Löwenfels
Swiss Software Built to Last

Digitale Souveränität in der öffentlichen Verwaltung

Handlungsfelder und Strategien für eine unabhängige Verwaltung.

Inhaltsverzeichnis

Executive Summary

Die **digitale Souveränität** der Schweiz steht unter Druck. Während Bund, Kantone und Gemeinden ihre **digitalen Dienstleistungen** konsequent ausbauen, nehmen **technologische und politische Abhängigkeiten** zu. Dazu gehören etwa **globale Cloud-Anbieter, proprietäre Softwarelösungen** oder **Dateninfrastrukturen** mit unklarem Speicherort und unklaren Prozessen.

Digitale Souveränität geht über reine **Datensouveränität** hinaus. Sie beschreibt die Fähigkeit, **digitale Infrastrukturen, Anwendungen** und **Daten** selbstbestimmt, kontrolliert und im Einklang mit nationalen Werten sowie rechtlichen Rahmenbedingungen zu steuern. Für die öffentliche Verwaltung bedeutet das: Jede Entscheidung über **Technologie-Architekturen** und **Anbieter** ist zugleich eine Entscheidung über **Kontrolle, Sicherheit** und **demokratische Gestaltungsfreiheit.**

Dieses Whitepaper untersucht, wie die öffentliche Hand in der Schweiz ihre digitale Souveränität stärken kann. Es analysiert bestehende **Abhängigkeiten**, benennt **kritische Bereiche**, insbesondere **Cloud-Dienste, KI-Anwendungen** und **Softwareplattformen**, und zeigt praxisnahe Strategien auf. Im Zentrum stehen konkrete **Handlungsempfehlungen** für Behörden, IT-Leitungen und politische Entscheidungsträger.

Zentrale Erkenntnisse

- Digitale Souveränität ist ein strategisches Staatsziel, kein rein technisches Detail.
- Die Schweiz benötigt resiliente, kompatible und vertrauenswürdige Infrastrukturen.
- Offene Standards, europäische Kooperationsmodelle und lokal kontrollierbare Cloud-Lösungen bilden wichtige Bausteine.
- Souveränität entsteht durch Gestaltungsmacht und Transparenz, nicht durch Abschottung.
- Wer Kontrolle über Schlüsseltechnologien behält, bleibt langfristig unabhängig und handlungsfähig.

1 Was bedeutet digitale Souveränität für die öffentliche Verwaltung?

Begriffsdefinition

Das deutsche Bundesministerium für Wirtschaft und Energie definierte **digitale Souveränität** 2018 wie folgt: *«Digitale Souveränität eines Staates oder einer Organisation umfasst zwingend die* ***vollständige Kontrolle über gespeicherte und verarbeitete Daten*** *sowie die* ***unabhängige Entscheidung darüber, wer darauf zugreifen darf.*** *Sie umfasst weiterhin die Fähigkeit, t****echnologische Komponenten und Systeme eigenständig zu entwickeln, zu verändern, zu kontrollieren*** *und durch andere Komponenten zu ergänzen.»*

Diese Definition verdeutlicht zwei zentrale Dimensionen:

1. **Kontrolle über Daten** – Staaten oder Organisationen müssen uneingeschränkten Zugriff und Entscheidungsgewalt über ihre Daten besitzen.
2. **Technologische Autonomie** – sie müssen in der Lage sein, Systeme eigenständig zu gestalten, zu verändern, zu kontrollieren und zu erweitern.

Relevanz für die Schweiz

Digitale Souveränität bezeichnet somit die Fähigkeit eines Staates, seine **digitalen Infrastrukturen unabhängig, rechtssicher und selbstbestimmt** zu betreiben. Für die öffentliche Verwaltung der Schweiz bedeutet dies insbesondere:

- **Kontrolle über Daten:** Sensible Informationen, zum Beispiel AHV- oder Gesundheitsdaten, dürfen nur im schweizerischen Rechtsraum verarbeitet werden.
- **Rechtsrahmen einhalten:** Daten und Infrastruktur müssen vor externem Zugriff geschützt sein, auch wenn dieser durch ausländische Rechtsordnungen eingefordert wird.
- **Unabhängiger Betrieb:** Behörden müssen jederzeit über ihre Software und Dienste verfügen können, ohne dass Dritte den Zugang sperren oder einschränken können.

Souveränität als Staatsprinzip

Digitale Souveränität ist keine rein technische oder juristische Fragestellung. Sie berührt **grundlegende staatsrechtliche Prinzipien**:

- die Fähigkeit des Staates zur **unabhängigen Entscheidungsfindung**,
- die **Handlungsfreiheit** der Verwaltung, gerade in Krisenzeiten,
- sowie das **Vertrauen** der Bürgerinnen und Bürger in **staatliche Institutionen.**

2 Abhängigkeiten erkennen - Risiken verstehen

Fehlt einem Staat **digitale Souveränität,** gerät er in **Abhängigkeiten**, sowohl technologisch als auch rechtlich oder wirtschaftlich. Für Verwaltungen bedeutet das, dass sie zentrale **Kontrollrechte über Daten und Systeme** verlieren können.

Typische Risikobereiche

Rechtliche Abhängigkeit

Werden Daten in **ausländischen Clouds** gespeichert, können **fremde Rechtsordnungen** darauf zugreifen, auch gegen den Willen der Schweiz. Ein Beispiel ist der **US-amerikanische CLOUD Act** (Clarifying Lawful Overseas Use of Data Act). Er verpflichtet **US-Cloud-Anbieter**, Strafverfolgungsbehörden Zugang zu Kundendaten zu gewähren, selbst wenn diese ausserhalb der USA gespeichert sind. Damit werden Bestimmungen der **internationalen Rechtshilfe** umgangen, die eigentlich durch v**ölkerrechtliche Abkommen geregelt** sind.

Vertrauensverlust

Wenn eine Verwaltung die **Integrität ihrer digitalen Dienste** nicht garantieren kann, schwindet das **Vertrauen der Bevölkerung.** Dies gefährdet nicht nur die **Akzeptanz staatlicher Dienstleistungen,** sondern kann im Extremfall auch **demokratische Prozesse** unterminieren.

Erpressbarkeit

Fehlt eine **souveräne Infrastruktur,** steigt das Risiko von **Fremdbestimmung**. Möglich ist dies durch **Lizenzentzug**, die **Abschaltung von Diensten** oder **Angriffe mit Schadsoftware**. Abhängigkeiten von externen Anbietern können in **Krisensituationen** zur Blockade führen.

Technologische Lock-ins

Proprietäre Software, geschlossene Datenformate oder **fehlende Schnittstellen** erschweren den Anbieterwechsel. Dadurch entstehen langfristige Bindungen, die Innovation hemmen und Kosten erhöhen.

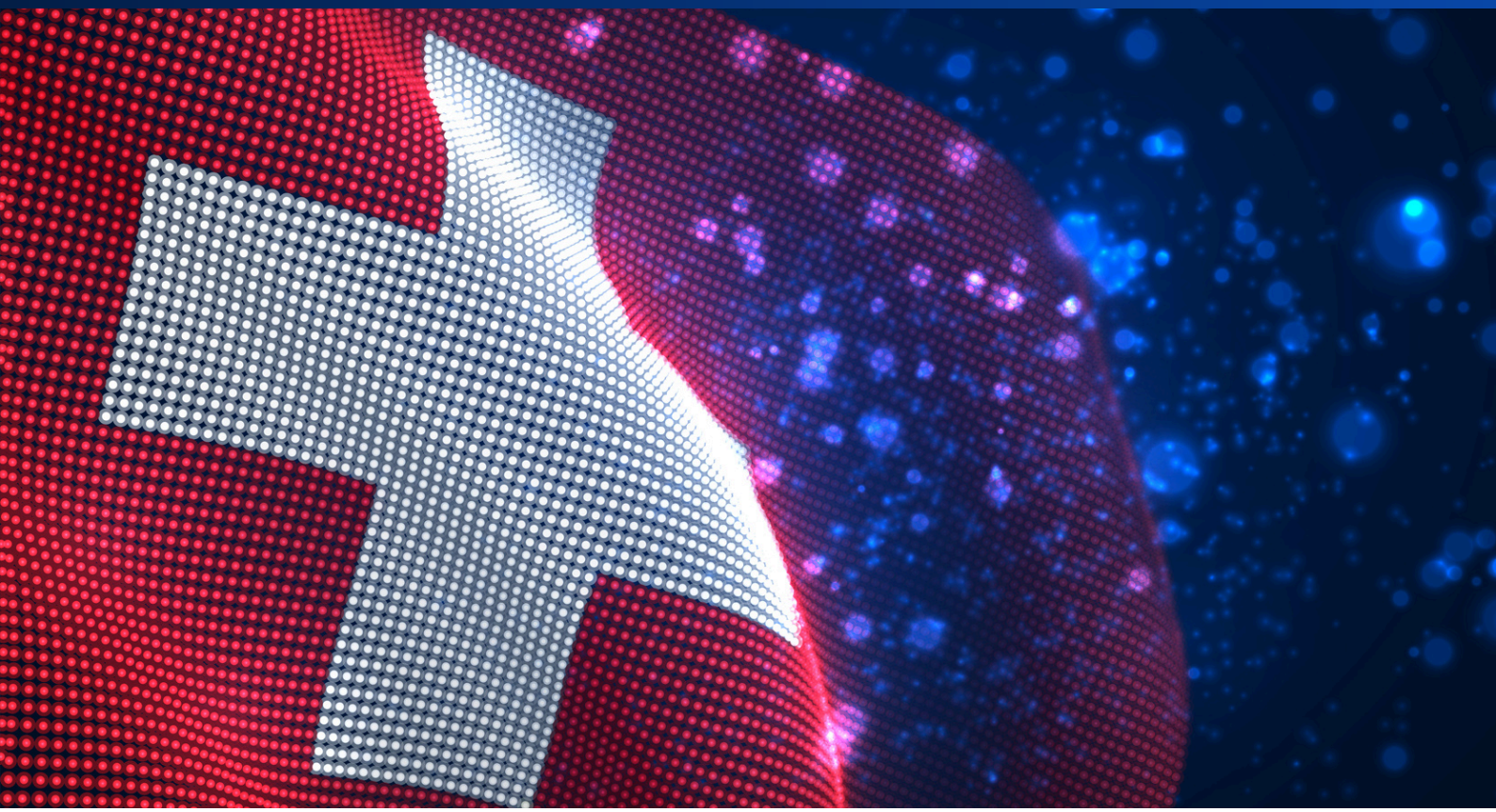
Souveränitätslücken

Besonders problematisch sind «Souveränitätslücken»: Bereiche, in denen Verwaltungen bewusst oder unbewusst **Kontrolle abgeben**, etwa bei Softwaremodulen, KI-Diensten oder der Wahl von Speicherorten. Solche Zonen der **Intransparenz** machen Organisationen verwundbar und schränken die Handlungsfähigkeit ein.

Differenzierung nach Sensibilität

Nicht alle digitalen Bereiche müssen maximal souverän ausgestaltet werden. Während **Geodaten** vergleichsweise unkritisch sind, erfordern **personenbezogene Informationen** aus der Sozialversicherung oder dem Gesundheitswesen den **höchsten Schutz**. Entscheidend ist, dass **Verwaltungen** Risiken systematisch **klassifizieren** und bewusst entscheiden, wo **Souveränität** unverzichtbar ist.

Wer diese Risikoanalysen aus Gründen der Bequemlichkeit oder kurzfristiger Kosteneinsparungen vernachlässigt, läuft Gefahr, zentrale IT-Systeme zu verlieren oder handlungsunfähig zu werden.



3 Handlungsfelder für mehr digitale Souveränität

Um die **digitale Souveränität** in der öffentlichen Verwaltung der Schweiz zu stärken, sind Massnahmen in mehreren **strategischen Handlungsfeldern** nötig. Diese betreffen nicht nur **Technologien**, sondern auch **Organisationen, Prozesse** und **rechtliche Rahmenbedingungen.**

1. Cloud & Infrastruktur

Die Wahl der **Infrastruktur** ist entscheidend. Wer **sensible Verwaltungsdaten** in globalen **Public Clouds** speichert, begibt sich in **rechtliche** und **operative Abhängigkeit.** Internationale Hyperscaler bieten zwar hohe Skalierbarkeit, unterliegen jedoch ausländischen Rechtsnormen (z. B. CLOUD Act, siehe Kapitel 2).
Eine **souveräne Cloud-Strategie** setzt daher auf **hybride** oder **Multi-Cloud-Modelle** und stellt sicher, dass besonders **schützenswerte Daten** im Inland verbleiben.

2. Software & Anwendung

Souveränität bedeutet auch **Kontrolle** über eingesetzte Software. Proprietäre **Lösungen** mit geschlossenen Formaten und fehlender API-Dokumentation führen zu Lock-ins und verhindern Anbieterwechsel. **Abhilfe schaffen offene Standards, klare Schnittstellen-Governance** und, **wo sinnvoll, Open-Source-Lösungen.**

3. Künstliche Intelligenz

KI-Anwendungen wie **grosse Sprachmodelle** oder **Entscheidungsalgorithmen** bringen neue Risiken. Eine zentrale Frage lautet, wie solche Systeme sicher mit **Verwaltungsdaten** arbeiten können, ohne **personenbezogene Informationen** zu gefährden. Klare **Regeln** und **Anonymisierung** sind notwendig, um **Missbrauch** zu verhindern.

4. Datenräume & Interoperabilität

Digitale Souveränität setzt die Fähigkeit voraus, **Daten** sicher und kontrolliert zu **teilen** – innerhalb einzelner Behörden ebenso wie zwischen verschiedenen Verwaltungsebenen. Dafür braucht es **interoperable Datenräume** mit verbindlichen **Standards**.

5. Beschaffungskriterien

Der grösste Hebel für digitale Souveränität liegt in der **Ausschreibungspraxis**. Wird der Preis als zentrales Kriterium gewichtet, entstehen kurzfristige Einsparungen, aber langfristige Abhängigkeiten. Digitale Souveränität muss deshalb explizit als **Zuschlagskriterium in Vergabeverfahren** aufgenommen werden, etwa durch Anforderungen an **Rechtszugriff, technische Kontrollierbarkeit** und **Datenhaltung im Inland.**

6. Organisation & Kompetenzen

Souveränität beginnt in den Köpfen der **Entscheidungsträger**. Verwaltungen müssen über **Wissen, Fähigkeiten** und **Haltung** verfügen, um Abhängigkeiten zu erkennen und souveräne Lösungen zu gestalten. Dafür sind **Schulungen** nötig, beispielsweise zu Cloud-Architekturen, Open-Source-Strategien, Datenschutzrecht, Ausschreibungsdesign oder KI-Governance.

Die Regel lautet:

- **Ohne Kompetenzen keine Kontrolle**
- **Ohne Kontrolle keine Souveränität**

4 Strategien

Digitale Souveränität lässt sich nicht kaufen – sie muss gestaltet werden. Verwaltungen benötigen nicht nur technische Mittel, sondern auch strategische Klarheit, rechtliche Sicherheit und organisatorische Disziplin. Erfolgreiche Strategien kombinieren daher stets mehrere Ebenen: rechtliche Rahmenbedingungen, technische Standards, organisatorische Zusammenarbeit und gezielte Investitionen.

a) Klassifizierung sensibler Daten

Nicht alle Informationen erfordern denselben Schutz. Ein strukturiertes Risikomanagement unterscheidet zwischen besonders sensiblen Daten (z. B. Sozialversicherungs-, Gesundheits- oder Justizdaten), solchen mit spezifischen gesetzlichen Vorgaben und weniger kritischen Informationen. Erst durch diese Klassifizierung können angemessene Schutzmassnahmen gewählt werden, ohne Ressourcen zu verschwenden.

b) Standardisierung als Grundlage der Handlungsfreiheit

Offene, standardisierte Formate ermöglichen es, Anbieter zu wechseln, Daten systemübergreifend zu nutzen und langfristig unabhängig zu bleiben. Proprietäre Schnittstellen oder geschlossene Formate schaffen hingegen Lock-ins und behindern Innovation. Souverän ist nur, wer jederzeit frei über seine Anbieterwahl entscheiden kann.

c) Bewusste Lücken akzeptieren – aber steuern

Komplette Unabhängigkeit in allen Bereichen ist weder wirtschaftlich noch technisch realistisch. Entscheidend ist, dass Verwaltungen wissen, wo sie Abhängigkeiten bewusst eingehen und warum. Beispielsweise können öffentliche Geodaten relativ problemlos über Cloud-Anbieter verteilt werden, während AHV-Daten oder Gerichtsakten ausschliesslich unter voller nationaler Kontrolle bleiben müssen.

d) Förderung lokaler Wertschöpfung

Regionale IT-Anbieter mit Sitz, Entwicklung und Hosting in der Schweiz bieten nicht nur rechtliche Vorteile, sondern stärken auch Innovationskraft und Resilienz. Voraussetzung ist jedoch eine faire Vergabepraxis, die lokale Anbieter nicht durch zu enge Kriterien oder Preisdumping benachteiligt.

5 Beispiele aus der Praxis

Kooperationen in der Spitalfinanzierung

Neun Kantone arbeiten im Bereich der Restkostenfinanzierung von Spitälern zusammen. Durch gemeinsame Standards und koordinierte Softwareentwicklung entstehen Interoperabilität und eine stärkere Verhandlungsposition gegenüber Lieferanten – bei gleichzeitiger Wahrung der kantonalen Souveränität.

Einkaufsgemeinschaft der Ausgleichskassen

Mehrere Ausgleichskassen haben sich zusammengeschlossen, um Software gemeinsam zu beschaffen und Standards festzulegen. Die Bündelung von Know-how und Ressourcen ermöglicht ein souveränes Ökosystem, das kosteneffizient und unabhängig agiert.

Onsite-Migration als Prinzip der Datensouveränität

Ein Beispiel aus der Praxis zeigt, wie Datensouveränität konkret umgesetzt werden kann: Bei der Migration eines Archivsystems wurden die Rechner während mehrerer Monate vor Ort bei der Behörde betrieben. Dieser Weg ist nicht der günstigste, aber der Souveränste.

6 Handlungsempfehlungen

Digitale Souveränität ist ein politisches, rechtliches und technisches Fundament für die Zukunftsfähigkeit der öffentlichen Verwaltung. In einer zunehmend vernetzten, datengetriebenen und automatisierten Welt ist es für Staaten und Verwaltungen essenziell, jederzeit handlungsfähig und unabhängig zu bleiben, gerade auch in Krisensituationen.

Bedeutung für die Schweiz

Für die Schweiz bedeutet digitale Souveränität konkret:

- Kontrolle über sensible Daten: Besonders schützenswerte Informationen dürfen nicht an externe Akteure abgetreten werden.
- Unabhängige Systeme: Technische Lösungen müssen so konzipiert sein, dass sie eigenständig betrieben und weiterentwickelt werden können.
- Entscheidungsfreiheit: Verwaltungen benötigen rechtliche, technische und organisatorische Möglichkeiten, souveräne Entscheidungen zu treffen.

Handlungsempfehlungen für Verwaltung, Politik und IT-Verantwortliche

1. Souveränitätsziele definieren

Jede Organisation sollte prüfen, welche digitalen Systeme für ihre Handlungsfähigkeit zentral sind und welche Schutzmassnahmen erforderlich sind, um diese langfristig unabhängig zu betreiben. Sensible Daten verdienen dabei besondere Aufmerksamkeit.

2. Beschaffung neu denken

Ausschreibungen dürfen nicht allein preisgetrieben sein. Digitale Souveränität muss als eigenständiges Kriterium berücksichtigt werden, zum Beispiel durch Vorgaben zur Datenhaltung im Inland, rechtliche Zugriffssicherheit, technische Kontrollierbarkeit und die Vermeidung von Lock-ins.

3. Standards fördern und einfordern

Offene, interoperable Standards bei Datenformaten, Schnittstellen und Prozessen sind entscheidend, um flexibel und unabhängig zu bleiben. Die öffentliche Hand sollte sich aktiv an Standardisierungsinitiativen beteiligen und diese vorantreiben.

4. Regionale Kooperationen und europäische Projekte nutzen

Digitale Souveränität bedeutet nicht, alles allein zu tun. Kantonsübergreifende Plattformen, Einkaufsgemeinschaften oder Beteiligungen an nationalen und internationalen Projekten wie Swiss Data Space oder X-Road schaffen Synergien ohne Kontrollverlust.

5. Kompetenzen aufbauen und erhalten

Ein souveräner Umgang mit digitalen Werkzeugen setzt Know-how voraus. Es braucht gezielte Schulungen, klare Verantwortlichkeiten und langfristige Investitionen in technologische Bildung – von der Sachbearbeitung bis zur strategischen Leitungsebene.

Fazit

Digitale Souveränität entsteht nicht allein durch Gesetze. Sie wird dort realisiert, wo Verwaltungen Verantwortung übernehmen, Entscheidungsfreiheit einfordern und die langfristigen Folgen ihrer Architekturentscheidungen mitdenken.

Die Schweiz verfügt als innovatives, föderal organisiertes Land über alle Voraussetzungen, wenn Bund, Kantone und Gemeinden bereit sind, bewusst und gemeinsam zu handeln.

Werden Sie aktiv!

Digitale Souveränität lebt von konkretem Handeln.
Wenn Sie souveräne IT-Strukturen umsetzen wollen, suchen Sie den Dialog mit Partnern, die Schweizer Werte teilen.

Löwenfels Partner AG unterstützt Schweizer Behörden seit vielen Jahren bei der Umsetzung souveräner IT-Lösungen.

Kontaktieren Sie uns. Wir beraten Sie gerne.

sales@loewenfels.ch

«Am Ende läuft alles auf Vertrauen hinaus. Vertrauen in Systeme, Vertrauen in Prozesse und Vertrauen in die Menschen, die diese gestalten.»

Oliver Meyer, CEO Löwenfels Partner AG

Löwenfels
Swiss Software Built to Last

Löwenfels Partner AG | Maihofstrasse 1 | 6004 Luzern | www.loewenfels.ch | sales@loewenfels.ch