

How to Achieve Maximum Data Sovereignty in the Cloud



When it comes to IT infrastructure, the question for most Swiss IT teams today is no longer whether to move to the Cloud or not. Forward-looking companies have long embraced Cloud adoption, making it a central component of their IT strategies. Budget, technical expertise, regulatory requirements, and strategic priorities all play a decisive role in determining which Cloud provider is the best fit for a company.

While hyperscalers such as Microsoft have historically been able to cover nearly every business scenario, calls for greater digital independence have grown louder in Switzerland in recent months and years.

On the following pages, we summarize why so many Swiss companies are more critical of hyperscalers in 2026 than they used to be in the past and what aspects should be considered specifically regarding data sovereignty when choosing a Cloud provider.

Growing Skepticism Toward Big Tech in Switzerland

According to a representative 2025 survey conducted by the research institute [gfs.bern](#) (report in German), public sentiment in Switzerland toward international technology companies ranges from ambivalent to negative. Many respondents are concerned about the political influence of Big Tech companies.

Around 84% fear that the home countries of major tech corporations, particularly the United States and China, could exert too much influence over politics and society. Additionally, 82% believe Switzerland risks becoming overly dependent on tech giants. According to [gfs.bern](#), this perception is closely linked to the growing importance of digital sovereignty in public discourse.

How Swiss Organizations Use Global Hyperscaler Clouds

According to [research by tech journalist Adrienne Fichter](#) (article in German), hyperscalers such as AWS and Microsoft process highly sensitive data in Switzerland. This includes classified information whose disclosure could significantly impact national security - such as military operational plans - as well as highly sensitive personal data like health records. Widely used customs applications run in the AWS Cloud, and the organ donor registry is based on Microsoft Azure services. Other Swiss federal offices are hesitant to adopt global Cloud solutions, partly due to their responsibility for data protection.

Meanwhile, an increasing number of Swiss organizations are turning away from Big Tech. For example, the Zurich

municipal health services opted against a Cloud solution when replacing their IT system Orion, which is used for managing and billing outpatient care services. Due to the sensitive nature of health data, the risks associated with cloud usage were deemed too high. Instead, the new solution will be operated locally to maintain greater control over data.

Did you know? To meet a growing customer demand, Xelon operates dedicated Swiss Private Cloud infrastructures in ISO-certified Swiss data centers, ensuring that customers retain full control over their data and systems at all times.

Does Swiss Politics Support Data Sovereignty?

At the political level, there are ongoing efforts in Switzerland to reduce dependence on Big Tech and rely more on European or open-source technologies. However, differing opinions exist within government and administration.

Some Swiss policymakers advocate for a consistent move away from Big Tech and the development of independent

solutions. Others emphasize the advantages of existing providers, particularly in terms of efficiency, innovation potential, and cost.

[According to the digital magazine Republik](#) (article in German), this divergence has led to growing polarization in political discussions.



The CLOUD Act: A Key Reason for Distrust Toward US Hyperscalers

Even with data centers in Switzerland, US-based companies remain subject to foreign laws such as the US CLOUD Act. Enacted in 2018, the CLOUD Act requires US companies to provide data to US authorities—even if that data is stored outside the United States. This means that even if a US-based Cloud provider operates data centers in Europe, it may still be compelled to hand over data.

Additionally, the policies of US President Donald Trump have been strongly focused on US interests, leaving limited room for stable international cooperation. This raises concerns among Swiss and European companies about the long-term reliability of Cloud providers from politically volatile environments. Trust in the political stability and reliability of the United States as a technology partner has significantly declined.

Even before Trump's second term, demand for greater digital sovereignty had been growing in both the EU and Switzerland. Swiss Cloud solutions can address this need by offering more control over data, infrastructure, and technological standards.

“The discussion around data sovereignty has grown more urgent,” says Roman Schweizer, CEO of Xelon. “We are also seeing a clear shift: Swiss companies have grown significantly more skeptical towards global Clouds - not due to technical limitations, but to safeguard independence and to meet both external as well as internal data sovereignty demands.”

Explore with our Cloud Architects which Cloud scenario is the best fit for your company.

Case study: When Customers Demand Swiss Data Residency

One Switzerland-based company that recently migrated its data from an international provider to a Swiss Cloud is Z83 AG. “We work with highly sensitive data every day, and it is crucial that it is stored exclusively in Switzerland,” says Luca Ferrari, CFO and Partner at Z83 AG.

Founded in 2020, Z83 AG has around 30 employees as of spring 2026. The rapidly growing company, based in Olten, is currently developing its own payroll software tailored specifically for Swiss SMEs. “There is currently no truly good payroll solution for smaller companies. That's why we decided to develop our own solution tailored to the needs of SMEs and startups,” Ferrari explains.

The expansion of the service portfolio requires a secure and stable IT infrastructure. Xelon's sovereign Swiss Cloud enables Z83 AG to focus on its mission while ensuring all customer data remains in Switzerland and subject to Swiss data protection laws.

Our Cloud Architects will be happy to show you how you can reliably meet the highest compliance and data security requirements with a Swiss Cloud from Xelon.

Schedule a non-binding consultation here.

Checklist: Questions to Ask a Cloud Provider About Data Sovereignty

Choosing a Cloud provider goes far beyond a technical decision. It directly impacts data sovereignty, security, compliance, and business control.

Which Cloud provider makes sense for your business depends on your specific requirements, regulatory environment, risk tolerance, and strategic goals.

Use this checklist to guide your evaluation:

- ✓ Where are the data centers located?

- ✓ In which countries is your data stored, processed, and backed up?

- ✓ Are there options for geographic data residency restrictions?

- ✓ Is data replicated across regions? If so, which ones?

- ✓ Which national and international laws apply to my data?

- ✓ Do extraterritorial laws such as the CLOUD Act apply?

- ✓ How are government data requests handled? Are processes transparent?

- ✓ Is data transferred to third countries? On what legal basis?

- ✓ What certifications (e.g., ISO 27001) does the provider have?
Are data centers certified?

- ✓ How is physical data center security ensured?

- ✓ What encryption standards are used?

- ✓ Who controls encryption keys and access?

- ✓ Who legally owns the data?

- ✓ Can I export my data at any time?

- ✓ Are independent audits conducted? How often and under which standards?

Once you have clear answers to these questions, you can confidently enter into a contract with a Cloud provider.





Extra Tip: Swiss Clouds Are Not Necessarily More Expensive

At first glance, global Cloud offerings often appear more affordable, with attractive entry prices and low barriers to entry. However, over time, the picture often becomes more complex.

Costs for data transfer, additional services, monitoring, and support can accumulate gradually and are not always immediately visible. As teams grow, customer bases expand, and infrastructure requirements evolve, complexity increases. This can lead to unexpected expenses and billing that is difficult to understand. That's why it's important not only to consider initial pricing but also to evaluate total cost of ownership over time and fully understand pricing structures.

[Calculate the costs for a tailored Swiss Cloud here.](#)