Digitale Souveränität neu gedacht

# Eine Continuity Architecture für Public Service

# Executive Summary

### Digitale Souveränität wird falsch diskutiert.

Die Debatte klebt an Cloud-Anbietern, Serverstandorten und geopolitischer Moral. Doch für regulierte Dienstleister liegt der eigentliche Hebel woanders:

> **Nicht im Besitz der Infrastruktur, sondern in der Sicherung des Auftrags.**

Digitale Souveränität bedeutet für Public Service nicht Autarkie. Sie bedeutet:

> **Service-Kontinuität trotz Plattformwechsel.**

Der Auftrag bleibt – auch wenn die Infrastruktur wankt.

Dieses Whitepaper zeigt, wie Fachbereiche durch **Service-Architektur, Migrationsmacht und Mandatsklarheit** echte Handlungsfähigkeit gewinnen – unter KI-Druck, Budgetrestriktionen und regulatorischer Komplexität.

# 1. Das Ende der Autarkie-Illusion

Die Vorstellung, man könne sich digital „abkoppeln", ist strategisch naiv.

So wie Europa nicht „ohne Energie" existieren kann, kann eine moderne Verwaltung nicht „ohne Plattformen" existieren.

Das Ziel ist nicht Isolation. Das Ziel ist **Umlenkungsfähigkeit.**

Im internen Strategiepapier wird das klar benannt:

> Souveränität ist nicht Unabhängigkeit, sondern Service-Kontinuität unter Bedingungen der Abhängigkeit

Für Fachbereiche bedeutet das konkret:

- Ihr Auftrag (z. B. Patientenversorgung, Leistungsgewährung, Energieversorgung) bleibt stabil.
- Ihre IT-Landschaft ist variabel.
- Ihre Verantwortung darf nicht implodieren, wenn Anbieter wechseln.

# 2. Die drei Ebenen der Souveränität

Das Briefing-Dokument beschreibt ein klares Alignment-Modell:

| Ebene | Fokus | Leitfrage |
|---|---|---|
| **Business** | Auftrag & Mandat | Wer haftet wofür? |
| **Service** | Nutzeffekt & Commit | Was versprechen wir konkret? |
| **System** | Tools & Infrastruktur | Welche Plattform unterstützt das? |

Der Fehler vieler Organisationen:

### Sie diskutieren Souveränität ausschließlich auf Ebene 3.

Doch:

> Wer nur die Technik optimiert, verschiebt Haftung nach oben – in den Fachbereich.

### **Digitale Souveränität beginnt oben. Nicht unten.**

# 3. Das Krankenhaus als Realitäts-Test

Die Szenarien-Analyse zum Krankenhaus macht das greifbar.

Ein Krankenhaus kann nicht sagen:

> „Die Software ist ausgefallen, also entfällt heute die Versorgung."

**Der Auftrag bleibt.**

### Szenario A – Vendor-Lock-in

- KI-Triage tief in proprietärem System integriert
- Kein Fallback
- Kein Datenstandard
- Wechsel dauert 24 Monate

**Ergebnis:** Der Chefarzt trägt die Haftung – ohne Mandat zur Systementscheidung.

### Szenario B – Continuity Architecture

- KI als modularer Service-Baustein
- Standardisierte Schnittstellen
- Manuelle Degradationsfähigkeit
- Geplanter Exit

**Ergebnis:** Die medizinische Verantwortung bleibt lieferfähig – unabhängig vom Anbieter.

**Das ist digitale Souveränität in der Praxis.**

# 4. Migrationsmacht: Die strategische Reserve

Das Strategiepapier definiert Migrationsmacht als strukturelle Fähigkeit, Verantwortung und Leistung zwischen Systemen zu bewegen.

Für Fachbereiche heißt das:

| | | | |
|---|---|---|---|
| **Switch-Fähigkeit statt Tool-Treue** | **Exit-Design bereits beim Entry** | **Daten-portabilität als Pflicht** | **Fallback-Workflows als Architektur-Bestandteil** |

Nicht: „Wir bauen alles selbst."

Sondern: **„Wir können wechseln, ohne zu zerbrechen."**

# 5. KI ist Verstärker – kein Retter

Das Briefing-Dokument ist hier unmissverständlich:

> KI löst keine organisatorischen Probleme. Sie macht unklare Verantwortungen sichtbar – und skaliert sie.

Wenn Service-Definitionen unscharf sind, skaliert KI falsche Entscheidungen schneller.

Wenn Haftung diffus ist, macht KI sie algorithmisch dokumentiert sichtbar.

Deshalb gilt:

**No AI without Service Architecture.**

# 6. Servicialisierung: Der methodische Kern

Die Ausbildungsreihe „ServicEducation" beschreibt Servicialisierung als Übertragung industrieller Prinzipien auf Services.

Services sind:

- immateriell
- nicht lagerbar
- simultan konsumiert
- variabel

Deshalb müssen sie präziser spezifiziert werden als Produkte.

**Souveränität entsteht durch:**

- klare Service-Objekte
- definierte Nutzeffekte
- transparente Service-Beiträge
- eindeutige Commit-Logik

### Nur was spezifiziert ist, ist migrierbar.

# 7. Die „Centurio"-Realität im Fachbereich

In vielen regulierten Organisationen trägt der Fachbereich faktisch:

| | | | |
|---|---|---|---|
| Lieferver-antwortung | Haftung | Eskalations-druck | Reputations-risiko |

Ohne strukturelles Mandat über Systementscheidungen.

Das Strategiepapier beschreibt genau dieses Phänomen.

> Digitale Souveränität ist deshalb kein IT-Thema.
>
> **Sie ist Schutzarchitektur für operative Verantwortung.**

# 8. Fünf harte Praktiken für Public Service

Für Fachbereichsleiter:innen:

01

### Service-Definition vor Systemwahl

Definieren Sie Nutzeffekt und Service-Typ – produktunabhängig.

02

### Commit-Logik klären

Wer verspricht wem was – mit welchen Grenzen?

03

### Degradationsfähigkeit designen

Wie liefern wir bei eingeschränkter Funktion weiter?

04

### Exit beim Entry planen

Wie verlassen wir die Plattform – realistisch?

05

### Haftungsarchitektur prüfen

Wo landet Verantwortung bei Systemausfall?

# 9. Strategisches Fazit

**Digitale Souveränität ist kein Produkt.**

Sie ist eine Eigenschaft der Organisationsarchitektur.

Für Public Service bedeutet das:

- Nicht „Cloud oder On-Prem".
- Nicht „USA oder Europa".
- Nicht „Open Source oder Proprietär".

Sondern:

> # Bleibt Ihr Auftrag lieferfähig, wenn sich die Infrastruktur ändert?

Wenn die Antwort „nein" ist, haben Sie ein Architekturproblem – kein Technikproblem.

## Schlussgedanke

# Der Auftrag bleibt. Auch wenn Infrastruktur ausfällt.

Digitale Souveränität ist die Fähigkeit, Systeme zu wechseln, ohne dass Verantwortung implodiert.

**Und genau dort beginnt die strategische Arbeit des Fachbereichs.**