Der Weg globaler Regierungsbehörden zur Souveränität

Eine neue Überlebensstrategie für Organisationen des öffentlichen Sektors

Für Organisationen des öffentlichen Sektors außerhalb der USA hat sich digitale Souveränität von einer Checkliste gesetzlicher Anforderungen zu einer Überlebensstrategie entwickelt. Den Regierungsbehörden ist bewusst, dass Souveränität oder Compliance mit Rechtsvorschriften allein nicht ausreichen. Das neue Ziel der digitalen Souveränität wird als strategische Autonomie bezeichnet: die Fähigkeit, kritische Services unabhängig voneinander zu betreiben, zu innovieren und zu warten, auch wenn der externe Support eingestellt oder globale Lieferketten unterbrochen werden.

Laut einem aktuellen Bericht der Konferenz der Vereinten Nationen für Handel und Entwicklung (UNCTAD) „sind 79 % der Länder, die über Gesetze zum Datenschutz verfügen, besorgt um ihre digitale Souveränität.“[1] Regierungen können die Abhängigkeiten, die geschlossenen, proprietären Systemen anhaften, nicht länger ignorieren. Die Transformation hin zu strategischer Autonomie wird von 3 Faktoren beeinflusst:

- **Geopolitisches Risiko:** In Friedenszeiten ist die Abhängigkeit von globalen Hyperscalern vertretbar. In Konfliktszenarien wird die Abhängigkeit von externem Support jedoch zu einer kritischen Schwachstelle. Physische Zerstörung oder Internetausfälle können cloudabhängige Abläufe zum Erliegen bringen. Staaten müssen die Fähigkeit besitzen, unabhängig zu handeln, wenn internationale Zusammenarbeit unmöglich oder unzuverlässig ist. Dies erfordert Systeme, die in DDIL-Umgebungen (Denied, Disrupted, Intermittent, Limited) funktionieren und sicherstellen, dass kritische Funktionen – von Kommando- und Kontrollsystemen für die Verteidigung bis hin zu Notfalldiensten für die Bevölkerung – auch dann weiterhin verfügbar sind, wenn das Land vom globalen Internet abgeschnitten ist.
- **Cyber-Resilienz:** Staatlich organisierte Cyberangriffe werden immer raffinierter, häufiger und wirksamer. Souveränität sorgt dafür, dass kritische Infrastrukturen wie Stromnetze, Gesundheitssysteme und Netzwerke von Verteidigungssystemen gegen externe Eingriffe und Sabotage in der Lieferkette resilient bleiben. Zu diesen Risiken zählen Datendiebstahl, aber auch das Einschleusen von schädlichem Code in Software-Updates während der Übertragung. Regierungsbehörden benötigen die Gewährleistung von Souveränität: die Fähigkeit, die Integrität ihrer Softwarelieferkette unabhängig zu überprüfen, um Spionage zu verhindern und sicherzustellen, dass ihre Systeme nicht kompromittiert wurden.
- **Wirtschaftliche Wettbewerbsfähigkeit:** Regierungsbehörden betrachten die digitale Souveränität zunehmend als einen Eckpfeiler der nationalen Sicherheit. Durch die Lokalisierung der KI-Entwicklung und der Daten-Governance bleiben die Motoren des zukünftigen Wirtschaftswachstums unter nationaler Hoheit und entziehen sich externer Kontrolle. Es bestehen zunehmende Bedenken, dass die Abhängigkeit von ausländischen Black Box-KI-Modellen zu einem Verlust geistigen Eigentums und kultureller Relevanz führt. Strategische Autonomie ermöglicht Staaten die Entwicklung dieser digitalen Fähigkeiten, fördert lokale Innovationsnetzwerke und stellt sicher, dass der durch die digitale Transformation generierte Wert in der nationalen Wirtschaft verbleibt.

1 „Data protection and privacy legislation worldwide.“ UNCTAD, 17. Feb. 2026

Globale Nachfrage, regionale Gegebenheiten

Obwohl der Bedarf an Kontrolle global ist, unterscheiden sich die spezifischen Auswirkungen und Hindernisse, mit denen der globale öffentliche Sektor konfrontiert ist, je nach Region erheblich.

Europa, Naher Osten, Afrika und Kanada (EMEA)

Die größte Herausforderung in der EMEA-Region ist das Spannungsverhältnis zwischen dem Bedarf an fortschrittlicher Technologie und der Abhängigkeit von Anbietern außerhalb der Europäischen Union (EU), was Regierungsbehörden einem Rechtshoheitsrisiko aussetzt, insbesondere durch extraterritoriale Gesetze wie die der USA, darunter der „Clarifying Lawful Overseas Use of Data (CLOUD) Act" oder der „Foreign Intelligence Surveillance Act" (FISA) von 1978.

Europäische Behörden sind mit einem komplexen Netz aus strengen Verordnungen konfrontiert, darunter die NIS-2-Richtlinie der EU für Cybersicherheit und der „Digital Operational Resilience Act" (DORA) für operative Resilienz sowie nationale Vorgaben wie SecNumCloud in Frankreich. Die Verteidigungsinfrastruktur ist nach wie vor fragmentiert, und Interoperabilitätslücken bei der NATO verzögern den Datenaustausch. Darüber hinaus gibt es in den Ländern einen kritischen Mangel an Personal mit Sicherheitsfreigabe zum Betrieb souveräner Umgebungen. Obwohl Kanada geografisch in Nordamerika liegt, bestehen auch dort die EMEA-typischen Herausforderungen in Bezug auf veraltete Infrastruktur. Das kanadische Verteidigungsministerium hat mit einem uneinheitlichen Patchwork der Consolidated Secret Network Infrastructure (CSNI) und behördenübergreifenden Hürden zu kämpfen, die eine Einführung moderner Funktionen verlangsamen. Das Risikoniveau führt dazu, dass Regierungsbehörden sensible Daten vor rechtlichen Eingriffen aus dem Ausland isolieren und die Softwarelücke durch den Aufbau interner Kapazitäten schließen.

Asien-Pazifik (APAC)

Die APAC-Region ist geprägt von strengen protektionistischen Vorgaben und hohen Compliance-Anforderungen, um technologische Eigenständigkeit zu erreichen.

- **Datenlokalisierung:** Länder wie China, Indien und Indonesien setzen eine strikte Datenlokalisierung durch. Kritische Daten müssen sich dabei vollständig innerhalb der nationalen Grenzen befinden, was die Nutzung globaler Public Clouds einschränkt.
- **Hohe Verantwortlichkeit:** In Singapur bestehen strenge End-to-End-Sicherheitsstandards, nach denen Verantwortliche bei Datenmissbrauch oder -verlust strafrechtlich verfolgt werden können, was zu einer risikoaversen Beschaffungskultur führt.
- **Globale und lokale Anforderungen:** Es besteht eine starke Präferenz für globale und lokale Modelle (glokal), also Partnerschaften, bei denen globale Technologie über lokale Unternehmen bereitgestellt wird, um für souveräne Kontrolle zu sorgen.

Ein Schwerpunkt der APAC-Länder ist die Entwicklung nativer Funktionen zur Verringerung der langfristigen Abhängigkeit von fremden Märkten, wobei die digitale Souveränität als Schutz vor geopolitischen Schwachstellen betrachtet wird.

Lateinamerika (LATAM)

Modernisierungen in der LATAM-Region werden durch operative Kontinuität beeinflusst und oft eher durch strukturelle Instabilität als durch Richtlinien behindert.

- **Instabilität und Diskontinuität:** Häufige Wechsel in der politischen Führung und wirtschaftliche Unsicherheit gefährden langfristige IT-Planungen und mehrjährige Beschaffungsverträge in einem unsicheren geopolitischen Umfeld.

- **Fokus auf interne Sicherheit:** Die Verteidigungsbehörden in Lateinamerika priorisieren interne Sicherheit (Grenzschutz, Drogenbekämpfung) und bevorzugen agile Überwachungstools statt einer komplexen strategischen Infrastruktur. [2]
- **Risiken bei der Beschaffung:** Ineffizienzen und Korruptionsrisiken im öffentlichen Beschaffungswesen mindern den tatsächlichen Wert von Technologiebudgets und führen zu einem Bedarf an kosteneffizienten, offenen und flexiblen Systemen, die Budgetkürzungen und politische Veränderungen überstehen, ohne dass das Land sich an teure und starre proprietäre Anbieter bindet.

Ein Ansatz von Red Hat für digitale Souveränität

Globale Behörden müssen sich mit der Souveränität in diesen unterschiedlichen Dimensionen befassen, um erfolgreich zu sein. Red Hat stellt die Tools und das IT-Ökosystem für jede einzelne davon bereit.

Datensouveränität und KI

Red Hat kennt die Kriterien der vollständigen Kontrolle und Autonomie über kritische Daten und KI-Modelle und stellt sicher, dass die Daten innerhalb der nationalen Grenzen gespeichert sind und Governance im Einklang mit den lokalen Gesetzen besteht. Behörden müssen souveräne KI-Strategien implementieren, die das Eigentumsrecht an ihren Modellen und Trainingsdaten wahren und diese auf einer lokalisierten Infrastruktur bereitstellen, anstatt sich auf den API-Zugriff auf im Ausland kontrollierte Modelle zu verlassen. Red Hat® OpenShift® AI ermöglicht den Einsatz souveräner KI-Funktionen dort, wo sich die Daten befinden. Wir ermöglichen die Kontrolle über Datenspeicherort und Datenzugriff, indem wir Confidential Computing zum Schutz der verwendeten Daten einsetzen und die Compliance mit Verordnungen wie dem KI-Gesetz der EU sicherstellen.

Technologische Souveränität

Die Fähigkeit, Workloads unabhängig von der Infrastruktur eines bestimmten Anbieters oder proprietärer Software auszuführen, ist nötig, um langfristige Unabhängigkeit und die Möglichkeit zu gewährleisten, Anwendungen ohne Einschränkungen zu verschieben. Regierungsbehörden sollten Vendor Lock-in vermeiden und offene Standards sowie portierbare Container-Plattformen einführen. Wenn sich die Richtlinien eines Cloud-Anbieters ändern oder geopolitische Spannungen zunehmen, können Workloads ohne Refactoring zu einer anderen Infrastruktur migriert werden. Red Hat reduziert Vendor Lock-in durch Open Source-Standards. Unsere Plattform unterstützt verschiedene Hardware-Architekturen (x86, Advanced RISC Machine (ARM), RISC-V), sodass nationale Systeme ohne externe Abhängigkeiten nach ihrem eigenen Zeitplan weiterentwickelt und aktualisiert werden können.

Operative Souveränität

Regierungsbehörden müssen die volle administrative Autorität und Unabhängigkeit über ihre kritischen IT-Abläufe bewahren, um auch bei einer Unterbrechung der Verbindung funktionieren zu können. Verteidigung und kritische Infrastrukturen müssen operative Resilienz priorisieren. Dazu gehört die Automatisierung von Disaster Recovery-Plänen, die die Bedingungen eines Konflikts berücksichtigen, sowie die Sicherstellung, dass Support und Operationen von Personen mit Sicherheitsfreigabe verwaltet werden. Red Hat bietet beispielsweise einen bestätigten souveränen Support, technischen Support durch überprüfte Bürgerinnen und Bürger vor Ort (beispielsweise innerhalb der EU) und stellt sicher, dass keine Daten, auf die Support-Mitarbeiter Zugriff haben, den Zuständigkeitsbereich verlassen. Zusätzlich automatisiert Red Hat Ansible® Automation Platform die Resilienz und ermöglicht eine schnelle Wiederherstellung und Patching selbst in nicht verbundenen (DDIL-)Umgebungen.

Sicherheitssouveränität

Die unabhängige Überprüfung der Integrität, Sicherheit und Zuverlässigkeit digitaler Systeme und Prozesse hilft Behörden bei der Einhaltung von Vorschriften. Behörden müssen von blindem Vertrauen zu überprüfbarem Vertrauen übergehen. Dieser Schritt erfordert eine strenge Prüfung

2 „New Pentagon strategy to focus on homeland, Western Hemisphere." DefenseNews, 25. Sept. 2025

der Softwarelieferkette sowie die Möglichkeit, Compliance mit Standards wie Common Criteria, FIPS (Federal Information Processing Standards) und NIS-2 nachzuweisen. Red Hat bietet eine vertrauenswürdige Softwarelieferkette mit kryptografisch signierter Software mit verifizierter Herkunft sowie einer Software Bill of Materials (SBOM), mit der Behörden sämtliche Komponenten prüfen und sicherstellen können, dass kein bösartiger Code eingeschleust wurde. Diese Sicherheitsmaßnahmen tragen dazu bei, dass die Behörden neue Anforderungen wie die des EU Cyber Resilience Act erfüllen.

Strategische Autonomie durch Open Source

Red Hat nutzt eine flexible, offene Basis zur Bewältigung von Herausforderungen und bietet Regierungsbehörden mehr Auswahlmöglichkeiten und Kontrolle statt starrer Isolierung. Dieser flexible Ansatz berücksichtigt, dass ein einzelner Anbieter selten digitale Souveränität gewährleisten kann. Red Hat bietet die Möglichkeit, eine souveräne Cloud über verschiedene Infrastrukturanbieter und Cloud-Zonen hinweg aufzubauen und vermeidet so die Einschränkungen einer einzelnen Lösung.

Seit mehr als 30 Jahren stellt Red Hat bewährte, unternehmensgerechte Open Source-Lösungen für Organisationen mit strengen Sicherheits- und Compliance-Anforderungen bereit. Open Source-Software für Unternehmen ist nicht nur eine Technologie, sondern eine grundlegende Architekturbasis, mit der Regierungsbehörden digitale Souveränität und strategische Autonomie erreichen können. Im Gegensatz zu proprietären Anbietern, die auf geschlossene, undurchsichtige Systeme setzen und blindes Vertrauen erfordern, hilft Red Hat Behörden dabei, die vollständige Kontrolle über ihre digitale Zukunft zu behalten, anstatt sich auf andere zu verlassen. Dieser offene Ansatz hilft dem öffentlichen Sektor weltweit, das Tempo globaler Innovationen zu steuern – vom taktischen Edge des Netzwerks bis hin zu souveräner KI – und gleichzeitig sicherzustellen, dass Workloads portierbar und resilient bleiben. Ein Open Source-Ansatz schützt auch geschäftskritische Abläufe vor den Risiken bei Vendor Lock-in und technologischer Veralterung. Durch den Einsatz von Open Source-Technologie orientiert sich Red Hat an der standardmäßig offenen Grundhaltung, die in Regionen wie der EU vorherrscht. Die Verwendung eines solchen Modells verhindert die Abhängigkeit von einem einzigen Anbieter und ermöglicht Überprüfungen und Änderungen des Codes, was für nationale Sicherheit und Vertrauen unerlässlich ist.

- **Transparenz und Vertrauen**

  Das Open Source-Modell von Red Hat bietet 100-prozentige Transparenz und ermöglicht es Regierungsbehörden, den Quellcode, die Sicherheit und die Softwarelieferketten zu prüfen. Diese Prüfbarkeit ist entscheidend für das Erfüllen der Sicherheitsanforderungen in den EMEA- und APAC-Regionen. Darüber hinaus stellt Red Hat kryptografisch signierte Software mit verifizierter Herkunft bereit, um neue Anforderungen wie die des EU Cyber Resilience Act zu erfüllen.

- **Operative Souveränität und lokaler Support**

  Zur Vermeidung von Risiken im Zusammenhang mit rechtlichen Fragen unterstützt Red Hat die Möglichkeit, zu steuern, wer die Infrastruktur betreibt, um operative Souveränität zu erreichen.

  - **Souveräner Support:** Wie bereits erwähnt, bietet Red Hat bestätigten souveränen Support in der EU und stellt sicher, dass der technische Support ausschließlich von überprüften EU-Bürgern innerhalb der EU bereitgestellt wird. Mit diesem technischen Support wird sichergestellt, dass keine Daten, auf die die Support-Teams Zugriff haben, die Region verlassen.
  - **Lokale IT-Ökosysteme:** Ein Netzwerk von Red Hat Partnern mit lokalen, zertifizierten Cloud-Anbietern stellt souveräne Cloud-Funktionen bereit, die strenge nationale Vorschriften einhalten.

- **Technologische Unabhängigkeit**

  Eine Open Hybrid Cloud-Strategie ermöglicht die Ausführung von Workloads in vielen Umgebungen, wie On-Premise, in einer Private Cloud, am taktischen Edge des Netzwerks oder in einer Air Gap-Umgebung.

- **Portierbarkeit:** Hierbei handelt es sich um die Basis für die Vermeidung von Vendor Lock-in, ein wichtiger Aspekt für Regierungsbehörden, insbesondere in Regionen wie LATAM und APAC. Die Fähigkeit dieser Regionen, Workloads und Daten effizient zu migrieren, ist eine entscheidende Voraussetzung für die Servicekontinuität und die effiziente Reaktion auf geopolitische Veränderungen, wie etwa politische oder wirtschaftliche Änderungen, die einen Wechsel des Technologieanbieters erforderlich machen können.
- **Isolierte Abläufe:** Lösungen von Red Hat wie Red Hat Device Edge und Red Hat OpenShift ermöglichen Verteidigungsbehörden den autonomen Betrieb in nicht verbundenen DDIL-Umgebungen. So ist das Weiterführen der Abläufe auch dann gesichert, wenn eine zentrale Cloud nicht erreichbar ist.

Red Hat bietet Regierungsbehörden die offene Basis, eine souveräne Cloud zu entwickeln, die Unsicherheit überstehen, zuverlässige Datensicherheit bieten und den Staat arbeitsfähig halten kann.

- **Souveräne KI**

  Während Regierungen die Nutzung von KI ausweiten, bietet Red Hat die Plattform für die Entwicklung souveräner KI. Dies stellt sicher, dass Staaten das Eigentum an ihren Modellen und Trainingsdaten behalten und diese auf lokalisierter Infrastruktur bereitstellen können, um Verordnungen wie das KI-Gesetz der EU einzuhalten, anstatt sich auf den API-Zugriff auf im Ausland kontrollierte Modelle zu verlassen.

Warum Red Hat für den öffentlichen Sektor?

Red Hat ist ein bewährter Partner des öffentlichen Sektors, der in 100 % der US-Ministerien[3] zum Einsatz kommt und in der NATO sowie in Verteidigungsministerien auf der ganzen Welt weit verbreitet ist. Das Lizenzmodell von Red Hat und die Verpflichtung zu offenen Standards stellen sicher, dass Behörden niemals auf Dauer an einen Anbieter gebunden sind. Organisationen behalten das Recht, Software auf unbestimmte Zeit zu nutzen und zu warten. So werden ihre langfristigen Investitionen vor sich ändernden Anbieter-Roadmaps oder geopolitischen Einschränkungen geschützt.

Bei steigenden Ausgaben, insbesondere im Verteidigungssektor, kann eine Investition in das Lösungs- und Serviceportfolio von Red Hat einen sichtbaren ROI erzielen. Die zugesagten Ausgaben der NATO-Mitglieder werden sich verdoppeln und 2035 5 % des nationalen BIP ausmachen.[4] Durch die Standardisierung auf eine einheitliche Plattform können Behörden ihre Investitionen von der Wartung fragmentierter konventioneller Systeme auf die Entwicklung neuer Einsatzfähigkeiten verlagern. So können sie die Betriebs- und Gesamtkosten erheblich senken.

Nächste Schritte für den Einstieg

- Erfahren Sie mehr über Red Hat im globalen öffentlichen Sektor, und sprechen Sie mit Red Hat.
- Möchten Sie Ihre Bereitschaft zur digitalen Souveränität einschätzen? Lesen Sie diesen Blog-Beitrag, um anzufangen.

3 Red Hat Kundendaten, Sept. 2025

4 „Defence expenditures and NATO's 5% commitment." NATO, 18. Dez. 2025

Über Red Hat

Red Hat, weltweit führender Anbieter von Open Source-Softwarelösungen für Unternehmen, folgt einem Community-basierten Ansatz, um zuverlässige und leistungsstarke Linux-, Hybrid Cloud-, Container- und Kubernetes-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Entwicklung cloudnativer Anwendungen, der Integration neuer und bestehender IT-Anwendungen sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. Als bewährter Partner der Fortune 500-Unternehmen stellt Red Hat vielfach ausgezeichnete Support-, Trainings- und Consulting-Services bereit, die unterschiedlichen Branchen die Vorteile der Innovation mit Open Source erschließen. Als Mittelpunkt eines globalen Netzwerks aus Unternehmen, Partnern und Communities unterstützt Red Hat Unternehmen bei der Steigerung ihres Wachstums und auf ihrem Weg in die digitale Zukunft.

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
#3613114_0326

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549