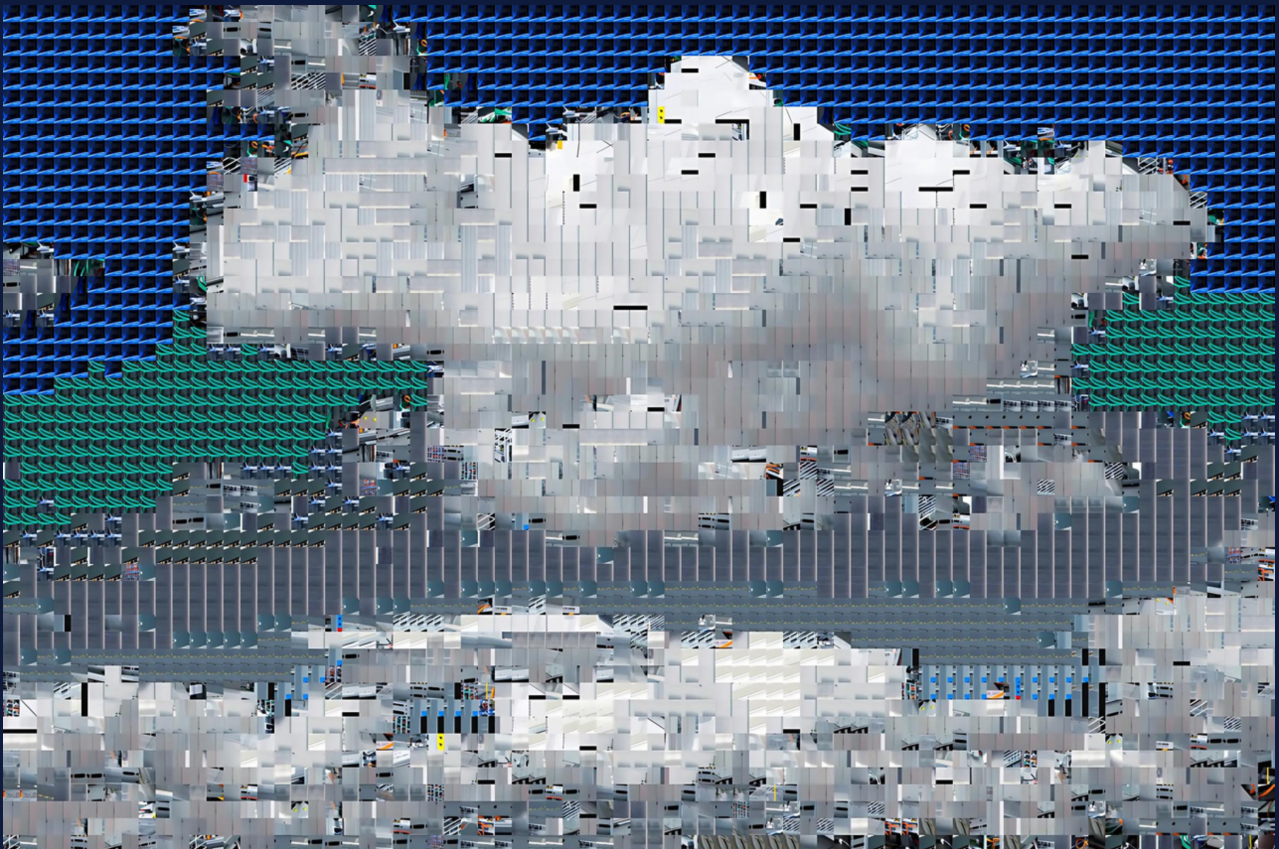


Taming the hyperscalers

A blueprint for an
open, competitive, and sovereign
European cloud market

Max von Thun and
George Colville



OPEN MARKETS
EUROPE

February 2026

Europe's concentrated cloud market is a threat to fair competition and digital sovereignty

Cloud computing increasingly serves as the infrastructural backbone of the 21st century economy. Today's cloud giants – Amazon, Google and Microsoft – control around two-thirds of the global cloud computing market¹ and sometimes more in individual EU Member States. This includes hosting the sensitive data and operations of major European governments and businesses. Yet despite this systemic role and the risks and responsibilities it entails, these corporations remain largely unregulated and free to wield their market dominance as they see fit.

The structure of today's cloud market is not an inevitable outcome of innovation, but one shaped by anticompetitive practices and abuses of market power.² These practices include bundling and tying, discriminatory pricing, restrictive licensing terms, unjustified technical limitations (especially on data portability and interoperability), cross-subsidisation from other business lines, and the leveraging of vertically integrated ecosystems to steer customers towards proprietary and closed cloud infrastructure. These practices have contributed significantly to European cloud providers' market share dropping from 29% in 2017 to its current 15%.³

Not only does this prevent European and other cloud competitors from competing on a level playing field, but the high prices charged by current cloud oligopolists mean that European businesses across all sectors of the economy are spending more than they should be on cloud services. This reduces their competitiveness and ultimately leads to higher prices for European consumers. Research by the UK's communications regulator shows that dominant cloud providers generate consistent profit margins of around 20-40%, a strong indicator that monopoly rents are being extracted from businesses and ultimately levied on end consumers.⁴ With 53% of European businesses buying cloud computing services in 2025⁵ and estimates for that number to rise to 75% by 2030,⁶ it is critical that they do so at fair prices.

Dominant cloud providers also exploit their market power to capture, weaken, or distort downstream innovation taking place on their infrastructure. For example, they have been accused of developing copycat versions of popular – often open-source – software applications on their cloud marketplaces and subsequently affording these greater visibility and technical functionality.⁷ More generally, Amazon, Google, and Microsoft receive unparalleled insights from their cloud businesses which they can use to compete unfairly against downstream rivals, whether by benefiting their own services or disadvantaging third-party offerings. They have not only the ability but also strong incentives to do so, given they compete in many of these downstream markets themselves.

When it comes to AI, Big Tech cloud providers naturally prioritise their own models' access to training and inference compute as well as those of companies they have partnerships with.⁸ At the same time, innovative AI challengers have little choice but to enter partnerships with dominant tech giants, given their control of critical computing inputs. As Microsoft's relationship with OpenAI and Amazon's partnership with Anthropic show, this enables cloud oligopolists to generate new revenue streams for

1 Richter, 'Infographic: AWS Stays Ahead as Cloud Market Accelerates'.

2 von Thun and Lavin, *Engineering the Cloud Commons: Tackling Monopoly Control of Critical Digital Infrastructure*.

3 Synergy Research Group, 'European Cloud Providers' Local Market Share Now Holds Steady at 15%'.

4 Ofcom, *Cloud Services Market Study (Final Report)*.

5 eurostat, 'Cloud Computing - Statistics on the Use by Enterprises'.

6 European Commission, 'Communication Establishing the Union-Level Projected Trajectories for the Digital Targets'.

7 Wakabayashi, 'Prime Leverage'.

8 Federal Trade Commission, 'FTC Issues Staff Report on AI Partnerships & Investments Study'.

their cloud businesses, gain privileged access to innovative new third-party technologies, and neutralise the competitive threat from new market entrants.⁹ As tech monopolies leverage their control over compute to steer AI development in ways that entrench their dominance, this severely restricts the overall diversity of innovation in the market.¹⁰

In today's fraught geopolitical and economic environment, the importance of genuine technological sovereignty – including in cloud infrastructure – is clearer than ever. The dominance of Amazon, Google, and Microsoft in providing Europe's cloud infrastructure is fundamentally incompatible with real sovereignty.

Firstly, the economic and political weight of these corporations, which increasingly includes the backing of the U.S. government, makes it difficult for Europe to hold them accountable. Secondly, these corporations could be pressured by the U.S. government to act in ways that undermine fundamental European interests, including by restricting, degrading or even shutting off cloud access to European customers. The reality of this threat was demonstrated in May 2025 when Microsoft revoked International Criminal Court chief prosecutor Karim Khan's access to Office services, including email, following the Trump administration's decision to sanction the Court.¹¹ French ICC judge Nicolas Guillou, also subject to sanctions, has since revealed the extent to which centralised dependence on U.S. technologies and systems has left him unable to access basic digital services.¹²

Our vision for a fair and competitive cloud market

To ensure real choice and tackle the harms caused by today's concentrated cloud market, a bold transformation is needed in how the industry is structured and governed. This is not about banning American firms (or firms of any nationality) from the European market, nor does it require all of Europe's cloud infrastructure to be supplied by European firms, although redirecting some existing public spending towards European providers would be a sensible measure. Neither is it about direct state provision of cloud infrastructure, even if this may be appropriate in certain circumstances.

Instead, what is needed is extensive regulation of both the behaviour and structure of the dominant cloud providers or “hyperscalers” with the aims of (1) limiting the ability of these actors to abuse their market power and (2) creating space for alternatives to emerge and scale.

The first step in this programme is to impose binding obligations on dominant cloud providers that both restrain their market power and ensure their infrastructure serves the public interest. In essence, this entails recognising these corporations as providers of “public utilities” or “essential infrastructure” and regulating them in similar ways to other such utilities and infrastructure – including electricity, telecoms and transportation infrastructure – while accounting for the unique characteristics of cloud computing.

Such “utility-style” regulation would include, among other things, obligations covering transparent and consistent pricing, fair and non-discriminatory access, interoperability and data portability, cybersecurity, resilience, privacy and sustainability. Dominant cloud providers should, for example, be mandated to provide fair and non-discriminatory access to their cloud infrastructure and required to price this access transparently and consistently for both existing and new customers. Interoperability and data portability requirements should be imposed to facilitate switching between providers, as well

9 Von Thun and Hanley, ‘Stopping Big Tech from Becoming Big AI’.

10 Varoquaux et al., ‘Hype, Sustainability, and the Price of the Bigger-Is-Better Paradigm in AI’.

11 Owen Sayers, ‘Microsoft’s ICC Email Block Reignites European Data Sovereignty Concerns’.

12 Maupas, ‘La vie de Nicolas Guillou, juge français de la CPI sous sanctions des Etats-Unis’.

as the ability of customers to run workloads across multiple cloud systems. Fortunately, as we point out below, many of the foundations for this regulatory approach already exist in Europe, albeit fragmented across different laws and authorities including the Digital Markets Act, the Data Act, and the upcoming Cloud and AI Development Act.

The second step entails addressing at root, through structural separation and targeted investment, the vertical integration and conflicts of interest that have enabled Big Tech firms to first dominate the cloud market and then subsequently leverage this dominance to capture other markets. They have done so through various practices enabled by vertical integration, including tying and bundling cloud services with other products, giving preferential treatment and visibility to their own cloud services on platforms they control, and funding (at least initially) their cloud arms with profits from other business lines.

The basic problem is simple: the same players that own the supposedly neutral “upstream” cloud infrastructure also compete on that infrastructure with third parties in “downstream” activities, such as AI model development. While the regulatory obligations detailed above – particularly non-discriminatory access – help address this problem, they are far harder to enforce on vertically integrated providers given information asymmetries and the strong incentives conglomerates have to favour their own services.

In this situation, the tried and tested solution is to separate control of upstream infrastructure from downstream services. This removes both the ability and incentive to give preferential treatment to one’s own services by severing the link between the two. There are several historical precedents for such separation or “unbundling” both in Europe and around the world. For example, EU law requires the unbundling of energy generation from energy transmission,¹³ while in the UK, telecoms services provider BT was required by regulators to spin off network infrastructure owner Openreach into an independent and legally distinct company.¹⁴

The most effective form of unbundling would require divestment to new owners, known as ownership separation. In addition to promoting effective competition, the sale of Big Tech’s cloud infrastructure to European owners would also promote Europe’s digital sovereignty by ensuring immunity from foreign laws (such as the CLOUD Act), economic coercion, and political interference (whether overt or covert).

Functional separation – where an independent legal entity is created but still owned by the same parent company – would make coordination more difficult but not impossible, leaving in place economic incentives to self-preference. While ownership separation is therefore a more effective solution from both a competition and sovereignty perspective, practical or political considerations may in some cases lead to functional separation being preferred. If functional separation is imposed and fails to achieve its objectives, then full ownership separation remains on the table as a subsequent step.

Alongside this regulatory activity, Europe needs to build the software services that are a major source of lock-in to hyperscaler cloud platforms. This requires public investment in the development, scaling, security and documentation of key cloud software components – prioritising open-source solutions where possible – so that European providers can offer credible, interoperable alternatives to proprietary US platforms. Public funding should identify critical gaps in the European cloud stack (e.g. identity management, object storage, and managed database services) and commission production-ready implementations and practical technical standards that make these services easy to procure and adopt.¹⁵

The rest of this paper looks at how this vision could be implemented within the current European legal and policy framework.

.....
13 European Commission, ‘Governance of the Internal Energy Market’.

14 Hutton and Priestley, *BT and Openreach*.

15 Bert Hubert, ‘A Coherent European/Non-US Cloud Strategy’.

The current EU regulatory landscape for cloud

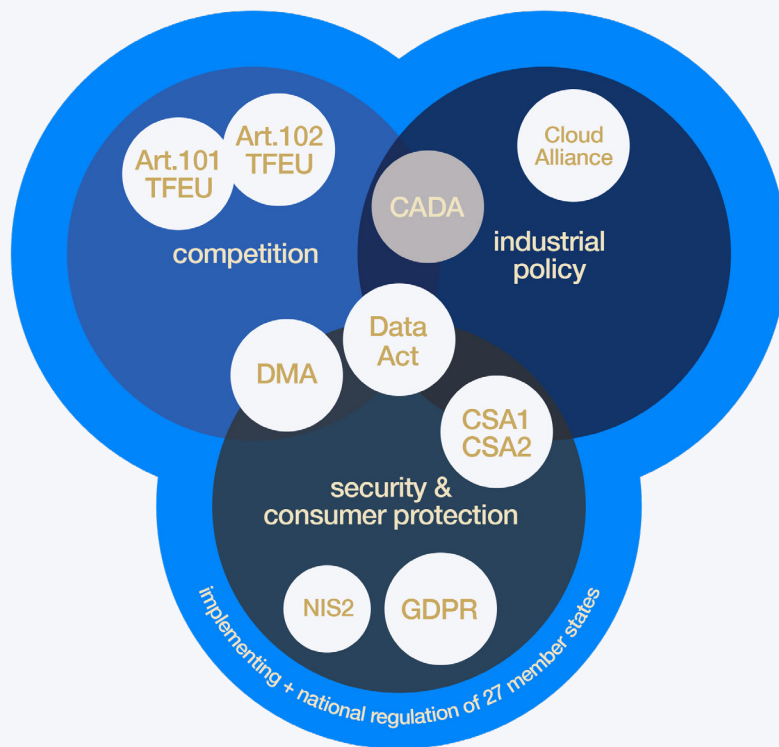


Figure 1. Taxonomy of the European cloud regulation landscape

Sectoral regulation of the cloud industry in Europe is fragmented at both at the EU and Member State level. Not only does this undermine the overall drive to promote competition, sovereignty, and security in the cloud market, but it also makes it harder for European players to scale and compete with the hyperscalers.

At the EU level, the Data Act (DA), the General Data Protection Regulation (GDPR), the Digital Markets Act (DMA) and the Cybersecurity Act (CSA), as well as the upcoming Cloud and AI Development Act (CADA), contain a range of powers and provisions with great potential to create a fair and competitive cloud market, including by implementing many of the reforms proposed above. The European Alliance for Industrial Data, Edge and Cloud was also set up to help coordinate and inform European cloud industrial policy. Yet despite these wide-ranging powers, EU cloud regulation risks failing to achieve its potential due to weak enforcement, coordination failures, and lack of a clear mission.

At the Member State level, regulation of the cloud industry is inconsistent and often driven by divergent national priorities. Several countries have introduced their own frameworks for cloud certification, data localisation, and public-sector procurement, creating barriers to cross-border service provision and duplicative compliance burdens for smaller providers (European and otherwise) operating across multiple jurisdictions.

Given the need for a centralised and consistent approach to both neutralising the market dominance of the hyperscalers and promoting the growth of European alternatives, EU-wide policies and enforcement will be most effective. Opportunities for national divergence should thus be strictly limited.

The Data Act

The Data Act contains numerous provisions that, if effectively implemented, could inject real competition into today's ossified cloud market. In particular, it promises to reduce customer lock in by requiring vendors of software-as-a-service, platform-as-a-service and infrastructure-as-a-service to remove contractual and technical barriers to data migration, enable interoperability, and clarify pricing for data transfers and disengagement.

Chapter VI of the Data Act bans pre-commercial, commercial, technical, and organisational obstacles that inhibit customers from: a) terminating contracts; b) concluding new contracts; c) porting data and digital assets to a new service; d) achieving functional equivalence once data has been exported to a new service; and e) unbundling cloud services offered by providers. It dictates pro-switching contractual terms (Art.25); mandates transparency regarding the possibility to switch/port data from a service (Art.26); creates a good faith obligation regarding switching (Art.27); provides for the total phase out of switching charges by January 2027 (Art.29); and mandates some basic technical features providers must offer to make switching more straightforward (Art.30).

Chapter VIII, meanwhile, focuses on interoperability between services, setting out requirements on the technical obligations, transparency requirements, and standardisation processes necessary to make inter-cloud service interoperability possible (Arts.33-36). This crucially includes a significant focus on the development of standards.

One major gap is the lack of any provision preventing cloud providers from arbitrarily discriminating in their treatment of different customers (e.g. in terms of access, pricing, contractual conditions). One possibility would be to add a non-discrimination provision to the Data Act, although other laws – in particularly the DMA (if amended) and the upcoming CADA – may offer more promising pathways (see below).

The Data Act is therefore an important piece of legislation which could address many of the causes and symptoms of today's oligopolistic cloud market. The real challenge, of course, will be in its operationalisation and enforcement. Factors including blurred lines between different types of cloud service, the diversity of cloud services offered, the dynamic nature of the technology, and the difficulty in ascertaining the technical feasibility of regulatory measures (such as interoperability) make this an inherently challenging sector to regulate consistently, clearly, and effectively.

Another challenge is the fragmented model of enforcement, with Member States rather than the EU responsible for enforcement, a challenge made even greater by varying levels of preparedness and ambition among responsible national regulators.¹⁶ To ensure a coherent and harmonised implementation of the law, enforcement of the Data Act's cloud provisions should instead be led (either exclusively or supported by national regulators) by an EU body, and ideally a new agency focused on supervising systemically significant cloud providers.

These considerations aside, the Data Act – the enforcement of which began in September 2025 – provides the most immediate tool for beginning to steer the cloud market in a more competitive, resilient, and innovative direction.

16 Cynthia Krouet, 'Some National Regulators Ill-Equipped to Enforce Incoming EU Data Act'.

The Omnibus Proposal and the Data Act

The Commission's November 2025 "Digital Omnibus" proposal, which seeks to "simplify" several of the EU's flagship digital laws including the Data Act, leaves the key competition-relevant provisions covered above largely untouched. The main changes of note are the introduction of two exemptions to Chapter VI, concerning switching between services. Two new clauses are introduced with the stated intention of reducing compliance costs for specialised and smaller providers by exempting their pre-September 2025 contracts from most of the Data Act's switching provisions, enabling them to avoid having to redraft or renegotiate these.

Article 31(1a) exempts custom-made services "where the majority of features and functionalities of the data processing service has been adapted by the provider to the specific needs of the customer," while Article 31(1b) exempts providers if they are "a small and medium-sized enterprise or a small mid-cap". Additionally, Art. 31(1b) allows the latter category of providers to include provisions "on proportionate early termination penalties" in fixed-duration contracts. Importantly and positively, the ban on switching charges created by Article 29 remains applicable to both these categories of service.

Provided these amendments remain narrow and applied exclusively to pre-September 2025 contracts, they are a sensible compromise. That said, given that many cloud service contracts cover extensive fixed time periods (often up to 10 years), it is crucial the scope of this exception is not open to abuse, particularly by dominant players.

This is particularly true for Article 31(1a), as large providers will inevitably claim that services which are in fact off the shelf have been adapted for the needs of the customer. The final text of the Digital Omnibus must therefore ensure the "custom-made" exemption is not exploited by dominant cloud providers to delay the application of the Data Act's switching provisions.

The DMA

'Cloud computing services' (as defined in Art. 4 GDPR) fall within the scope of the DMA as a 'core platform service' listed in the legislation. Nevertheless, to date the European Commission has failed to designate a single cloud provider. This may partly be due to an unsuitable definition of 'active end-users' in Annex E for the purposes of quantitative designation.¹⁷ The current wording requires cloud services to be platforms used directly by consumers or business users, in return for remuneration. This fails to account for the nature of cloud services, which, unlike traditional consumer-facing platforms, are predominantly used indirectly by consumer end-users. It is predominantly enterprises that use cloud services in exchange for remuneration, while consumer end-users generally interact with them indirectly when visiting websites or using applications.

The Commission is however empowered to designate cloud providers via a qualitative procedure (Art. 17). Making use of these powers, in November 2025 it opened three investigations into cloud computing: two into whether Microsoft Azure and Amazon AWS should be designated as gatekeepers in cloud and a third considering whether the DMA's current obligations would be effective in addressing unfair and anti-competitive practices in the cloud market.¹⁸ These investigations are welcome, if overdue, and should proceed on an accelerated timeline given the serious challenges in today's cloud market. The Commission should also launch a designation investigation into Google's cloud business, Google Cloud Platform; while GCP has a significantly smaller market share than AWS and Azure, the integration of

17 Open Markets Institute, *Submission to the Review of the Digital Markets Act: Considerations on Cloud and AI*.

18 European Commission, 'Commission Launches Market Investigations on Cloud Computing Services under the Digital Markets Act'.

GCP into Google's broader digital empire enhances the gatekeeper's power in numerous other markets, including AI (Gemini), search, video streaming (YouTube), and digital advertising.

Several existing DMA obligations would immediately address harmful practices by dominant cloud providers. Art. 6(2) would prevent designated cloud providers from using confidential commercial data generated by their business users (such as software developers) to benefit their cloud and non-cloud services, while Art. 6(9) would (similarly and complementarily to the Data Act) oblige designated gatekeepers to ensure the full data portability of Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) products free of charge.

In the DMA's current form, however, several provisions that should apply to cloud service gatekeepers would not do so even if they were designated. This is fully or partially the case for Art. 6(5) (banning self-preferencing in marketplaces), Art. 6(12) (requiring fair, reasonable, and non-discriminatory (FRAND) general conditions of access for business users), Art. 5(8) (prohibiting bundling), and Art. 6(7) (interoperability). If the DMA is to achieve the vision for the cloud market outlined above, it should be amended to ensure that its obligations are effective in addressing unfair practices by cloud hyperscalers (see [here](#) our detailed analysis of the applicability of the DMA to cloud).

While the DMA does include provisions on structural remedies (Art. 18), these are reserved as a last resort for punishing "systematic non-compliance," making them difficult to apply to dominant cloud providers quickly and as a whole.

Competition law

To date, neither the EU's foundational competition laws (Article 101 prohibiting anti-competitive agreements between firms and Article 102 TFEU prohibiting abuses of a dominant position) nor their Member State equivalents have been applied to the cloud market. While national competition authorities in countries including the UK, France, the Netherlands, and Spain have all conducted in-depth studies, all of which found numerous serious competition issues in the cloud market, none resulted in enforcement measures.

This is a mistake. Competition enforcement has an important role to play in tackling anti-competitive conduct in the cloud industry and creating space for challengers, particularly when it comes to conduct that is not currently covered by ex-ante rules like the DMA and Data Act.

More concretely, competition enforcement (via Art.102 TFEU) could be used to impose structural separation on cloud providers as a remedy for proven anti-competitive conduct. As stated in Art. 7 of Regulation 1/2003 (which sets out the procedural framework for enforcement of Articles 101 and 102 TFEU), the European Commission may impose "any behavioural or structural remedies which are proportionate to the infringement committed and necessary to bring the infringement effectively to an end."

However, the nature of EU competition law means that remedies – including structural separation – can only be imposed once it has been demonstrated that an individual firm has violated the law, a process that can take many years.¹⁹ For addressing urgent and systemic harms that involve not just one actor, but an industry as a whole, regulation is a more appropriate and effective tool.

19 David Zuluaga, 'The Google Case Shows Why Competition Policy in the Digital Economy Needs to Change'.

The Cloud and AI Development Act (expected Q1 2026)

The upcoming Cloud and AI Development Act (CADA) aims to boost cloud capacity and reduce reliance on U.S. hyperscalers by tripling Europe's data centre capacity, promoting research and development in sustainable data processing, and fostering secure EU-based cloud infrastructure for critical use cases. Based on what is known so far, the CADA may fail to address the problem of cloud market concentration, and, worse, may support the further entrenchment of Big Tech's cloud dominance in Europe.

If Europe really does triple its cloud capacity (and there are legitimate questions about whether this is actually necessary or desirable),²⁰ the current moment is a pivotal one. Choices made now about competition and market structure will determine how this growth occurs and who its biggest winners are. They will determine whether this growth merely consolidates Big Tech's grip on Europe's cloud infrastructure or instead begins steering the industry's trajectory away from concentration and innovation-crushing monopoly power.

Instead of reinforcing today's broken cloud market, the CADA should work alongside the DMA, the Data Act, and competition law to promote open and diversified digital infrastructure that puts the needs and interests of Europe's citizens, businesses, and governments first. This should include mandating the formal separation – on either an ownership or functional level – of cloud computing (i.e. AWS, GCP, and Azure) from Amazon, Google, and Microsoft.

The Cybersecurity Act

The CSA, passed in 2019, tasked the European Cybersecurity Agency (ENISA) with developing and implementing common European certification frameworks, recognising the importance of harmonising the European cloud market. However, what began as a technical initiative to harmonise cybersecurity standards for cloud services across the EU has found itself deadlocked for over five years as member states fail to agree on key details – notably the inclusion of a so-called sovereignty requirement.

While further attempts to break that deadlock will likely come after the review of the CSA, it is critically important that Europe manages to establish a harmonised standard (or standards) for cloud security as soon as possible. The CSA experience should also be cautionary: it is imperative that standardisation processes under the Data Act avoid this fate. We quite simply cannot afford for it to take five years to develop the standards necessary to enable effective interoperability and porting as envisaged by the Data Act.

The Commission's January 2026 proposal to revise the CSA recognises that cybersecurity goes beyond the technical.²¹ Acknowledging that information and communication technology (ICT) supply chain concentration and material digital infrastructure ownership and control can create opportunities for geopolitical leverage and designed vulnerabilities, the new proposal establishes a framework to identify "Key ICT Assets" and permit the designation of 'High-Risk Suppliers' where a third country appears to pose non-technical risks to the ICT supply chain that are both serious and structural. High-risk suppliers will be subject to Union-wide restrictions, including exclusion from European standardization work and participation in public procurement or Union-funded programs. While the immediate focus of this appears to be telecommunications infrastructure, European authorities should not hesitate to use these new powers to address the security risks arising from use of U.S. cloud services.

20 Arvind Narayanan and Sayash Kapoor, 'AI as Normal Technology'.

21 Mark Young et al., 'European Commission Proposes Cybersecurity Act 2'; Proposal for a Regulation for the EU Cybersecurity Act.

The blueprint: policy recommendations for an open, competitive, and sovereign European cloud market

Short term

Accelerate the designation of Microsoft Azure and Amazon Web Services as gatekeepers under the DMA; launch a separate designation investigation into Google Cloud Platform;

Enforce the DMA, the Data Act, and EU competition law to tackle ongoing and pervasive anti-competitive conduct by dominant cloud providers;

Impose a formal FRAND access obligation on cloud providers through either the DMA or CADA, taking inspiration from similar provisions in the energy, transportation, and telecoms markets.

Medium term

Amend the DMA to ensure it fully applies to cloud services, notably by expanding the scope of Articles 6(5), 6(12), 5(8) and 6(7). See our more detailed recommendations [here](#);

Facilitate private enforcement of both the DMA and competition law (both collective and individual claims) so that citizens and businesses are able to hold hyperscalers accountable for their abuses;

Establish a centralised EU-level body to oversee regulation of dominant cloud providers (and potentially Big Tech firms as a whole), including implementation and enforcement of the Data Act, DMA, CSA, and eventually CADA;

Allocate public funding for European open-source software in the most important cloud services and components (e.g. key-value stores, S3-like services, customer identity and access management).

Long term

Full ownership (or functional) separation of hyperscaler cloud businesses to:

- eliminate conflicts of interest;
- prevent anti-competitive cross-financing;
- preserve system resiliency;
- disperse excessive concentration of power;
- promote sovereignty;
- facilitate public oversight and accountability.



Bibliography

Arvind Narayanan and Sayash Kapoor. 'AI as Normal Technology'. *Knight First Amendment Institute*, 15 April 2025. <http://knightcolumbia.org/content/ai-as-normal-technology>.

Bert Hubert. 'A Coherent European/Non-US Cloud Strategy: Building Railroads for the Cloud Economy'. *Posts. Bert Hubert's Writings*, 7 May 2025. <https://berthub.eu/articles/posts/a-coherent-non-us-cloud-strategy/>.

Cynthia Krouet. 'Some National Regulators Ill-Equipped to Enforce Incoming EU Data Act'. *Euronews*, 12 September 2025. <https://www.euronews.com/next/2025/09/12/some-national-regulators-ill-equipped-to-enforce-incoming-eu-data-act>.

David Zuluaga. 'The Google Case Shows Why Competition Policy in the Digital Economy Needs to Change'. *Euractiv*, 23 April 2015. <https://www.euractiv.com/opinion/the-google-case-shows-why-competition-policy-in-the-digital-economy-needs-to-change/>.

European Commission. 'Commission Launches Market Investigations on Cloud Computing Services under the Digital Markets Act'. 18 November 2025. https://digital-markets-act.ec.europa.eu/commission-launches-market-investigations-cloud-computing-services-under-digital-markets-act-2025-11-18_en.

European Commission. 'Communication Establishing the Union-Level Projected Trajectories for the Digital Targets'. 27 September 2023. <https://digital-strategy.ec.europa.eu/en/library/communication-establishing-union-level-projected-trajectories-digital-targets>.

European Commission. 'Governance of the Internal Energy Market'. Accessed 23 January 2026. https://energy.ec.europa.eu/topics/markets-and-consumers/governance-internal-energy-market_en.

eurostat. 'Cloud Computing - Statistics on the Use by Enterprises'. January 2026. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises.

Federal Trade Commission. 'FTC Issues Staff Report on AI Partnerships & Investments Study'. 17 January 2025. <https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-issues-staff-report-ai-partnerships-investments-study>.

Hutton, Georgina, and Sara Priestley. *BT and Openreach*. 21 January 2026. <https://commonslibrary.parliament.uk/research-briefings/cbp-7888/>.

Mark Young, Dan Cooper, Paul Maynard, Anna Sophia Oberschelp de Meneses, and David Brazil. 'European Commission Proposes Cybersecurity Act 2: New EU Supply Chain Rules and Certification Reforms'. *Inside Privacy*, 23 January 2026. <https://www.insideprivacy.com/cybersecurity-2/european-commission-proposes-cybersecurity-act-2-new-eu-supply-chain-rules-and-certification-reforms/>.

Maupas, Stéphanie. 'La vie de Nicolas Guillou, juge français de la CPI sous sanctions des Etats-Unis : « Vous êtes interdit bancaire sur une bonne partie de la planète »'. *International, Justice Internationale. Le Monde*, 19 November 2025. https://www.lemonde.fr/international/article/2025/11/19/nicolas-guillou-juge-francais-de-la-cpi-sanctionne-par-les-etats-unis-face-aux-attaques-les-magistrats-de-la-cour-tiendront_6654016_3210.html.

Ofcom. *Cloud Services Market Study (Final Report)*. 2023. <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/244808-cloud-services-market-study/associated-documents/cloud-services-market-study-final-report.pdf?v=330228>.

Open Markets Institute. *Submission to the Review of the Digital Markets Act: Considerations on Cloud and AI*. 2025. <https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/68f78e9e0264e81c99b58ace/1761054366764/OMI+-+DMA+submission+on+cloud+and+AI.pdf>.

Owen Sayers. 'Microsoft's ICC Email Block Reignites European Data Sovereignty Concerns'. *Computer Weekly*, 23 May 2025. <https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns>.

Proposal for a Regulation for the EU Cybersecurity Act, COM(2026) 11 final (2026). <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>.

Richter, Felix. 'Infographic: AWS Stays Ahead as Cloud Market Accelerates'. Statista Daily Data, 4 November 2025. <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers>.

Synergy Research Group. 'European Cloud Providers' Local Market Share Now Holds Steady at 15%'. 24 July 2025. <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15?>

Thun, Max von, and Claire Lavin. *Engineering the Cloud Commons: Tackling Monopoly Control of Critical Digital Infrastructure*. Open Markets Institute, 2025. <https://www.openmarketsinstitute.org/publications/report-rethink-regulatory-approach-to-essential-cloud>.

Varoquaux, Gaël, Alexandra Sasha Luccioni, and Meredith Whittaker. 'Hype, Sustainability, and the Price of the Bigger-Is-Better Paradigm in AI'. arXiv:2409.14160. Preprint, arXiv, 1 March 2025. <https://doi.org/10.48550/arXiv.2409.14160>.

Von Thun, Max, and Daniel Hanley. 'Stopping Big Tech from Becoming Big AI: A Roadmap for Using Competition Policy to Keep Artificial Intelligence Open for All'. *SSRN Electronic Journal*, ahead of print, 2024. <https://doi.org/10.2139/ssrn.4990780>.

Wakabayashi, Daisuke. 'Prime Leverage: How Amazon Wields Power in the Technology World'. *Technology. The New York Times*, 15 December 2019. <https://www.nytimes.com/2019/12/15/technology/amazon-aws-cloud-competition.html>.