen

Damit KI ihr volles Potenzial entfalten kann, müssen Daten verfügbar und souverän verwaltet werden. Datensouveränität stellt sicher, dass die Interessen der Datenbesitzer geschützt bleiben, während Innovationen vorangetrieben werden.

Unabhängigkeit und Flexibilität

Datensouveränität gewährleistet Unabhängigkeit von Cloud Service Providern und ermöglicht es Unternehmen, agil auf neue Marktanforderungen und regulatorische Veränderungen zu reagieren.

Mehr Effizienz

Wenn Daten sicher und kontrolliert verwaltet werden, können sie schneller und gezielter genutzt werden. Dies fördert die Fähigkeit zur Datenanalyse, trägt zur Interoperabilität zwischen Systemen und Anwendungen bei und steigert schließlich die Unternehmenseffizienz.

Gesteigertes Vertrauen

Für viele Kunden und Partner wird die Einhaltung hoher Datenschutzstandards zu einem zentralen Kriterium bei der Auswahl von Dienstleistern. Unternehmen, die ihren Kunden garantieren können, dass deren Daten sicher und im Einklang mit den geltenden Datenschutzbestimmungen verarbeitet werden, gewinnen das Vertrauen im Markt.

Höhere Sicherheit

Das Prinzip der Datensouveränität fördert die Implementierung starker Sicherheitsmaßnahmen. Durch klare Kontrollmechanismen über die Datenverarbeitung und -speicherung können Unternehmen Sicherheitslücken minimieren und sich besser vor Datenverlusten oder Cyberangriffen schützen.

Gesetze und Richtlinien

Wichtige Regularien im Überblick

Diese Gesetze und Richtlinien sollten Sie kennen

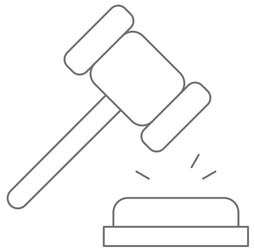
In hochregulierten Branchen wie dem Finanzsektor, der Gesundheitsbranche oder der kritischen Infrastruktur (z. B. Energieversorgung) stehen Unternehmen vor besonderen Herausforderungen, wenn es um den Einsatz von Cloud-Technologien geht. Die geltende und künftige Gesetzgebung in diesen Sektoren legt strenge Anforderungen an den Datenschutz und die Datensouveränität fest, die oft über die generellen Datenschutzgesetze wie die DSGVO hinausgehen.

Wichtige Regelwerke bei der Nutzung von Cloud-Diensten sind unter anderem:

DSGVO (Datenschutz-Grundverordnung):
Die DSGVO bildet das Fundament für den Datenschutz in der EU und legt fest, wie personenbezogene Daten verarbeitet werden dürfen. Sie setzt hohe Standards für den Schutz der Privatsphäre und die Kontrolle über persönliche Informationen. Alle Organisationen und Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, müssen die DSGVO erfüllen.
Sie müssen sicherstellen, dass Cloud-Dienste vollständig den Vorgaben entsprechen, etwa durch Pseudonymisierung, Verschlüsselung und gegebenenfalls durch lokale Speicherung in der EU.

DORA (Digital Operational Resilience Act):
Diese EU-Verordnung soll die operationelle Resilienz von Finanzinstituten und -dienstleistern stärken. Ab 2025 werden Finanzunternehmen in der EU sowie deren IT-Dienstleister verpflichtet sein, strenge Anforderungen an das Risikomanagement und die Informationssicherheit in Bezug auf ihre IT-Systeme und Prozesse zu erfüllen. Dies umfasst das systematische Erkennen von Risiken, Prävention und Schutzmaßnahmen sowie das regelmäßige Testen der digitalen operationalen Resilienz. Dazu gehört auch die Absicherung von Cloud-Diensten, die als kritisch für die Finanzinfrastruktur betrachtet werden.

NIS-2 (Network and Information Systems Directive 2):
Diese EU-Richtlinie ersetzt die ursprüngliche NIS-Richtlinie und erweitert den Geltungsbereich auf weitere kritische Sektoren, einschließlich des Finanzsektors, des Gesundheitswesens und der digitalen Infrastruktur für ein hohes gemeinsames Cybersicherheitsniveau in der EU. Sie stellt Anforderungen unter anderem an die Governance, ein strukturiertes und umfangreiches Risikomanagement oder auch Meldepflichten. Sie gilt für Firmen ab 50 Mitarbeitenden und einem Umsatz von zehn Millionen Euro, die ihre Dienste beziehungsweise Tätigkeiten in der EU ausüben. Als EU-Richtlinie wird diese noch in nationales Recht zu überführen sein. Ein Gesetzesentwurf der Bundesregierung zur Umsetzung der NIS-2-Richtlinie liegt bereits vor.



KRITIS-Verordnung (Kritische Infrastrukturen):
Diese nationale Verordnung resultiert aus dem BSI-Gesetz und zielt auf die Sicherheit und Resilienz kritischer Infrastrukturen ab, wie zum Beispiel Energie, Wasser und Telekommunikation. Für Unternehmen, die als Betreiber kritischer Infrastrukturen gelten, ist Datensouveränität besonders wichtig. Sie müssen spezifische Sicherheitsanforderungen erfüllen und unterliegen strengen Meldepflichten. Dies betrifft auch Cloud-Dienste, die viele Unternehmen in KRITIS-Sektoren nutzen und die daher ebenfalls als kritische Infrastruktur gelten.

Cloud Act:
Der Cloud-Act ist ein US-amerikanisches Gesetz, das US-Behörden befähigt, auf Daten zuzugreifen, die von US-Unternehmen in der Cloud gespeichert werden, auch wenn diese Informationen im Ausland liegen. Dies kann zu Konflikten mit der DSGVO führen, wenn es um den Transfer von Daten in die USA geht.

Es ist wichtig zu beachten, dass die hier genannten Regularien nur eine Auswahl an Vorschriften im Zusammenhang mit der Nutzung von Cloud-Diensten darstellen. Jedes Unternehmen muss individuell, je nach Branche, Unternehmensgröße und spezifischem Anwendungsfall, prüfen, welche rechtlichen Anforderungen für seine Situation relevant sind.

Sprechen Sie gerne mit uns über Ihre Anforderungen. Wir unterstützen Sie dabei, branchenspezifische Vorgaben in die Praxis zu überführen.

Jetzt Kontakt aufnehmen

Datensouveränität

Sieben Kernfragen, um die Kontrolle über die eigenen Daten zu behalten

In die Cloud? Aber souverän!

Das bedeutet Datensouveränität in der Praxis

Datensouveränität in der Cloud ist von zentraler Bedeutung – nicht nur, um gesetzlichen Anforderungen gerecht zu werden, sondern auch um sensible Informationen zu schützen und die operative Kontrolle über kritische Geschäftsdaten zu behalten. Bevor Sie Ihre Daten in die Cloud verlagern, sollten Sie sich deshalb mit folgenden Kernfragen beschäftigen:

1. Wie schützenswert sind Ihre Daten und Prozesse?

Nicht alle Daten und Prozesse sind gleich: Je nach Sensibilität der Daten und ihrer Bedeutung für die Prozessabläufe gelten unterschiedliche Schutzbedarfe. Diese wiederum bilden die Grundlage für die Auswahl der notwendigen technischen und organisatorischen Schutzmaßnahmen. Hierzu zählen beispielsweise Zugriffsrechte und Verschlüsselungstechniken. Die Klassifikation und Bewertung Ihrer Daten und Geschäftsprozesse ist somit der Ausgangspunkt jeglicher Informationssicherheitsmaßnahmen.

2. Haben Sie eine Cloud-Strategie definiert?

Im Rahmen einer Cloud-Strategie sollten Sie festlegen, welche Prozesse und Daten für eine Migration in die Cloud in Frage kommen und welche Rahmenbedingungen einzuhalten sind. Neben der Analyse der Wirtschaftlichkeit sind weitere Themen wie Sicherheit, Datenschutz, Exit-Möglichkeiten und der Ort der Datenhaltung wichtige, zu analysierende Punkte. Diskutieren Sie die Vor- und Nachteile. Finden Sie passgenaue und nachhaltige Lösungen, die auf Ihren Bedarf bzw. Ihr Unternehmen ausgerichtet sind.

3. Haben Sie einzuhaltende Soll-Maßnahmen definiert?

Durch die vorherigen Fragen haben Sie beleuchtet, welche Daten und Prozesse grundsätzlich in die Cloud migriert werden sollen. Zudem kennen Sie den Schutzbedarf dieser Daten und Prozesse. Nun gilt es, festzulegen, welche technischen und organisatorischen Maßnahmen einzuhalten sind, um Ihre Daten ausreichend zu schützen. Hierbei ist darauf zu achten, welche regulatorischen und gegebenenfalls vertraglichen Anforderungen zwingend einzuhalten sind.

Den Rahmen bilden die sogenannten Soll-Maßnahmen. Der Soll-Maßnahmenkatalog kann sich an gängigen Marktstandards orientieren und definiert die Mindestanforderungen, die je nach Schutzbedarf einzuhalten sind. Basierend auf diesen Anforderungen kann auch die Passgenauigkeit von Cloud-Lösungen und Cloud-Dienstleistern bewertet werden.

Wichtige Aspekte in einem Soll-Maßnahmenkatalog sind:

Sicherheitsanforderungen und -Settings

Beispiele:

- Verschlüsselung
- Intrusion Detection / Prevention
- DDoS-Schutz
- Kontrollmöglichkeiten über die Daten und Metadaten wie etwa Rollen und Berechtigungen
- Festlegung von Regionen und Zonen
- Verwaltung von Zugriffsrechten und Löschen von Daten

Anforderungen an das Notfallmanagement

Beispiele:

- Datensicherungs- und -Wiederherstellungsprozesse sowie -zeiten
- Notfallpläne
- Tests der Disaster-Recovery-Szenarien

Datenschutzanforderungen

Beispiele:

- Erfassung der Verarbeitungsprozesse im Verzeichnis der Verarbeitungstätigkeiten (VVT)
- Durchführung von Schwellwertanalysen und Datenschutzfolgeabschätzungen
- Prüfung des Verarbeitungsortes (Inland / Ausland)
- Wenn Daten im Ausland verarbeitet werden: Durchführung und Dokumentation besonderer datenschutzrechtlicher Überprüfungen gemäß DSGVO

Anforderungen an das Auslagerungsmanagement

Beispiele:

- Überprüfung der regulatorischen und institutsindividuellen Anforderungen
- Überprüfung des Dienstleisters und der ggf. eingesetzten Subdienstleister
- Überprüfung der Dienstleistungsgüte

4. Kennen Sie die möglichen Cloud-Lösungen und Cloud-Dienstleister und können diese bewerten?

Schaffen Sie Transparenz durch eine strukturierte Bewertung der Cloud-Dienstleister und Cloud-Dienstleistungen, die für Ihr Vorhaben in Frage kommen – unter anderem von Infrastructure-as-a-Service- bis hin zu Software-as-a-Service-Angeboten. Nutzen Sie die definierten Soll-Maßnahmen, um die passgenauste Marktlösung für Ihre Bedürfnisse und Daten zu finden. Bewerten Sie diese Lösung anschließend innerhalb des Auslagerungsprozesses und überführen Sie bestehende Risiken in den Risikomanagementprozess.

5. Enthalten die Verträge und Service Level Agreements alle relevanten Anforderungen?

Die vertraglichen Anforderungen ergeben sich aus Ihren individuellen Anforderungen (vgl. Punkt 1 bis 4) sowie gegebenenfalls aus gesetzlichen und regulatorischen Vorschriften und Standards. So definiert beispielsweise der Digital Operational Resilience Act (DORA) vertragliche Mindestanforderungen, die von Unternehmen im Finanzsektor einzuhalten sind. Es empfiehlt sich, die wesentlichen vertraglichen Vereinbarungen in einer Vertragsdatenbank zu hinterlegen und die Anforderungen im Zuge des Outsourcing-Prozesses zu managen und zu überwachen.

6. Welche Konfigurationen haben Sie vorgenommen?

Cloud-Dienstleistungen bieten eine Vielzahl an Konfigurationen, die Nutzer beim Aufsetzen vornehmen können. Sie sollten die Konfigurationsmöglichkeiten kennen und eine Standardkonfiguration festlegen. Mit technischen Compliance Scans können Sie die vorgenommenen Konfigurationseinstellungen vor der Produktivnahme oder auch während des Betriebs überprüfen und bei Bedarf anpassen. Orientierung bieten hierbei unter anderem einschlägige Frameworks. Außerdem gibt es Möglichkeiten, Cloud-Konfigurationen automatisiert zu bewerten. Solche Scans können als Bestandteil des Vulnerability Managements prozessual etabliert und langfristig umgesetzt werden.

7. Haben Sie einen Überblick über die Performance des Dienstleisters?

Über die Verträge und Service Level Agreements wurden Mindestanforderungen an die Dienstleistungsgüte definiert. Hierzu sind während des Auslagerungsprozesses sowie der laufenden Steuerung des Dienstleisters Nachweise wie beispielsweise Zertifikate und SLA-Berichte einzuholen und die Performance regelmäßig anhand von Key-Performance-Indikatoren zu bewerten. Dies betrifft sowohl die Dienstleistung als auch den Dienstleister. Auch Audits und Review-Meetings sind Bestandteil des turnusmäßigen Bewertungsprozesses.

Cloud never felt more solid

Souveräne Strategie – auch in der Cloud

Die Kombination aus technologischem Fortschritt, verschärften Sicherheitsanforderungen und strengen Regularien macht es unerlässlich, Cloud-Dienste sorgfältig auszuwählen und umfassende Sicherheits- und Compliance-Strategien zu implementieren, um die Datensouveränität zu gewährleisten.

Eine Cloud-Strategie ist unerlässlich und bildet den Rahmen, um die Kontrolle über die eigene Daten- und IT-Landschaft zu behalten. msg unterstützt Sie bei der Planung, Umsetzung und Überwachung Ihrer Cloud-Transformation. Mit unserem interdisziplinären Team und unserer Expertise in verschiedenen Branchen, berücksichtigen wir alle relevanten Faktoren und mögliche Risiken, damit Sie Ihr Business sicher und souverän in der Cloud betreiben.

Über msg

msg ist eine unabhängige, international agierende Unternehmensgruppe mit weltweit über 10.000 Mitarbeitenden. Sie ist in 31 Ländern vertreten und unterstützt ihre Kunden bei der digitalen Transformation. Zum Leistungsspektrum des im Jahr 1980 gegründeten Unternehmens zählen Business- und IT-Consulting sowie die Entwicklung von Standardsoftware und Individuallösungen für die Branchen Automotive, Banking, Consumer Products, Food, Healthcare, Insurance, Life Science & Chemicals, Manufacturing, Public Sector, Telecommunications, Travel & Logistics sowie Utilities. Die Bandbreite unterschiedlicher Branchen- und Themenschwerpunkte decken im Unternehmensverbund eigenständige Gesellschaften ab. Dabei bildet die msg systems ag den Kern der Unternehmensgruppe.

value – inspired by people

Jetzt Kontakt aufnehmen

Besuchen Sie auch unsere Themenseite:

msg systems ag
Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0
www.msg.group | info@msg.group