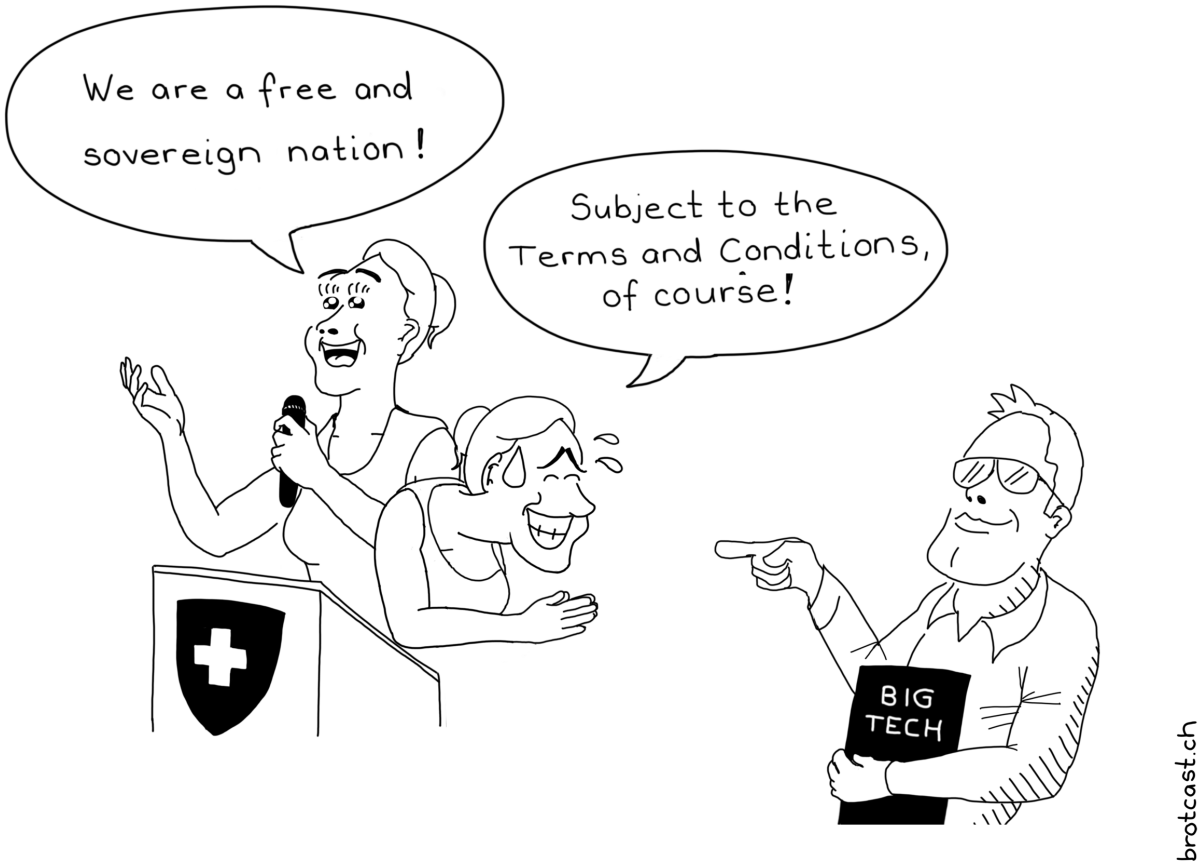
November 2025
Version 1.0 EN

DIGITAL SOCIETY

DIGITAL SOVEREIGNTY

POSITION

Authors: David Sommer, Thomas Mandelz, Alexander Steiner, Alfred Seiler, Ralph Bachmann, Marcel Waldvogel, Ryan Kougionis



DIGITAL SOCIETY / CH-4000 BASLE
OFFICE@DIGITALE-GESELLSCHAFT.CH / DIGITAL-SOCIETY.CH

Abstract

Digital sovereignty is crucial for Switzerland's resilience and competitiveness in the digital age. Digitale Gesellschaft calls on policymakers and business leaders to regain control of the country's digital infrastructure and data in order to reduce its dependence on global providers. The paper outlines specific fields of action such as promoting sovereign software solutions, establishing government guidelines, and training skilled personnel. In the long term, only a sovereign digital infrastructure can safeguard Switzerland's security, self-determination and innovative capacity.

1 Without Digital Services, Society Grinds to a Halt

Digital systems have become part of today's critical infrastructure – like water, electricity and transport. If these system were to fail, it would immediately result in a state of emergency for both the public and private sectors.

Unlike a bicycle, a digital service cannot simply be repaired at a local workshop. Its components are distributed around the globe, placing them beyond the control of users. Many parts are neither adaptable nor replaceable. Disruptions – whether caused by errors, cyberattacks or geopolitical crises – can leave users with a system that cannot be further developed or operated.

2 Digital Sovereignty as a Necessity

Dependence carries risks: Outsourcing essential digital infrastructure without the ability to operate or adapt it independently in an emergency creates structural vulnerabilities. Society loses its ability to act in times of crisis. Digital sovereignty means regaining a minimum level of control. This is not only a matter of governmental resilience but also of economic competitiveness.

The biggest challenges are dominant providers, complex IT systems and insufficient resilience. Legal barriers, financial pressure, and a shortage of skilled professionals further limit the ability to build or adapt systems to address specific needs. At the same time, as our data is processed, it passes through an increasing number of infrastructures and jurisdictions, leading to a loss of control. Legal safeguards such as data-protection agreements do not change the fact that Switzerland has little influence over the availability and further development of the digital systems it relies on.

In order to remain flexible and independent, companies depend on adaptable IT infrastructures. Having control over digital systems fosters innovation and mitigates dependence on dominant providers. A sovereign digital infrastructure strengthens not only the economy but also Switzerland's overall competitiveness and its ability to actively shape its IT landscape.

3 Strategic Goal of Digital Policy

The Digital Society therefore calls on Switzerland to make digital sovereignty a central goal of its digital policy.

The following definition, based on and slightly expanded from that used at the 2018 German *Digital-Gipfel*, serves as a foundation:

Digital sovereignty of a state or organisation requires full control over stored and processed data, as well as over the applications used to process that data. It encompasses the independent decision of who may access which data. It also includes the capability to develop, modify, control and augment technological components and systems autonomously, and to operate those systems effectively.

Digital sovereignty covers the entire technology stack: From raw material extraction to the development and governance of artificial intelligence systems.

Switzerland cannot face these challenges alone and must collaborate with like-minded partners, such as the European Union. This paper focuses on operating national data centres and network infrastructures, as well as ensuring the availability and adaptability of software.

The path ahead is long but unavoidable. Each procurement decision that incorporates sovereignty criteria represents a significant step forward.

4 Core Demand: Independence of IT Infrastructure

In an emergency, IT infrastructure – including hardware, software and data – must be operable and adaptable in Switzerland by locally based professionals, i.e. independently of foreign entities. We explicitly do not require that the entire digital infrastructure be built or managed within Switzerland. What matters is that key components can be operated autonomously and tailored to specific requirements.

The Digital Society has identified three key areas of action:

4.1 Development and Promotion of Software and System Architectures

- **Vendor independence and interoperability:** Systems must be operable without a long-term lock-in to a particular vendor. This requires interchangeable components, migratable and standardised data formats, and open protocols.
- **Adaptability and security:** It must be possible to assess the quality and security of systems independent from one another, and software must be customisable to meet defined criteria. Access to source code under appropriate licensing models is therefore necessary.

4.2 Binding Public Governance

- **Adjust procurement guidelines:** Public procurement and contract development must be tied to sovereignty criteria.
- **Strengthen IT resilience:** Political and economic leaders must assume responsibility for identifying technological, economic and political dependencies and for assessing or mitigating risks associated with them.
- **International coordination:** Build cross-border partnerships for the joint creation of sovereign solutions.

4.3 Education and Training of Sufficient Skilled Professionals

- **Provide a sufficient number of qualified professionals and connect them:** Professionals must be able to develop and operate sovereign systems. While skilled and motivated individuals exist at least in part, they are not efficiently organised within networks.
- **Crisis response capability:** In the event of outages or threats, a sufficient pool of trained personnel must be readily available to respond swiftly and effectively.

4.4 Measures

From our perspective, the following measures are particularly urgent and feasible in the short term:

- Introduce sovereign solutions for office automation (email, calendar, collaboration, document creation and storage).
- Build and maintain secure, scalable and independent hosting infrastructure.
- Standardise cloud environments to simplify switching providers .
- Provide economic support for technologies, products and companies offering sovereign solutions. Create appropriate incentives and ecosystems.
- Promote the training and networking of experts in key technologies.
- Prioritise open, replaceable components in public IT procurement (open source), also at cantonal and municipal levels.

The time to act is now – before existing dependencies become even more entrenched. Only if we can operate and shape our digital infrastructure independently over the long term will Switzerland remain digitally competitive, secure, and self-determined.