OPEN _FUTURE

CLOUD INFRASTRUCTURE AS A FOUNDATION FOR DIGITAL SOVEREIGNTY

Policy Building Blocks for the Digital Commons #1

OPEN FUTURE POLICY BRIEF

Authors: dr Zuzanna Warso & Aditya Singh

19 MARCH 2026

ABOUT THIS POLICY BRIEF

Funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

NGI Commons (Open Source and Internet Commons for Europe's Digital Sovereignty) project is funded by the European Union's Horizon Europe research and innovation programme under Grant Agreement number 101135279. This work has received funding from the Swiss State Secretariat for Education, Research, and Innovation (SERI).

Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

The text of this document is based on a report—Deliverable 3.4—submitted to the European Commission as a deliverable of the NGI Commons project. It is part of a series of policy briefs to inform advocacy on Digital Commons and digital sovereignty in the context of the upcoming Multiannual Financial Framework (2028–2034). All NGI Commons deliverables are available on the project website.

Open Future is a European think tank that develops new approaches to an open internet that maximize societal benefits of shared data, knowledge and culture. Open Future advocates for Digital Commons—characterized by distributed production, collective governance, and shared stewardship—as offering the most viable path towards a resilient digital ecosystem.

dr Zuzanna Warso is the Research Director at Open Future. She has fifteen years of experience with human rights research and advocacy. In her work, she focuses on the intersection of science, technology, human rights, and ethics. She holds a Ph.D. in International Law from the University of Warsaw.

Aditya Singh is a Senior Policy Analyst at Open Future with expertise in digital rights, data governance, and technology ethics. His doctoral research on agricultural data governance informs his interests in commons, food systems, and knowledge infrastructures.

INTRODUCTION

Digital sovereignty, understood as the ability of states, organizations, and individuals to independently shape and control their digital environments, has become a central concern for the European Union. Achieving it requires more than regulatory oversight of dominant technology providers: it requires building credible alternatives.

Geopolitical pressures, a growing awareness of strategic dependencies, and a series of upcoming legislative initiatives—including the Cloud and AI Development Act and the revision of public procurement rules—have put cloud dependency on the top of the policy agenda. This policy brief sets out what a well-designed policy intervention targeting cloud infrastructure would look like. The objective is to address the structural roots of Europe's cloud dependency, open the market to genuine alternatives, and ensure that public investment builds digital infrastructure that works for Europe.

PROBLEM DEFINITION: DEPENDENCY CHALLENGE[1]

Cloud computing has become the foundational infrastructure of the digital economy. Rather than owning and operating their own servers, many organizations rely on remote computing resources delivered as on-demand services over the internet.

This infrastructure operates across several layers. At the base, infrastructure services (infrastructure-as-a-service, or IaaS) provide raw computational resources. Above this, platform services (platform-as-a-service, or PaaS) offer pre-configured environments for building and running applications (i.e., databases, development tools, machine learning frameworks). At the top layer, software services (software-as-a-service, or SaaS) deliver complete applications such as email or productivity suites. Today's dominant cloud providers—Amazon Web Services, Microsoft Azure, and Google Cloud, collectively known as the hyperscalers—have bundled these layers into tightly integrated offerings. These three US corporations now control the majority of the European cloud market.

Cloud computing enabled the rapid development of software startups since the mid-2000s, transforming what were once major capital expenditures into variable operating costs.[2] But this transformation of the computing infrastructure model has created dependencies, and they affect more than just corporate players: Europe's governments, civil society, and critical services depend on computing capacity owned, operated, and ultimately controlled by actors beyond European jurisdiction. Unlike energy or telecommunications, where EU law mandates unbundling of infrastructure from services and ensures non-discriminatory third-party access,

[1] This brief benefited from discussions held at the side event 'Bridging Proposals for a Sovereign European Cloud' during the Sovereignty Summit in Berlin on 19 November 2025, organised by the Konrad-Adenauer-Stiftung, the Future of Tech Institute, and the Open Markets Institute.

[2] Ewens, M., Nanda, R., and Rhodes-Kropf, M. (2018). *The Cost of Experimentation and the Evolution of Venture Capital*. Harvard Law School Forum on Corporate Governance. 11 June 2018. Available at: https://corpgov.law.harvard.edu/2018/06/11/cost-of-experimentation-and-the-evolution-of-venture-capital/.

cloud computing lacks a comprehensive framework addressing vertical integration, market concentration, interoperability, or fair access.

The dependency on hyperscalers also affects Digital Commons. Many commons-based projects depend on hyperscaler infrastructure to operate, making them vulnerable to the same risks as all other enterprises and initiatives relying on it. This reflects a broader trend identified in recent literature on patterns of innovation and technological regimes: in the case of cloud, the hyperscalers organize ecosystems in which many contributors, including open source projects, drive innovation, while the platform owners capture the bulk of the associated rents through their control of the underlying infrastructure.[3] Despite these challenges, the commons are also part of the solution to Europe's cloud dependency.

Europe's cloud dependency creates vulnerabilities that span economic, political, and democratic domains. While these vulnerabilities are not new, recent geopolitical developments have accelerated a wider recognition of the risks. A November 2025 Gartner survey found that 61% of CIOs and IT leaders in Western Europe plan to increase their reliance on local cloud providers, driven primarily by geopolitical factors.[4] This creates a window of opportunity: organizations seeking alternatives may accept financial and operational transition costs they previously considered not worth bearing.

The Concentration Problem

Seizing that opportunity requires addressing the structural dynamics that have produced this dependency in the first place. The cloud market exhibits characteristics that drive powerfully toward concentration. The same dynamics that lock in users also starve commons-based alternatives of the oxygen they need to grow. The European Commission recognizes the potential of Open Source to underpin viable alternatives in critical sectors, including cloud, and in January 2026 launched a call for evidence on a European Open Digital Ecosystems Strategy[5] alongside the forthcoming Cloud and AI Development Act (CAIDA). At present, however, these alternatives cannot reach the scale needed to offer genuine choice.

This lock-in operates through compounding technical, financial, and institutional mechanisms:

- **Closed proprietary architectures:** Each major cloud platform has developed its own interfaces, tools, and service designs. Applications built using the services of one hyperscaler cannot easily run on the cloud provided by another without significant re-engineering.

---

[3] Rikap, C. (2024). Intellectual monopolies as a new pattern of innovation and technological regime. Industrial and Corporate Change, 33(5), 1037–1062. https://doi.org/10.1093/icc/dtad077.

[4] Gartner (2025). Gartner Survey Reveals Geopolitics Will Drive 61% of CIOs and IT Leaders in Western Europe to Increase Reliance on Local Cloud Providers. Press release, 12 November 2025. Stamford, CT: Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2025-11-12-gartner-survey-reveals-geopolitics-will-drive-61-percent-of-cios-and-information-technology-leaders-in-western-europe-to-increase-reliance-on-local-cloud-providers

[5] European Commission (2025). European Open Digital Ecosystems (initiative page). Better Regulation – Have Your Say. Brussels: European Commission. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en (accessed 18 February 2026).

- **Data egress fees[6] and switching costs:** Moving data out of a cloud platform incurs substantial costs. The Data Act requires providers to enable migration within 30 days and to phase out switching fees by January 12, 2027. However, awareness remains low, enforcement is fragmented across national authorities, and technical barriers to achieving functional equivalence persist. The Data Act is a powerful tool, but its potential is not yet fully utilized.[7]

- **Bundled offerings and vertical integration:** Hyperscalers bundle infrastructure with platform and software offerings such as productivity suites, AI services, and security tools. Microsoft's integration of Azure with Office 365, or Google's combination of cloud infrastructure with Workspace and AI capabilities, creates ecosystems where each additional service deepens overall dependency.[8] For hyperscalers, many cloud platform services (such as managed databases, AI tools, developer platforms, and authentication systems) often carry minimal margins. This means that the provider makes little or no profit on these services directly. These services are not intended to generate profit themselves, but rather to drive consumption of the underlying infrastructure (compute, storage, networking), where hyperscaler margins are substantial. Hyperscalers use these high infrastructure margins to subsidize cheap or free platform services.[9] Standalone providers, by contrast, must generate profit at the service layer to survive, which is why smaller cloud providers commonly face operating losses. This creates a competitive asymmetry that is unrelated to efficiency. European providers may be more cost-effective at the infrastructure level, but cannot compete against rivals who give away services that non-hyperscalers must charge for.[10]

- **Financial incentives:** Hyperscalers offer startups substantial free credits (typically worth tens or hundreds of thousands of dollars) to build on their platforms. While startup programs are the most visible, similar financial incentives are offered across enterprise, academic, and public sector actors. These programs create dependency from inception: by the time credits expire, startups have built their architecture around proprietary services and lack resources to re-engineer for alternative providers. The French Competition Authority has flagged these practices as a competition concern, noting that the scale and duration of such credits risk

---

[6] Charges imposed by cloud providers when data is transferred out of their systems.

[7] Open Markets Institute (2024). Engineering the Cloud Commons: Tackling Monopoly Control of Critical Digital Infrastructure. Available at: https://www.openmarketsinstitute.org/publications/report-rethink-regulatory-approach-to-essential-cloud

[8] Ofcom (2023). Cloud Services Market Study: Final Report. Available at: https://www.ofcom.org.uk/internet-based-services/cloud-services/cloud-services-market-study

[9] Microsoft's model goes further: its dominance in productivity software (Microsoft 365) creates independent lock-in at the application layer, distinct from cloud platform services, which it uses both to extract high margins directly and to drive adoption of Azure. European providers offer infrastructure at significantly lower prices, but struggle to win customers: once a business builds its systems using hyperscaler services, switching requires costly re-engineering, and customers report weak bargaining power relative to hyperscalers.

[10] Schulze, M., and van Veen, C. (2025). Why Europe Doesn't Need New Infrastructure — Just an Open Cloud Market. Leitmotiv Digital. Available at: https://leitmotiv.digital/publications/why-europe-doesnt-need-new-infrastructure-just-open-cloud-market

locking customers into a single ecosystem while creating potentially anticompetitive effects for the smallest suppliers, who could not profitably replicate such terms.[11]

- **Knowledge lock-in:** Technical switching barriers are compounded by human capital dependencies. A generation of specialists has been trained on hyperscaler interfaces. If European technologists cannot operate infrastructure independently of dominant platforms, legal and contractual freedoms become meaningless. This issue is particularly acute in the public sector, where critical infrastructure, from tax systems to healthcare records to defense networks, relies on a workforce predominantly trained on proprietary platforms.

- **Regulatory gaps:** Cloud computing lacks a comprehensive regulatory framework that addresses market concentration, mandates interoperability, or establishes conditions for fair access. This point is discussed in more detail in the section below on the regulatory context.

These mechanisms are further reinforced by the structure of cloud purchasing, where enterprise IT consultancies and system integrators mediate decisions in ways that favor incumbents.

The Procurement Barrier

Growing sovereignty concerns are precisely why governments and public institutions should lead by example in addressing cloud dependency. However, public sector adoption of alternatives to hyperscalers remains limited. Despite their stated policy goals of digital sovereignty, public buyers—who collectively represent one of the largest sources of IT demand in Europe—continue to default to incumbent providers. The explanation partially lies in the way public institutions purchase digital services. Public procurement is structurally risk-averse. This results in a bias toward established vendors, particularly in cloud computing, where it means the hyperscalers who offer well-integrated solution bundles. Two additional barriers related to procurement by public institutions compound the status quo:

- **Intermediary channeling:** Much of cloud procurement, particularly for larger organizations, is mediated through enterprise IT consultancies and system integrators. These intermediaries operate revenue-sharing arrangements with dominant platforms and invest heavily in platform-specific certifications required to maintain partner status. The result is systematic channeling, a phenomenon whereby organizations seeking guidance on cloud infrastructure receive recommendations from consultants trained primarily in hyperscaler platforms, who also earn financial rewards for steering clients toward those same providers. Whether a European or open source alternative might be more suitable often remains beyond consideration.

- **Fragmentation and lack of practical tools for procurement:** Many public institutions navigate cloud procurement largely independently, without access to standardized contract clauses, evaluation frameworks, or shared learning about alternatives. The expertise required to

[11] Autorité de la concurrence (2023). Cloud Computing: The Autorité de la concurrence Issues Its Market Study on Competition in Cloud Services. Press release. Paris: Autorité de la concurrence. Available at: https://www.autoritedelaconcurrence.fr/en/press-release/cloud-computing-autorite-de-la-concurrence-issues-its-market-study-competition-cloud

assess open source or European offerings is scarce and unevenly distributed. Political declarations favoring sovereign solutions do not translate into changed behavior without implementation resources.

PROPOSED INTERVENTION

The following, mutually reinforcing, set of measures would be necessary to address the major financial, technical, and institutional barriers identified in the previous section. The forthcoming CAIDA legislation and the revision of the Public Procurement Directives present an opportunity to embed these reforms in binding legislation.

Addressing Cloud Market Lock-in

Transparent pricing and structural separation: Providers should be required to offer infrastructure, platform, and software as separately purchasable layers. This would enable customers to mix and match components from different vendors. The costs of different cloud services should be separated by layer to enable meaningful comparisons and expose cross-subsidization, which occurs when services are offered below cost to drive infrastructure consumption. This would create more market space for Digital Commons providers that excel in specific layers, allowing them to compete based on their strengths rather than on ecosystem breadth.

Open source first: The response to EU's cloud dependency should aim to give users greater control over their digital assets and ensure that technical autonomy is guaranteed structurally, not merely contractually. This requires a cloud policy rooted in the principles of openness and interoperability. The approach favoring open source and interoperability aligns with the Commission's recognition that strengthening Open Source and open digital ecosystems is central to Europe's technological sovereignty, competitiveness, and cybersecurity agenda.

Counter-incentives for startups and investment in skills: Equivalent credit programs for European and open source infrastructure (for instance, through the European Competitiveness Fund) could balance the incentives currently offered by the dominant hyperscalers. Competition enforcement should address anti-competitive credit practices flagged by national authorities. Moreover, to rebuild the human capital necessary for digital sovereignty, there is a need for funding education and training programs on Open Source and European platforms.

Transforming Public Procurement

Supply-side measures will yield limited returns if public procurement, which represents Europe's most powerful underutilized lever for steering toward digital sovereignty, continues channeling spending toward hyperscalers. Public procurement reform can operate at multiple layers: directly at the infrastructural layer when cloud infrastructure is procured, and indirectly at the software and platform layers, where procurement choices can strategically steer demand towards providers that meet defined "sovereign cloud" criteria. In practice, this requires embedding the following conditions and criteria in digital procurement:

Transparency requirements for intermediaries: To avoid conflicts of interest and distorted recommendations, public sector buyers should require consultancies and intermediaries involved in cloud procurement to disclose any revenue-sharing or incentive arrangements with cloud providers.

Award criteria beyond price: Evaluation criteria must recognize the long-term resilience provided by compliant cloud providers and interoperability as strategic criteria that advance core policy objectives, not as secondary or "nice-to-have" features. Public procurement frameworks should permit preference for EU-controlled and sovereign solutions when dependencies create sovereignty risks. Article 10 of the draft European Competitiveness Fund Regulation already envisions such preferences when strategic interests are at stake.

Practical tools and guidance: Procurement agencies need tender templates with model clauses addressing, among other, data export, downtime during migration, exit rights, and migration tooling and support, as well as evaluation frameworks embedding openness and interoperability. Procurement procedures should also incorporate switching performance tests, in which vendors demonstrate live migration of representative workloads to a competing platform within specified timeframes. A public procurement framework should also mandate multiple providers for mission-critical systems, with at least one EU-based provider or open source solution where strategic considerations justify.

Institutional capacity: Dedicated competence centers are needed to provide technical and legal support to contracting authorities. Expertise in assessing open source and European offerings should be built systematically, rather than relying on individual officers to develop it ad hoc.

Open source and commons-based bundling: European and open source providers should coordinate to offer integrated service bundles that combine infrastructure, platforms, and supported open source solutions. These bundles should meet public sector expectations for reliability, usability, and accountability. By forming consortia around commons-based components, alternative providers can match the convenience of hyperscaler bundles while preserving structural openness, interoperability, and reversibility.

Monitoring and enforcement: Procurement authorities in the EU should track spending on open source and EU providers and publish data that enables course correction by contributing to the Public Procurement Data Space.

REGULATORY CONTEXT: CHALLENGES AND OPPORTUNITIES

The EU regulatory landscape already contains some instruments relevant to steering the cloud market towards greater sovereignty and openness, though key provisions remain underutilized. The forthcoming Cloud and AI Development Act and the Public Procurement Reform have the potential to address existing gaps on both the supply and demand sides.

Cloud Market Regulation

Data Act (Regulation 2023/2854): Chapter VI of the Data Act addresses switching between data processing services, banning contractual, commercial, and technical obstacles to termination, migration, and achieving functional equivalence. Providers must enable switching within 30 days, with switching charges fully phased out by January 12, 2027. Chapter VIII establishes interoperability requirements and standardization processes. This remains a potentially powerful instrument that is not being used. Awareness is low, and enforcement is fragmented across national authorities.

Digital Markets Act (Regulation 2022/1925): Cloud computing services fall within the scope of a 'core platform service.' Several obligations under the DMA would address hyperscaler practices if applied to them as gatekeepers: Article 6(2) would prevent the use of business user data to benefit the provider's own services; Article 6(9) requires data portability for PaaS and SaaS services. However, no cloud provider has been designated as a gatekeeper to date. The Commission opened investigations in November 2025 to assess whether AWS and Microsoft Azure meet designation thresholds. Even if designated, other relevant provisions, including Article 6(5) on self-preferencing, Article 6(12) on fair and non-discriminatory access conditions, Article 5(8) on bundling, and Article 6(7) on interoperability, prohibiting would not currently apply to cloud services and would require amendment.[12]

Cybersecurity Act (Regulation 2019/881): It tasked the European Cybersecurity Agency (ENISA) with developing harmonized certification frameworks for cloud services.[13] The European Cloud Services Certification Scheme (EUCS) has been deadlocked for over five years as member states dispute inclusion of 'sovereignty requirements' specifying that highest-assurance certifications require EU-based ownership and control.[14] A March 2024 draft removed these requirements, but France and others continue to push for their reintroduction, and adoption remains stalled.[15] The continued delay undermines harmonization and leaves fragmented national approaches in place.

IPCEI-CIS: In 2023 the European Commission approved an Important Project of Common European Interest (IPCEI) for Next Generation Cloud Infrastructure and Services (IPCEI-CIS) with up to €1.2 billion in public funding expected to mobilize an additional €1.4 billion in private

---

[12] See: Open Markets Institute (2025). Open Markets Submits Review of the Digital Markets Act: Considerations on Cloud and AI. Available at: https://www.openmarketsinstitute.org/publications/open-markets-submits-review-of-the-digital-markets-act-considerations-on-cloud-and-ai

[13] European Union Agency for Cybersecurity (ENISA) (2025). Cybersecurity Certification Framework. Available at: https://www.enisa.europa.eu/topics/product-security-and-certification/cybersecurity-certification-framework (accessed 18 February 2026)

[14] Bômont, C. (2025). Technical or Political? When a Cloud Certification Scheme Divides Europe. EUISS Brief No. 26. Available at: https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe.

[15] Euronews (2024). Cyber certification fix sought by mid-April over sovereignty issue. Euronews Next, 4 April 2024. Available at: https://www.euronews.com/next/2024/04/04/cyber-certification-fix-sought-by-mid-april-over-sovereignty-issue.

investment. [16] The project places interoperability and Open Source at the centre of its design. IPCEI-CIS is another attempt at building sovereign cloud infrastructure in the EU.[17] Its predecessor, the Gaia-X project, which launched in 2019 as an "Airbus for cloud," has been assessed as a failure and reoriented toward standard-setting rather than building competitive infrastructure. It is not yet possible to assess the impact of the IPCEI-CIS on the (rapidly growing) European cloud market, which remains dominated by the three hyperscalers. Whether the new initiative will break the pattern of earlier ones remains to be seen.

Cloud Sovereignty Framework: The Cloud Sovereignty Framework[18] is the European Commission's tool for evaluating how "sovereign" a cloud service is when public institutions purchase cloud infrastructure and services published alongside a competition for sovereign cloud solutions.[19] It defines sovereignty across eight objectives: strategic alignment, legal jurisdiction, data control, operational independence, supply chain resilience, technology openness, security compliance, and environmental sustainability. Digital Commons and open source considerations fall under one objective, Technology Sovereignty, (SOV-6), which is weighted at 15% of the total score. Within that category, open licensing is one contributing factor among several.

Cloud and AI Development Act (forthcoming, expected 2026): It aims to triple European data center capacity and reduce reliance on non-EU hyperscalers. The latter represents a critical opportunity: CAIDA could mandate structural separation, embed interoperability requirements, establish non-discrimination obligations, and link public investment to open source and sovereignty criteria. However, based on current signals, CAIDA risks focusing on capacity expansion without addressing market concentration. Without tackling this issue, expanded capacity may simply consolidate existing dependencies and exacerbate environmental concerns.

Public Procurement

Public Procurement Directives (2014/24/EU and related): Currently under revision with an emphasis on digital technologies and sovereignty. The revised directives present an opportunity to embed criteria outlined in section 2.2, favoring Open Source, interoperability, and European solutions.

---

[16] European Commission (2025). Approved IPCEI Next Generation Cloud Infrastructure and Services. Directorate-General for Competition. Available at: https://competition-policy.ec.europa.eu/state-aid/ipcei/approved-ipceis/cloud_en (accessed 18 February 2026).

[17] For a review of the EU's attempts at sovereign cloud see: Calcara, Antonio. 'European Cloud Computing Policy: Failing in Europe to Succeed Nationally?' West European Politics, 30 April 2025, 1–25. https://doi.org/10.1080/01402382.2025.2491962.

[18] European Commission, Directorate-General for Digital Services (2025). Cloud Sovereignty Framework. Available at: https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf.

[19] European Commission, (October 2025). The Commission moves forward on cloud sovereignty with a EUR 180 million tender: https://commission.europa.eu/news-and-media/news/commission-moves-forward-cloud-sovereignty-eur-180-million-tender-2025-10-10_en

Interoperable Europe Act (Regulation 2024/903): It establishes a framework for interoperability of public services across the Union, including governance mechanisms and the obligation to assess interoperability impacts. It provides a legal basis for mandating open standards in public sector digital services, though implementation guidance remains limited.

FIT WITH THE UPCOMING MULTIANNUAL FINANCIAL FRAMEWORK

The implementation of the interventions proposed in this brief would require coordination across MFF instruments, enforcement of the existing legislation (see the previous section), and alignment with forthcoming legislation, notably CAIDA, the revised Public Procurement Directive, and the upcoming European Open Digital Ecosystems Strategy.

While the Horizon Europe programme with the proposed budget of €175 billion is meant to continue funding foundational research, the European Competitiveness Fund (€409 billion) emerges as the centrepiece for sovereignty-related investments, structured around four policy windows including "digital leadership" and "resilience and security, defence industry and space." The ECF is meant to consolidate programmes that currently fund digital infrastructure—the Digital Europe Programme and the Connecting Europe Facility–Digital—and promises a "seamless investment journey from research to deployment." Its financing toolkit, encompassing grants, loans, guarantees, and procurement, can support the diverse economic models underpinning sovereign cloud alternatives, from cooperative structures to public utility approaches.

Article 10 of the draft ECF Regulation establishes an "EU Preference" mechanism, allowing award procedures to favor Union entities when strategic interests are at stake. This provision addresses the ownership but not necessarily the architecture of the digital assets. The current MFF proposals do not embed the criteria of openness or interoperability. The ECF's framing around "strategic autonomy" and "reducing dependencies" creates conceptual space for openness requirements, but explicit language mandating interoperability standards, open source components, and no-lock-in clauses as conditions for funding would ensure that the ECF investment aligns with the more ambitious plans to further embed support for the European open source sector.[20]

The InvestEU instrument within the ECF provides guarantees, loans, and equity to de-risk private investment. For sovereign cloud infrastructure, which combines public good characteristics with commercial viability, InvestEU could mobilize the private capital necessary to achieve scale without crowding out European providers or requiring unsustainable levels of public subsidy. European providers have indicated willingness to form consortia and expand capacity given credible demand signals; InvestEU can help convert those signals into projects.

---

[20] European Commission (2025). European Open Digital Ecosystems (initiative page). Better Regulation – Have Your Say. Brussels: European Commission. Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en (accessed 18 February 2026).

Creating the conditions for European and open source alternatives to reach users at scale requires demand-side reforms. The ECF draft proposal recognizes procurement as a tool for sovereignty, and if the upcoming reform of the public procurement framework addresses digital sovereignty concerns, these instruments could be mutually reinforcing.

The National and Regional Partnership Plans, which are meant to combine fourteen existing EU funds implemented by Member States and regions, represent a promising lever for procurement transformation. These plans could require Member States to adopt open source and sovereignty-aligned procurement rules as a condition for accessing EU funds. The Single Market Programme, which funds standardization, governance, and enforcement of single market legislation, could support the development of model procurement clauses and interoperability standards.

RESOURCE REQUIREMENT

European spending on public cloud services was estimated to reach approximately €200 billion in 2025, and most likely will continue to grow. Within this total, cloud infrastructure services are estimated to account for approximately €73 billion, according to Synergy Research Group.[21] Platform services (PaaS) are the fastest-growing segment, driven by demand for AI applications and scalable infrastructure for digital transformation.[22]

AWS, Microsoft Azure, and Google Cloud together hold about 70% of the EU market while European providers' share has fallen to 13%. Even Europe's largest player, SAP, captures only around 2% of the European cloud computing market.[23]

At current spending levels, Europe is effectively financing the infrastructure dominance of hyperscalers. Redirecting a part of this expenditure could transform the market.

Digital commons, including open source technologies, offer a path to reducing Europe's dependence on hyperscalers and strengthening cloud sovereignty. This does not require additional resources, but rather a redirection of existing public and private spending away from hyperscalers towards open digital infrastructure—as European cloud providers often emphasize, they do not need subsidies; they need customers. However, reaching the market requires the structural conditions outlined in this brief. These measures would create space for commons-based and European alternatives to compete and scale.

---

[21] Fierce Network (July, 2025). Europe's cloud market poised for 24% growth: https://www.fierce-network.com/cloud/europes-cloud-market-poised-24-growth

[22] IDC (2025). Banking Leads European Cloud Spending Growth While Manufacturing Industries Slow Down, Says IDC. Press release, 13 February 2025. Available at: https://my.idc.com/getdoc.jsp?containerId=prEUR253190125.

[23] European Parliament, Policy Department for Transformation, Innovation and Health, Directorate-General for Economy, Transformation and Industry (2025). European Software and Cyber Dependencies. Study requested by the Committee on Industry, Research and Energy (ITRE). PE 778.576. December 2025. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU(2025)778576_EN.pdf

RISKS AND MITIGATION MEASURES

Translating these proposals into practice will require overcoming entrenched structural and institutional barriers.

First, there is a persistent disconnect between political declarations and procurement practice. Experts with long-standing experience in the field note, somewhat wryly, that IT departments operate largely independently of high-level policy objectives on digital sovereignty. Within large enterprises, incentives discourage moving away from hyperscalers. Overcoming this requires a shift in how organizations assess and price long-term strategic risk.[24]

Second, European cloud companies offer infrastructure components and not integrated bundles that clients expect and are used to. Building viable competition to hyperscalers requires a complete service catalog, which points to the importance of (commons-based) bundling: open source components and interoperable services that can be assembled into coherent offerings without requiring a single provider to replicate the entire hyperscaler stack.

Third, European providers may, in fact, have limited incentive to change course. Their market share has fallen from 29% in 2017 to around 15%, but has held steady since 2022. With the European cloud market growing at 24% annually, they remain profitable.[25] Serving local niches and sovereignty-conscious customers may be a comfortable position while the significant investment required to compete with hyperscalers carries additional risk.

Finally, there is a risk of complacency. Some stakeholders assume that US political conditions will revert to a more cooperative form, reducing the urgency for action. This is a dangerous assumption because the structural dependencies will remain regardless of who occupies the White House.

IMPLEMENTATION PATHWAY

2026 is a defining year for EU cloud policy: the Cloud and AI Development Act and the revision of public procurement legislation, both expected in the first half of the year, have the potential to enshrine structural unbundling, interoperability mandates, open source requirements, and sovereignty criteria in law. The European Open Digital Ecosystems strategy is a non-legislative instrument, but it will set the direction for EU open source policy and inform future funding and procurement guidance. Enforcing the Data Act and the Digital Markets Act should ensure effective switching and address technical barriers.

Legislation, however, will not be sufficient. Reducing Europe's cloud dependencies requires action now, in parallel with the legislative process.

---

[24] On the issues of managing risk and responsibility, see: https://berthub.eu/articles/posts/aws-and-microsoft-are-selling-much-more-than-cloud/

[25] Fierce Network (July, 2025). Europe's cloud market poised for 24% growth: https://www.fierce-network.com/cloud/europes-cloud-market-poised-24-growth

European cloud and open source providers are already coordinating through initiatives such as the IPCEI-CIS[26] or the EuroStack Industry Initiative, which proposes an industrial strategy to federate existing European assets across the digital supply chain to match demand and supply. Public institutions that have or are in the process of diversifying away from hyperscalers—for example, the German State of Schleswig-Holstein, the Danish Digital Ministry, or the International Criminal Court—offer practical blueprints for others to follow. A structured exchange of experiences between these pioneers and other institutions would accelerate diversification and moving away from hyperscalers without requiring new funding or legislation.

Progress in achieving the goals of the intervention described in this brief could be tracked against the following indicators:

Market Structure and Public Sector Transition

- Market share of cloud providers in the EU, broken down by IaaS, PaaS, and SaaS.
- Share of EU public cloud spending directed to open source and EU-based providers, broken down by IaaS, PaaS, and SaaS, number of contracts with multi-sourcing and exit provisions.
- Number of public bodies migrated to open source and EU-based cloud infrastructure.

Tracking these indicators will require a significant improvement in the transparency and accountability of public spending data. At present, only around 20% of public procurement data is accessible at the EU level.[27] Without progress on this front, monitoring will remain patchy and course correction difficult to track.

Availability and Robustness of Alternatives

- Number and market share of commons-based and open source service offerings meeting public and private sector requirements.
- Total investment mobilized, including under IPCEI-CIS and ECF-linked instruments, directed to open source and EU-based cloud infrastructure.

Environmental Sustainability

- Compliance rate with sustainability and energy-efficiency targets among EU cloud providers. Ensures sovereignty goals do not come at the expense of environmental commitments.

---

[26] See for example: Deutsche Telekom, Orange, Telefonica, TIM, and Vodafone Achieve the First Pan-European Federated Edge Continuum at MWC 2026,' Telefonica, 23 February, https://www.telefonica.com/en/communication-room/press-room/deutsche-telekom-orange-telefonica-tim-vodafone-logran-el-primer-edge-continuum-federado-paneuropeo-en-el-mwc-2026/

[27] These are mainly contract notices published on the Tenders Electronic Daily (TED) platform for procedures above EU thresholds. See: https://www.public-procurement-data-space.europa.eu/en and https://www.oecd.org/en/about/programmes/sg-reform/leveraging-the-eu-public-procurement-data-space-ppds.html

Taken together, these indicators would show whether Europe is moving towards greater digital sovereignty in the cloud market.

Europe's dependence on a handful of US-based cloud providers is the result of deliberate market choices, policy gaps, and decades of institutional inertia, none of which are inevitable. The current momentum for digital sovereignty and the policy agenda of 2026 offer an opportunity to act. The goal is not technological nationalism but a cloud market that is resilient, trustworthy, and built to serve the people and institutions that rely on it.