BÄR & KARRER BRIEFING APRIL 2026

CLOUD USAGE AND DIGITAL SOVEREIGNTY: STRATEGIC OPTIONS FOR SWISS AUTHORITIES

Cloud services form an integral part of modern administrative work. At the same time, when federal, cantonal and municipal authorities outsource data processing, they must comply with data protection requirements, confidentiality obligations such as official secrecy and information security regulations, while ensuring long-term operational capacity. In the public debate – which has gained additional momentum due to current political developments in the US – the focus is currently on the use of US cloud services by Swiss authorities in the context of digital sovereignty[1,2] This debate was intensified by the resolution published in November 2025 by privatim, the Conference of Swiss Data Protection Commissioners, which can be read as a *de facto* ban on the use of hyperscalers in public administration. This thrust is also already becoming concrete in procurement: for example, the FOPH's tender for the SwissHDS infrastructure (February 2026) stipulates that all infrastructure components must not be technically or legally dependent on external jurisdictions (e.g., the US CLOUD Act).

Digital sovereignty of Swiss authorities means neither self-sufficiency nor isolation, but rather the ability to manage and control the use of external digital services independently. This briefing categorises the arguments presented, highlights areas of tension and provides orientation for the use of the cloud in administration. The analysis shows that there are no completely risk-free solutions: Every option – be it a US cloud service, a Swiss or European provider, an on-premises or open-source solution – requires case-by-case trade-offs between functionality, security, sovereignty and operational costs.

[1] The Federal Council defines digital sovereignty as the ability to exercise control and take action necessary for the fulfillment of state functions in the digital sphere (report "Digital Sovereignty of Switzerland" dated November 26, 2025, p. 6).

[2] The question of whether cloud usage complies with official secrecy (Art. 320 SCC) and data protection obligations has been largely clarified: cloud providers may be engaged as auxiliary persons of the authority in the fulfilment of public duties, provided that they are carefully selected, instructed and supervised. They are thereby themselves subject to official secrecy. From a data protection perspective, outsourcing to a cloud provider constitutes commissioned processing and is permissible subject to the conditions set out in Art. 9 FADP. These two aspects are not discussed further in the present briefing.

A. KEY MESSAGES

- **Digital sovereignty** means neither self-sufficiency nor isolation, but rather the ability of public authorities to manage and control the use of external digital services independently.
- The **US CLOUD Act does not establish a direct right of access by US authorities** to data stored abroad. Production orders require a court order, reasonable suspicion and a concrete purpose of criminal prosecution. Additionally, constitutional safeguards limit their reach.
- **Production orders** under the US CLOUD Act primarily serve the investigation of **serious crimes** (such as terrorism and cybercrime). Ordinary administrative data such as project documents, statistics or personnel files are typically not the focus of US investigations.
- **Transparency reports** from US hyperscalers confirm this: **disclosures of content data** from **foreign enterprise customers** to US law enforcement agencies are **extremely rare** (0.008% of all requests at Microsoft). No cases involving public sector customers are known to date (as of April 2026).
- **EU/CH cloud providers** also **do not** guarantee **complete freedom from risk**. Subprocessors, global supply chains or emergency failovers in third countries can indirectly trigger extraterritorial access rights. Furthermore, there are often operational limitations regarding portfolio, scalability, support and certification depth, which can result in additional integration and testing efforts.
- **Open-source and on-premises solutions** shift the entire burden of security and operational responsibility to the public authority and come with significant costs as well as specific cyber risks. Open-source projects are also subject to sanctions-related risks and supply chain risks. While on-premises solutions offer physical control, they are limited in terms of scalability and reliability.
- Consequently, every (cloud) project requires a **risk analysis**, regardless of whether a US, EU, or Swiss provider, or an open-source or on-premises solution, is chosen. On this basis, the public authority must make a **risk-based decision** as to whether the remaining residual risks are acceptable and the project can be approved.

B. US CLOUD ACT: SCOPE, LIMITATIONS, AND PRACTICAL RELEVANCE FOR SWISS AUTHORITIES

I. LEGAL CLASSIFICATION: SIGNIFICANCE OF THE CLOUD ACT

The CLOUD Act, which entered into force in March 2018, clarifies the *Stored Communications Act* (SCA) and specifies that US authorities, in investigations related to serious crimes such as terrorism, violent crime, child sexual exploitation and cybercrime, may demand the production of communications data stored or processed by a provider subject to the CLOUD Act on the basis of a warrant, a subpoena or a court order, even if such data is stored on servers outside the United States. The purpose of the CLOUD Act is therefore to support investigations into serious crimes.

The personal scope of the CLOUD Act is broad: it covers all providers of electronic *communication services* or *remote computing* services that are based in the United States, have a branch there, or conduct business in the United States.

The key factor determining applicability is the US legal interpretation of "*possession, custody or control*." Under this interpretation, de facto or de jure control over data by a provider is sufficient, even if the data is stored in data centres in Switzerland or Europe. The CLOUD Act therefore establishes extraterritorial disclosure obligations that may potentially conflict with Swiss legal safeguards (such as administrative and judicial assistance).

Since the CLOUD Act is at the forefront of the current discussion, this briefing focuses on the CLOUD Act. This must be distinguished from Section 702 of *the Foreign Intelligence Surveillance Act* (FISA), which allows US intelligence agencies to conduct program-based collection of foreign intelligence data. Unlike the CLOUD Act, no individual court order is required. The authority to access data is based on a programmatic framework approved by *the Foreign Intelligence Surveillance Court*, which requires US providers to cooperate.

II. NO FREE PASS: THE CONSTITUTIONAL LIMITS OF THE CLOUD ACT

Despite the risks of a production order, a blanket questioning or a general ban on the use of US cloud services by Swiss authorities is not appropriate. When assessing the risks, the decisive factor is not merely the theoretical scope of US laws, but the existing legal safeguards that limit and control requests for data stored by Swiss authorities, as well as the practical likelihood that US authorities will actually access this data.

In this context, the formal disclosure orders under the CLOUD Act are counterbalanced by various constitutional safeguards and procedural guarantees that limit and structure such requests. For

instance, data may only be disclosed based on a US court order if it is relevant to an ongoing criminal investigation in the United States. For such an order to be issued, there must be *probable cause* for a specific criminal offence, and the requested data must specifically contribute to the investigation or prosecution of that offence. A general, blanket, or merely interest-driven data request does not meet the requirements of the CLOUD Act.

Furthermore, the CLOUD Act does not stipulate that data must be automatically disclosed. Rather, the text of the law expressly provides for the possibility of challenging or modifying a court order if a provider falling within the scope of the CLOUD Act has reasonable grounds to believe that disclosure would violate the law of another country. This so-called *comity analysis* requires that, in the event of such objections, a US court can examine whether a disclosure obligation conflicts with the laws of the relevant foreign jurisdiction and, if certain conditions are met, modify or even vacate the order. In practice, this means that orders that do not meet legal requirements are not automatically enforced but are subject to a review process, thereby significantly limiting the theoretical scope of the CLOUD Act due to constitutional safeguards.

After all, the CLOUD Act does not generally prevent cloud providers from informing affected customers about the disclosure of their data. In certain cases, however, an administrative or court order may restrict or temporarily prohibit such notification (*gag orders*), though such measures must be justified and limited in scope and duration.

III. TRANSPARENCY REPORTS FROM US CLOUD PROVIDERS: DATA DISCLOSURES AS A RARE EXCEPTION

The practical experience gathered since 2018 with such requests is also decisive. The transparency reports of major US cloud providers show that actual data disclosures involving enterprise customers are rare.

At Microsoft[3], in the first half of 2025 (as in previous years[4]), fewer than 0.7% of global requests from law enforcement agencies involved enterprise customer data at all. In most cases, these requests were rejected, withdrawn or redirected in such a way that the authorities had to request the information directly from the customer. To the extent that corporate customer data was disclosed, the majority consisted of non-content data (e.g., basic subscriber information or IP logs), while content data was disclosed in only a minority of cases. Cross-border disclosures of content data remained rare: Microsoft provided content data to US authorities in five cases involving non-US enterprise customers whose data was stored outside the US. Only one of these cases involved a customer based in the EU, who was a contractor for the US government.

When viewed in relation to the total number of requests received by Microsoft since the CLOUD Act came into force, the rarity of requests based on the CLOUD Act becomes even more apparent: disclosures of content data from foreign enterprise customers to US law enforcement agencies accounted for only 0.008% of all global requests.[5] According to Microsoft, none of these rare cases involved government agencies or state institutions.[6]

Amazon Web Services (AWS) states that, since records began, it has not disclosed any data from corporate customers or government agencies located outside the US in response to CLOUD Act orders,[7] and follows a practice whereby requests are – where possible – first addressed to the customer itself. This practice reflects the fact that a duty to disclose exists only when there is a legally valid, binding order, and not automatically in response to every request for disclosure. Furthermore, AWS explicitly clarifies that neither the US government nor any other government is granted unrestricted or automatic access to customer data – including data stored in the cloud.[8]

IV. MINIMAL IMPACT OF CLOUD ACT ORDERS ON TYPICAL ADMINISTRATIVE DATA

The CLOUD Act does not generally limit the categories of data that can be requested – potentially, it covers all data stored by a provider subject to the CLOUD Act, regardless of its location. However, as mentioned, the stated purpose of the law is to enable access to electronic communications in the context of investigations into serious crimes, specifically terrorism, violent crime, child sexual exploitation and cybercrime. In practice, court-authorised production orders in US criminal proceedings typically focus on communication content (emails, chats, messages), communication metadata, and identity data, as these have the greatest evidentiary value for criminal investigations. Communication data is typically relevant for uncovering collusion or planning of crimes, and identity data is used to link accounts to real individuals. Technical system data, internal documents or personnel files, by contrast, are likely to be of interest only in specific investigative contexts and are significantly less frequently affected.

Swiss authorities, on the other hand, primarily store administrative data: internal documents, correspondence, project files, statistics or personnel files. These types of data are typically not of interest for investigations into terrorism, violent crime or

[3] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H1-2025.pdf
[4] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MSFT-GRR-Enterprise-One-Pager-H2-2024.pdf
[5] https://news.microsoft.com/source/emea/2026/02/how-microsoft-is-addressing-digital-sovereignty-in-switzerland/
[6] https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/CLOUD-Act-What-it-is-and-is-not.pdf
[7] https://d1.awsstatic.com/onedam/marketing-channels/website/aws/en_US/whitepapers/compliance/Amazon_AWS_Information_Request_Report_H2_2025.pdf
[8] https://aws.amazon.com/compliance/cloud-act/

cybercrime and are therefore significantly less exposed than, for example, the communication data of private users.

V. DIFFERENTIATED RISK ASSESSMENT INSTEAD OF BLANKET EXCLUSION

Against this backdrop, the risk of actual disclosure of content data to US law enforcement agencies is significantly lower than what a purely theoretical analysis of the CLOUD Act would suggest. Requests from US authorities cannot be ruled out – and this possibility must be considered in the risk assessment. However, concrete figures and established processes show that requests by US authorities for content stored outside the US by cloud services are rare and heavily regulated in real-world scenarios. This puts the practical relevance of the theoretical disclosure obligations into perspective, particularly regarding the use of cloud services by public authorities.

This does not mean that a low statistical risk constitutes an acceptable risk per se. Particularly in the public sector, even a single incident – such as the disclosure of intelligence-related information or documents sensitive to foreign policy – can have significant constitutional and political consequences. What is decisive, therefore, is not merely the probability of occurrence, but the interplay between probability of occurrence and the potential extent of damage. The protection needs analysis, to be conducted by the government agency, serves this purpose precisely: it determines the required level of protection for the information in question. Data subject to official secrecy has heightened confidentiality requirements. The results must be documented in a transparent manner in an information security and data protection (ISDP) concept. The protection needs analysis therefore ensures that data requiring a higher level of protection – regardless of the statistical rarity of an access attempt – is afforded an appropriate level of protection. In individual cases, this may also involve the use of additional technical protective measures or the decision not to outsource data to the cloud. A data protection impact assessment (DPIA) must also be conducted on a regular basis. It assesses the risks of data processing from the perspective of the data subjects, supplements the ISDP concept, and may trigger a prior review by the data protection supervisory authority.

In contrast, a blanket ban on the use of US cloud services does not do justice to this assessment: risks vary considerably depending on the data category, protection requirements and security measures in place, and technical, contractual and legal hurdles further reduce the likelihood that data will actually have to be disclosed in response to requests from US authorities. The fact that these hurdles cannot eliminate all risks completely does not argue against the use of US cloud services as such, but rather in favour of a differentiated, risk-based decision by the authority on a case-by-case basis.

C. Alternatives to US Cloud Services: Opportunities, Limitations and Specific Risks

The discussion is increasingly turning to other procurement options, ranging from cloud offerings from European and Swiss providers to open-source solutions and on-premises infrastructures. Since each of these options carries its own legal, technical and operational risks, they should not be treated across the board as lower-risk alternatives to the use of US cloud services. Here, too, operational suitability and risk profile must be carefully assessed.

I. CLOUD OFFERINGS FROM EU/SWISS PROVIDERS

1. Remaining extraterritorial disclosure obligations

The use of cloud offerings from EU/CH providers reduces the risk of a production order under the CLOUD Act, provided the provider is not subject to the CLOUD Act. Nevertheless, even such models are not free from risks regarding access from third countries. For example, foreign group companies, the use of sub processors based in third countries or the involvement of global suppliers – such as through global content delivery network (CDN) or domain name system (DNS) chains, 24/7 support, or emergency failover in non-EU/CH regions – can indirectly trigger extraterritorial access rights or disclosure obligations.

A current example of this is the OVHcloud case: In late September 2025, the Ontario Superior Court of Justice upheld a production order against OVHcloud's French parent company to transfer customer data stored in Europe to the Royal Canadian Mounted Police. The basis for this was the company's presumed "virtual presence" in Canada through its subsidiary there. The case demonstrates that even such a corporate presence in a third country can trigger extraterritorial production orders, even if local law conflicts with this.

Furthermore, the EU Regulation on European Production and Preservation Orders for Electronic Evidence (*E-Evidence Regulation*) provides that, under certain conditions, authorities of EU member states will be able to issue cross-border production orders directly to service providers in other member states.

Regardless of this, access by authorities via international administrative and judicial assistance (e.g., based on the Second Additional Protocol to the Budapest Convention) remains possible. Such requests are not made directly through the cloud provider but are addressed to the competent domestic authority and are subject to the procedural requirements of administrative and judicial assistance (including the Swiss Federal Act on International Mutual Assistance in Criminal Matters).

2. Increased integration effort due to limited portfolio and platform maturity

In addition, EU/CH providers face de facto and operational risks compared to US hyperscalers. The service and application portfolio is often less broad or mature, particularly in the areas of AI and analytics functions, as well as platform and managed services, which can lead to additional and increased integration efforts or functional limitations. Interfaces and integrations are often less standardised, making migrations, automations and the operation of complex architectures – which are necessary in modern administrative work – more time-consuming, costly and prone to errors.

3. Limited scalability, support depth and certification coverage

In addition, the pace of innovation and release cycles is slower. Scalability and resilience also tend to be limited: EU/CH providers have fewer regions and availability zones as well as lower global network coverage, which results in higher latencies, tighter capacity limits and greater dependence on individual data centres.

In day-to-day operations, limitations are observed in incident response management and 24/7 support, for example regarding response times, escalation paths or language coverage. Certifications and compliance evidence also cover industry-specific frameworks less frequently. While larger, established cloud providers regularly hold recognised certifications such as ISO 27001 or SOC 2 Type II and proactively extend these to meet additional sector-specific requirements, smaller providers often lack not only the corresponding formal evidence but also the internal governance structures that would enable a reliable assessment of actual compliance with such frameworks.

4. Increased audit and validation effort due to the shift effect

This gap results in the testing and validation burden effectively shifting to the procuring authority, which must then ensure compliance with regulatory and security requirements itself through due diligence reviews, contractual audit rights and individual approval procedures. For authorities that already operate with limited personnel and technical resources in the areas of IT security, data protection law and procurement, this represents an additional burden. This burden is particularly acute when multiple smaller providers must be reviewed and monitored simultaneously, as each provider requires individual risk analyses, customised contract clauses and ongoing control mechanisms, without the synergy effects typically achieved when working with a certified large-scale provider.

In practice, this often leads either to a reduction in the depth of the review, which increases the risk of undetected compliance deficiencies, or to significant delays in procurement procedures because the necessary internal approval processes exceed available capacity. Finally, smaller providers are more heavily impacted by price fluctuations, market consolidation and insolvency risks, which must be considered in long-term planning.

II. OPEN-SOURCE SOLUTIONS

1. Operational and Legal Risks Associated with Self-Managed Operations

The administration's own open-source solutions enable a high degree of control over operations, architecture and key management. They can therefore contribute to greater operational independence and protection against disclosure requests under the CLOUD Act. However, such requests cannot be completely ruled out even with open-source solutions, for example, if operations are conducted via the infrastructure of a provider subject to the CLOUD Act. Regardless, self-managed operation requires a permanent staff of sufficiently qualified specialists, clearly defined security and operational processes, and reliable 24/7 operation.

In addition to operational risks, there are also specific legal and factual risks: These include security vulnerabilities resulting from delayed updates, misconfigurations in complex software stacks, insufficient monitoring (e.g., lack of vulnerability monitoring, inadequate dependency tracking) and compliance risks due to a lack of licence management, particularly in connection with copyleft licences. Added to this are liability and warranty issues, as open-source software is regularly provided "as is," which assigns corresponding responsibility to the authorities. The authority bears full operational responsibility in this regard: system failures, compliance violations or security incidents resulting from insufficient documentation of architecture and dependencies, concentration of expertise in individual personnel or delayed patch deployment are entirely at its own expense.

Independent operation also entails significant costs: in addition to ongoing personnel costs for specialised staff, there are expenses for infrastructure, security audits, licence compliance and continuous development. The total cost of ownership for open-source solutions is often underestimated, as these costs arise not from licence fees but from operational and maintenance expenses.

2. Sanctions, Supply Chain and Cyber Risks

There are also sanctions-related risks associated with the (further) development and, indirectly, the use of open-source software. The most significant current operators of open-source software hosting platforms are based in the US or listed on US stock exchanges. As such, they are subject to the US sanctions regime, which may require them to restrict access for sanctioned developers to avoid violations of the US sanctions regime. If a Swiss public authority obtains open-source software from such hosting platforms, changes to the sanctions regime – such as expansions

of sanctions lists or the inclusion of new countries and organisations – can pose significant risks to operation, maintenance and further development. The example of the Linux kernel demonstrates that such risks are not merely theoretical: In October 2024, eleven Russian kernel developers were removed from their roles for compliance reasons, illustrating the operational dependence of large open-source projects on the sanctions status of individual developers.

In addition, specific cyber risks exist: Because of its publicly viewable codebase, open-source software can be specifically targeted for vulnerabilities. There is also the risk of supply chain attacks, in which malicious code is injected via compromised dependencies or manipulated contributions—as illustrated by the backdoor discovered in March 2024 in the xz-utils library, which had been successfully embedded in the code by the still-unknown actor "Jia Tan" but was detected in time before it could spread widely.

Similar considerations apply to open-source hardware, the use of which is also associated with availability and supply chain risks.

III. ON-PREMISES SOLUTIONS

1. Limitations in Scaling, Resilience and Hardware Dependencies

On-premises solutions, in which the systems are fully under the authority's control (in the authority's own server room, in the authority's own data centre, or at a colocation provider with exclusive authority access), strengthen physical control over infrastructure and data. However, this is offset by specific operational, legal and economic risks. For example, scaling is often limited in the event of short-term increased demand, the risk of failure is higher compared to large cloud infrastructures, and there are dependencies on hardware supply chains.

2. Sole responsibility for security and operations without task sharing

In addition, there is an increased need for qualified specialists to operate an on-premises solution. The government agency must meet and demonstrate compliance with all operational and security requirements – including protection against cyber risks – on its own. Unlike the *Shared Responsibility Model*, in which cloud providers and customers share responsibilities and the provider assumes key security and operational tasks, with on-premises solutions, the agency bears sole responsibility for availability and recovery, data integrity and traceability, archiving and retention obligations, as well as data protection and information security overall. This includes technical and organisational security measures, access controls, role-based and segregation concepts, as well as emergency and recovery processes.

In addition, there are significant investment and operating costs, as well as additional challenges in procurement and operation, such as those related to renewal cycles, vendor lock-in, and maintenance and support contracts.

D. Conclusion: Risk-based case-by-case decision-making as the key to legally compliant cloud usage

The above analysis shows that the CLOUD Act does not constitute a general obstacle to the use of US cloud services by Swiss authorities: Actual figures and established procedures demonstrate that requests by US authorities for content data stored outside the United States are rare in practice and subject to significant legal restrictions. Nevertheless, the public-law context in particular calls for a nuanced assessment: Since even a single incident can have significant constitutional and political consequences, it is not merely the probability of occurrence that matters, but its interaction with the potential extent of damage – which argues for a risk-based, case-by-case decision by the authority, not for a blanket exclusion of US cloud services.

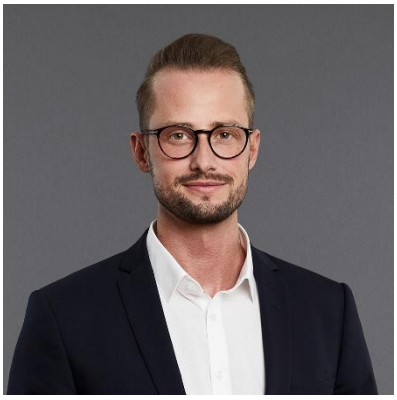
Every (cloud) project therefore depends on a risk decision by the relevant authority, which must be based on its own, well-founded risk analysis. Every cloud solution – whether from a US, Swiss or European provider – is, just like proprietary open-source and on-premises solutions, fraught with specific legal, factual and operational challenges. The authority must systematically identify the specific risks, considering the protection requirements of the information in question, assess the extent to which they are mitigable, and, as part of an informed decision, determine whether the remaining residual risks are acceptable and the project can be approved.

The risk analysis may reveal that for certain projects – such as those involving intelligence-sensitive information or documents of foreign policy sensitivity – a hybrid approach is the more suitable solution. In such cases, for example, a public cloud service is specifically combined with an on-premises or open-source solution to meet different protection requirements.

This conclusion is also based on a contemporary understanding of digital sovereignty: digital sovereignty for Swiss authorities means neither self-sufficiency nor isolation, but rather the conscious ability to manage and control the use of external digital services independently. Relationships with external service providers are standard practice in modern administration and do not constitute a loss of sovereignty provided they are transparent, clearly defined and effectively manageable. A future-proof cloud strategy for the public sector will therefore not fail due to the question of whether cloud services may be used, but rather on whether the authorities create the institutional, technical and legal prerequisites to shape this use independently, in a risk-based manner, and in accordance with the requirements of the rule of law.

AUTHORS

Dr. Christian Kunz
Partner
christian.kunz@baerkarrer.ch
T: +41 58 261 52 66



Ferdinand Rombach
Associate
ferdinand.rombach@baerkarrer.ch
T: +41 58 261 54 12

Dr. Katharina Cardon
Associate
katharina.cardon@baerkarrer.ch
T: +41 58 261 52 82