



Whitepaper **Digitale Souveränität** Innovation nutzen und Kontrolle behalten



Inhalt

Digitale Souveränität – eine Schlüsselfrage unserer Zeit	3
Digitale Souveränität im Experten-Check: Interview mit Prof. Dr. Matthias Stürmer	6
Wichtige Hebel für digitale Souveränität: Datenspeicherung und -verschlüsselung	8
Digitale Souveränität im Experten-Check: Interview mit David Rosenthal	11
Fazit: Souverän ist, wer handlungsfähig bleibt	12

Digitale Souveränität – eine Schlüsselfrage unserer Zeit

Digitale Technologien prägen nahezu alle Lebens- und Wirtschaftsbereiche. Staatliches Handeln, wirtschaftliche Wertschöpfung und gesellschaftlicher Alltag basieren auf digitalen Infrastrukturen. Gleichzeitig wird der globale Technologiemarkt von wenigen grossen Anbietern dominiert. Diese treiben Innovationen voran, schaffen aber auch Abhängigkeiten. Deshalb rückt die digitale Souveränität zunehmend in den Fokus.

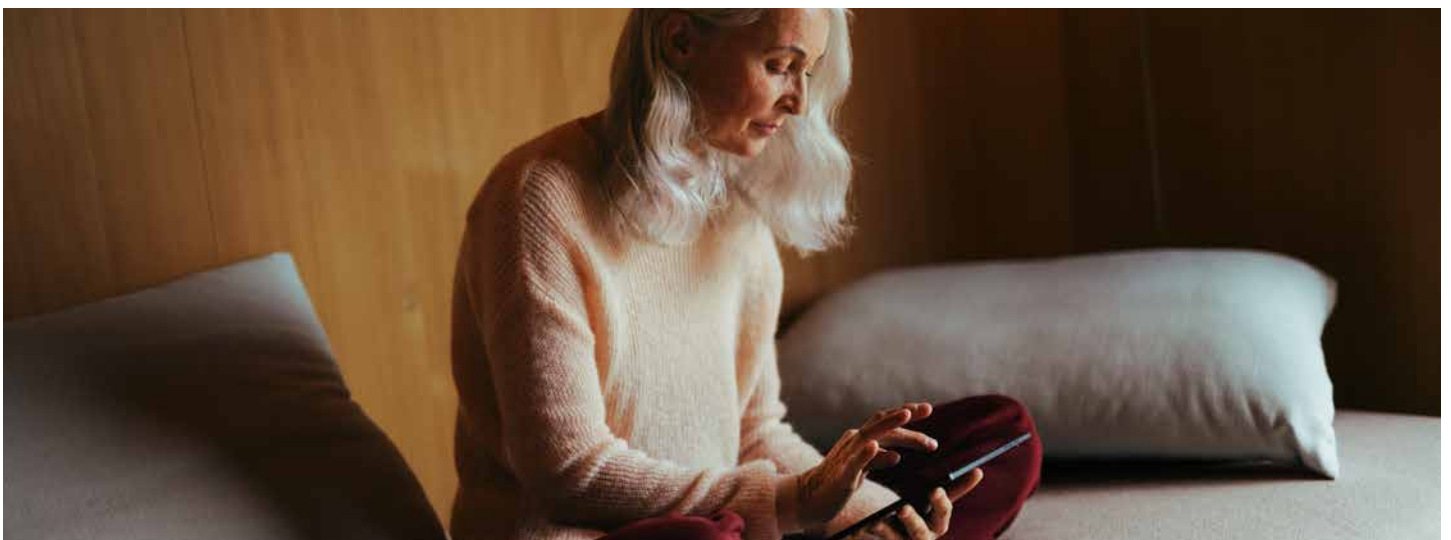
Dabei ist klar: Die digitalen Möglichkeiten sind für Unternehmen und die Gesellschaft nicht mehr wegzudenken. Auch ein vollständiger Verzicht auf ausländische Lösungen ist im globalisierten Markt weder realistisch noch zielführend.

Dieses Whitepaper stellt daher die Frage nach der Balance: Wie können Behörden, Unternehmen und Organisationen von Innovation profitieren und gleichzeitig die Kontrolle über ihre Daten, Systeme und digitalen Ressourcen behalten? Oder kurz: Wie gelingt digitale Souveränität in einer globalisierten und vernetzten Welt?

Swiss Post Digital – für eine starke digitale Schweiz

Für die Schweizerische Post bedeutet digitale Souveränität, Innovation zu nutzen und gleichzeitig die Kontrolle über Daten, Sicherheit und kritische Prozesse zu behalten. Entscheidend ist, dass Organisationen ihre Risiken verstehen, Abhängigkeiten bewusst steuern und jederzeit handlungsfähig bleiben. Die Schweizerische Post bietet verschiedene Lösungen für die sichere digitale Kommunikation, anschlussfähige Softwarelösungen und Cybersecurity Services. Offene Lösungsarchitekturen, Datenschutz und modernste Verschlüsselungsmethoden stellen die digitale Souveränität der Lösungen der Schweizerischen Post sicher.

Darüber hinaus engagiert sich die Schweizerische Post im Netzwerk «SDS – Souveräne Digitale Schweiz» sowohl im Beirat als auch in verschiedenen Netzwerkaktivitäten, um den Austausch zu fördern und die digitale Souveränität in der Schweiz mitzugestalten.



Vom Schlagwort zur praxisnahen Definition

Eine einheitliche Definition von digitaler Souveränität gibt es bislang nicht. Je nach Perspektive umfasst der Begriff unterschiedliche Erwartungen an Technologie, Daten und Infrastruktur. Einigkeit besteht darin, dass digitale Souveränität die Fähigkeit beschreibt, digitale Technologien selbstbestimmt zu nutzen und die Kontrolle über Daten, Systeme und digitale Prozesse zu behalten.

Der Bundesrat definiert digitale Souveränität wie folgt: «Digitale Souveränität bedeutet, als Staat über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung staatlicher Aufgaben sicherzustellen.»¹

Entdecken Sie im Whitepaper weitere konkrete Lösungen für eine effiziente und sichere Digitalisierung.

IncaMail

IncaMail ist der sichere E-Mail-Verschlüsselungsdienst der Schweizerischen Post. Mit IncaMail können Unternehmen, Behörden und Privatpersonen vertrauliche Informationen und Dokumente verschlüsselt, nachvollziehbar und datenschutzkonform (DSG- und DSGVO-konform) per E-Mail versenden.



- Die Infrastruktur, über die der gesamte Empfang und die Weiterleitung von IncaMails an die Empfänger läuft, wird in der Schweiz betrieben.
- Das Kundenportal, über das IncaMails auch online abgefragt werden können, ist in der Cloud gehostet. Es findet jedoch keine Datenhaltung in der Cloud statt. Jede Abfrage läuft über die lokale Infrastruktur, die verschlüsselt ist.



¹ Bundesrat (2025): Digitale Souveränität der Schweiz. Bericht des Bundesrates in Erfüllung des Postulats 22.4411 Z'graggen, «Digitale Souveränität der Schweiz», Bern, 26. November 2025, Kapitel 5.1 Definition.

Vier Prinzipien stützen die digitale Souveränität

Mit offenen Lösungsarchitekturen können Organisationen Abhängigkeiten vermeiden, um jederzeit handlungsfähig zu bleiben. Vier Prinzipien dienen als Handlungsanleitung:

1 Kritische Daten identifizieren

Daten sollten nach Schutzbedarf und regulatorischen Anforderungen klassifiziert werden. Nicht alle Informationen benötigen dieselben Schutzmassnahmen. Besonders bei der Nutzung von Cloud-Diensten ist eine differenzierte Betrachtung entscheidend.

2 Daten wirksam schützen

Eine starke Verschlüsselung, eigenes Schlüsselmanagement, Zero-Trust-Architekturen sowie klare Zugriffs- und Berechtigungskonzepte bilden die Grundlage für den Schutz von Daten.

3 Handlungsalternativen schaffen

Wer Exit-Szenarien einplant, Abhängigkeiten von einzelnen Anbietern reduziert und auf offene Schnittstellen sowie Standards setzt, bleibt handlungsfähig.

4 Kompetenzen im Unternehmen stärken

Digitale Souveränität entsteht nicht allein durch Technologie. Entscheidend sind Mitarbeitende und Führungskräfte, die Chancen, Risiken und Abhängigkeiten verstehen und fundierte Entscheidungen treffen können.

Der Digitale Brief



Die Post stellt eine Infrastruktur für den digitalen Versand und Empfang von Briefen bereit und bringt damit das Briefgeheimnis ins digitale Zeitalter. Der Digitale Brief gehört seit 2026 zum Grundversorgungsauftrag der Post.

- Der Digitale Brief wird in der Schweiz verarbeitet. Die moderne Cloud-Infrastruktur ermöglicht die sichere Verarbeitung grosser Sendungsvolumen und einen hohen Schutz vor Cyberrisiken. Dank separatem Schlüsselmanagement hat der Cloud-Anbieter keinen Zugriff auf die Briefinhalte.
- Ist der Brief zugestellt, ist er nur für die Empfängerin oder den Empfänger lesbar. Weder die Post noch Dritte haben die Möglichkeit, auf die Briefinhalte zuzugreifen.
- Die Plattform erfüllt die Vorgaben der Postverordnung, wurde einer Datenschutz-Folgenabschätzung beim EDÖB unterzogen und von der PostCom geprüft.

Digitale Souveränität im Experten-Check:

Interview mit Prof. Dr. Matthias Stürmer

Zwei Experten, zwei Perspektiven: Prof. Dr. Matthias Stürmer und David Rosenthal ordnen ein und teilen ihren Blick auf Chancen, Risiken und Handlungsoptionen. Das Interview mit Matthias Stürmer lesen Sie nachstehend, jenes mit David Rosenthal auf Seite 11.

Herr Stürmer, Kritiker sagen, Souveränität klinge nach Abschottung. Wo endet Souveränität und wo beginnt Autarkie?

Wir leben in einer vernetzten Gesellschaft, und es wäre weder sinnvoll noch realistisch, alles selbst herstellen oder betreiben zu wollen. Digitale Souveränität bedeutet keine Abschottung, sondern Unabhängigkeit und Entscheidungsfreiheit. Wichtig ist konkret die Wechselfähigkeit bei den Lieferanten, denn sie führt letztlich zu mehr Wettbewerb und Innovation. Hier haben wir in der Schweiz und generell in der Informatikbranche einen grossen Aufholbedarf. Eine Veränderung ist möglich, wenn wir dies konkret angehen.

Welche Fragen sollten sich Behörden und Organisationen deshalb heute stellen?

Eine zentrale Frage lautet: Wie können wir die Abhängigkeit von IT-Firmen, also den sogenannten «Vendor Lock-in», reduzieren? Das fängt damit an, sich über den Schweizer Markt für IT-Dienstleister zu informieren. Oftmals besteht das Vorurteil, dass nur die bekannten amerikanischen IT-Anbieter die gefragten Cloud Services anbieten. Wenn man sich jedoch umschaut, stellt man fest, dass wir auch hierzulande viele kompetente, innovative IT-Firmen haben.

Ein häufiges Argument lautet, Hyperscaler seien beim Thema Cybersicherheit überlegen. Wie sehen Sie das?

Grossen Anbietern stehen zweifellos mehr Ressourcen zur Verfügung. Gleichzeitig sind sie aber auch ein attraktiveres Angriffsziel. Gelingt

«Digitale Souveränität bedeutet nicht Abschottung, sondern Entscheidungsfreiheit»

ein Angriff, sind potenziell sehr viele Daten betroffen. Cybersicherheit ist kein Argument für oder gegen einen Anbieter – sie ist eine Daueraufgabe für alle. Behörden, Unternehmen und kleinere Anbieter arbeiten hier letztlich am selben Ziel.

Sind andere Länder weiter als die Schweiz, wenn es um digitale Souveränität geht?

Ja. Deutschland investiert seit Jahren gezielt in unabhängige Cloud-Lösungen und Open-Source-Software und hat mit dem ZenDiS ein eigenes Zentrum für digitale Souveränität aufgebaut, das openDesk als M365-Alternative anbietet. Auch Frankreich verfolgt mit «LaSuite» einen mutigen staatlichen Ansatz, um digitale Souveränität konkret umzusetzen. In der Schweiz herrscht oft noch die Haltung, dass nur grosse Big-Tech-Konzerne gute IT-Dienstleistungen erbringen können.

Was muss die Schweiz in den nächsten drei Jahren konkret tun, um digital souveräner zu werden?

Wir brauchen ein nationales Zentrum für digitale Souveränität. Eine Stelle, die Fachwissen bündelt, Behörden berät und den Know-how-Transfer

sicherstellt. Mit der Gründung des Zentrums «SDS – Souveräne Digitale Schweiz» haben wir an der BFH hier einen ersten Schritt unternommen. Der Bedarf ist enorm: Ich erhalte täglich Anfragen aus Verwaltung, Politik und Organisationen. Der politische Druck wächst spürbar, von links bis rechts. Jetzt braucht es Investitionen in die Grundlagen und eine koordinierte Umsetzung.



Über den Experten:

Prof. Dr. Matthias Stürmer ist Leiter des Instituts Public Sector Transformation an der Berner Fachhochschule (BFH) und Dozent am Institut für Informatik der Universität Bern. Er gilt als einer der bekanntesten Schweizer Experten für digitale Souveränität, Open Source und Digitalisierung von Staat und Gesellschaft.

Tresorit SecureCloud



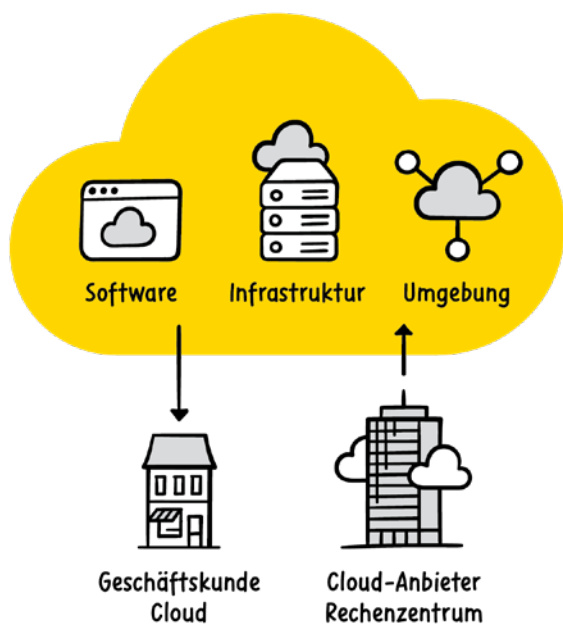
Als Baustein digitaler Souveränität zeigt sich Datensouveränität besonders dort, wo Daten geteilt und gemeinsam bearbeitet werden. Ob bei der Zusammenarbeit mit Teams, Kunden und Partnern oder beim sicheren Austausch sensibler Dokumente: Mit Lösungen wie Tresorit SecureCloud gestalten Unternehmen die digitale Zusammenarbeit sicher und effizient und behalten gleichzeitig die Hoheit über ihre Daten, Zugriffsrechte und Speicherorte.

- Ende-zu-Ende-Verschlüsselung stellt sicher, dass ausschliesslich berechnete Personen auf Inhalte zugreifen können. Die Zero-Knowledge-Architektur gewährleistet, dass Unternehmen die Kontrolle über ihre kryptografischen Schlüssel behalten.
- Damit Unternehmen ihre individuellen regulatorischen und organisatorischen Anforderungen erfüllen können, stehen flexible Optionen zur Datenresidenz in der EU, der Schweiz und weiteren Regionen zur Verfügung.

Wichtige Hebel für digitale Souveränität:

Datenspeicherung und -verschlüsselung

Digitale Plattformen, Datenanalysen und künstliche Intelligenz – die Entwicklung und der Betrieb digitaler Lösungen erfordern leistungsfähige Infrastrukturen. Über Cloud-Dienste können Organisationen Rechenleistung, Speicherplatz und Software flexibel als Dienstleistung beziehen. Dadurch erhalten sie Zugang zu modernsten Technologien, können Innovationen schneller umsetzen und den Einsatz nach Bedarf skalieren.



Civetica Cloud



Civetica ist die E-Government-Plattform der Post, die kommunale Verwaltungsprozesse durchgängig in einer einheitlichen, sicheren und kontrollierten Umgebung vereint. Sie ersetzt isolierte Einzellösungen durch eine integrierte Gesamtlösung. Rund 20 Prozent der Schweizer Gemeinden setzen auf die ERP-Lösung Civetica.

- Civetica Cloud speichert Daten ausschliesslich in Rechenzentren in der Schweiz.
- Die Lösung gewährleistet eine kontrollierte Datenlokalisierung und einen Ansatz, der auf die Souveränitätsanforderungen von Schweizer Organisationen abgestimmt ist.

Cloud ist nicht gleich Cloud

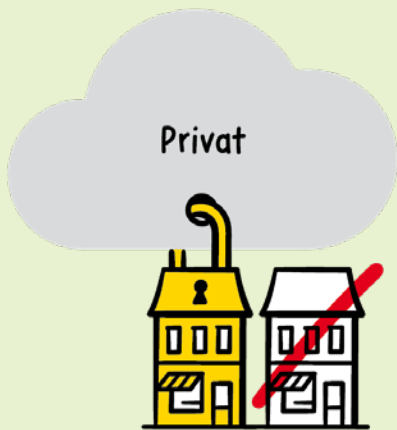
Im Zusammenhang mit Cloud-Diensten und Digitaler Souveränität steht die Frage im Zentrum: Wer kann auf die Cloud-Infrastruktur zugreifen und wie sind die Daten in der Cloud geschützt?

Je nach Anforderungen und regulatorischen Rahmenbedingungen sind unterschiedliche Cloud-Umgebungen zu empfehlen. Auch die Verschlüsselung der Daten und das Schlüsselmanagement sind entscheidend.

Welche Cloud-Dienste gibt es?

Privat

Eine dedizierte Cloud-Umgebung, die nur von einer Organisation genutzt wird. Sie kann entweder im eigenen Rechenzentrum oder von einem externen Drittanbieter betrieben werden und bietet erhöhte Kontrolle und Sicherheit.



Mischform

Kombination aus öffentlicher und privater Cloud, bei der Daten und Anwendungen je nach Anforderungen zwischen beiden Umgebungen migriert werden können.



Öffentlich

IT-Ressourcen werden von einem externen Drittanbieter über das öffentliche Internet bereitgestellt und von mehreren Kunden gemeinsam genutzt.



Sicherheit für Ihre Daten

Kann der Anbieter die in der Cloud gespeicherten Daten einsehen? Werden sensible Daten in einer Cloud-Umgebung verarbeitet, sollten organisatorische und technische Massnahmen sicherstellen, dass nur berechtigte Stellen Zugriff auf die Daten haben. Der Cloud-Anbieter kann durch ein getrenntes Schlüsselmanagement explizit vom Zugriff ausgeschlossen werden.

Folgende Massnahmen schützen Daten und Dienste in der Cloud:

- **Eigenes Schlüsselmanagement:** Die Organisation verwaltet die Verschlüsselungsschlüssel selbst und behält dadurch die Kontrolle über den Zugriff auf die Daten.
- **Datenverschlüsselung:** Daten bleiben während Speicherung und Übertragung geschützt und sind für Dritte nicht lesbar.
- **Zugriffs- und Berechtigungskonzepte:** Nur autorisierte Personen erhalten Zugriff auf Systeme und Informationen.
- **Kontinuierliche Risiko- und Sicherheitsprüfungen:** Regelmässige Assessments stellen sicher, dass Sicherheits-, Datenschutz- und Compliance-Anforderungen eingehalten werden.

Souveränität mit globalem Cloud-Dienstleister?

Globale Grossunternehmen spielen eine zentrale Rolle am Cloud-Markt. Sie betreiben weltweit verteilte Infrastrukturen und investieren jährlich hohe Beträge in Sicherheit, Entwicklung und technologische Innovation. Dadurch ermöglichen sie einen schnellen Zugang zu modernen Technologien, eine hohe Verfügbarkeit und eine wirtschaftlich effiziente Nutzung von IT-Ressourcen.

Wenn Organisationen diese Vorteile nutzen und trotzdem die Unabhängigkeit ihrer Dienste und den Schutz ihrer Daten gewährleisten wollen, sollten sie die Cloud-Umgebung bewusst wählen:

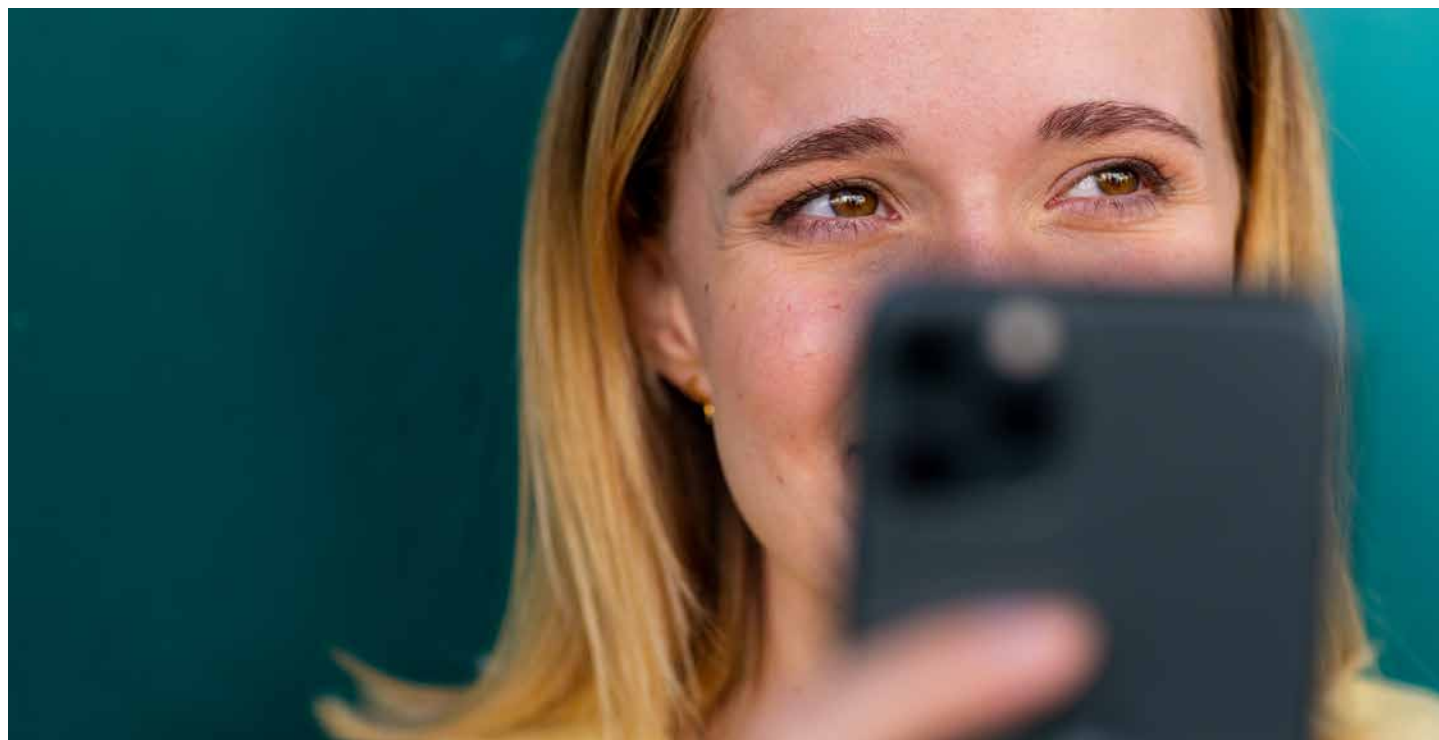
- Cloud-Umgebung wählen: private Cloud, öffentliche Cloud, Mischform
- Zugangs- und Verschlüsselungskonzept definieren und kontinuierliche Sicherheits- und Risikoprüfung sicherstellen

TLS-Zertifikate



TLS-Zertifikate (Transport Layer Security) bestätigen die Identität und Authentizität von Websites (Domains) und Organisationen und ermöglichen die verschlüsselte Übertragung von Daten zwischen Nutzern und Onlinediensten. Als zentraler Bestandteil einer sicheren Infrastruktur bilden sie die Grundlage für Vertrauen im Internet und in der digitalen Kommunikation. Als einziger Schweizer Anbieter von TLS-Zertifikaten trägt der Trust Service Provider SwissSign zu einem vertrauenswürdigen digitalen Ökosystem bei.

- Die Vertrauensinfrastruktur wird von SwissSign in der Schweiz und unter eigener Kontrolle in geografisch redundanten Rechenzentren betrieben.
- Organisationen profitieren von international anerkannten TLS-Zertifikaten, während Governance, Kontrolle und rechtliche Zuständigkeit in der Schweiz verbleiben.



Digitale Souveränität im Experten-Check:

Interview mit David Rosenthal

Herr Rosenthal, viele warnen vor Abhängigkeiten von Cloud-Anbietern aus den USA. Wird dieses Risiko aus Ihrer Sicht überschätzt oder unterschätzt?

Es wird falsch verortet. Die meisten fürchten die Abhängigkeit, weil die Anbieter aus den USA stammen. Für mich sind die Marktbeherrschung und die Klumpenrisiken das grössere Problem. Abhängigkeiten gab es in der IT aber schon immer, und sie waren noch nie gut – aber eben auch unvermeidbar. Es gibt hier keine Patentrezepte.

Der US CLOUD Act steht häufig im Zentrum der Debatte: Wie real ist die Gefahr eines Zugriffs auf Schweizer Daten in der Praxis wirklich?

Diese Gefahr wird überschätzt. Erstens ist der CLOUD Act nichts Besonderes; wir haben den quasi auch in der Schweiz. Zweitens gibt es Gegenmassnahmen auch ohne End-to-End-Verschlüsselung; das ignorieren manche Warner leider konsequent. Und drittens kommen US-Behörden auch ohne CLOUD Act an Daten aus der Schweiz, und zwar ganz legal über die Rechtshilfe. Die gängige Fixierung auf den CLOUD Act lenkt von wesentlich grösseren Risiken wie etwa der Gefahr durch Hacker ab: Vielerorts besteht eine grosse Zurückhaltung gegenüber Cloud-Lösungen, und so bleiben unsere Daten auf eigenen Servern, wo sie oft schlechter geschützt sind.

Woran erkennt man, dass eine Organisation genug souverän ist, und wo beginnt der Punkt, an dem Abhängigkeit kritisch wird?

Hat sie einen «Plan B» oder sogar einen «Plan C», sollte ein Anbieter ausfallen oder aufgegeben werden müssen? Gibt es Backups – und zwar

«Die Fixierung auf den CLOUD Act lenkt von wesentlich grösseren Risiken ab»

woanders? Hat sie ihre IT-Lösungskomponenten bewusst auf verschiedene Anbieter verteilt, also nicht überall auf dasselbe Pferd gesetzt? Hat sie genügend Know-how im Haus, damit sie ihre Optionen überhaupt versteht und umsetzen kann? Ich spreche daher lieber von digitaler Resilienz als von digitaler Souveränität.

Welche Missverständnisse begegnen Ihnen in der öffentlichen Debatte am häufigsten?

Dass die USA beim Einsatz von aus den USA stammenden Cloud-Providern freien Zugriff auf unsere Daten hätten.



Über den Experten:

David Rosenthal ist einer der führenden Schweizer Experten für Daten- und Technologierecht. Er ist Partner bei der Wirtschaftskanzlei VISCHER und berät Unternehmen und Behörden zu Datenschutz, IT und KI-Recht.

Fazit: Souverän ist, wer handlungsfähig bleibt

Digitale Souveränität bedeutet, den Einsatz digitaler Technologien bewusst zu gestalten, Risiken zu steuern und auch in einer vernetzten Welt handlungsfähig zu bleiben. Wer seine Daten kennt, Abhängigkeiten versteht und technologische Alternativen behält, kann Innovation nutzen, ohne die Kontrolle zu verlieren:

- 1** Erfolgreiche Organisationen kombinieren unterschiedliche Technologien und Betriebsmodelle entsprechend ihren Anforderungen und den gesetzlichen Vorgaben.
- 2** In Sonderfällen oder wenn die Datenhaltung gesetzlich verankert ist, können für besonders schützenswerte Daten lokale Infrastrukturen oder spezielle Betriebsmodelle sinnvoll sein.
- 3** Für standardisierte Anwendungen bieten Cloud-Plattformen oft entscheidende Vorteile hinsichtlich Innovation und Effizienz.
- 4** Open-Source-Komponenten können zusätzlich helfen, Transparenz zu erhöhen und Abhängigkeiten zu reduzieren.

Digitale Souveränität ist da garantiert, wo Organisationen ihre technologischen Abhängigkeiten verstehen, Risiken aktiv steuern und jederzeit handlungsfähig bleiben. Genau dieser bewusste und differenzierte Umgang mit Technologie bildet das Fundament digitaler Souveränität.

E-Voting



Das E-Voting-System der Post ermöglicht es, geschützt elektronisch zu wählen und abzustimmen. Spezielle sicherheitstechnische und kryptografische Vorkehrungen sorgen dafür, dass das Stimmgeheimnis gewährleistet ist und gleichzeitig der gesamte Urnengang auf Manipulationen überprüft werden kann. E-Voting ist seit 2023 in mehreren Kantonen erfolgreich im Einsatz.

- Die E-Voting-Software sowie die Server und Daten werden in der Schweiz betrieben.
- Die Post stellt die wesentlichen Komponenten und Dokumente zum System öffentlich zur Verfügung und lädt Fachleute zur Überprüfung des Systems ein. Mit einem sogenannten Bug-Bounty-Programm setzt sie auch finanzielle Anreize für die öffentliche Überprüfung und Meldung von Schwachstellen.
- Die Post stellt wichtige Teile des Codes unter einer freizügigen Open-Source-Lizenz bereit. Somit ist die freie Nutzung und Weiterentwicklung der entsprechenden Quellcode-Teile möglich.

