

How the Commission's Tech Sovereignty Package Misdiagnoses Europe's Digital Challenge

Dr Diana Năsulea

Programmes Manager and Researcher, IES Europe

15 July 2026

Summary

- On 3 June 2026, the European Commission adopted the European Technological Sovereignty Package, its most far-reaching intervention in digital markets to date. The package combines two legislative proposals, the Chips Act 2.0 and the Cloud and AI Development Act (CADA), with two non-legislative initiatives: the EU Open-Source Strategy and a Strategic Roadmap for Digitalisation and AI in Energy. The Commission presents the package as a measure to protect Europe from a foreign 'kill switch', meaning the ability of a non-EU government or provider to cut off, degrade, or take control of the digital services that critical infrastructure depends on.
- This briefing does not dispute that Europe faces real technological dependencies. It argues, however, that the chosen instruments – subsidies and origin-based 'sovereignty' requirements that treat nationality as a proxy for trust – are poorly matched to the problem and risk raising costs for consumers and companies of all sizes.
- The Union's own recent record serves as a warning. The 2023 Chips Act is on course to achieve a global production share of only 11.7% by 2030, well short of its 20% target, while the GAIA-X 'sovereign cloud' project never achieved deployment at scale. Data localisation requirements of the kind introduced by CADA are estimated to cost the EU economy around 0.4–1.1% of GDP.
- The package also creates loopholes that invite 'sovereignty washing' and capture, favours the largest member states by allowing them to make greater use of relaxed state aid rules, and sits in tension with the Commission's parallel commitment to simplification. The resulting burden of higher costs and reduced choice is likely to fall most heavily on SMEs and startups.
- The briefing offers evidence-based recommendations to address Europe's genuine digital weaknesses, including fragmented capital, high energy costs, and an incomplete Single Market, while reserving narrowly defined sovereignty requirements for the small set of cases, where the security case is strongest.

TABLE OF CONTENTS	1
INTRODUCTION	3
THE COMMISSION’S PROPOSAL	4
ANALYTICAL FRAMEWORK: COMPETITION, OPENNESS, AND THE TEST OF EVIDENCE	6
KEY FINDINGS	6
ASSESSMENT OF THE COMMISSION’S PROPOSAL	11
POLICY RECOMMENDATIONS	13
CONCLUSION: SOVEREIGNTY BY SUBSTANCE, NOT BY SUBSIDY	14
REFERENCES	15

About the author

Dr Diana Năsulea holds a PhD in Economics and serves as Programmes Manager and Researcher at IES Europe (Institute for Economic Studies Europe), where she designs and coordinates educational programmes, international seminars, and policy research projects promoting classical liberal ideas and economic freedom across Europe. Her research focuses on EU digital and trade policy, exploring their effects on competitiveness, SMEs, and national economies. She has authored numerous research and academic papers in these areas. Beyond her work with IES-Europe, Diana is a Teaching Associate at the University of Bucharest’s Faculty of History.

About EPICENTER

EPICENTER, the European Policy Information Center, is an independent initiative of thirteen leading think tanks from across Europe. It seeks to inform the European policy debate and promote the principles of a free society by bringing together the expertise of its members.

EPICENTER is formed by the Center for Political Studies (Denmark), Civil Development Forum (Poland), Fundalib (Spain), the Institut économique Molinari (France), the Institute of Economic Affairs (UK), the Institute of Economic and Social Studies (Slovakia), the Institute for Market Economics (Bulgaria), Istituto Bruno Leoni (Italy), KEFiM (Greece), the Lithuanian Free Market Institute, Prometheus (Germany), the Institute of Economic Studies – Europe (Romania), and Timbro (Sweden). Like its members, EPICENTER is politically independent and does not accept taxpayer funding.

Introduction

The European Union's dependence on technologies developed outside its borders is real and well-documented. Mario Draghi's 2024 report on European competitiveness found that the Union relies on non-EU suppliers for more than 80% of its digital products, services, infrastructure, and intellectual property (Draghi 2024). In cloud computing, the three largest US hyperscalers account for roughly 70% of the European market, while the combined share of EU-headquartered providers fell from around 29% in 2017 to about 15% in 2022.¹ In advanced semiconductors, Europe manufactures only a small fraction of global output. These dependencies involve genuine economic and security implications, and addressing them is a legitimate public policy concern.

On 3 June 2026, the European Commission responded with the European Technological Sovereignty Package, its most ambitious intervention in digital markets to date.² The package combines two legislative proposals, the Chips Act 2.0 and the Cloud and AI Development Act, with two non-legislative initiatives: the EU Open-Source Strategy and a Strategic Roadmap for Digitalisation and AI in Energy. When presenting the package, President Ursula von der Leyen emphasised that Europe cannot afford to depend on others for the technologies that keep its hospitals, energy grids, and public services running.³ Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy, stated that the aim was to ensure that no external provider of critical workloads could threaten European infrastructure with a 'kill switch'.⁴

The package arrives at a moment of tension within the Commission's broader agenda. Since taking office, the second von der Leyen Commission has built much of its identity around 'simplification', promising to reduce administrative burdens for businesses by 25% overall and by 35% for small and medium-sized enterprises (SMEs), while rolling back elements of recent digital legislation through the Digital Omnibus.⁵ The Tech Sovereignty Package moves in the opposite direction. It marks an explicit turn towards industrial policy by introducing subsidies, demand-side interventions, procurement preferences, and origin-based requirements for cloud and chip suppliers.

This briefing evaluates the package against its stated objectives: will the chosen instruments reduce Europe's strategic dependence and at what cost to consumers and companies? This briefing does not dispute that Europe faces genuine technological vulnerabilities. Rather, it argues that the Commission's chosen instruments – subsidies and 'sovereignty' requirements – are poorly matched to the problem. The Union's own recent experience suggests that it risks imposing high costs on consumers and on companies of every size while delivering little of the autonomy it seeks to foster. The analysis identifies the key loopholes and risks in the proposals and offers evidence-based recommendations to address Europe's underlying digital weaknesses, including fragmented capital, high energy costs, and an incomplete Single Market, without resorting to protectionism. As the

¹ 'European cloud providers' local market share now holds steady at 15%', *Synergy Research Group*, 24 July 2025 (<https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>).

² 'Europe unveils tech sovereignty package amid growing concerns over reliance on US tech', *CNBC*, 3 June 2026 (<https://www.cnn.com/2026/06/03/europe-tech-sovereignty-us-tech-reliance.html>).

³ 'Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience', European Commission press release IP/26/1187, 3 June 2026 (ec.europa.eu/commission/presscorner/detail/en/ip_26_1187).

⁴ Ibid.

⁵ 'An EU Compass to regain competitiveness and secure sustainable prosperity', European Commission press release IP/25/339, 29 January 2025 (ec.europa.eu/commission/presscorner/detail/en/ip_25_339).

package's two legislative components are still in the early stages of development, their provisions and thresholds may change as they progress through the European Parliament and the Council.

The Commission's proposal

The Tech Sovereignty Package consists of four components.

Chips Act 2.0

The first legislative proposal revises the 2023 EU Chips Act, shifting its focus from research to commercialisation and demand (European Commission 2026a). Its main provisions include a twelve-month cap on permitting for strategic facilities; 'Grand Challenges' targeting strategic chip types, such as advanced AI processors; 'Demand Accelerators' linking producers and buyers through offtake agreements; extended state aid for 'First-of-a-Kind' facilities across the value chain; the 'Semiconductor Regions of Excellence' initiative; a reinforced Chips for Europe Initiative and European Semiconductor Board; and a proposal for the Union's first open foundry for sub-three-nanometre manufacturing, with pilot production envisaged between 2030 and 2033. The proposal does not earmark significant new funding from the EU budget. Instead, it seeks to tap into public and private investment, with a headline ambition of mobilising around €120 billion by 2035, compared with the €43 billion associated with the original act.⁶

Cloud and AI Development Act (CADA)

The second legislative proposal aims to at least triple the Union's data-centre capacity within the next five to seven years – an objective that the Commission estimates would require roughly €200 billion, the majority of which would come from private investment (European Commission 2026b). CADA is built around three pillars. The first supports research and innovation in next-generation cloud and AI technologies. The second focuses on data-centre capacity, aiming to create 'data-centre acceleration zones' with streamlined twelve-month permitting, preferential grid access, and improved access to land, water, energy, and finance. The third pillar, and the one most consequential for this analysis, establishes a Union-wide 'sovereignty' framework with four ascending levels of assurance.

Under this framework, the lowest level requires only that infrastructure, assets, and customer data remain within the European Union. It requires any third-country-controlled provider to demonstrate that no law in its home country requires it to report unexploited security vulnerabilities to a foreign authority before those vulnerabilities are publicly known. The second level requires that all personnel, infrastructure, customer data and assets be located in the EU; that providers obtain EU cloud certification; that measures be taken to prevent third-country access to data; and that a full software bill of materials (i.e., an inventory of all software components and dependencies), including source-code audits of third-country components, be maintained. The third level requires providers to be owned and controlled within the EU. An exception is available only for providers from third countries that have received a data-protection adequacy decision from the European Commission and maintain an open market. The fourth and strictest level permits no third-country control and no derogation, while requiring the highest tier of EU cybersecurity certification and full control over all software components.⁷ CADA also directs public authorities to consider 'Union added value' as a

⁶ 'EU says it needs EUR 120 billion to revive local chip production', Bloomberg, 28 May 2026 (<https://www.bloomberg.com/news/articles/2026-05-28/eu-says-it-needs-120-billion-to-revive-local-chip-production>).

⁷ 'EU sets out plans to reduce reliance on US cloud providers', *Computerworld*, 3 June 2026 (<https://www.computerworld.com/article/4180801/eu-sets-out-plans-to-reduce-reliance-on-us-cloud-providers.html>); and

non-price award criterion in procurement. If the preferred option in the Commission's impact assessment is implemented, this criterion will become mandatory rather than voluntary. The proposal also codifies an 'open-source first' principle for the public sector (European Commission 2026b). The framework extends beyond government. Its sovereignty assessments and procurement criteria also affect private essential entities operating in critical sectors covered by the NIS2 Directive, including energy, health, transport, and water. The Commission also envisages secondary legislation that could later require these entities to apply the same tests.

The EU Open-Source Strategy

The third component of the package is a non-legislative strategy that places open-source software at the centre of the sovereignty agenda (European Commission 2026c). The Commission notes that the Union spends roughly €264 billion annually on information technology, much of it on proprietary software developed outside the EU. The strategy proposes an open-source maintenance instrument, procurement guidance that favours open standards, a catalogue of the Open Internet Stack, and measures relating to stewardship and skills, with a reported funding envelope of around €2 billion over seven years.⁸

Strategic Roadmap for Digitalisation and AI in Energy

The fourth component is a non-legislative roadmap that addresses the energy dimension of digitalisation (European Commission 2026d). It seeks to respond to the projected rapid growth in data-centre electricity demand, which the International Energy Agency projects will increase from around 70 terawatt-hours in 2024 to approximately 115 terawatt-hours by 2030. The roadmap promotes AI applications for grid management, a data-centre sustainability rating scheme with first labels expected in 2027, smart-meter deployment, and a European Energy Data Space.⁹

The strain is already visible. The Commission's own impact assessment records that data centres accounted for 22% of electricity demand in Ireland in 2025; that Dublin's grid operator imposed a de facto moratorium on new data-centre connections; and that this stalled an estimated €8–10 billion in planned investment, with comparable moratoria around Amsterdam (European Commission 2026f).

The Commission presents the package as a response to strategic dependency and as contributing to competitiveness. Virkkunen insists that 'technological sovereignty does not mean protectionism' and that Europe remains committed to openness and fair competition.¹⁰ This briefing examines whether the chosen instruments are consistent with that commitment and whether they will achieve their stated objectives.

⁷ 'The EU Cloud and AI Development Act in depth', *Covington*, 11 June 2026 (<https://www.globalpolicywatch.com/2026/06/the-eu-cloud-and-ai-development-act-in-depth/>).

⁸ 'EU tech sovereignty: a milestone for public code? Now implementation is key', *Free Software Foundation Europe*, 3 June 2026 (<https://fsfe.org/news/2026/news-20260603-01.en.html>).

⁹ The European Energy Data Space is a planned EU framework for the secure, standardised sharing of energy data among grid operators, suppliers, regulators, and consumers, intended to support better grid management and market transparency.

¹⁰ 'Remarks by Executive Vice-President Virkkunen and Commissioner Jørgensen on the tech sovereignty package', *European Commission* SPEECH/26/1244, 3 June 2026 (ec.europa.eu/commission/presscorner/detail/en/speech_26_1244).

Analytical framework: competition, openness, and the test of evidence

The analysis that follows rests on two foundations: well-established economic theories about how innovation, competition, and trade generate prosperity, as well as evidence on how comparable interventions have performed in practice.

First, competition, rather than central direction, is the primary driver of innovation and falling prices. Markets aggregate dispersed knowledge that no planner possesses and discipline failure in ways that politically directed investments rarely can.

Second, openness outperforms protection. Access to the best technologies, wherever they originate, lowers costs and raises productivity for the firms and consumers that use them. Barriers to that access, whether tariffs, local-content rules, or origin tests, raise domestic costs and invite retaliation abroad.

Third, government failure is as real as market failure. Subsidies and industrial targets are vulnerable to capture by well-resourced incumbents, rent-seeking, and the political temptation to support visible projects regardless of their returns. The case for intervention is justified only where there is not only a market imperfection but also confidence that it will improve upon the market outcome.

Fourth, technology neutrality protects competition. When the state mandates a particular technology or business model, whether proprietary or open source, domestic or foreign, it forecloses the discovery process through which better solutions emerge.

Fifth, regulatory burdens and market distortions affect the smallest actors the most. Large firms can absorb compliance costs and navigate discretionary criteria, while SMEs, startups, and scale-ups cannot. A policy that appears neutral may prove regressive in its effects.

Based on these principles, the briefing applies a simple empirical test: has the Union's recent experience with comparable interventions, most notably the 2023 Chips Act and the GAIA-X cloud initiative, delivered the autonomy and competitiveness it promised? Where evidence shows that targets were missed, funds misallocated, or markets fragmented, the burden of proof for a broader repetition of the same approach rises accordingly. The following sections apply this test to each pillar of the package.

Key findings

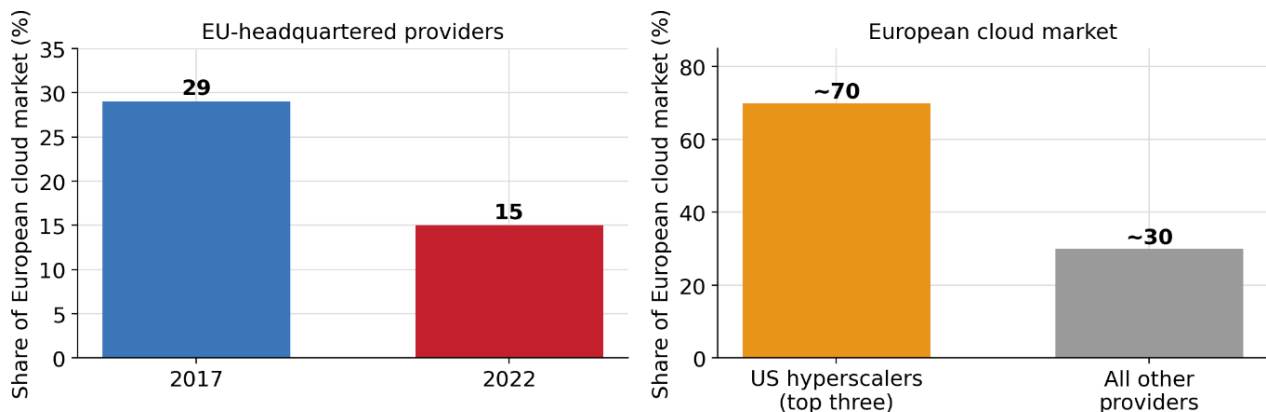
The sections that follow apply the test set out above to each part of the package. They start from a point of agreement, that Europe's dependence on non-EU technology is real, before showing why the instruments the Commission has chosen are unlikely to reduce that dependence and are likely to raise costs for the firms and consumers they are meant to help.

The dependency is real, but the diagnosis requires a different cure

Europe's dependence on non-EU cloud providers is not in dispute. According to data compiled by Synergy Research Group and cited by the Commission, the combined share of EU-headquartered providers in the European cloud market fell from approximately 29% in 2017 to about 15% in 2022 (Figure 1) and has broadly remained at that level. Meanwhile, the three largest US hyperscalers

together account for roughly 70% of the market. The two largest European providers, SAP and Deutsche Telekom, hold around 2% each.¹¹

Figure 1. Europe's cloud dependency



Source: Synergy Research Group (2025); European Commission (2026b)

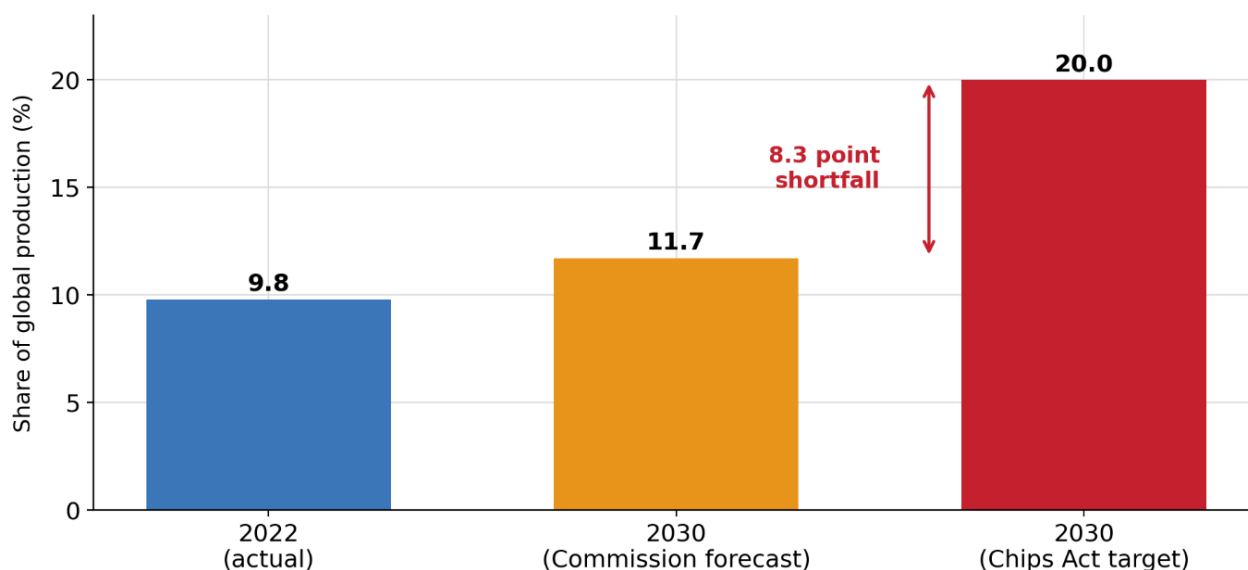
These figures support a different diagnosis from the Commission's. The Commission treats the declining market share of European providers as the problem to be solved and concludes that European firms should be promoted through procurement mandates and subsidies. A more persuasive reading is that European firms lost market share because they were less competitive in terms of price, performance, and scale. The appropriate response, therefore, is to address the conditions that constrain competitiveness: fragmented national markets, regulatory burdens that weigh most heavily on firms seeking to scale, scarce growth capital, the absence of a sufficiently deep and integrated capital market, and high energy costs. Restricting access to providers that businesses and consumers have chosen does not address any of these challenges. A policy that raises costs or reduces the quality of the cloud services on which European firms depend does not strengthen competitiveness but weakens it.

The Chips Act track record: targets unmet, money misallocated

The clearest test of the package's likely success is the EU's experience with the 2023 Chips Act, which Chips Act 2.0 is designed to extend. The results are not encouraging. In Special Report 12/2025, the European Court of Auditors concluded that the Union is highly unlikely to reach its target of securing a 20% share of global semiconductor production by 2030 (Figure 2) (European Court of Auditors, 2025). The Commission's own forecast projects a share of just 11.7% by 2030, up from 9.8% in 2022, leaving a shortfall of more than 8.3 percentage points against the target (European Commission, 2024). The Court's reporting member observed that the 20% target was largely aspirational and that achieving it would require a near quadrupling of European production capacity within a few years.

¹¹ 'European cloud providers' local market share now holds steady at 15%', Synergy Research Group, 24 July 2025 (<https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>).

Figure 2. EU share of global semiconductor production: target versus forecast



Source: European Court of Auditors (2025); European Commission (2024)

The diagnosis matters as much as the headline figure. The Court found that the Commission directly manages only around €4.5 billion, roughly 5% of the €86 billion mobilised under the original act, with most funding dependent on member states and private investors whose decisions the Union does not control. The cancellation of Intel's planned €30 billion facility in Magdeburg¹² illustrated the concentration risk inherent in tying strategic targets to a small number of flagship projects. The broader global context compounds the challenge. Leading manufacturers outside the Union budgeted more than €400 billion for new capacity between 2020 and 2023 alone (European Court of Auditors, 2025), compared to which European subsidies remain modest. The lesson is not that Europe spent too little, but that production-share targets set in Brussels are a poor instrument to influence an industry shaped by global capital flows, scarce specialised labour, and decade-long investment cycles. Chips Act 2.0 retains both the target and the underlying logic.

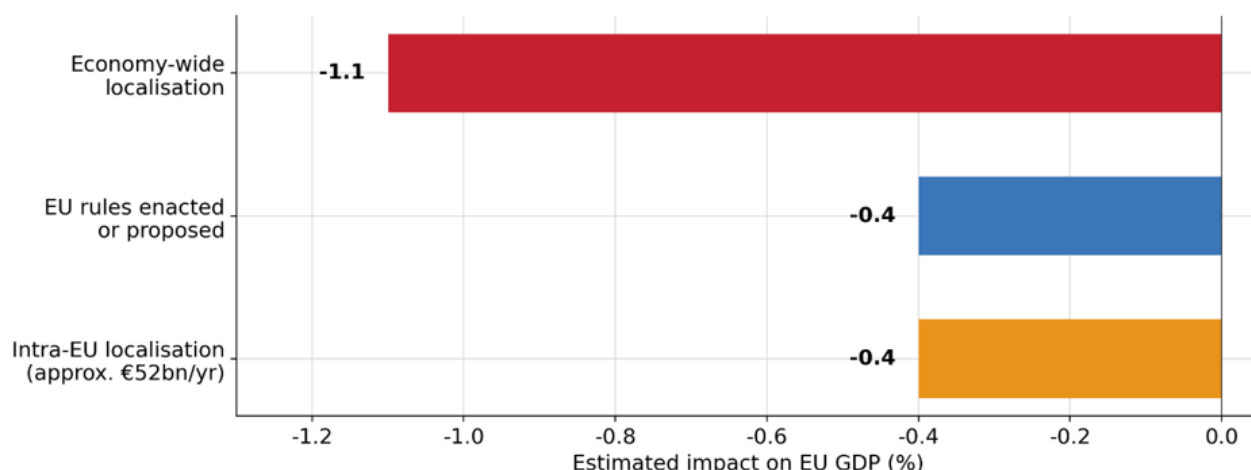
Sovereignty as protectionism: the cost of origin tests and data localisation

CADA's four-level assurance framework sits at the heart of the package and represents its greatest risk. By making ownership and control by EU entities a condition for the higher assurance levels – towards which the public sector and operators of critical infrastructure will be steered – the framework treats nationality as a proxy for security. As the Bruegel economist Mario Mariniello has argued, the package deploys many of the same protectionist tools that the EU has spent decades opposing in the name of open markets, while presenting them as sovereignty grounded in openness.¹³ The mechanism is similar to the US CHIPS Act (2022) and Buy American provisions (dating back in 1933), as well as China's semiconductor fund (2014). The novelty lies in the EU's adoption of the same approach.

¹² 'Intel cancels multi-billion euro chip factory in Germany', *Brussels Signal*, 25 July 2025 (<https://brusselssignal.eu/2025/07/intel-cancels-multi-billion-euro-chip-factory-in-germany/>).

¹³ 'To achieve tech sovereignty, Europe must not mimic its rivals', *Bruegel*, 11 June 2026 (<https://www.bruegel.org/first-glance/achieve-tech-sovereignty-europe-must-not-mimic-its-rivals>).

Figure 3. Estimated impact of data localisation on EU GDP



Source: Bauer et al. (2014); Bauer et al. (2016)

The economic costs of this approach are well documented. Requirements that data and infrastructure remain within a jurisdiction, and that providers be locally owned, are forms of data localisation and ownership discrimination. In a 2014 study, the European Centre for International Political Economy estimated that data-localisation measures enacted or proposed within the Union reduce EU GDP by around 0.4% (Figure 3), rising to as much as 1.1% under economy-wide localisation, while reducing domestic investment by nearly 4% (Bauer et al. 2014). These are estimates of a one-off reduction in the level of output and investment, not annual losses, and they predate the far more extensive localisation now under discussion. A later study focused on intra-EU barriers estimated that a Union-wide localisation regime would reduce GDP by roughly 0.4%, equivalent to around €52 billion annually (Bauer et al. 2016). These losses are not abstract. They will affect every firm that relies on cloud services and will disproportionately affect SMEs and startups, which depend on affordable, best-in-class infrastructure they cannot build or readily replace themselves.

The framing of the localisation mandate as ‘sovereignty’ obscures a basic trade-off. The Centre for European Policy Network notes that cloud prices have fallen consistently for two decades and that most European firms rely on multi-cloud strategies that an origin-based framework could disrupt.¹⁴ For the narrow set of genuinely sensitive workloads, the security concern is real and is addressed in the Assessment section, where the case for a tightly scoped sovereignty requirement is set out. For the vast majority of cloud use cases, however, steering demand towards ‘sovereign’ providers is likely to result in higher prices and reduced choice, with the costs ultimately borne by European businesses and, through public procurement, European taxpayers.

There is a deeper point that emerges from the Commission’s own evidence. The real source of consumer harm is not the provider’s nationality but the risks associated with lock-in. Where switching is costly and alternatives are limited, the Commission’s own impact assessment acknowledges that users are, in its own words, ‘defenceless against price increases’, citing Broadcom’s acquisition of VMware, after which customers reported licence fee increases of 800–1,500% (European Commission 2026f). Origin tests do nothing to address that vulnerability and may deepen it by narrowing the field of providers. The measures that genuinely protect customers are portability,

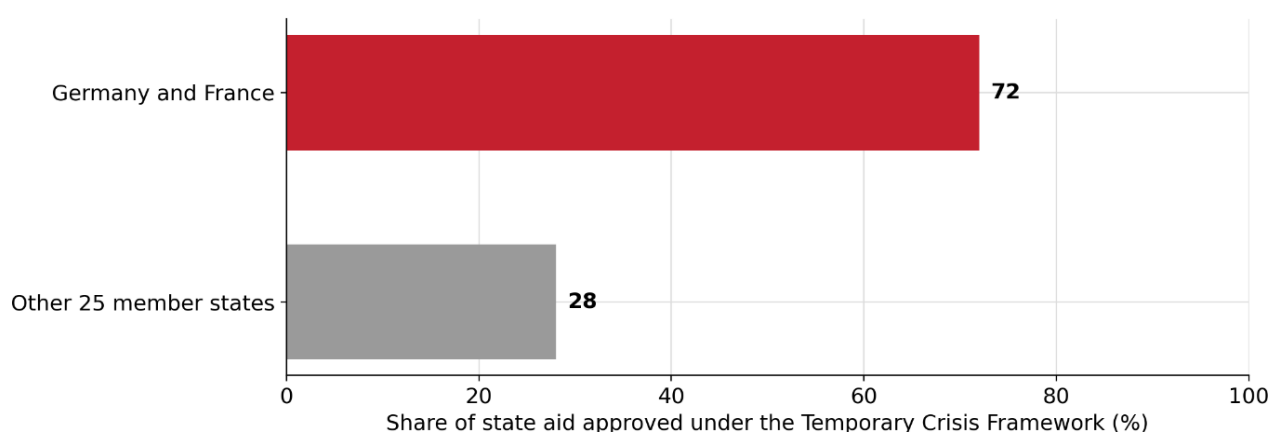
¹⁴ ‘EU tech sovereignty package: Sovereignty as a prerequisite of openness in times of geopolitical shift’, Centre for European Policy Network, 2026 (<https://www.cepn.eu/eu-topics/details/eu-tech-sovereignty-package.html>).

interoperable open standards, and the freedom to switch, not a requirement that the provider be domestically owned.

Subsidies, state aid, and the risk to cohesion

The package relies heavily on relaxed state-aid rules for 'First-of-a-Kind' and 'strategic' projects. Subsidy competition of this kind does not affect all EU member states equally. Since the loosening of state aid rules in March 2022, Germany and France together accounted for around 72% of the aid approved under the Temporary Crisis Framework to mid-2023 (Figure 4) (European Commission, Directorate-General for Competition, Ferraro, S., Cannas, G. and Van de Castele, K. (2024).

Figure 4. Concentration of state aid approvals since March 2022



Source: European Commission, Directorate-General for Competition, Ferraro, S., Cannas, G. and Van de Castele, K. (2024)

A framework that makes it easier for member states to subsidise favoured projects will predictably benefit those with the deepest fiscal resources. This risks distorting competition within the Single Market and disadvantaging firms in smaller and less affluent member states that cannot match the scale of subsidies offered by Germany or France for a single facility. The result is a transfer of resources from taxpayers across the EU to a small number of large recipients, without any guarantee that the spending will generate the productivity gains it is intended to achieve. The broader empirical literature on industrial policy remains, at best, mixed on whether such subsidies generate positive net returns. It is, however, consistent on one point: the most difficult discipline for political systems to apply is allowing failing projects to fail.

Loopholes, capture, and the GAIA-X precedent

The package's reliance on discretionary and loosely defined criteria creates significant scope for circumvention and capture. Key terms, including 'Union added value', 'trusted', 'EU-based', and 'control', are left to secondary legislation and member-state risk assessments. Discretion of this kind invites lobbying and favours firms with the resources to shape and navigate the rules. The maximum weighting reportedly attached to 'Union added value' in procurement – around 15 points out of 120 – can be engineered. Ownership structures can also be arranged so that non-EU technologies are delivered through EU-controlled joint ventures.

This is not a hypothetical concern. The regulation's own annex states that a joint venture between an EU entity and a third-country entity can qualify for higher assurance levels, while the impact assessment describes these 'sovereign joint ventures' as typically operating a hyperscaler's software stack with a security layer controlled by the EU partner. Vehicles of this kind already exist,

including Bleu (a Capgemini and Orange joint venture offering Microsoft services) and Delos Cloud (an SAP subsidiary running on Microsoft software). Their limitations are already apparent. A German state interior ministry concluded that Delos is not fully sovereign above the infrastructure layer because the application layer remains Microsoft software and, therefore, continues to be subject to the US CLOUD Act (European Commission, 2026f), which permits data access without notifying the customer. The Commission acknowledges the broader risk, warning in its own impact assessment that ‘sovereignty washing’ is likely to occur in the absence of a clear definition of sovereign services and the means to enforce it. The most likely beneficiaries of a complex, discretion-heavy framework are therefore large incumbents, European and non-European alike, rather than the SMEs and startups the package claims to support.

The EU has also been here before. The GAIA-X initiative, launched in 2019 and 2020 as a Franco-German project to build a ‘sovereign’ European cloud, never delivered production services at scale, even as European cloud market share continued to decline.¹⁵ Its former chief executive observed that there was never a common definition of digital sovereignty and that politicians displaced industry in determining how the project should be built.¹⁶ Critics argue that once the major hyperscalers were admitted as members, the initiative was effectively captured from within. CADA’s definition-light, discretion-heavy design recreates precisely the conditions under which GAIA-X struggled, yet the proposal offers little explanation for why the outcome would differ this time.

The contradiction with the simplification agenda

Finally, the package sits uneasily alongside the Commission’s flagship commitment to simplification. While the Digital Omnibus promises to reduce administrative burdens by 25% for all businesses, and by more than a third for SMEs, CADA introduces new sovereignty risk assessments, certification requirements, source-code audits, software bills of materials, and procurement criteria that public authorities and suppliers must apply. The Open-Source Strategy adds further procurement obligations. A reform programme cannot credibly claim to reduce red tape while simultaneously layering origin tests and assurance audits for procuring cloud, AI, and chips. The tension suggests that the package’s objectives, i.e., competitiveness, sovereignty, and simplification, are being pursued without a clear hierarchy and that, where they conflict, businesses and consumers will bear the cost.

Assessment of the Commission’s proposal

The Commission’s underlying objective – reducing Europe’s exposure to strategic dependency in critical technologies – is legitimate and, if pursued through the right instruments, could yield real benefits. However, assessed against the empirical evidence, the package presents substantial risks that warrant careful consideration.

The central concern is that the package treats the symptom, i.e., the market share of non-EU providers, rather than the cause, i.e., the conditions that make European firms less competitive. As the experience of the Chips Act suggests, subsidising production to achieve a fixed market-share target does not reliably increase that share. Steering demand towards locally owned providers raises costs without addressing why European providers lost ground in the first place. Several specific risks follow:

¹⁵ ‘Gaia-X and the sovereign cloud: from unicorns and rainbows to storm clouds’, *Forrester*, 25 May 2022 (<https://www.forrester.com/blogs/gaia-x-and-the-sovereign-cloud-from-unicorns-and-rainbows-to-storm-clouds/>).

¹⁶ ‘Why Europe’s cloud ambitions have failed’, *AI Now Institute*, 15 October 2024 (<https://ainowinstitute.org/publications/xi-why-europes-cloud-ambitions-have-failed>).

- **Higher costs and reduced choice.** Origin-based assurance levels and ‘Union added value’ procurement criteria increase costs and narrow the range of cloud, AI, and semiconductor inputs available to European firms. The burden falls disproportionately on SMEs and startups, which rely on affordable access to best-in-class technologies and have the least capacity to absorb higher prices or switching costs.
- **A fiscal bill with uncertain returns.** CADA's impact assessment acknowledges that sovereign cloud services carry a price premium of roughly 10–30% over standard public-cloud services, representing a recurring cost that will ultimately be borne by public bodies and regulated firms. It also estimates that porting the systems of approximately 6,400 public essential entities could cost up to €86 billion. The Commission itself notes that this is a maximalist estimate that assumes the simultaneous migration of every entity and likely overstates the true cost of the intervention (European Commission, 2026e; 2026f).
- **Fragmentation and retaliation.** By embedding origin-based discrimination, the package risks fragmenting the global market on which European exporters depend and inviting reciprocal treatment of European firms abroad. Preferential procurement that discriminates on the basis of nationality also sits uneasily with the Union’s commitments under the World Trade Organization (2012) Government Procurement Agreement. The Commission frames its intervention differently, arguing that it will prevent the national fragmentation and regulatory divergence that uncoordinated member-state rules might create. The relevant distinction, however, is that a genuine Single Market can only be built through openness and mutual recognition, not through a shared preference for domestic ownership.
- **Capture and loopholes.** As discussed above, discretionary criteria and loosely defined concepts favour well-resourced incumbents and create opportunities for ‘sovereignty washing’, undermining both the package’s stated objectives and the interests of smaller competitors.

In fairness, the Commission reaches a different conclusion on some of these issues. Its impact assessment judges the effects on SMEs and competitiveness to be predominantly positive, arguing that a harmonised market lowers barriers for smaller firms and that a single EU-wide sovereignty audit, valid across all member states, would replace today’s patchwork of national schemes and reduce compliance costs (European Commission 2026f). Those benefits are real as far as they go. However, they accrue primarily to providers that can already satisfy EU ownership requirements and do not offset the costs associated with new origin assessments, source-code audits, and bill-of-materials obligations imposed on those firms and their public-sector customers. Harmonisation is welcome, but harmonisation achieved through origin discrimination is not the same thing.

It is also important to acknowledge the strongest argument on the other side. The security concern motivating the package is not imaginary. Microsoft conceded before a French parliamentary hearing that it could not guarantee that data stored in the EU would be protected from access requests under the United States CLOUD Act, while the temporary suspension of the email account of the International Criminal Court’s prosecutor demonstrates that the risk of a foreign ‘kill switch’ is not purely hypothetical.¹⁷ For a narrowly defined set of genuinely sensitive workloads in defence, intelligence, and critical infrastructure, a degree of jurisdictional control is a legitimate requirement, and a carefully scoped sovereignty obligation may therefore be justified.

The objection is not to that narrow case but to the use of the wrong policy instruments to address it. Extending origin tests, procurement preferences, and subsidies across the broader digital economy raises costs in areas that should be governed by competition, portability, and price, while doing little

¹⁷ ‘Microsoft can’t keep EU data safe from US authorities’, *Forbes*, 22 July 2025 (<https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/>).

to address security risks. The proportionate response is targeted: encryption, customer-held keys, auditing, and data localisation only where strictly necessary, rather than a blanket preference for national ownership borne by the wider economy.

Policy recommendations

The following evidence-based recommendations would address Europe's genuine technological dependencies while avoiding the risks inherent in the Commission's current approach.

1. **Scope sovereignty requirements narrowly and set them in primary law.** Restrict mandatory sovereignty tiers to a clearly defined set of genuinely sensitive public-sector and critical infrastructure workloads. Any binding sovereignty obligations should be enacted by co-legislators on the basis of a robust impact assessment, rather than delegated to certification schemes or implementing acts, the approach that led earlier cloud-security initiatives to stall.
2. **Prefer technical and legal safeguards to origin tests.** Mandate encryption, customer-held keys, interoperability through open application programming interfaces, portability, and independent auditing. These measures mitigate the 'kill switch' risk without closing markets or inviting retaliation. The Commission's own analysis supports this approach: it acknowledges that open licensing removes the legal mechanisms that make vendor lock-in difficult to escape, strengthening the case for interoperability and portability rather than nationality tests.
3. **Subject every subsidy to rigorous cost-benefit analyses and hard sunset clauses.** Tie state aid and 'strategic project' funding to transparent, measurable outcomes and automatic expiry. Reassess the 20% semiconductor target in light of the findings of the European Court of Auditors and measure progress in terms of strategic importance and innovation rather than production quotas.
4. **Avoid data-localisation and sovereign-only procurement mandates.** The evidence shows these cost around 0.4% of EU GDP, equivalent to roughly €52 billion a year, and burden SMEs and startups disproportionately. Procurement should remain open, with security concerns addressed through targeted technical measures.
5. **Guarantee technology neutrality.** Encourage open-source solutions through fair evaluations based on the total cost of ownership, but do not mandate them. Blanket open-source mandates have been struck down elsewhere as discriminatory; procurement should allow the best solution to prevail on its merits.
6. **Complete the Digital Single Market and improve framework conditions.** Remove the internal barriers identified in the Draghi report, which the International Monetary Fund estimates are equivalent to a tariff of roughly 44% on goods (IMF 2024). Advance the Capital Markets Union, reduce industrial energy costs, and invest in skills and research. These measures address the underlying sources of the competitiveness gap – i.e., fragmented capital and high energy costs – which the Commission itself identifies but does not adequately address.

7. **Guard against capture and ‘sovereignty washing’.** Replace discretionary and loosely defined criteria such as ‘Union added value’ and ‘trusted’ with transparent, non-discriminatory, performance-based standards. The methodology behind any preference weighting should be published.
8. **Keep trade open and compliant with international commitments.** Buy European preferences risk breaching the non-discrimination provisions of the World Trade Organization (2012) Government Procurement Agreement and inviting retaliation. Security carve-outs should be reserved for genuine national-security procurement.

Conclusion: sovereignty by substance, not by subsidy

The Tech Sovereignty Package responds to a genuine problem. Europe's dependence on non-EU cloud services, semiconductors, and software is real, and the security risks that flow from it are not imaginary. The question is not whether to act, but how.

The evidence presented in this briefing points to a clear conclusion. The Union's recent experience with the 2023 Chips Act and the GAIA-X cloud initiative suggests that production-share targets set in Brussels and origin-based ‘sovereignty’ mandates do not reliably deliver autonomy or competitiveness. They miss their targets, lead to misallocation of public resources, fragment markets, and create loopholes that favour large incumbents while raising costs for consumers and the smaller firms they claim to support. Repeating the same approach on a larger scale is unlikely to produce a different outcome.

The alternative is not inaction. It is to reserve narrowly scoped sovereignty requirements for the limited set of genuinely sensitive workloads where they are justified; to address security concerns through targeted technical and legal safeguards rather than blanket nationality tests; to subject subsidies to rigorous cost–benefit analyses and sunset clauses; to keep procurement open and technology-neutral; and, above all, to complete the Digital Single Market and improve the framework conditions that will ultimately improve European firms' capacity to compete, including access to capital, energy, and skills. Such an approach would strengthen Europe's technological position by making it more open and more competitive.

As the proposals move through the legislative process, the European Parliament and the Council face a choice: whether the Tech Sovereignty Package will genuinely reduce Europe's strategic dependency or merely substitute the appearance of sovereignty for the substance of competitiveness at the expense of consumers and companies of every size. The answer will shape the openness, dynamism, and prosperity of Europe's digital economy for years to come.

References

- Bauer, M., Ferracane, M. F. and van der Marel, E. (2016) Unleashing internal data flows in the EU: an economic assessment of data localisation measures in the EU member states. ECIPE Policy Brief No. 3/2016. Brussels: European Centre for International Political Economy (<https://ecipe.org/wp-content/uploads/2016/12/Unleashing-Internal-Data-Flows-in-the-EU.pdf>).
- Bauer, M., Lee-Makiyama, H., van der Marel, E. and Verschelde, B. (2014) The costs of data localisation: friendly fire on economic recovery. ECIPE Occasional Paper No. 3/2014. Brussels: European Centre for International Political Economy (https://www.ecipe.org/wp-content/uploads/2014/12/OCC32014_1.pdf).
- Draghi, M. (2024) The future of European competitiveness. Brussels: European Commission (https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en).
- European Commission (2024) State of the Digital Decade 2024. COM(2024) 260 final. Brussels: European Commission (<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2024:260:FIN>).
- European Commission (2026a) Proposal for a regulation establishing a framework of measures to strengthen Europe's semiconductor ecosystem (Chips Act 2.0). Brussels: European Commission (<https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20>).
- European Commission (2026b) Proposal for a Cloud and AI Development Act (CADA). Brussels: European Commission (<https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>).
- European Commission (2026c) EU Open Source Strategy. Brussels: European Commission (<https://digital-strategy.ec.europa.eu/en/policies/open-source-strategy>).
- European Commission (2026d) Strategic Roadmap for Digitalisation and AI in Energy. Brussels: European Commission (https://energy.ec.europa.eu/publications/strategic-roadmap-digitalisation-and-ai-energy-sector_en).
- European Commission (2026e) Commission staff working document, impact assessment report accompanying the Cloud and AI Development Act. SWD (2026) 502 final, Annex 12, Section 12.4, 3 June. Brussels: European Commission ([https://ec.europa.eu/transparency/documents-register/detail?ref=SWD\(2026\)502&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2026)502&lang=en)).
- European Commission (2026f) Commission staff working document, impact assessment report accompanying the proposal for a Cloud and AI Development Act. SWD (2026) 502 final, 3 June. Brussels: European Commission ([https://ec.europa.eu/transparency/documents-register/detail?ref=SWD\(2026\)502&lang=en](https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2026)502&lang=en)).
- European Commission, Directorate-General for Competition, Ferraro, S., Cannas, G. and Van de Castele, K. (2024) The use of crisis state aid measures in response to the Russian invasion of Ukraine (until end-June 2023). Brussels: European Commission (https://competition-policy.ec.europa.eu/document/download/22938d94-beaa-44bf-97ca-8a1785ca1a1c_en).
- European Court of Auditors (2025) The EU Chips Act. Special report 12/2025. Luxembourg: European Court of Auditors (<https://www.eca.europa.eu/en/publications?ref=sr-2025-12>).
- IMF (2024) Regional economic outlook Europe. Washington, DC: International Monetary Fund (<https://www.imf.org/-/media/files/publications/reo/eur/2024/october/english/text.pdf>).

Synergy Research Group (2025) European cloud providers' local market share now holds steady at 15%. Reno, NV: Synergy Research Group (<https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>).

World Trade Organization (2012) Revised Agreement on Government Procurement (GPA). Geneva: World Trade Organization (https://www.wto.org/english/docs_e/legal_e/rev-gpr-94_01_e.htm).