Dein Kompass für mehr digitale Souveränität

Ein Kompendium mit Strategien und Checklisten für bewusste Entscheidungen

Management Summary

Souveränität ist kein Zufall, sondern deine strategische Entscheidung.

In einer Welt, in der Daten dein wertvollstes Asset und Software dein zentraler Innovationsmotor sind, wird digitale Souveränität zur unternehmerischen Kernfrage. Die Cloud gilt als «Fast Track» zur Agilität – doch mit der Bequemlichkeit wächst oft unbemerkt die Abhängigkeit: **Vendor Lock-in, intransparente Datenzugriffe und eingeschränkte strategische Handlungsfreiheit können potenziell zur strukturellen Schwäche werden.**

Viele Diskussionen rund um digitale Souveränität drehen sich heute primär um Cloud Lock-in oder die Frage, ob Daten physisch in der Schweiz gespeichert werden. Das greift jedoch zu kurz. **Wirkliche digitale Souveränität entsteht nicht allein durch die Wahl eines Cloud-Providers. Sie entscheidet sich ebenso in Architekturprinzipien, Betriebsmodellen, Governance-Strukturen und der Fähigkeit, auch im Krisenfall handlungsfähig zu bleiben.**

Digitale Souveränität bedeutet deshalb weder «Cloud-Bashing» noch die Rückkehr zu On-Premises. Sie beschreibt die Fähigkeit, Abhängigkeiten bewusst zu steuern und gezielt Entscheidungen zu treffen.

Unternehmen haben heute die Wahl,

- wie sie mit ihren Daten umgehen,
- wie ihre Architektur aufgebaut ist,
- wie resilient ihre Betriebsmodelle sind,
- und von welchen Anbietern sie abhängig sein wollen.

Diese Wahl erfordert klare Prioritäten und eine aktive Steuerung. Nur so behalten Organisationen die Kontrolle über ihre Daten, Systeme und strategischen Handlungsspielräume.

Dieses Kompendium zeigt dir, worum es bei digitaler Souveränität wirklich geht und weshalb wir das Thema entlang von vier Dimensionen betrachten:

- Datensouveränität
- technologische Souveränität
- operative Souveränität
- Governance

Wir zeigen auf, wie du die Vorteile globaler Hyperscaler, SaaS- und KI-Plattformen nutzen kannst, ohne dich vollständig abhängig zu machen. Mit gezielten Architekturentscheidungen, überlegten Cloud-Strategien und klarer Governance gewinnst du Wahlfreiheit. Zu jeder Dimension erhältst du konkrete Denkmodelle, Praxisbeispiele und Checklisten mit den relevanten Fragen für dein Unternehmen.

Digitale Souveränität ist kein binärer Zustand, sondern ein steuerbares Risikomanagement.

Es geht nicht um Ideologie, sondern um Kontrolle. Nicht um Verzicht, sondern um bewusste Gestaltung.

Strategische Autonomie: Triffst du bewusste Entscheidungen oder überlässt du sie dem Zufall?

Liebe Leser:innen: Digitale Souveränität ist heute die Voraussetzung für langfristige Handlungsfähigkeit in einer vernetzten Wirtschaft. In einer Zeit, in der Cloud-Plattformen und KI-Services integraler Bestandteil fast jeder Wertschöpfungskette sind, geht es nicht mehr darum, Abhängigkeiten komplett zu vermeiden. Vielmehr müssen wir uns die zentrale Frage stellen: Unter welchen Bedingungen ist eine Abhängigkeit für uns akzeptabel? Und wo müssen wir aus Risiko- und Governance-Gründen zwingend eine genaue Sicht haben?

In vielen Unternehmen wird digitale Souveränität heute fast ausschliesslich mit Cloud Lock-in oder Datenresidenz gleichgesetzt. Die Debatte dreht sich häufig um die Frage, ob Daten in der Schweiz liegen oder wie stark die Abhängigkeit von Hyperscalern ist. Diese Perspektive ist wichtig – aber zu eindimensional.

Aus unserer Sicht entsteht digitale Souveränität nicht allein durch die Wahl eines Cloud-Providers. Sie entscheidet sich ebenso in Architekturprinzipien, Betriebsmodellen, Governance-Strukturen und der Fähigkeit, auch im Krisenfall handlungsfähig zu bleiben. Genau deshalb betrachten wir digitale Souveränität entlang von vier Dimensionen.

Den Kompass richtig ausrichten

Wir bei ipt begleiten Unternehmen dabei, diese Souveränität strategisch zu definieren und technologisch umzusetzen. Unsere Perspektive ist geprägt durch die Arbeit in hoch regulierten Branchen wie dem **Finanz- und Bankensektor, Versicherungen, der öffentlichen Verwaltung und dem Gesundheitswesen.** Wir wissen: Souveränität ist kein Zufallsprodukt, sondern das Ergebnis einer bewussten Gestaltung der IT-Landschaft.

Um dieses komplexe Thema steuerbar zu machen, nutzen wir den ipt Souveränitäts-Kompass. Dieser unterteilt digitale Souveränität in vier entscheidende Dimensionen, die wir in diesem Kompendium detailliert beleuchten:

1. **Datensouveränität:** Es geht um die Entscheidungshoheit über den gesamten Lebenszyklus deiner eigenen Daten. Du entscheidest unabhängig von externen Akteuren über deren Nutzung, Schutz und Erhalt.

2. **Technologische Souveränität:** Dies beschreibt deine Fähigkeit, die benötigten IT-Systeme selbstbestimmt auszuwählen und auszutauschen. Ziel ist es, einseitige Abhängigkeiten von einzelnen Anbietern oder globalen Lieferketten aktiv zu vermeiden und den Zugang zu neuen Technologien wie KI zu ermöglichen.

3. **Operative Souveränität:** Hier steht die Fähigkeit im Fokus, deine IT-Systeme in allen Lagen zu betreiben, insbesondere in Ausnahme- und Krisenfällen. Dies gelingt mithilfe von internem Know-how, BCM/DR und klaren Exit-Strategien. Nur wer auch im Krisenfall handlungsfähig bleibt, ist wirklich souverän.

4. **Governance:** Dies bildet den strategischen und organisatorischen Rahmen. Hier definierst du, überprüfst und schärfst laufend deine Ziele für die digitale Selbstbestimmung.

Inhaltsverzeichnis

1. Datensouveränität: Jenseits der Residenz 10

1.1 Die drei strategischen Säulen der Datensouveränität 13

1.2 Das Schlüssel-Dilemma: reicht CMK? 14

1.3 Checkliste: Datensouveränität 15

Explizite Risikotreiber: Warum Abwarten keine Option ist 16

2. Technologische Souveränität: Beweglich bleiben durch Architektur 18

2.1 Die drei Ebenen der technologischen Souveränität 20

2.2 Der «Portabilitäts-Architekt» versus der «Speed-Junkie» – die IAM Edition 21

2.3 Souveräne Microservice-Architektur 22

2.4 Checkliste: Technologische Souveränität 23

3. Operative Souveränität: Handlungsfähig, wenn es brennt 24
3.1 Drei Bereiche operativer Souveränität 26
3.2 Lokale Alternativen zu US-Hyperscalern 27
3.3 Checkliste: Operative Souveränität 29

4. Governance: Die Schaltzentrale deiner Souveränität 30
4.1 Die sechs ipt-Prinzipien für souveräne Governance 32
4.2 Der Guardrail-Ansatz: Freiheit mittels Leitplanken 34
4.3 Checkliste: Souveräne Governance 35

5. Wirtschaftlichkeit: Souveränität als Renditebringer 36

6. Der Weg zur Umsetzung: Dein Souveränitäts-Kompass 38

Gemeinsam zur digitalen Selbstbestimmung

Wahre Souveränität erreichst du nicht durch theoretische Konzepte, sondern durch die praktische Befähigung deines Teams. In unserem Mixed-Team-Modell bei ipt arbeiten wir Seite an Seite mit deinen Experten, um Wissen direkt zu transferieren und deine Handlungsfähigkeit nachhaltig zu stärken.

Dieses Kompendium dient dir als Leitfaden, um die Cloud als kraftvolles Werkzeug zu nutzen – ohne dabei deine strategische Autonomie aus der Hand zu geben. Die behandelten Themen setzen Impulse, eröffnen Perspektiven und laden zur Vertiefung ein. Sie verstehen sich jedoch nicht als abschliessende Betrachtung.

Lass uns gemeinsam den Kompass neu ausrichten – klar, souverän und zukunftsorientiert.

Wir wünschen eine gute Lektüre,
das Team digitale Souveränität von ipt

Jakob Beckmann

Noemi Haag

Silvan Tschopp

Andreas Pfenninger

Dominik Liebmann

Christian Fehlmann

Daniel Albisser

Datensouveränität

- Datenhoheit
- Datenschutz
- Datenräume

Technologische Souveränität

- Portabilität
- Unabhängigkeit durch Open Source
- Zugang zu neuen Technologien

Operative Souveränität

- Verfügbarkeit & Skalierbarkeit
- BCM/DR & Exit-Strategie
- Kompetenzaufbau

Governance

- Strategie und KPIs
- Risiko-Mgmt. & Compliance
- Audit

01 Datensouveränität:

Jenseits der Residenz

«Datenresidenz ist die Basis. Datensouveränität ist eine strategische Wahl.»

In der aktuellen Cloud-Debatte wird Datensouveränität oft fälschlicherweise auf die Datenresidenz reduziert: «Steht der Server physisch in der Schweiz?». Für dich als IT-Entscheider ist das jedoch nur die regulatorische Grundvoraussetzung. Wahre Datensouveränität bezeichnet die Kontrolle über den gesamten Lebenszyklus deiner Daten.

Es geht darum, unabhängig von Providern oder geopolitischen Einflüssen über Nutzung, Schutz und Erhalt deiner digitalen Assets zu bestimmen.

Datensouveränität: 5 Entscheidungen für echte Kontrolle

Wie viel Kontrolle über Daten ist sinnvoll und wo entsteht unnötige Komplexität? Viele Organisationen stehen genau in diesem Spannungsfeld. Datensouveränität lässt sich nicht allein technisch lösen – sie erfordert klare Prioritäten und bewusste Abwägungen.

Jetzt in den Blogpost eintauchen

1.1 Die drei strategischen Säulen der Datensouveränität

Um Datensouveränität operativ umzusetzen, müssen wir drei Handlungsfelder betrachten, die weit über den Speicherort von Daten hinausgehen:

1

Datenhoheit: Die Macht über den Zugriff

Es reicht nicht aus, Daten lokal zu speichern. Du musst technisch erzwingen und nachvollziehen können, wer was mit ihnen tut. Das funktioniert über folgende Hebel:

- **Nutzungssteuerung:** Implementierte Policies sollten nicht nur definieren, wer auf Daten zugreifen darf, sondern auch klar regeln, wie diese Daten verwendet werden dürfen (beispielsweise für Analytics, jedoch nicht für das KI-Training eines Providers).
- **Durchsetzung und Nachweisbarkeit:** Policies müssen nicht nur definiert, sondern technisch durchgesetzt und auditierbar sein. Organisationen sollten jederzeit nachweisen können, wer wann auf welche Daten zugegriffen hat und wie sie verwendet wurden.

2

Datenschutz: Abwehr unberechtigter Zugriffe

Technischer Datenschutz ist notwendig, um unberechtigten Zugriffen vorzubeugen und die Einhaltung rechtlicher Rahmenbedingungen sicherzustellen. Diese Aspekte helfen dir dabei:

- **Nutze die Datenklassifizierung:** Digitale Souveränität bedeutet, bewusst zu entscheiden, welche Daten welches Schutz- und Kontrollniveau benötigen. Eine mögliche Klassifizierung ist: öffentlich, intern, sensitiv und hochkritisch.
- **Mache dir Gedanken zu Kryptographie und Schlüsselmanagement:** Die Kontrolle über kryptografische Verfahren und Schlüssel ist zentral für den Schutz sensibler Daten und digitale Souveränität. Insbesondere mit Blick auf Cloud-Abhängigkeiten und die zukünftigen Risiken durch Quantencomputing gewinnt die Auswahl und Kontrolle kryptografischer Verfahren zusätzlich an Bedeutung.

3

Datenräume: Im Spannungsfeld zwischen Innovation und Kontrolle

Datenräume ermöglichen es, Daten kontrolliert, sicher und zweckgebunden nutzbar zu machen – auch über Organisations- und Unternehmensgrenzen hinweg. Ziel ist es, Innovation zu fördern, ohne dabei die Kontrolle über sensible Daten zu verlieren. Dies geschieht insbesondere über folgende Mechanismen:

- **Datenportabilität:** Datenräume brechen bestehende Silostrukturen auf und ermöglichen die Mehrfachnutzung von Daten – beispielsweise im Gesundheits-, Energie- oder Industriesektor. Daten können kontrolliert zwischen verschiedenen Akteuren ausgetauscht und für neue digitale Services, Analysen oder KI-Anwendungen genutzt werden.
- **Datenstandardisierung:** Gemeinsame Standards schaffen die Grundlage für Interoperabilität und erleichtern den Datenaustausch über Organisationsgrenzen hinweg. Gleichzeitig reduzieren offene Standards die Abhängigkeit von einzelnen Anbietern, da relevante Marktteilnehmer dieselben Schnittstellen und Formate unterstützen.

1.2 Das Schlüssel-Dilemma: reicht CMK?

Ein wichtiger Punkt deiner Datensouveränität ist das **Schlüsselmanagement.** Hier gibt es kein Schwarz-Weiss, sondern eine bewusste Risikoabwägung, welche basierend auf der Datenklassifizierung getroffen werden soll. Hier diskutieren wir verschiedene Optionen:

Provider-Managed Keys: Der Cloud-Anbieter verwaltet die Schlüssel vollständig selbst. Vorteil ist die Einfachheit (Plug & Play) und native Integration in Cloud-Services. Demgegenüber steht jedoch eine vollständige Abhängigkeit vom Provider sowie keine eigene Kontrolle über den Schlüssel.

Customer-Managed Keys (CMK): Du definierst den gesamten Lebenszyklus der Schlüssel (Erstellung, Zugriff, Rotation, Löschung), während der Cloud-Anbieter die operative Verwaltung übernimmt. Dies ermöglicht mehr Kontrolle, allerdings bleibt die physische Schlüsselverwaltung (beispielsweise Hardware Security Module/HSM) weiterhin beim Provider. **CMK ist in der Regel unsere Empfehlung für die meisten Daten.**

Bring Your Own Key (BYOK): Die Schlüssel werden von dir selbst generiert und in die Cloud überführt. Damit liegt die Hoheit über die Schlüsselgenerierung zwar beim Unternehmen, gleichzeitig steigen jedoch Komplexität und Anforderungen an die sichere Übergabe und Verwaltung erheblich.

Hold Your Own Key (HYOK): Die Schlüssel verlassen die eigene Infrastruktur nicht. Dies bietet maximale Kontrolle und Sicherheit, führt jedoch zu starken Einschränkungen in der Cloud-Nutzung und reduziert viele Dienste faktisch auf reine Speicherfunktionen. Oft ein Innovationskiller und in der Praxis selten sinnvoll.

Fazit von ipt: Wir empfehlen, die Wahl des Schlüsselmanagements an der Datenklassifizierung auszurichten: Für öffentliche und interne Daten sind Customer-Managed Keys (CMK) meist die richtige Wahl. Für vertrauliche oder besonders schützenswerte Daten kann Bring Your Own Key (BYOK) die richtige Wahl sein, falls entsprechende Vorgaben bestehen oder man schon eine HSM-Infrastruktur zur Verfügung hat. Damit lassen sich Sicherheits- und Compliance-Anforderungen erfüllen, ohne auf die Vorteile moderner Cloud- und KI-Plattformen verzichten zu müssen.

Success Story – SWICA: Eine dezentrale Datenplattform für die Zukunft

Die SWICA stand vor der Herausforderung, ihr erweitertes Data Warehouse (eDWH) zu modernisieren. Das Ziel: Eine innovative Datenplattform, die höchste Sicherheitsstandards erfüllt und gleichzeitig flexibel, effizient und skalierbar ist.

- **Die Lösung:** Durch gezieltes Platform Engineering und eine enge Zusammenarbeit zwischen SWICA und ipt entstand eine dezentrale Architektur.
- **Souveränitäts-Aspekt:** Die Plattform entkoppelt die Daten von Anwendungen und schafft die Basis für Analytics und KI, ohne die Kontrolle über die Datenqualität und Sicherheit zu verlieren. SWICA wählte bewusst die Zusammenarbeit mit einem Provider, um die Komplexität und Kosten niedrig zu halten. Gleichzeitig verfügte SWICA über Exit-Möglichkeiten.

Jetzt Success Story lesen

1.3 Checkliste:
Datensouveränität

- ❒ **Datenresidenz:** Wo sind deine Daten gespeichert und kann jederzeit darauf zugegriffen werden?
- ❒ **Klassifizierung:** Sind deine kritischen Daten identifiziert und werden diese speziell behandelt?
- ❒ **Transparenz:** Hast du eine Sicht darauf, wer wann auf welche kritischen Daten zugegriffen hat?
- ❒ **Steuerung von Datenzugriff:** Kannst du Zugriffserlaubnisse granular und autonom steuern (z. B. über Rollen, Policies oder Attribute) und konsistent durchsetzen?
- ❒ **Auditierbarkeit:** Werden alle Zugriffe und Datenbewegungen revisionssicher protokolliert und zentral auswertbar gemacht?
- ❒ **Schlüsselmanagement:** Wo sind deine Schlüssel gespeichert und wer managt sie?
- ❒ **Standardisierung:** Liegen deine Daten in offenen Formaten vor, oder sind sie in proprietären Provider-Silos gefangen?
- ❒ **Post Quantum Cryptography:** Sind deine Verschlüsselungs- und Sicherheitsmechanismen bereits auf zukünftige kryptografische Anforderungen vorbereitet?
- ❒ **Vertragliche Hoheit:** Ist explizit ausgeschlossen, dass der Provider deine Daten verwendet, z. B. für das Training eigener KI-Modelle?
- ❒ **Datenräume:** Nutzt du strukturierte Datenräume für den sicheren, kontrollierten und standardisierten Datenaustausch anstelle von unkontrollierten Punkt-zu-Punkt-Integrationen?

Explizite Risikotreiber:

Warum Abwarten keine Option ist

Digitale Souveränität ist kein theoretisches Konstrukt, sondern eine Reaktion auf reale, messbare Risiken. Folgende Themen gilt es zu beachten und für dein Unternehmen einzuordnen:

1. Rechtliche Grauzonen & Zugriffskonflikte (US CLOUD Act, FISA Act)

Der **US CLOUD Act** erlaubt US-Behörden den Zugriff auf Daten, die von US-Unternehmen oder deren Tochtergesellschaften verwaltet werden – unabhängig davon, wo die Daten physisch gespeichert sind (beispielsweise auch in der Schweiz), sofern ein gültiger US-Gerichtsbeschluss vorliegt. Er erlaubt keine Massenüberwachung und US-Hyperscaler publizieren, wie oft Daten herausgegeben wurden.

FISA Act (insbesondere Section 702) ermöglicht US-Geheimdiensten unter bestimmten Voraussetzungen den Zugriff auf Kommunikations- und Nutzungsdaten bei US-Anbietern, teilweise ohne klassischen richterlichen Beschluss im europäischen Verständnis.

Dadurch können Konflikte mit dem Schweizer Datenschutzgesetz (DSG) oder der EU-DSGVO entstehen, insbesondere wenn personenbezogene oder besonders schützenswerte Daten betroffen sind.

2. Regulatorischer Druck (FINMA & DORA)

Für den Finanz- und Versicherungssektor verschärfen sich die regulatorischen Anforderungen deutlich. FINMA-Rundschreiben (insbesondere zu Outsourcing und operationellen Risiken) sowie auf europäischer Ebene der DORA (Digital Operational Resilience Act) fordern unter anderem klare Exit-Strategien, Resilienz und die Kontrolle über kritische ICT-Dienstleistungen und Infrastrukturen.

Digitale Souveränität wird damit zunehmend von der Kür zur regulatorischen Pflicht.

3. Geopolitische Instabilität

In einer zunehmend multipolaren Welt können Handelskonflikte, Sanktionen oder geopolitische Spannungen den Zugriff auf kritische Software- und Cloud-Services kurzfristig einschränken, verteuern oder regulatorisch erschweren. Die starke Marktdominanz der US-Hyperscaler führt dabei zu Abhängigkeiten, die heute nur schwer umgangen werden können.

4. Wirtschaftliche Erpressbarkeit (Commercial Lock-in)

Abhängigkeit ist teuer. Wenn Anbieter ihre Preisstrukturen ändern oder Funktionen nur noch in teureren Bundles verfügbar machen, fehlt ohne digitale Souveränität oft die notwendige Verhandlungsmacht.

Dies zeigte sich in der Vergangenheit beispielsweise bei den Lizenzänderungen rund um Java oder Datenbankprodukte, die für viele Unternehmen kurzfristig zu massiv steigenden Kosten führten. Ein schneller Technologiewechsel war aufgrund bestehender Abhängigkeiten häufig kaum möglich.

5. Opportunitätskosten

Das wohl am häufigsten unterschätzte strategische Risiko: Unternehmen, die nicht auf moderne Technologien wie Large Language Models (LLMs), Cloud-Plattformen oder SaaS-Lösungen setzen, verlieren gegenüber ihren Wettbewerbern an Innovationsfähigkeit und Geschwindigkeit. Entscheidend ist dabei, die richtige Balance zwischen technologischer Nutzung und digitaler Souveränität zu finden.

02 Technologische Souveränität:

Beweglich bleiben durch Architektur

Success Story – Schweizer Armee: Das Dienstbüchlein wird digital

Die Schweizer Armee stand vor der Herausforderung, das papierbasierte Dienstbüchlein durch eine moderne digitale Lösung zu ersetzen. Das Ziel: Höchste Anforderungen an Verfügbarkeit, Datenschutz und Datenintegrität mit einer zukunftsfähigen Plattform zu verbinden.

- **Die Lösung:** Durch die enge Zusammenarbeit zwischen dem Projektteam der Armee und ipt entstand eine durchgängig digitalisierte und automatisierte Plattform. Diese basiert auf einer modernen, event-basierten und portablen Architektur mit Microservices.
- **Souveränitäts-Aspekt:** Die Plattform setzt konsequent auf Open-Source-Technologien und wird in einer Private Cloud betrieben. Dadurch bleibt die Lösung portabel und unabhängig von einzelnen Anbietern. Gleichzeitig wurde gezielt internes Know-how aufgebaut, um den langfristigen Betrieb und die Kontrolle über sensible militärische Daten sicherzustellen.

Jetzt Success Story lesen

«Technologische Souveränität bedeutet nicht, alles selbst zu bauen oder nur noch Open Source zu verwenden. Es bedeutet, Architekturen so zu gestalten, dass man einen Anbieterwechsel mit wenig Aufwand und Kosten vollziehen kann.»

In der technologischen Dimension entscheidet sich, wie hoch der Preis für einen potenziellen Wechsel oder eine Erweiterung deiner IT-Landschaft ist. Technologische Souveränität bezeichnet dabei die Fähigkeit, die benötigten IT-Systeme selbstbestimmt auszuwählen, um einseitige Abhängigkeiten zu vermeiden. Oft wird fälschlicherweise «Geschwindigkeit» gegen «Souveränität» ausgespielt. Wir bei ipt sind überzeugt: Wer die richtigen architektonischen Leitplanken setzt, kann die Innovationskraft der Hyperscaler nutzen, ohne grosse Abstriche hinsichtlich Souveränität machen zu müssen.

2.1 Die drei Ebenen der technologischen Souveränität

Um die technologische Souveränität greifbar zu machen, unterteilen wir sie in drei wesentliche Ebenen:

1

Portabilität:

Je einfacher du einen Cloud- oder Software-Anbieter wechseln kannst, desto unabhängiger bist du. Hierbei spielen offene Standards eine zentrale Rolle, z. B. bei Datenformaten (JSON, YAML) oder im IAM Bereich (OAuth2, OIDC), da diese unter anderem die Schnittstellen definieren. Somit kannst du einen Anbieter wechseln, ohne dass du deine Umsysteme anpassen musst.

Du könntest, wenn es für dein Unternehmen sinnvoll ist, auch einen Schritt weitergehen und eine durchdachte Multi-Cloud-Strategie umsetzen.Damit hättest du die Option, schnell auf einen Anbieter zu verzichten, falls dies notwendig ist. Als absolutes Minimum solltest du zumindest sicherstellen, dass du alle Daten in einem strukturierten Format exportieren kannst.

2

Unabhängigkeit durch Open Source:

Open Source ist ein zentraler Hebel, um technologische Souveränität zu stärken, ohne alles selbst bauen zu müssen. Basierend auf deinem Souveränitätsanspruch kannst du Open Source Software selbst betreiben oder diese von einem Cloud-Anbieter beziehen, da die meisten Cloud-Dienste auf Open Source basieren. Während du beim Cloud-Anbieter den Integrationslayer und Support mitgeliefert bekommst, musst du beim Self-Hosting ein tieferes technisches Verständnis der Software aufbauen, was dir dafür im Krisenfall zugutekommt. Flexibel bleibst du auf jeden Fall und kannst bei Bedarf auch eigene Erweiterungen implementieren.

3

Zugang zu neuen Technologien:

Die Agilität einer IT-Infrastruktur zeigt sich darin, wie effizient sie neue Durchbrüche von KI-Diensten bis hin zu Quantencomputern adaptieren kann. Dabei gilt es abzuwägen, ob du eine bewusste, temporäre Abhängigkeit von diesen Anbietern in Kauf nehmen möchtest, um die besten Plattformen und Dienste zu nutzen. Ein solches Risiko ist dann legitim und wirtschaftlich sinnvoll, wenn man sich damit von der Konkurrenz differenzieren kann.

2.2 Der «Portabilitäts-Architekt» versus der «Speed-Junkie» – die IAM Edition

Der Portabilitäts-Architekt: Investiert bewusst Zeit und Budget in offene Standards, Open Source und Multi-Cloud-Fähigkeit, um jederzeit die Kontrolle zu behalten und flexibel den Anbieter wechseln zu können.

Der Speed-Junkie: Akzeptiert den Vendor Lock-in als notwendigen Preis für schnelle Markteinführungen. Dies kann eine bewusste und richtige Wahl sein, solange das Risiko bekannt ist.

Die Realität ist kein Entweder-oder: **Jedes Unternehmen muss seine eigene Position zwischen Geschwindigkeit und Unabhängigkeit finden.** Zwischen tief integrierten Provider-Services und bewusst gewählter Abstraktion. Wir möchten dies am Beispiel IAM illustrieren:

Die Falle der tiefen Integration

Viele Unternehmen nutzen Microsoft Entra ID (früher Azure AD) für Single Sign-On (SSO). Das ist für die User Experience und Sicherheit hervorragend. Wenn nun aber zusätzlich das eng integrierte Microsoft Entra ID Governance eingesetzt wird, welches die Berechtigungsverwaltung übernimmt, steigt die Abhängigkeit von Microsoft massiv an. Um souverän zu bleiben, musst du die «Run-time» von der «Admin-time» trennen:

1. **Authentisierung (Run-time):** Nutze Entra ID als modernen Login-Dienst für deine Mitarbeitenden. Dieser implementiert offene Standards, und es gibt daher viele Konkurrenzprodukte, zu denen du bei Bedarf wechseln kannst.
2. **Governance (Admin-time):** Verankere die Logik – also wer welche Berechtigungen aus welchem Grund erhält – in einem unabhängigen, souveränen IGA-System (Identity Governance & Administration System).

Diese Trennung stellt sicher, dass du die Kontrolle über deine Identitäts- und Berechtigungslogik behältst, selbst wenn du den Cloud-Provider wechselst oder eine Multi-Cloud-Strategie fährst.

IAM als Innovation-Enabler

Ein souveränes IAM ist kein Bremsklotz. Im Gegenteil: In Bereichen wie Open Finance oder im Gesundheitswesen ist ein robustes IAM der entscheidende Enabler. Es schafft das nötige Vertrauen bei Kunden und Partnern, dass Daten sicher geteilt werden können, ohne die Kontrolle darüber aufzugeben.

Souveränität in der Cloud? Auch eine Frage des IAM

Digitale Souveränität bedeutet nicht, auf Public Cloud zu verzichten. Mit einem durchdachten Identity & Access Management (IAM) lassen sich Microsoft Entra ID und andere Dienste nutzen, ohne die Kontrolle zu verlieren.

Jetzt in den Blogpost eintauchen

2.3 Souveräne Microservice-Architektur

Open-Source-Software ermöglicht es dir, eine hohe Flexibilität und Portabilität für deine Services zu erreichen. Da der Quellcode frei zugänglich ist, entfallen restriktive Lizenzvorgaben, wodurch sich Anwendungen plattformunabhängig betreiben lassen. Dies möchten wir anhand einer konkreten Microservice-Architektur aufzeigen.

Compute: Als Basis für deine Rechenleistung dient Kubernetes im Zusammenspiel mit Knative, um eine moderne Compute-Infrastruktur aufzubauen. Praktisch alle modernen Cloud-native Anwendungen laufen heute auf Kubernetes, und das Ökosystem ist entsprechend breit und etabliert. Gleichzeitig schafft dieser Standard ein hohes Mass an Portabilität: Workloads lassen sich vergleichsweise einfach zwischen verschiedenen Hyperscalern oder auch von On-Premises in die Cloud verschieben. Genau diese Flexibilität ist ein zentraler Baustein digitaler Souveränität.

Data: Für ein souveränes Datenmanagement setzen wir auf bewährte relationale Datenbanken wie Postgres, dokumentenbasierte NoSQL-Datenbanken wie MongoDB sowie ultraschnelle In-Memory-Speicher wie Valkey. Ergänzt wird die Architektur durch Apache Kafka als Event-Streaming-Plattform, die kontinuierliche Datenströme hochverfügbar und plattformunabhängig verarbeitet.

Storage: Um unstrukturierte Daten flexibel zu speichern, nutzen wir einen S3-kompatiblen Objektspeicher. Nachdem die weit verbreitete Lösung MinIO Ende 2025 in den Maintenance Mode gewechselt ist, stehen bereits mehrere Alternativen bereit, um diese Rolle zu übernehmen – beispielsweise RustFS, Ceph oder Garage. Für Kubernetes-native Umgebungen bietet zudem Rook eine etablierte Möglichkeit, Ceph effizient zu betreiben. Dies zeigt: Auch im Storage-Bereich gibt es starke offene Standards und genügend Optionen, um flexibel und souverän zu bleiben.

Network: Die Absicherung und Steuerung des Netzwerks zwischen deinen Microservices wird durch ein Service Mesh und Network Policies realisiert. Lösungen wie Istio und Cilium nutzen den performanten Envoy-Proxy, um den gesamten Datenverkehr intelligent zu routen, tiefgehend zu überwachen und automatisch per mTLS zu verschlüsseln. Dadurch lässt sich ein echtes, souveränes Zero-Trust-Netzwerk aufbauen.

Security: Das Identitäts- und Rechtemanagement wird durch Keycloak abgedeckt und kann mit dem Open Policy Agent (OPA) um moderne, policy-basierte Zugriffskontrollen erweitert werden. Dieses Zusammenspiel ermöglicht es dir, Benutzeranmeldungen (Single Sign-On) sowie komplexe Sicherheitsrichtlinien zentral, konsistent und herstellerunabhängig für all deine Services zu definieren.

Basierend auf diesem souveränen Stack kannst du weitere Plattformdienste hinzufügen oder einzelne Komponenten durch für dich passendere Implementierungen ersetzen. Aus Sicht der Enterprise-Architektur solltest du zudem vermeiden, für dieselbe Anforderung mehrere unterschiedliche Lösungen einzusetzen. Dadurch bleibt dein Betriebsbudget überschaubar, weil der Know-how-Aufbau fokussierter erfolgt, die Komplexität reduziert wird und Optimierungen ihre Wirkung breiter entfalten können.

ipt Lösung: Architektur-Review für Souveränität

Wir unterstützen dich dabei, eine Architektur aufzubauen, die digitale Souveränität bereits by Design berücksichtigt. In unseren Reviews bewerten wir die Exit-Fähigkeit deiner Systeme und identifizieren kritische technologische Abhängigkeiten. **Ergebnis:** Ein klarer Plan, wie du die Innovationskraft von grossen Cloud-Anbietern nutzt, aber die strategische Kontrolle über deine betriebskritischen Prozesse behältst.

Mehr dazu hier

2.4 Checkliste:
Technologische Souveränität

- ❒ **Infrastruktur-Check:** Sind die Abhängigkeiten bei Hardware und Netzwerk bekannt und bewertet?
- ❒ **Portabilität:** Sind Anbieter-Lock-ins erhoben und Entscheide dazu getroffen? Wie einfach kann man (geschäftskritische) Applikationen auf einen anderen Provider wechseln?
- ❒ **Offene Standards:** Werden für Integrationen und Datenablagen konsequent offene Standards eingesetzt?
- ❒ **Applikations-Design:** Setzt du bei Neuentwicklungen auf Open Source und Interoperabilität?
- ❒ **Software-Entwicklung:** Wie hoch ist die Portabilität der Tools inkl. deren Daten (Code Repo, CI/CD, Artifact Registry), welche für die Softwareentwicklung und -deployment eingesetzt werden?
- ❒ **Entkoppelung:** Verwende unterschiedliche Anbieter für Authentisierung (Login) und Governance (Berechtigungslogik).

03 Operative Souveränität:

Handlungsfähig, wenn es brennt

«Operative Souveränität ist deine Lebensversicherung. Wer den Betrieb und das Know-how komplett auslagert, verliert im Krisenfall nicht nur die Kontrolle, sondern die Fähigkeit zu überleben.»

Unter operativer Souveränität verstehen wir die Fähigkeit, IT-Systeme eigenständig zu betreiben, zu kontrollieren und insbesondere im Krisenfall handlungsfähig zu bleiben. Viele Organisationen stützen sich im Alltag stark auf die Management- und Monitoring-Tools ihrer Cloud-Anbieter. Diese bieten wertvolle Unterstützung, sind aber nutzlos, wenn der Anbieter eine Störung hat. Deshalb ist es entscheidend, auch unabhängig davon Transparenz und Steuerungsfähigkeit sicherzustellen. Denn echte Souveränität zeigt sich vor allem dann, wenn es zu Störungen kommt oder die Verbindung zum Provider eingeschränkt ist.

3.1 Drei Bereiche operativer Souveränität

Aus unserer Erfahrung bei Kunden erachten wir folgende drei Bereiche als relevant:

1

Verfügbarkeit und Skalierbarkeit:

Um einen stabilen IT-Betrieb auch in Ausnahmesituationen zu garantieren, sollten Systeme über eine gewisse offline-Fähigkeit verfügen und robust gegen gezielte DDoS-Angriffe abgesichert sein.

Gleichzeitig erfordert moderne Resilienz eine elastische Skalierung der Infrastruktur, damit sich die Anwendungen dynamisch und vollautomatisch an plötzliche Lastspitzen anpassen können.

Neu benötigt es zudem einen verlässlichen Zugang zu hochleistungsfähigen GPUs, um Agenten und KI-Dienste jederzeit stabil zu betreiben. Durch diese Kombination aus Ausfallsicherheit und Skalierbarkeit sichert sich deine Organisation ihre operative Handlungsfähigkeit in jeder Lage.

2

BCM/DR und Exit-Strategie:

Wie gut ist dein Unternehmen auf den langfristigen Ausfall eines Cloud-Anbieters oder einer geschäftskritischen Applikation vorbereitet? Die Absicherung erfolgt auf verschiedenen Ebenen: Während klassisches Business Continuity Management (BCM) und Disaster Recovery (DR) die Verfügbarkeit einzelner Anwendungen sichern, erfordert der Ausfall eines gesamten Cloud-Providers strategischere Ansätze.

Wer auf eine aktive Multi-Cloud-Strategie setzt, kann Workloads meist flexibel verschieben; bei der Nutzung einer passiven Secondary Cloud steigt der Synchronisationsaufwand bereits signifikant. Die aufwendigste Option bleibt der vollständige Cloud-Exit. Damit diese Szenarien im Ernstfall reibungslos funktionieren, ist eine regelmässige und realitätsnahe Erprobung aller Notfallpläne essenziell.

3

Kompetenzaufbau:

Operative Souveränität steht und fällt mit der Qualifikation der eigenen Mitarbeitenden. Durch KI verschiebt sich die Anforderung hin zu einer hybriden Problemlösungskompetenz: Teams müssen in der Lage sein, komplexes Troubleshooting sowohl traditionell als auch unter Einsatz moderner KI-Werkzeuge durchzuführen. Durch den Aufbau zentraler Plattform-Teams und einer gezielten KI-Lernkultur kannst du dieses Wissen nachhaltig in deinem Unternehmen verankern. Die strategische Kooperation mit lokalen Partnern beschleunigt diesen Kompetenzaufbau und hilft in anspruchsvollen Situationen.

3.2 Lokale Alternativen zu US-Hyperscalern

Rund 70 Prozent des europäischen Cloud-Markts liegen in den Händen der US-Hyperscaler (European Parliament Research Service, *Digital sovereignty and infrastructure dependence in Europe,* 2025). Doch neben den grossen Anbietern wächst ein leistungsfähiges europäisches Cloud-Ökosystem heran. **Operative Souveränität heisst jedoch nicht, auf Hyperscaler zu verzichten.** Diese sollten **je nach Anforderungen bewusst mit europäischen Alternativen verglichen werden:** als Primärlösung, Secondary Cloud oder im Multi-Cloud-Setup.

Digital sovereignty and
infrastructure dependence in Europe

Europäische Provider wie Scaleway, STACKIT oder Exoscale zeigen eindrücklich, dass sie Kernkomponenten wie ein Netzwerk, Managed Kubernetes, DBaaS oder GPUs einfach und kosteneffizient bereitstellen können. Zwar hinken sie bei spezialisierten Zusatzdiensten und integrierten Governance-Tools den US-Riesen noch hinterher; wer hier jedoch aus Souveränitätsgründen ohnehin auf unabhängige Drittanbieter-Produkte setzt, kann diese Lücke elegant schliessen. Die Herausforderung liegt beim Zugang zu spezifischem Wissen. Da der Grossteil aller Dokumentationen im Internet auf US-Hyperscaler zugeschnitten ist, benötigt dein IT-Team ein tieferes Verständnis der eingesetzten Technologien. Dies zahlt letztlich direkt auf die digitale Souveränität des eigenen Unternehmens ein.

Die Entwicklung des europäischen Cloud-Ökosystems stellt einen strategischen Wendepunkt dar. Obwohl die meisten europäischen Provider noch nicht die volle Flexibilität oder Skalierbarkeit der US-Hyperscaler bieten, stellen sie für die meisten Unternehmen praktikable Ergänzungen oder Alternativen dar.

Da europäische Clouds tendenziell spezialisierter sind, wird die Wahl der Provider für die Enterprise Architektur komplexer. Doch auch wenn die Entscheidung schwieriger sein mag, bieten sie echte Vorteile in Form von Einfachheit, Souveränität, oder schlicht durch ihre preisliche Attraktivität.

5 europäische Cloud-Provider als Ergänzung für eine souveräne IT-Strategie

Digitale Souveränität heisst nicht, auf Hyperscaler zu verzichten. Diese sollten jedoch je nach Anforderungen bewusst mit europäischen Alternativen verglichen werden: als Primärlösung, Secondary Cloud oder im Multi-Cloud-Setup.

Jetzt in den Blogpost eintauchen


N
W
E
S
DIGITALE SOUVERÄNIT

3.3 Checkliste:
Operative Souveränität

- ❒ **Dynamische Skalierung:** Können deine Applikationen mit einer (unerwarteten) hohen Anzahl von Anfragen umgehen und selbständig skalieren?
- ❒ **Monitoring:** Verfügst du über eine providerunabhängige Sicht auf deine Systemgesundheit?
- ❒ **BCM/DR:** Können kritische Prozesse bei einem länger andauernden Cloud-Ausfall weiterlaufen?
- ❒ **Exit-Bereitschaft:** Gibt es für (geschäftskritische) Anwendungen einen dokumentierten und getesteten Plan für einen Providerwechsel?
- ❒ **Multi-Cloud:** Laufen deine Workloads bei mehr als einem Provider und können diese einfach zwischen den Providern verschoben werden?
- ❒ **Wissen:** Ist das Wissen für den Notbetrieb in den Köpfen deiner internen Mitarbeitenden und vertrauenswürdigen Partnern (Kompetenzmatrix)?
- ❒ **Plattform-Teams:** Habt ihr spezialisierte Plattform-Teams, welche ein tiefes Verständnis der eingesetzten IT-Infrastruktur und Shared Services haben?
- ❒ **Lokalität:** Wo sind deine IT-Administratoren ansässig?
- ❒ **Zugang zu neuer Hardware:** Ist dein Unternehmen fähig, zeitnah die neuesten GPUs zu verwenden?

04 Governance:

Die Schaltzentrale deiner Souveränität

Orientierung am Bund

Die Cloud-Strategie des Bundes verfolgt einen Hybrid Multi-Cloud Ansatz. Die Cloud-Prinzipien der Bundesverwaltung konkretisieren die Grundsätze für die Public und Private Cloud-Nutzung. Dabei steht die bewusste Entscheidung im Zentrum, welches Cloud-Modell für eine konkrete Anwendung geeignet ist. Genau diesen Empfehlungen folgt auch der ipt Souveränitäts-Kompass: Risiken verstehen, Wahlfreiheit erhalten und Handlungsfähigkeit sichern.

Mehr dazu hier

«Governance ist kein bürokratisches Hindernis, sondern das Regelwerk deiner Freiheit. Ohne klare Leitplanken wird die Autonomie kurzfristigen ‹Quick Wins› geopfert.»

Souveränität lässt sich nicht allein durch Technik lösen. Sie benötigt einen organisatorischen Rahmen, der sicherstellt, dass Architekturentscheidungen auch in fünf Jahren noch tragfähig sind. Genau hier bewegen sich viele Organisationen in einem Spannungsfeld: Auf der einen Seite stehen Governance-Skeptiker, die befürchten, dass starre Regeln die Agilität und Innovationskraft ausbremsen. Auf der anderen Seite besteht die Notwendigkeit, regulatorische Vorgaben einzuhalten und nicht blind in Abhängigkeiten zu geraten. Bei ipt verfolgen wir deshalb den Ansatz des Guardrail-Architekten: Wir bauen Leitplanken, die Orientierung geben und Risiken minimieren, ohne den Weg zu versperren. Dafür haben wir sechs Governance-Prinzipien definiert, die als Kompass für eine nachhaltige und zukunftsfähige Souveränitätsstrategie dienen.

4.1 Die sechs ipt-Prinzipien für souveräne Governance

01 Verantwortung über digitale Souveränität klar definieren

02 Entscheidungsleitplanken vor Technologieentscheiden festlegen

03 Governance und Architektur konsequent verzahnen

04 Abhängigkeiten sichtbar und messbar machen

05 Exit-Fähigkeit regelmässig überprüfen

06 Souveränitätsstrategie systematisch überprüfen und nachschärfen

Diese Prinzipien orientieren sich an den strategischen Eckwerten moderner IT-Steuerung – etwa der Weisung 012 des Bundes zur digitalen Souveränität (11.12.2025) – und machen Souveränität operativ messbar.

01 Verantwortung über digitale Souveränität klar definieren

Digitale Souveränität braucht eine explizite Verankerung in der Führung des Unternehmens. Es muss klar definiert sein, wer die Gesamtverantwortung trägt. Nicht nur für Security oder Compliance, sondern auch für die strategische Balance zwischen Abhängigkeit und Kontrolle. Ohne eindeutige Ownership bleibt Souveränität ein diffuses Thema ohne Durchsetzungskraft.

02 Entscheidungsleitplanken vor Technologieentscheiden festlegen

Governance darf nicht reaktiv sein. Bevor Cloud-Anbieter, KI-Services oder Plattformen gewählt werden, müssen klare Leitplanken definiert sein: Welche Daten dürfen wohin? Welche Abhängigkeiten sind akzeptabel? Welche Exit-Fähigkeiten sind zwingend? Erst wenn diese Fragen vorab geklärt sind, wird Technologie zur bewussten Wahl.

03 Governance und Architektur konsequent verzahnen

Souveränität ist kein reines Policy-Thema, sie manifestiert sich auch in der Architektur. Modularität, offene Schnittstellen, Portabilität und standardisierte Integrationsmuster erhöhen die strategische Beweglichkeit. Governance sollte deshalb integraler Bestandteil von Enterprise Architektur, Plattformstrategie und Cloud Operating Model sein.

04 Abhängigkeiten sichtbar und messbar machen

Was nicht sichtbar ist, kann nicht gesteuert werden. Technologische Lock-ins, vertragliche Bindungen, Betriebsabhängigkeiten und Datenflüsse über Jurisdiktionen hinweg sollten systematisch erfasst werden. Ein strukturiertes Scoring-Modell schafft Vergleichbarkeit und verhindert opportunistische Einzelentscheide ohne Gesamtperspektive.

05 Exit-Fähigkeit regelmässig überprüfen

Digitale Souveränität zeigt sich nicht im Normalbetrieb, sondern im Ernstfall. Organisationen sollten periodisch prüfen, wie realistisch ein Anbieterwechsel ist, wie lange die Migration dauern würde, welche Kosten anfallen und welche regulatorischen Hürden bestehen. Souverän ist nicht, wer unabhängig ist, sondern wer wechseln kann.

06 Souveränitätsstrategie systematisch überprüfen und nachschärfen

Digitale Souveränität ist kein Zielzustand, sondern ein fortlaufender Prozess. Geopolitische, regulatorische und technologische Rahmenbedingungen verändern sich laufend. Organisationen müssen ihre Annahmen regelmässig überprüfen, Risiken neu bewerten und Prioritäten anpassen.

3.2 Der Guardrail-Ansatz: Freiheit mittels Leitplanken

Wir bei ipt glauben nicht an Verbotsschilder. Sinnvolle Governance funktioniert nach dem Guardrail-Prinzip: Wir bauen automatisierte Leitplanken (Policy-as-Code). Deine Entwickler können sich innerhalb dieser Grenzen frei und schnell bewegen. Erst wenn eine Entscheidung die Souveränität gefährdet (beispielsweise durch die Nutzung eines hochproprietären Dienstes), greift das System ein und wir können in einen Dialog treten, um eine bewusste Wahl zu treffen.

Zudem sollten die Entwickler Zugriff auf eine Sandbox-Umgebung mit minimaler Governance haben, in der sie mit neuen Technologien und Produkten experimentieren und diese evaluieren können.

Entscheidet sich digitale Souveränität in der Cloud oder mit Governance?

Digitale Souveränität wird oft geopolitisch diskutiert. In der Praxis entstehen die grössten Risiken jedoch durch fehlende Governance, unklare Verantwortlichkeiten und technologische Abhängigkeiten.

Jetzt in den Blogpost eintauchen

3.3 Checkliste:
Souveräne Governance

- ❒ **Strategie:** Ist eine digitale Souveränitätsstrategie vorhanden?
- ❒ **Verantwortung:** Trägt jemand auf der Führungsebene die Verantwortung für die digitale Souveränität?
- ❒ **Übersicht:** Hast du eine Liste, die Workloads nach Souveränitätsbedarf klassifiziert?
- ❒ **Ausschreibungen:** Sind Anforderungen an Souveränität Teil der IT-Ausschreibungen?
- ❒ **Vertragliche Hoheit:** Ist explizit ausgeschlossen, dass der Provider deine Daten verwendet, z. B. für das Training eigener KI-Modelle?
- ❒ **Exit-Plan:** Ist ein Exit-Plan für alle geschäftskritischen Applikationen Pflicht, vorhanden und geprüft?
- ❒ **Anbieterabhängigkeit:** Wird die Anbieterabhängigkeit gemessen und sichtbar gemacht?
- ❒ **Risiko-Check:** Werden Souveränitäts-Risiken regelmässig im Risiko-Board besprochen?
- ❒ **Automatisierte Reports:** Können Reports zur Einhaltung regulatorischer Vorgaben in Bezug auf Souveränität automatisiert erstellt werden?

05 Wirtschaftlichkeit:

Souveränität als Renditebringer

Digitale Souveränität wird oft als Kostenfaktor missverstanden. In Wahrheit ist sie eine strategische Investition in die langfristige finanzielle Handlungsfähigkeit. Diese vier Überlegungen zur Wirtschaftlichkeit sind notwendig:

1. **Total Cost of Ownership (TCO) neu denken**
   Ein Cloud-only-Ansatz ohne Exit-Strategie wirkt initial günstig. Doch die Rechnung ändert sich drastisch, wenn die indirekten Kosten miteinbezogen werden: steigende Lizenzgebühren bei Monopolstellung oder Verkauf und der enorme Aufwand einer Migration unter Zeitdruck. Eine souveräne Architektur senkt das Risiko teurer Ad-hoc-Anpassungen deutlich.

2. **Verhandlungsmacht durch glaubwürdigen Exit**
   Wirtschaftlichkeit entsteht durch Wettbewerb. Nur wer technisch in der Lage ist, den Provider zu wechseln, verfügt über echte Verhandlungsmacht bei Vertragsverlängerungen. Die Fähigkeit zum Wechsel (Exit-Readiness) ist der wirksamste Hebel gegen einseitige Preiserhöhungen eines Anbieters.

3. **Entgangene Gewinne bei Service-Unterbrechungen**
   Entgangene Gewinne durch eine Serviceunterbrechung werden von Providern nie übernommen. Wer komplett von ihnen abhängig ist, muss dieses geschäftliche Risiko entweder akzeptieren oder eine teure Migration ins Auge fassen.

4. **Innovationsschutz**
   Abhängigkeit bedeutet, an die Roadmap eines Anbieters gebunden zu sein. Wenn der Anbieter einen Service einstellt oder strategisch verändert, entstehen Migrationskosten. Souveräne Unternehmen behalten die Kontrolle über ihren Innovation Stack und können schneller auf Marktveränderungen reagieren, ohne auf die Entwicklungen eines Providers zu warten.

	Ohne Souveränität (Lock-in)	Mit Souveränität (Unabhängig)
Initialkosten	Niedrig	Moderat
Betriebskosten	Niedrig	Niedrig–Moderat
Kostensteigerungen	Unvorhersehbar (Preishoheit Anbieter)	Kontrolliert (Wettbewerbsfähig)
Datenexport	Moderat	Niedrig
Exit-Aufwand	Hoch	Moderat und Planbar

06 Der Weg zur Umsetzung:

Dein Souveränitäts-Kompass

Digitale Souveränität ist kein Hindernis für Innovation – sie ist deren Ermöglicher. Wer technologische Abhängigkeiten aktiv steuert, schafft die Grundlage, um moderne Cloud- und Plattformtechnologien gezielt zu nutzen, ohne die eigene strategische Autonomie zu verlieren. Doch Souveränität entsteht nicht durch ein einmaliges Projekt oder reine Technologieentscheidungen. Sie ist ein kontinuierlicher Prozess bewusster Gestaltung – von Governance und Architektur bis hin zu Daten, Betrieb und Resilienz.

Mit dem Souveränitäts-Kompass zeigt ipt auf, wie Organisationen die richtige Balance zwischen Kontrolle, Flexibilität und Innovationsfähigkeit finden. Statt starrer Vorgaben setzen wir auf klare Leitplanken, die Orientierung geben und nachhaltige Entscheidungen ermöglichen. Ob Schutz sensibler Daten, resiliente Plattform-architekturen oder die bewusste Steuerung von Abhängigkeiten: Die Entscheidung liegt bei dir.

Wir bei ipt glauben nicht an Blackbox-Consulting. Wir berücksichtigen deine individuellen Souverä-nitätsanforderungen, nachdem wir diese zusam-men im Workshop erarbeitet haben.

Bist du bereit, deinen Kompass neu auszurichten?

Digitale Souveränität bei ipt

Mehr zum Workshop

Souveränitäts-Kompass von ipt

Das Vorgehen auf einem Blick

Kick off & Briefing

- Gemeinsames Verständnis von Digitaler Souveränität schaffen
- Ziele, Erwartungen und Rahmenbedingungen festlegen

WORKSHOP 1
Standort-bestimmung, Risiko-/ Gap-Analyse

- Aufnahme des IST-Zustands in den vier Dimensionen der digitalen Souveränität
- Erste Definition des angestrebten SOLL-Zustands
- Identifikation zentraler Risiken und Abhängigkeiten

Souveränitäts-Fragebogen

- Vertiefung und Validierung der Erkenntnisse
- Ergänzung von Perspektiven aus Business, IT, Data und Governance

WORKSHOP 2
Handlungsfelder & Routenwahl

- Ableitung konkreter Handlungsfelder
- Diskussion und Priorisierung möglicher technologischer Lösungsoptionen
- Definition einer geeigneten Umsetzungsroute

Abschluss-bericht

- Zusammenfassung von IST- und SOLL-Zustand
- Dokumentation der identifizierten Risiken
- Empfehlungen zu Handlungsfeldern und Lösungsoptionen
- Management Summary für Entscheidungsträger

Navigation & Kurskorrektur
(im Vorgehen nicht inbegriffen)

- Begleitung bei der Umsetzung
- Regelmässige Überprüfung der Zielerreichung
- Anpassung der Route bei veränderten Rahmenbedingungen

Infos und Anmeldung

Teilnehmende: 3–5 Schlüsselpersonen aus Business, IT, Data und Governance (ideal: CIO/CTO/CDO)

Ort: 2 Halbtages-Workshops (vor Ort)

Kosten: 10'000 CHF

Mehr dazu hier

Impressum

Verfasser:innen von Innovation Process Technology (ipt):

Redaktion: Noemi Haag
Texte: Christian Fehlmann, Jakob Beckmann, Noemi Haag, Silvan Tschopp
Lektorat: Vera Biehl, Thomas Schaller
Design: Melanie Wettstein

Publikationsdatum: 2026

Innovation Process Technology AG
Zürich | Bern
info@ipt.ch | www.ipt.ch

Souverän ist nicht, wer unabhängig ist,
sondern wer jederzeit die Wahl behält.