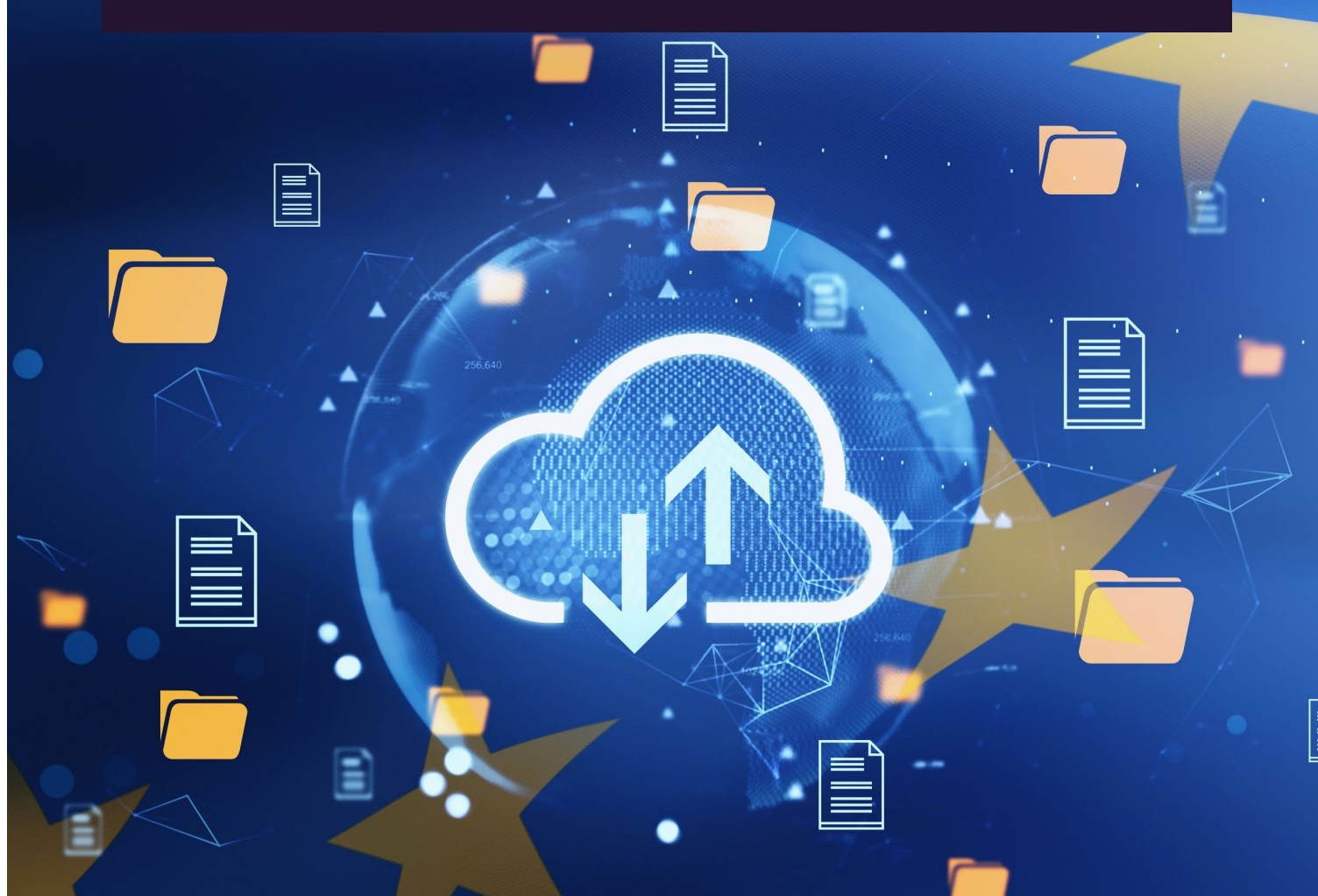


OCCASIONAL PAPER – No. 09/2026

Cloud Sovereignty and the Single Market: A Better Understanding of Government Procurement and National Cloud Technology Preferences

By **Matthias Bauer** (Director), **Andrea Dugo** (Economist), **Fredrik Erixon** (Director), **Dyuti Pandya** (Analyst), **Elena Sisto** (Economist) at ECIPE.



This study was made possible with support from Microsoft. The authors thank Laura Fransen for her research assistance.

EXECUTIVE SUMMARY

Europe is right to pursue better digital sovereignty, but the ambition is marked by a conceptual ambiguity. “Sovereignty” is often used to describe two distinct logics that policymakers treat as mutually reinforcing, even though they can diverge in practice. The first is functional sovereignty, a term we use in this paper to describe sovereignty as a security and resilience objective: whether the risks associated with cloud services can be effectively managed by keeping data secure, limiting legal exposure, maintaining operational continuity and preserving the ability to switch providers when needed. The second is industrial sovereignty, which treats sovereignty as an industrial-policy objective. Here, the focus shifts from the public authority as a user of cloud services to the origin, ownership and market position of the provider, with EU headquarters or other origin-based criteria used as proxies for sovereignty.

Understood substantively, sovereignty is a matter of security, resilience and risk management, delivered through risk-based technical, contractual and organisational safeguards rather than inferred from the nationality, ownership or location of the provider. Industrial-sovereignty criteria can operate as proxies for control, but they do not necessarily demonstrate that the underlying risks have been mitigated. When sovereignty is pursued through such proxies rather than verifiable safeguards, it can narrow competition, reduce supplier choice and reinforce national market boundaries.

The proposed Cloud and AI Development Act (CADA) brings both logics together. Its four EU assurance levels are framed around the legitimate objectives of security and resilience, but they also operationalise sovereignty through requirements concerning EU establishment, EU-located infrastructure and personnel, EU citizenship or residence, and restrictions on third-country control. These conditions go beyond the assessment of technical and operational risk. At the higher assurance levels, particularly Levels 3 and 4, eligibility increasingly turns on a provider’s territorial, corporate and personnel links to the Union. As industrial-sovereignty conditions become progressively more prominent, the framework begins to operate not only as a risk-management regime but also as a nationality-, territory- and control-based market filter.

The empirical analysis that follows examines whether this risk is already visible in public cloud procurement across Member States. The paper tests the market assumption behind this design by using a novel dataset of 8,725 cloud-related procurement contracts drawn from Tenders Electronic Daily (TED) across nine Member States between 2018 and 2025. Three findings stand out in the quantitative analysis:

- **European cloud procurement was already highly concentrated nationally before sovereignty became a policy objective:** roughly 97 per cent of contracts went to domestically registered providers, with negligible intra-EU cross-border competition.
- **Sovereignty framings deepen this concentration and narrow competition.** Contracts invoking the post-2019 vocabulary are associated with greater national concentration and narrower competition. This newer framing includes references

to frameworks such as SecNumCloud, GAIA-X and cloud de confiance as well as data-residency requirements. Contracts invoking this vocabulary reach **100 per cent domestic awards**, and the **sole-bidder rate rises from 28 per cent where no sovereignty language is present to 46 per cent** under the new framing, a contraction of the very optionality that user-level sovereignty requires.

- **Domestic winners frequently rely on hyperscaler infrastructure beneath the prime contractor.** Sovereignty attaches to the nationality of the operator, not to the infrastructure layer on which the service depends.

The empirical analysis points to what we call the sovereignty paradox: current frameworks already nationalise the contract layer while leaving important dependencies at the infrastructure layer. CADA's Levels 3 and 4 can be understood as an attempt to close this gap. But if applied too broadly, they risk doing so by excluding many of the operator-partner arrangements on which European sovereign-cloud provision currently relies, reducing serviceability, supplier choice and redundancy without necessarily increasing resilience.

A possible counterargument is that some fragmentation may be a price worth paying if it reduces strategic dependencies and redirects demand towards European providers. Yet the experience of Member States that have pursued similar approaches for years is instructive in this regard. These policies have sustained national providers serving domestic markets, but they have not produced European providers with the scale and capabilities to compete across the single market or meet the full range of public-sector cloud needs. At the same time, narrowing the supplier pool reduces choice and redundancy, which are themselves essential components of resilience.

The paper's central recommendation is that CADA should define sovereignty through the logic of functional sovereignty: as a demonstrated, risk-based outcome rather than a status inferred from ownership or origin, and should build resilience through supplier choice, redundancy and an open operating-partner model. The paper recommends:

- **Define sovereignty through demonstrated security, resilience and risk management, not ownership or origin.** CADA should assess whether risks are effectively controlled through verifiable technical, contractual and organisational safeguards, rather than relying on establishment, nationality or ownership as proxies for control. This would better protect data, continuity, auditability and switching options while preserving supplier choice and redundancy.
- **Apply higher assurance levels proportionately and through a binding EU-wide risk methodology.** The most restrictive requirements should be reserved for genuinely sensitive and critical workloads. The Article 29 methodology should be applied consistently across Member States, with any departures justified, transparent and limited, to prevent twenty-seven different interpretations from reproducing existing fragmentation.
- **Make Article 18 recognition objective and predictable.** Recognition of associated third countries should be based on clear and realistic criteria, defined procedures and timelines. A predictable recognition pathway would support investment in European cloud and AI capacity while preserving appropriate security requirements.

- **Protect the single market through effective Union-wide recognition and an open operating-partner model.** Recognition under Article 17 should be genuinely portable across the Union, so that providers do not face repeated qualification requirements across Member States. The review mechanism should also work in both directions – addressing requirements which are also unnecessarily restrictive. This would allow European systems integrators, cloud operators and managed-service providers to compete across borders while implementing and auditing the safeguards required for functional sovereignty.
- **Avoid extending restrictive sovereignty requirements beyond the public sector.** Any mandatory extension to highly critical private-sector entities under Article 31 would represent a significant and disproportionate expansion of the framework that lacks justification. Any expansion beyond the public sector should therefore be subject to ordinary legislative procedure through a review clause rather than through delegated acts, subject to clear criteria and a full impact assessment, given the risks to serviceability, supplier choice and resilience identified in this paper.

1. INTRODUCTION

The European Union is rightly placing the idea of “One Europe, One Market” at the heart of its efforts to revive the region’s competitiveness and economic growth. It is also a central part of building stronger European capabilities in an age of rapid technological change and innovation, and a world featuring an increasing number of conflicts. The single market brings scale opportunities through a larger market and more consumers, but also allows for deeper scope in how firms specialise, invest, and innovate. The technology market is going to change profoundly in the next ten years through quantum technology, supercomputing, edge computing, 6G, space and satellite expansion, and more. A deeper single market would help Europe to be a region for frontier innovation.

There is a different vision for Europe – one that risks being in opposition to a thriving single market. Rather than building stronger capabilities for cutting-edge innovation in Europe, its central idea claims that Europe should pursue policies that weans itself of foreign technology suppliers, especially in the field of cloud services. Principally, the ideal is for the region to become independent of foreign markets for its technology supply. This vision comes in different shapes and forms, but the unifying element is that Europe is at an “Independence Moment” and that it, now, should use policies to achieve sovereignty by restricting the market access for foreign cloud suppliers, regardless of what services they supply and how they supply it.

While there are good and legitimate reasons for Europe to build stronger cloud sovereignty, it matters crucially how it is done and if it includes policies barring foreign-owned providers from the European market. It is not a black-or-white choice between building European capacities and integrating the single market with the assistance of large cloud providers: both features are necessary. But an ideological version of sovereignty risks taking Europe in that direction. In that development, the danger is that the very instruments designed to secure sovereignty could undermine the objective they are meant to advance. The proposed Cloud and AI Development

Act (CADA)¹ illustrates this risk. Rather than strengthening Europe's collective capacity, it may instead exacerbate the current structure of the public cloud market producing 27 fragmented national markets rather than one European market.

There is a conceptual confusion that runs through the political debate. European cloud sovereignty is invoked to present two different logics that are often presented as mutually reinforcing by policymakers. However, they diverge in practice.

- The first treats **sovereignty as a security and resilience objective** – it deals with **functional sovereignty** and issues that are core to any real meaning of the term. Here, the relevant perspective is that of the public authority as a buyer and user of cloud services. The question is whether governments can manage the risks attached to the services they procure: securing data, managing risks, limiting foreign legal exposure, verifying technical systems, maintaining continuity, and switching providers when necessary. Sovereignty, in this sense, is for the user to have choice and optionality for the design of their cloud service needs. If anything, resilience from that perspective will be better served by providing a larger supply chain diversity than by reducing the supply chain options. For any real sovereignty at the user level, it is necessary to have market variety and be able to attract many and different bidders for a contract.
- The second treats **sovereignty as an industrial policy objective**. Here, the relevant perspective is that of EU-headquartered firms as "producers" in various parts of the cloud economy, usually cloud infrastructure. The question is whether Europe-headquartered firms can be made to grow faster if they are not exposed to competition with non-European providers. Sovereignty, in this sense, is about the market positioning of firms in Europe.

CADA includes the two different logics and, confusingly, aims to achieve both outcomes. Although it frames the four European Union assurance levels as criteria for security, resilience and trustworthy cloud provision, the criteria operationalise sovereignty through requirements concerning EU establishment, EU-located infrastructure and personnel, EU citizenship or residence, restrictions on third-country control, and control over software supply chains.² These requirements do not merely assess technical risk. At higher assurance levels (in particular at Levels 3 and 4) they also condition market access on the provider's territorial, corporate and personnel links to the Union. In that sense, these criteria combine important risk-management elements with industrial sovereignty conditions. At the higher assurance levels, industrial sovereignty conditions become sufficiently prominent that the framework will operate as a nationality-, territory-, and control-based market filter.

The growing emphasis on cloud sovereignty further raises a broader question about the future

¹ European Commission. (2026). Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final). <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

² European Commission. (2026). Annexes to the proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act) (COM(2026) 502 final, Annex II). <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>

organisation of Europe's digital economy. The EU has long sought to build a single market based on common rules, cross-border competition, and economies of scale. As sovereignty considerations increasingly shape procurement, certification, and public-sector cloud strategies, policymakers must reconcile legitimate security and resilience objectives with the need to preserve an open and integrated European market. If each jurisdiction develops its own understanding of sovereign cloud, Europe risks creating fragmented compliance regimes, incompatible technical requirements, and smaller protected national markets. The debate is no longer simply about who provides cloud services. It is about how sovereignty policies affect competition, innovation, investment, strategic capability, and the future coherence of the European single market.

This paper contributes new empirical evidence to the cloud sovereignty debate by examining public procurement outcomes rather than policy statements alone. Drawing on a dataset of 8,725 cloud-related public procurement contracts published in Tenders Electronic Daily (TED)³ across nine EU member states between 2018 and 2025, it reveals three key findings:

- European cloud procurement was already highly concentrated at the national level before cloud sovereignty became a prominent policy objective: approximately 97 per cent of procurement contracts were awarded to domestically registered providers, with very limited cross-border competition within the single market.
- The emergence of sovereignty-oriented procurement frameworks, particularly after 2019, is associated with even greater domestic concentration, effectively reinforcing national preferences in public cloud procurement. Importantly, the development gradually leads to a high single-bidder ratio, reaching almost 50 per cent of all public cloud contracts.
- Domestic contract awards frequently rely on infrastructure provided by US providers. In many cases, contract awards are attached to the nationality of the prime contractor rather than the underlying infrastructure on which services depend.

These findings reveal a central characterisation of the current policy framework. While sovereignty measures shift procurement towards domestic suppliers, they rely on the participation of many different companies that also include US hyperscalers. This comes off as one of its features. While sovereignty demands lead to more EU fragmentation in actual contract awards, there are no EU cloud companies with full-stack capabilities to deliver across many EU markets.

The idea of a single European alternative to US hyperscalers rests on the assumption that European cloud firms either already have, or will soon develop, the scale, investment capacity, and service portfolio needed to serve customers across the EU. In practice, that supply offering does not exist at the necessary scale and with similar capabilities for risk management that respond to Europe's digital growth ambitions. Moreover, the larger EU companies in the cloud stack are, out of scale necessity, also going global – and, in the process, anchoring themselves in a global and multi-legal environment that sovereignty frameworks are supposed to limit. The reality is that all layers of cloud computing are increasingly shaped by large economies of scale, global networks, and rising AI-related investment requirements. The more realistic outcome

³ Publications Office of the European Union. (n.d.). Tenders Electronic Daily (TED) [Database]. Retrieved June 6, 2026, from <https://ted.europa.eu>

of cloud sovereignty frameworks is therefore that national cloud providers will come to serve national markets, supported by domestic procurement rules and political preferences. They are not creating a European cloud market. They are fragmenting it.

One might argue that CADA is intended precisely to address this risk of fragmentation by establishing a single Union cloud sovereignty framework and Union-wide recognition of services meeting the relevant assurance level. Under Article 29, however, Member States retain discretion to identify which public-sector activities are subject to particular assurance levels. While the Commission may intervene where the assurance level identified by a Member State is considered "not appropriate", the proposal does not establish an equally clear mechanism to address disproportionate national classifications or additional requirements that could, in practice, restrict access to public procurement beyond the conditions attached to the relevant Union assurance level. The Commission's consistency mechanism should operate in both directions, addressing both insufficient protection and national requirements that are unnecessarily restrictive or disproportionate.

In this process, the aspired cloud sovereignty is therefore at risk of becoming a vehicle for policies that favour selected providers, restrict competition and fragment digital markets, even while nominally pursuing resilience and risk management. The risk is also that they hamstring European cloud companies seeking to build global scale. This may further translate risks associated with data location, operational continuity, and third-country control into escalating assurance levels and procurement criteria that increasingly condition market access to establishment, ownership, and control and supply-chain origin.

A more legally and economically coherent approach would keep those resilience objectives, but discipline their use through proportionality and technological neutrality requirements that preserve interoperability, portability, and multi-cloud options. The paper proceeds as follows. **Section 2** examines the different dimensions of cloud sovereignty and shows how CADA's four assurance levels translate legitimate objectives – data security, legal exposure, technical auditability, and operational continuity – into nationality-based market requirements. **Section 3** presents procurement evidence showing that Europe is already operating through fragmented national cloud markets and that sovereignty conditions function as a domestic-concentration filter. **Section 4** sets out policy recommendations for the European single market.

2. CLOUD SOVEREIGNTY AS REGULATORY DESIGN: FROM RESILIENCE TO MARKET FILTER

The cloud sovereignty debate is often framed as a question of dependence versus independence. This framing is very broad and its level of abstraction tends to invite interpretations that translate sovereignty into a question of provider ownership or nationality. This issue was already visible in

the EU Cloud Certification Scheme (EUCS) debate.⁴ EUCS began as a cybersecurity certification scheme under the Cybersecurity Act, but its highest-assurance levels became the site of a broader sovereignty debate over Union establishment, Union control, exposure to non-Union legal compulsion, and the location of personnel, data and operations. The proposed CADA does not simply revive that debate. It moves it into a stronger legal and procurement setting. EUCS remained, formally, a certification debate, whereas CADA links sovereignty classification to public-sector adoption and government procurement demand through a Union-wide sovereignty assessment framework and a public-sector adoption mechanism. What EUCS struggled to settle as a certification question, CADA reintroduced as a procurement, market-access and industrial-policy question.

It is unlikely that CADA will resolve the frictions between the competing logics – security, resilience, and risk management versus industrial policy and ownership control. While some define technological sovereignty on the basis of ownership or nationality, the reality is far more complex than what such ideology-tinged categories allow. A greater presence of European providers may strengthen industrial capacity, but it does not automatically improve Europe's ability to achieve resilience, secure data, ensure service continuity, reduce legal exposure, or exercise effective control over critical technologies. Conversely, the use of non-European providers does not necessarily imply a loss of sovereignty.⁵

2.1 What Sovereignty Requires and What CADA Filters

Technological sovereignty is best understood not as self-sufficiency but effective control: the capacity to secure, operate, adapt, and exit from critical technologies under conditions of interdependence, regardless of who owns or supplies them. In this perspective, sovereignty is primarily about resilience, security, and the ability to manage and protect against some dependencies rather than eliminate them. Crucially, that control is something to be demonstrated through specific, auditable technical, operational and contractual safeguards – not inferred from a provider's ownership, nationality or place of establishment. This is what a functional sovereignty approach is, and this is also where the current European debate becomes conceptually unstable. The 2026 Tech Sovereignty Package⁶ captures a broader shift in EU digital policy: technological

⁴ European Commission. (2021, June 9). EU cloud certification scheme. <https://ec.europa.eu/newsroom/cipr/items/713799/en>; see also Salmon, J., Crawford, L., Thasarathakumar, L., Lee, D., Nicol, A., & Leung, J. H. W. (2024, June 12). EUCS: Controversial sovereignty issues continue to drive debate for cloud services. Hogan Lovells. <https://www.hoganlovells.com/en/publications/eucs-controversial-data-sovereignty-issues-continue-to-drive-debate-around-the-eu-certification-scheme-for-cloud-services>

⁵ For example, AWS describes its European infrastructure in terms of cloud Regions and Availability Zones, with European regions including Frankfurt, Ireland, London, Milan, Paris, Stockholm, Spain, and Zurich. Microsoft's EU Data Boundary commits to storing and processing customer data and personal data for core cloud services, including Azure, Microsoft 365, Dynamics 365 and Power Platform, within the EU and EFTA, subject to defined exceptions. Google Cloud similarly operates regional infrastructure in Europe as part of its global network of 43 regions and 130 zones, allowing customers to select locations for latency, availability and sovereignty requirements. Oracle's EU Sovereign Cloud is designed to restrict operations and support to EU-resident personnel employed by dedicated EU legal entities. These examples show that non-European and non-EU-headquartered cloud providers participate in Europe as infrastructure operators, employers, contractors and regulated service providers, rather than merely exporting cloud services from abroad. This does not remove concerns about foreign legal exposure, dependency or strategic control, but it does suggest that sovereignty cannot be assessed by provider nationality alone. See: Amazon Web Services. (n.d.). AWS Regions. <https://docs.aws.amazon.com/global-infrastructure/latest/regions/aws-regions.html>; Microsoft. (n.d.). What is the EU Data Boundary? <https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn>; Google Cloud. (n.d.). Cloud locations. <https://cloud.google.com/about/locations>; Oracle. (n.d.). Oracle EU Sovereign Cloud. <https://www.oracle.com/cloud/eu-sovereign-cloud/>

⁶ European Commission. (2026, June 3). Commission proposes tech sovereignty package to strengthen Europe's digital autonomy and resilience [News]. <https://digital-strategy.ec.europa.eu/en/news/commission-proposes-tech-sovereignty-package-strengthen-europes-digital-autonomy-and-resilience>

sovereignty is increasingly being framed not only as a matter of control, resilience, and security, but also as a strategy for building European industrial capacity and reducing structural reliance on foreign technology providers.

Early on, the package was billed as part of Europe's transition from a "Regulatory Superpower" to becoming a "Production Powerhouse."⁷ CADA illustrates this evolution. Article 7 requires Member States to adopt national cloud and AI strategies covering adoption, data-centre capacity, high-intensity computing infrastructure, public procurement, open cloud-stack technologies, and access to high-quality data. These strategies are instruments through which the state can shape demand, direct investment, prioritise certain technological architectures, and influence the structure of cloud and AI markets. In this respect, CADA shows how sovereignty can move from a framework for securing operational control to a broader justification for state-led market formation.

This may be presented as capacity-building, but it is also expanding the discretionary role of governments in technology markets. The difficulty is that, once sovereignty is framed as an industrial-policy objective, it can justify measures that go beyond resilience and security, or sometimes even go against them. Procurement preferences, European-made technology mandates, or support for particular cloud-stack models may privilege politically defined industrial objectives over openness, competition, interoperability, supply chain diversity, and technological pluralism. The challenge is that industrial capacity and technological sovereignty are not the same thing. A European-owned provider may still depend on foreign infrastructure, software, semiconductors, or services, just as foreign-owned providers may contribute to resilience, innovation, and capability within Europe. And restrictions on using non-EU providers may reduce supply chain diversity and thereby de facto reduce resilience.

Where ownership, localisation or nationality become proxies for resilience, they can determine access to procurement and regulated markets without necessarily improving security or operational controls. In this respect, sovereignty requirements risk functioning as de facto market access conditions with consequences for competition, interoperability, and the integration of the European digital market.

This stronger industrial-policy reading of sovereignty is also visible in the broader EuroStack debate. EuroStack makes explicit what is more indirectly reflected in CADA: that technological sovereignty is not only about controlling data, infrastructure, or critical technologies, but also about redirecting European demand towards European providers and supply chains. It argues that, for strategic digital technologies, procurement should move from an open default toward a "procure sovereign" default, with exceptions only where no viable European alternative exists.⁸

At the same time, many EuroStack advocates admit that data location alone is insufficient for sovereignty, insisting that sovereignty requires a broader set of jurisdictional, technical, operational,

⁷ Calisti, M. (2026, March 19). The 2026 tech sovereignty package and its dilemmas. Martel Innovate. <https://martel-innovate.com/news/2026/03/19/the-2026-tech-sovereignty-package-and-its-dilemmas/>

⁸ Caffarra, C., Fermigier, S., Gambardella, A., Hidalgo, A., Lechelle, Y., Parsons, C., Styma, F., & Yen, A. (2025). Deploying the EuroStack: What needs to happen now (White paper). EuroStack Initiative. <https://eurostack.eu/wp-content/uploads/2025/08/eurostack-white-paper-final-19-05-25-3.pdf>

data, and economic controls. This is analytically useful because it reveals the ambivalence of the sovereignty agenda. EuroStack recognises that sovereignty is multidimensional but then translates that insight into a European-preference procurement model.⁹ Sovereignty therefore becomes not only the ability to control technology, but also a justification for steering public demand, favouring European providers and reorganising supply chains around politically defined autonomy goals.

CADA brings this same logic into legal form through Article 16 and Annex II, which translate cloud sovereignty into a graduated assurance architecture. Rather than treating sovereignty as a binary question of data localisation, the proposal constructs it as a composite compliance standard. Each assurance level combines requirements concerning establishment, infrastructure, personnel, cybersecurity, subcontracting, third-country control, operational support, software supply chains and control over software development.

Read this way, CADA's assurance levels target four dimensions of cloud sovereignty. **Data sovereignty** is addressed through rules on the location of customer data, metadata, telemetry, data flows, backups, logs, and restrictions on transfers outside the Union. **Legal sovereignty** is addressed through Union establishment, ownership and control tests, restrictions on third-country control, legal separation from third-country subsidiaries, and safeguards against foreign access or disruption. **Technical sovereignty** is addressed through cybersecurity certification, software bills of materials, dependency mapping, software supply-chain transparency, source-code auditability, open-source controls, protections against remote tampering, and migration planning. **Operational sovereignty** is addressed through requirements concerning infrastructure, assets, personnel, support, administration, monitoring, incident response, privileged access, backup handling, and disaster recovery.

The difficulty is not that these dimensions are irrelevant. The difficulty is that CADA bundles them into assurance levels that become progressively more restrictive. Requirements originally intended to enhance resilience and operational control can also function as eligibility criteria, specifying where a provider is established, how its infrastructure and personnel are managed, who oversees it, and how its software stack is governed. The cumulative effect is a tiered framework in which access to higher-assurance public-sector cloud resources depends on increasingly demanding legal, organisational, technical, and control-related conditions.

This raises a proportionality and opportunity question: whether the stricter levels are necessary to secure resilience, legal autonomy and operational continuity, or whether they also operate as market-access restrictions that privilege certain providers and architectures independently of demonstrable qualities, as regards e.g. security, sustainability, privacy or accessibility, and more. This question becomes especially important because CADA does not leave assurance levels as abstract classifications. The question also arises to what extent these stricter origin-focused levels will reduce the ability of European players to have access to a plethora of cloud-based solutions to protect themselves against the risk of becoming over-dependent on a single solution.

⁹ Ibid.; see also Bria, F., Timmers, P., & Gernone, F. (2025). EuroStack – A European alternative for digital sovereignty. Bertelsmann Stiftung. <https://doi.org/10.11586/2025006>

Articles 29 and 30 connect the assurance architecture to public-sector cloud procurement. Article 29 requires Member States and Union entities to identify public-sector activities using cloud services that contribute to the preservation of public order in specified sectors and areas, and to determine whether Union assurance level 2, 3 or 4 is appropriate for those activities. That assessment must consider, among other things, the sensitivity and criticality of the data processed, the risk of unlawful third-country access, the risk of service disruption, and whether a multi-vendor or multi-cloud strategy is appropriate. Article 30 then gives this assessment procurement consequences: ordinary public-sector cloud uses must rely on services recognised at Union assurance level 1, while public-order-relevant activities must only procure services recognised at Union assurance level 2, 3 or 4, subject to exceptional derogations where no suitable recognised service exists, where a previous comparable procedure failed, or where compliance would entail disproportionate cost.

Two features of this design deserve emphasis. First, the trigger for higher-tier obligations – whether a public activity “contributes to the preservation of public order” – is left undefined in the CADA text and has no settled meaning in Union law. Absent a narrow and binding circumscription, Member States are likely to read it expansively, drawing ordinary government functions such as human-resources systems, public-communication platforms and non-sensitive analytics into Levels 2, 3 or 4. To the extent the concept is fit for purpose it should instead be confined – whether through a closed list of qualifying activities or a common Commission methodology that sets a genuinely high threshold – to the most critical use cases in defence, law enforcement, border management, and comparable functions. Second, because Level 1 already operates as the universal procurement floor, an over-expansive risk assessment does not merely raise the bar for a handful of sensitive workloads; it narrows the pool of eligible providers for the majority of public-sector cloud use, raising costs and slowing the digitalisation of public services. A genuinely risk-based approach would calibrate assurance requirements to the sensitivity of the workload, keep the set of highly critical use cases narrowly and strictly defined – not least to avoid undue discrimination under the Union’s commitments in the WTO Government Procurement Agreement (GPA) – and preserve flexibility for everything else.

Article 32 is where this logic moves most clearly from classification to procurement-based market steering. It requires Member State contracting authorities, in public procurement procedures for innovative cloud computing services and AI systems within the scope of the Regulation, to include “Union added value” criteria as part of the quality evaluation of the tender. These criteria allow contracting authorities to assess whether a tenderer strengthens the Union’s digital technology supply chain, including through software or hardware designed or manufactured in the Union; whether it integrates technologies developed in the Union, including Union-funded research and development; whether the innovation required to deliver the service strengthens security of supply and the development of a European cloud and AI ecosystem; and whether the service is delivered, as far as feasible, through critical computing, storage and networking hardware designed or manufactured in the Union. Article 33 reinforces this logic by requiring Member States to monitor procurement of innovation in cloud computing services and AI systems and to link procurement practices to national cloud and AI strategies.

These “Union added value” criteria warrant particular scrutiny. In so far as they reward hardware or software “designed or manufactured in the Union,” they risk operating as de facto domestic-content or “Buy European” requirements that sit uneasily with the Union’s obligations under the WTO’s GPA and likely prompt reciprocal restrictions on European providers in third-country markets. A more durable course would reward “Made with Europe” capabilities – strong data protection and GDPR compliance, cybersecurity assurance backed by EU-based operations and threat monitoring, EU data-residency options, transparent and auditable supply chains, sustained investment in European research, infrastructure and skills, and legally binding commitments to service continuity that hold even under geopolitical stress – rather than “Made in Europe” localisation as such. This framing is consistent with the June 2026 D9+ declaration, which calls for digital sovereignty to be pursued in an open manner that reduces critical dependencies and builds European capacity while preserving the strategic role of international partnerships, risk-based approaches, and interoperability.

There are also broader market risks of deepening the nationality restrictions in European cloud sovereignty frameworks. The assumption behind CADA’s demand-side design is that assurance-based and Union-added-value procurement can help build a competitive European cloud market. If sovereignty-oriented procurement works in that way, one would expect it to broaden the pool of qualified providers and support cross-border participation by European cloud firms.

However, the evidence points in a different direction. Sovereignty certification at Member State level is associated with a substantially higher sole-bidder rate, suggesting that stricter sovereignty requirements may narrow rather than broaden competition. On this evidence, user-level sovereignty is decreasing. Public cloud contracts are also awarded predominantly to providers registered in the same Member State as the contracting authority, while cross-border awards to European providers remain rare, if not non-existent. In other words, sovereignty-oriented procurement operates through national procurement markets rather than through an integrated European market.

The reliance of domestic prime contractors on US hyperscaler infrastructure does not, in itself, imply a failure of sovereignty – provided the applicable framework secures effective control over data access, operational continuity, auditability and legal separation. There are practical aspects that are important: avoiding being exposed to a single point of failure. Just like the EU banking sector has built redundancy solutions, other critical sectors need to make additional investments to reduce risk exposure, regardless of the supplier. Increasingly, that continuity risk – including the risk that a foreign government orders a provider to suspend service – is addressed contractually as well as through redundancy: through binding commitments to contest any such order in court, and designated European operational-continuity partners.

However, this issue is different from a domestic versus foreign approach. It does not presume that foreign hyperscaler participation in Europe is incompatible with sovereignty.¹⁰ Rather, it shows the limits of treating provider nationality or domestic establishment as a proxy for effective control. CADA's own risk-assessment logic points in this direction: Article 29 focuses on the sensitivity and criticality of data, the risk of unlawful third-country access, the risk of service disruption, and whether a multi-vendor or multi-cloud strategy is appropriate.

Annex II confirms this by regulating not only establishment and location, but also data access, operational continuity, support arrangements, third-country control, software supply-chain transparency, auditability and migration planning. A domestic contractor may therefore satisfy a formal procurement preference while still depending on non-European infrastructure or software capabilities. Conversely, a non-European hyperscaler may contribute to resilience where it is subject to enforceable requirements. The relevant question is therefore not whether hyperscalers are present in the European market, but whether the applicable legal framework secures effective control over the specific cloud service being procured.

This is where CADA's assurance architecture raises a market-design concern. Its Union-wide assurance levels (see Table 1) and procurement rules are framed as common resilience standards, but they will operate in procurement markets that are already nationally segmented. Requirements concerning establishment, infrastructure and personnel location could be justified for sensitive use cases. Yet if they are applied through national procurement practices that already favour domestic providers, they may reinforce national market structures without necessarily improving effective control or resilience. The risk is that sovereignty frameworks treat provider nationality or local presence as a proxy for effective control – turning sovereignty into a formal eligibility label rather than a functional assessment of whether the service is secure, auditable, portable, and resilient.

This is also a live challenge for EU cloud suppliers that are subject to many cross-border data collection powers by foreign governments. This is not just about the US Cloud Act. Major EU cloud suppliers must comply with laws in other countries too. Indeed, the Ontario Court of Justice recently compelled a major French cloud provider to disclose data stored in France. The lesson is that legal exposure follows where data can be compelled and who effectively controls it, not the provider's nationality. It is best mitigated by technical and contractual means – customer-held encryption keys so the provider cannot disclose readable data, together with binding commitments to challenge unlawful access demands and to compensate customers for any disclosure that breaches EU law.

¹⁰ This further creates a broader tension with existing pan-European procurement models, including GÉANT-style arrangements built around cross-border access, demand aggregation, compliance, scalability and user choice. The issue is not that CADA necessarily prohibits such frameworks. Rather, CADA introduces a different procurement logic: cloud purchasing becomes not only a way to acquire secure and resilient services, but in the process becomes a tool for advancing European industrial capacity. Fragmentation precedes CADA, and CADA's assurance-level and Union-added-value criteria may formalise rather than overcome that fragmentation.

TABLE 1: CADA AND ASSURANCE LEVELS

Assurance Level	Core Sovereignty Requirements	Legal Effect / Regulatory Concern
Level 1	Union establishment; Union-located infrastructure and assets, unless the public sector body explicitly requires otherwise; customer data, metadata and telemetry retained in the Union, unless explicitly required otherwise; state-of-the-art cybersecurity standards; subcontractor transparency; controls over outsourced support; and assurances concerning third-country vulnerability-reporting laws where relevant.	Establishes the baseline assurance level for sovereign cloud services. While Level 1 provides a legitimate common floor, it already incorporates requirements beyond technical security, including EU establishment, infrastructure location and data territoriality; subsequent assurance levels build progressively more restrictive sovereignty requirements on that baseline.
Level 2	Union establishment for the audited provider and relevant subcontractors; Union-located infrastructure, assets and personnel; customer data, metadata and telemetry retained in the Union; cybersecurity certification at least at "substantial" level, or equivalent standards where no scheme exists; restrictions on use of service-generated data for third-country AI training; mitigation of third-country control risks; Union-only technical and operational support; software bill of materials (SBOMs), dependency lists, source-code auditability, anti-tampering controls and migration planning.	Converts sovereignty into a broader compliance test covering operational support, supply-chain governance and third-country influence. Assurance begins to operate as an ex ante condition for access to higher-assurance public-sector cloud use, rather than merely as a security or resilience standard.
Level 3	Union establishment; Union-located infrastructure, assets and personnel; customer data, metadata and telemetry retained in the Union; relevant personnel must be Union citizens, with security clearance where appropriate; cybersecurity certification at least at "substantial" level; no use of service-generated data for third-country AI training; Union-only support by Union residents; stronger software supply-chain controls; and, in principle, absence of third-country control, subject to a possible Article 18 derogation with additional safeguards.	Introduces identity- and control-based conditions into the assurance framework, including citizenship and limits on third-country control. The legal issue is that the framework moves from regulating service characteristics to regulating the provider's corporate control, personnel and governance structure.
Level 4	Union establishment; Union-located infrastructure, assets and personnel; sensitive customer data, metadata and telemetry retained in the Union following a risk assessment; Union citizenship and security clearance where appropriate for relevant personnel; cybersecurity certification at "high" level; no third-country control; Union-only operational support; SBOMs and dependency transparency; and effective control over the design, development, maintenance and evolution of relevant software components.	Makes access to the highest assurance category conditional on Union-based establishment, infrastructure, personnel, support, software control and absence of third-country control. The concern is that the level may function less as a proportionate resilience measure and more as a legally structured market filter for high-assurance public-sector cloud services.

Source: Annex II, CADA, authors' own elaborations

3. SOVEREIGNTY IN PRACTICE: EVIDENCE FROM EUROPEAN CLOUD PROCUREMENT

The preceding section showed that CADA's assurance framework combines risk-management objectives with increasingly restrictive eligibility conditions concerning establishment, control, personnel, infrastructure and software governance. This section tests whether sovereignty-oriented procurement, when applied in already nationally concentrated markets, is likely to strengthen effective control or instead reinforce domestic concentration and market fragmentation:

- First, whether European public cloud procurement is already nationally concentrated before sovereignty language formalises that concentration;
- Second, whether sovereignty language deepens domestic concentration and narrows competition when it is applied; and
- Third, whether the domestic prime contractor model actually delivers infrastructure-layer sovereignty, or whether it reproduces the use of data infrastructure by non-EU headquartered companies that it nominally replaces.

The analysis draws on a novel dataset assembled from the EU's Tenders Electronic Daily (TED) portal. It covers 8,725 awarded lots from nine member states,¹¹ over the eight years from 2018 to 2025. Cloud-relevant contracts were identified through a dual keyword and Common Procurement Vocabulary (CPV) code flag across nine national languages. The sample of countries is chosen to account for the diversity found across the European Union, while remaining tractable for systematic analysis given the volume of procurement data involved. Table 2 summarises the key methodological definitions used in the empirical analysis.¹²

TABLE 2: DEFINITIONS AND METHODOLOGY

Item	Note
Full TED extraction	53,881 notices across nine Member States, 2018–2025
Analytical sample	8,725 cloud-flagged awarded lots used for procurement-outcome analysis
Geography	France, Germany, Netherlands, Sweden, Finland, Italy, Denmark, Poland, and Estonia
Domestic winner	The registered country of the winner matches the contracting authority country
Strict nationality	Ultimate parent company nationality, used to identify winners regardless of where the subsidiary is registered
EU-headquartered winner	Ultimate parent headquartered in the EU

¹¹ France, the Netherlands, Germany, Sweden, Finland, Italy, Denmark, Poland, and Estonia.

¹² For the full methodology, refer to the Annex.

3.1 Who Wins Cloud Procurement Contracts?

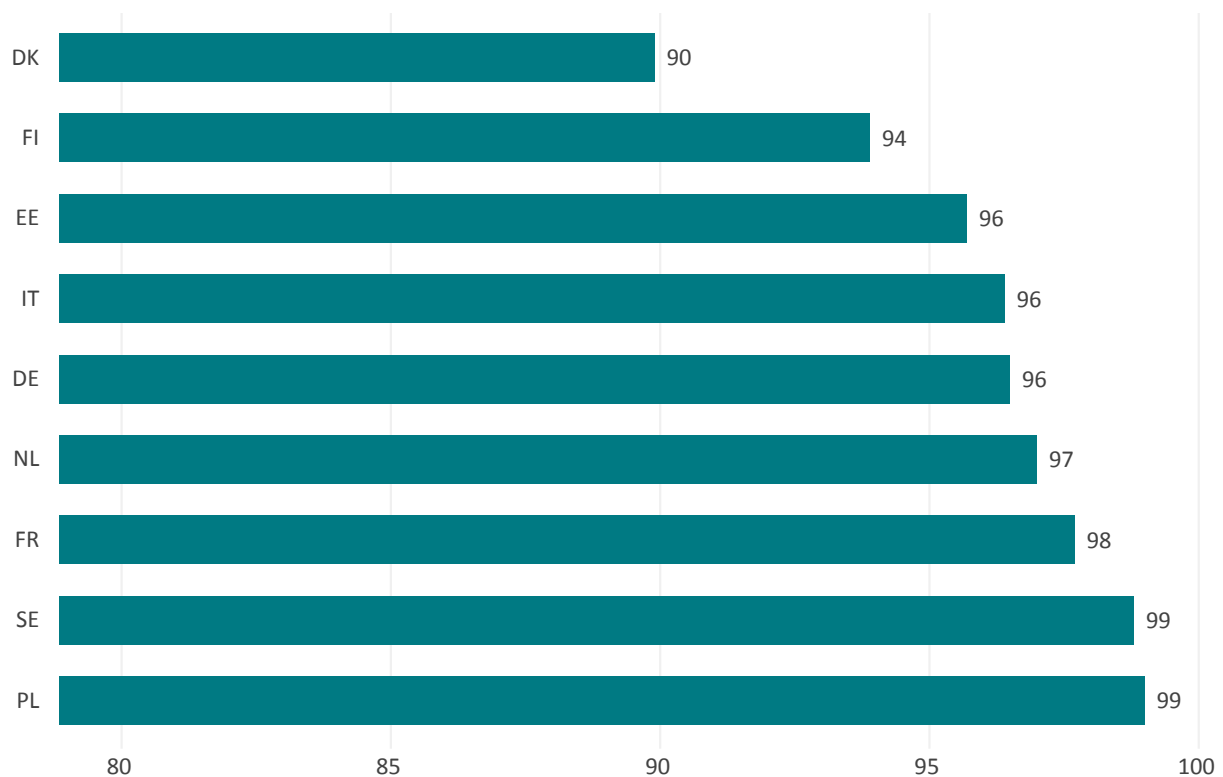
Across the nine countries, 97 per cent of cloud-flagged contracts are awarded to domestic providers – that is, providers whose registered country matches the contracting authority's member state.¹³ As seen in Figure 1, between roughly 90 per cent and 99 per cent of cloud contracts go to a provider registered in the buyer's own country.¹⁴ The limited number of cross-border wins are concentrated in smaller member states, such as Denmark and Finland.

The GÉANT exclusion isolates market-driven outcomes from a structurally mandated cross-border instrument. GÉANT is the pan-European research and education network, registered in the Netherlands, whose OCRE framework aggregates cloud procurement from AWS, Azure, and Google Cloud on behalf of universities and research institutions across more than forty countries. Because these contracts are awarded through a single EU-wide instrument rather than through national market processes, including them would inflate apparent cross-border competition and misrepresent the underlying commercial pattern.

US cloud platforms – AWS, Microsoft Azure, and Google Cloud – record zero direct contract wins anywhere in the cloud-flagged dataset. Their local subsidiaries win 16 contracts, which amounts to 0.2 per cent of awarded contracts. The lack of intra-EU cross-border competition is equally striking. This shows that direct cross-border competition is close to absent.

¹³ As a robustness check, winners were reclassified by ultimate parent company nationality rather than registered country. For example, treating firms such as Atea Sverige and CGI Suomi as Norwegian and Canadian respectively. Under this strict parent-nationality definition, domestic winner rates fall by around 10–15 percentage points. The reclassification also reveals a small set of intra-EU cross-border wins at the corporate group level: several EU-headquartered companies – including large French and German IT services groups – hold local subsidiaries that win contracts in other member states. Some cross-border EU activity exists at the group level, but the number remains modest and the dominant pattern of national concentration persists regardless of how nationality is defined.

¹⁴ The 97 per cent figure excludes lots awarded under the GÉANT Vereniging pan-European framework agreement. GÉANT is a Dutch-registered intergovernmental network organisation whose structural mandate is cross-border cloud and connectivity procurement for European research and education institutions; its 21.1 per cent domestic rate reflects deliberate multi-national award design, not market openness. The full-sample rate including GÉANT is 88.9 per cent. The Netherlands' own non-GÉANT cloud procurement awards at 96.9 per cent domestic concentration, indistinguishable from the other eight countries, confirming that the exclusion isolates a structurally distinct instrument rather than suppressing a genuine Dutch open-market effect.

FIGURE 1: DOMESTIC WINNER RATE BY COUNTRY (% , EXCLUDING THE PAN-EUROPEAN GÉANT FRAMEWORK)

Source: EU's Tender Electronic Daily (TED) and authors' calculations.¹⁵

Sovereignty vocabulary is rising steadily: notices containing sovereignty language represented 28 per cent of cloud IT procurement notices in 2018, rising to 39 per cent in 2024 where it peaked.

Yet high domestic winner rates persist across all countries throughout the observation period. Importantly, this pattern is visible even in years and countries where sovereignty-related vocabulary is almost absent. On this evidence, domestic concentration in public cloud procurement cannot be attributed to the sovereignty turn alone. Instead, sovereignty language appears to build on, and further entrench, a market that was already predominantly contracted on national lines.

If CADA's assurance levels are adopted across Member States, the pre-existing concentration documented here risks being translated into formal procurement requirements. This would raise important questions about whether such requirements are compatible with the intra-EU competition principles that underpin the single market in cloud services.

This suggests that sovereignty-based procurement frameworks have limitations. In the first place, they lead to a market that is very nationally oriented. In the second place, they do not remove the inclusion of foreign cloud suppliers as, in many circumstances, the awarded company relies

¹⁵ ECIPE's dataset covers 53,881 notices from the TED (Tenders Electronic Daily) portal, the official repository of EU public procurement notices published under Directive 2014/24/EU. Award notices were downloaded in bulk XML format for nine member states – France (FR), Germany (DE), the Netherlands (NL), Sweden (SE), Finland (FI), Italy (IT), Denmark (DK), Poland (PL), and Estonia (EE) – covering the years 2018 to 2025.

on infrastructure, software stacks, and operational dependencies that sit behind the domestic prime contractor – the very dimensions that CADA's Levels 3 and 4 are designed to target. But if there are no other suppliers than national operators that can substitute for foreign-headquartered companies in the full stack, it seems obvious that a stronger reliance on public procurement instruments will exacerbate existing patterns of EU market fragmentation.

3.2 National Sovereignty Frameworks

Sovereignty language in the dataset falls into two analytically distinct categories. The first, "old compliance frameworks", covers national technical and data-governance certification schemes that predate the cloud sovereignty political debate by several years – among them IT-Grundschutz and Drittland in Germany, HDS and the National Agency for the Security of Information Systems (ANSSI) in France, BIO and NEN 7510 in the Netherlands; MBS guidance in Sweden; and Valtori in Finland.

The second, "new sovereignty framing", covers vocabulary that emerged directly from the post-2019 policy debate including SecNumCloud, BSI C5-Testat, GAIA-X, "cloud de confiance", and explicit data-residency language. The new framing was catalysed by three developments: the US CLOUD Act (2018) and FISA Section 702, which created legal risk for data held by US-headquartered providers; ANSSI's SecNumCloud v3.2 requirements (2022), which introduced mandatory operational separation and the EUCS, under development since 2020.

Each major country in the dataset has developed a distinctive national approach. France has the most formally developed sovereignty framework: ANSSI's SecNumCloud certification (now at version 3.2) requires mandatory operational separation and imposes strict requirements on ownership structure and exposure to non-EU legal compulsion. Contracts labelled "cloud de confiance" must be delivered by SecNumCloud Niveau 3+ certified providers. At the time of the procurements in this dataset, the certified provider set consisted almost exclusively of French-origin or French-configured firms (Docaposte, Cloud Temple, OVH). SecNumCloud's core requirements – mandatory operational separation, no exposure to non-EU legal compulsion, and effective exclusion of third-country-controlled providers – closely mirror the criteria that CADA would formalise at Union assurance Level 3.

Germany relies primarily on BSI C5-Testat, which is a cloud-specific audit scheme administered by the Federal Office for Information Security. It has become embedded in procurement through two principal legal channels. At the federal level, supplementary contract terms (EVB-IT Cloud, in force March 2022) oblige authorities procuring cloud services to require C5 compliance under §55 Bundeshaushaltsordnung; in the healthcare sector, §393 SGB V (Digital Act, DigiG, 2024) extended this obligation to all cloud processing of patient data, with a Type 2 attestation required since July 2025. BSI C5's technology-neutral compliance approach corresponds broadly to CADA Level 2; C3A's mandatory functional disconnect, EU citizenship requirements, and exclusion of non-EU-jurisdiction providers place it at the boundary of Levels 3 and 4 – the most demanding alignment with CADA's highest assurance tiers among the national frameworks in the dataset.

Unlike SecNumCloud, C5 imposes no ownership or nationality restrictions: AWS, Microsoft Azure, and Google all hold attestations, making it formally technology-neutral. In practice, however, certification requirements function as mandatory pass/fail specifications that narrow the effective bidder pool, frequently producing sole-bidder outcomes. In April 2026 the BSI published C3A (Criteria Enabling Cloud Computing Autonomy),¹⁶ a supplementary framework introducing genuinely hard sovereignty criteria: a mandatory functional disconnect capability from non-European parent infrastructure, tested and documented annually; a requirement that all personnel with logical or physical access hold EU citizenship and reside in the EU (with a stricter tier requiring German residency); and a requirement that the provider not be subject to non-EU jurisdiction. C3A is currently advisory, but BSI's Vice-President has indicated it will become the benchmark for federal administration, with an embedding path through IT-Grundschutz's OPS 2.2 module.

Italy has structured national cloud sovereignty around the Polo Strategico Nazionale (PSN), a public-private partnership concession awarded under the PNRR recovery plan to a consortium of state-adjacent Italian entities: TIM S.p.A. (lead), Leonardo S.p.A., Sogei S.p.A., and CDP Equity S.p.A. The PSN illustrates the national-wrapper model in its most explicit form. The concession grants a domestic prime contractor control over the construction and long-term management of Italy's national cloud infrastructure for up to 13 years, while industry reporting indicates that hyperscaler platforms including AWS, Microsoft Azure, and Google Cloud, underlie the PSN service catalogue as sub-contractors whose identities are not disclosed in the award notice. Sovereignty therefore attaches to the nationality of the operator, not to the infrastructure layer beneath it.

The Netherlands applies BIO (Baseline Informatiebeveiliging Overheid) as its primary cloud governance standard. BIO is formally nationality-neutral: its security classification requirements do not restrict ownership or exclude providers from specific jurisdictions, and both US hyperscalers and European providers hold BIO-compliant certifications. In practice, however, Dutch procurement follows the same domestic-concentration pattern as the rest of the dataset. The Amsterdam public cloud procurement (notice 536142-2025) illustrates the structure: the contracting authority explicitly designated Azure Sovereign Cloud as the platform for its high-trust landing zone (BIO Beschermingsniveau 2+), yet awarded the contract to a Dutch managed services provider.

Finland has institutionalised sovereignty through Valtori, Valtion tietö- ja viestintätekniikkakeskus (State IT and Communications Technology Centre). It operates under the Ministry of Finance as the mandatory ICT infrastructure provider for Finnish central-government ministries and agencies. Valtori's cloud environment spans major hyperscaler platforms including AWS and Oracle, accessed through competitive tenders for Finnish managed-service providers and system integrators rather than through direct hyperscaler contracts. What appears in TED award records is accordingly the secondary layer: consultancy expertise and managed services above the infrastructure.

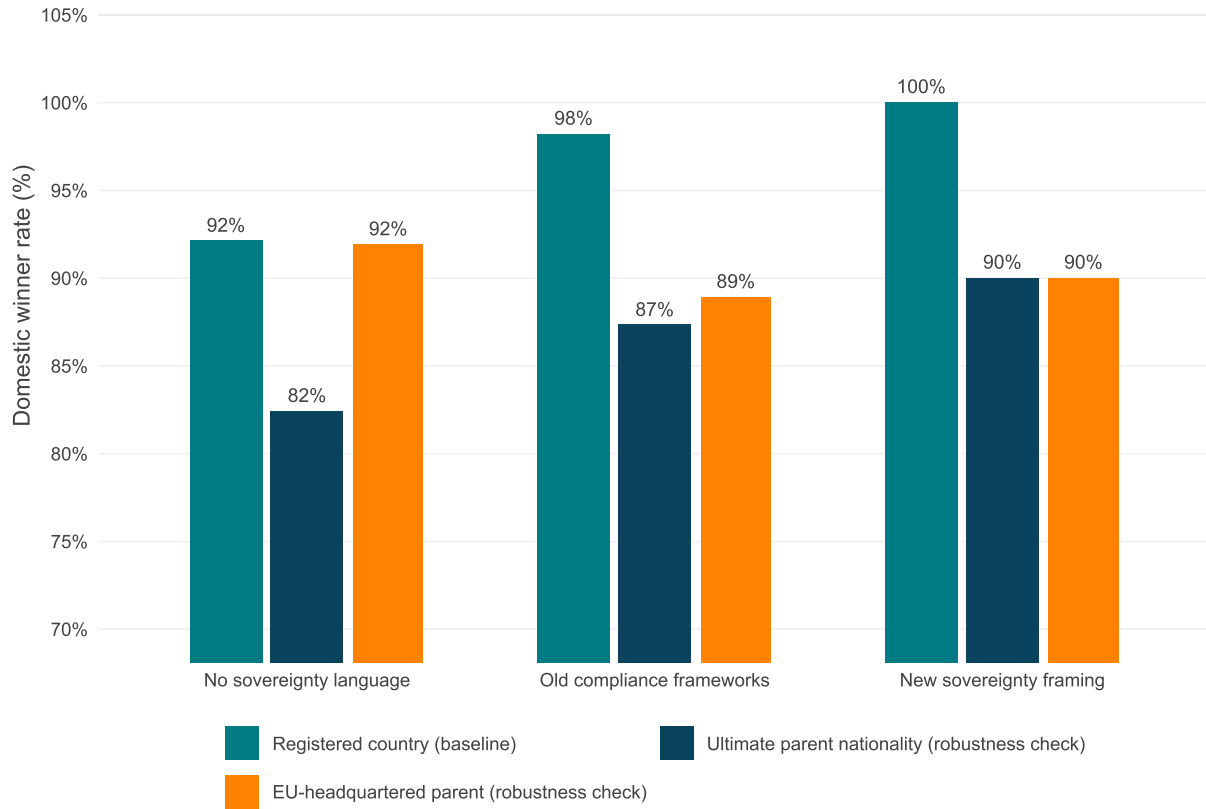
¹⁶ BSI Federal Office for Information Security. (2026, April 27). Criteria Enabling Cloud Computing Autonomy (C3A). https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/C3A/C3A_node.html

The remaining countries in the dataset – Sweden, Poland, Estonia, and Denmark – operate without formal cloud-sovereignty certification schemes analogous to SecNumCloud or BSI C5. Denmark channels much public-sector cloud procurement through Statens IT and Digitaliseringsstyrelsen standing frameworks; Sweden operates analogous framework contracts through Kammarkollegiet and relies on the MSB guidance for information security classification, and Estonia's procurement is organised around X-Road-compatible service delivery and the ISKE classification standard.

Splitting the sample by the type of sovereignty language reveals a graduated concentration pattern, shown in Figure 2. Figure 2 presents three bars per sovereignty category, each applying a different nationality definition: the grey baseline assigns nationality by the provider's registered country; the dark blue bars ("national strict") apply a robustness check that traces ownership to the ultimate parent company nationality; and the orange bars further restrict the domestic definition to EU-headquartered parent companies. The gradient is preserved under the ultimate-parent definition; under the EU-level definition the three categories are within about three points of each other.

Contracts with no sovereignty language are awarded domestically in about 92 per cent of cases. Contracts invoking only an old compliance framework rise to roughly 98 per cent. Contracts invoking the new sovereignty framing reach 100 per cent: every such contract in the dataset was won by a domestic provider, and no US-multinational parent won under new-framing language.¹⁷ This shows that sovereignty language acts as a filter, and one whose weight is increasing: while the older policy frameworks still account for 88 per cent of the sovereignty-flagged notices, sovereignty vocabulary is rising sharply, with notices invoking the post-2019 framing growing roughly tenfold between 2018 and 2025.

¹⁷ The new-framing category calls for caution before drawing strong conclusions. Notices invoking the post-2019 vocabulary account for a small number of cloud notices in the dataset.

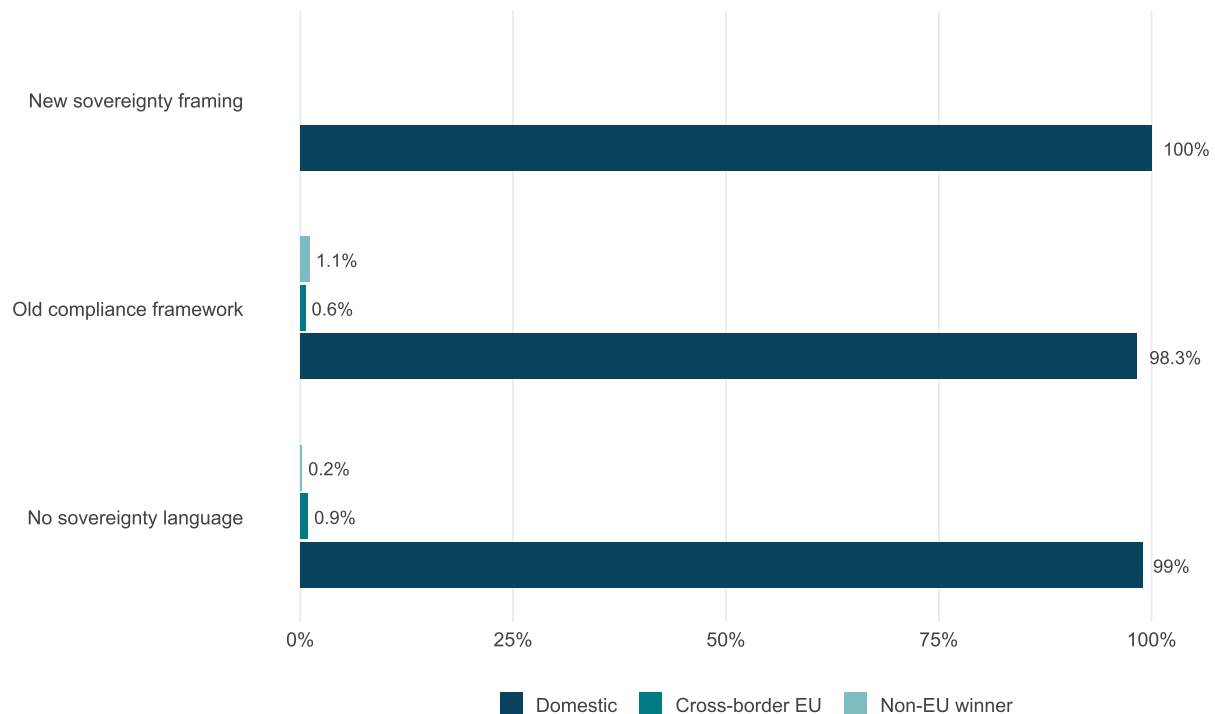
FIGURE 2: DOMESTIC WINNER RATE BY SOVEREIGNTY CATEGORY (NO SOVEREIGNTY LANGUAGE; OLD COMPLIANCE FRAMEWORKS; NEW SOVEREIGNTY FRAMING)

Source: EU's Tender Electronic Daily (TED) and authors' calculations.

Contract value data confirm the same pattern.¹⁸ Domestic providers account for 99 per cent of awarded value where no sovereignty language is used, 98 per cent under old compliance frameworks, and 100 per cent under new sovereignty framing. The concentration documented in Figure 2 holds by expenditure as well as by contract count (Figure 3).

¹⁸ Lot values are reported voluntarily in TED award notices. Value coverage across the nine countries is 83 per cent. Coverage varies: Estonia (100 per cent), Poland (97 per cent), Denmark (96 per cent), Italy (95 per cent), the Netherlands (94 per cent), France (88 per cent), Sweden (77 per cent), Finland (63 per cent), Germany (61 per cent). Lots with missing or zero reported values are excluded.

FIGURE 3: SHARE OF AWARDED CONTRACT VALUE BY WINNER GROUP AND SOVEREIGNTY LANGUAGE CATEGORY (PER CENT, EXCLUDING THE PAN-EUROPEAN GÉANT FRAMEWORK)



Source: EU's Tender Electronic Daily (TED) and authors' calculations.

The formal rationale for new sovereignty requirements, as articulated in frameworks like SecNumCloud and the CADA assurance levels, centres on protecting sensitive data from foreign legal access particularly under the US CLOUD Act and FISA Section 702. This is a tall order given that many EU-headquartered companies do business in the US and other countries that demand access to data. But assuming that is a workable requirement, one would expect the new framing to filter out non-EU providers while leaving intra-EU cross-border competition largely intact: a German provider bidding on a French contract poses no extraterritorial legal risk of the kind these frameworks were designed to address. Yet the data shows no such pattern. Cross-border wins within the EU are low regardless of sovereignty framing. If that pattern holds as national frameworks multiply and formalise under CADA, the result will be 27 smaller national markets, rather than a more sovereign European one.

This further illustrates the fragmentation dynamic identified earlier. France has SecNumCloud, Germany has BSI C5, and Finland has Valtori's approach: each framework creates a nationally bounded eligibility set. Firms seeking to operate across borders face a patchwork of national certification requirements, each calibrated to the preferences and risk assessments of a single member state. The national frameworks do not only diverge in form, they diverge in the depth of sovereignty they demand. SecNumCloud and Germany's emerging C3A standard require operational separation from non-EU parent infrastructure which, under Article 16 and Article 18 (associated third-country mechanism) of CADA, would disqualify the operator-parent arrangements on which Italy's PSN and Finland's Valtori model are built. CADA's individual risk

assessment provision under Article 29, which allows member states to calibrate the required assurance level by use case, will likely not resolve the divergence, but it will accommodate it.

Two correctives would narrow this divergence. On the demand side, the sovereignty risk-assessment methodology should be set centrally and applied uniformly: a mandatory, harmonised Commission template with limited national discretion, supported by a central, openly accessible and actively maintained repository of recognised services, would give public buyers and pan-European providers the predictability that cloud-investment and procurement-planning decisions require.

On the supply side, the Article 18 mechanism governing recognition of providers from trusted third countries should be transparent, rules-based, timely and grounded in existing EU adequacy and trade-equivalency frameworks, and activated promptly and objectively wherever its cumulative conditions are met – rather than functioning as a discretionary political lever. A predictable recognition pathway would itself signal that large-scale investment in European data-centre and AI capacity will be met with stable and reliable market access, encouraging the very capacity expansion that CADA seeks to accelerate. That signal is not hypothetical: major providers have already committed to large-scale European build-out on the assumption of stable market access. A discretionary recognition regime would place precisely this investment at risk.

3.3 How Sovereignty Requirements Operate

A sovereignty certification may enter a procurement in two ways: as a hard pass/fail technical specification, which excludes non-certified providers before any quality or price evaluation begins; or as a scored award sub-criterion, under which certification earns points, but non-certified providers may still compete. In ECIPE's dataset, hard pass/fail use of sovereign certification is rare and highly concentrated. It appears in only about 9 per cent of old-framework notices, and almost entirely with a single buyer, Finland's Valtori, which acts as the mandatory ICT infrastructure provider for the Finnish central government. The newer certifications behave differently. None of the new-framing notices uses certification as a pass/fail specification; instead, certification appears exclusively as a scored sub-criterion. Yet this formally less exclusionary instrument is associated with the sharper collapse in competition.

The share of contracts attracting only a single bidder rises from 28 per cent when no sovereignty language is present to 46 per cent under the new framing, as seen in Figure 4. Old-framework contracts show a sole-bidder rate of around 22 per cent, consistent with their wider, multi-provider applicability. This is a remarkable feature of sovereignty frameworks: they limit choice and optionality for the user, which contradicts user-level sovereignty. In half of the recorded cases, there is no effective competition that could help reinforce user sovereignty to make relevant design choices.¹⁹

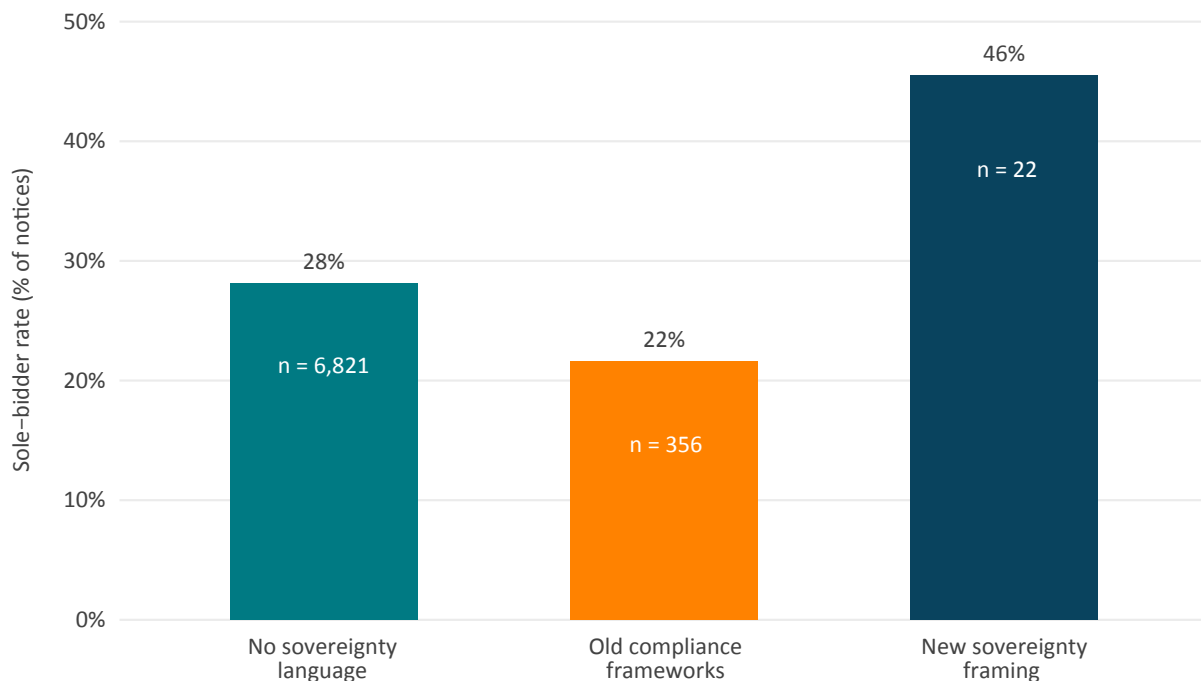
¹⁹ As per our dataset, all ten sole-bidder awards were won by large, established incumbents rather than new cloud entrants. In Italy, four sole-bidder lots were awarded to a Leonardo S.p.A.-led consortium, including Fastweb, IBM Italia and Sistemi Informativi. In France, the relevant winners were Thales, Orange Business Services, Docaposte, Cloud Temple and Keynectis – corporate groups closely linked to the sovereign-cloud initiatives discussed in this paper, including Thales/S3NS, Orange/Bleu and Docaposte's SecNumCloud-certified services. The remaining case involved Aditinet, a smaller Italian IT consultancy. The Italian RTI structure does not alter the competitive landscape: it allowed major incumbents such as Leonardo, Fastweb and IBM Italia to submit a joint offer, but did not generate rivalry between alternative bidders. The pattern is therefore better understood as incumbent-led capture by defence, telecoms, postal and established IT groups, rather than evidence of new cloud-market entry.

The new-sovereignty effect shows up primarily through sole-bidder incidence rather than median bid counts. This points to a market in which most sovereign-labelled contracts attract a normal handful of bidders while a disproportionate minority attract only one.²⁰ A certification need not be written as a formal exclusion to be exclusionary in effect. Although the procurement is merit-based on paper, the requirement can still foreclose cross-border competition in practice. The most proportionality-sensitive structure is where sovereignty certification functions as a hard market-access filter while the sole differentiating criterion among those who pass is price. Twenty-eight per cent of sovereignty-language notices in the dataset use price-only award criteria structured in precisely this way.

84 per cent of cloud procurement, measured by number of awarded lots, is undertaken by sub-national or semi-autonomous contracting authorities rather than by central government ministries. That distribution is legally significant for the scope of proportionality review. Sovereignty-based requirements adopted by regional governments, municipalities, hospital trusts and universities will ordinarily be assessed under the general regime of Directive 2014/24/EU, rather than under the exceptional security exclusions in Article 15 of that Directive or the Treaty derogation in Article 346 TFEU.

Neither a general preference for a "sovereign" cloud provider nor the mere involvement of sensitive data remains sufficient to displace the Directive's ordinary requirements. Unless the restriction is linked to a genuine Member-State essential-security interest and it can be demonstrated that less restrictive measures would be inadequate to protect that interest, such requirements remain subject to Article 18(1) of Directive 2014/24/EU, including the principles of equal treatment, non-discrimination, transparency and proportionality. The sub-national segment is therefore both the most commercially significant part of the dataset and the segment in which insufficiently substantiated sovereignty criteria are most vulnerable to legal challenge.

²⁰ The new-framing figures rest on a small base (22 notices with bidder data) and should be read with corresponding caution; the direction of the result is nonetheless consistent across all years with sufficient observations.

FIGURE 4: SOLE-BIDDER INCIDENCE BY SOVEREIGNTY VOCABULARY CATEGORY (2018–2025)

Source: EU's Tender Electronic Daily (TED) and authors' calculations.

3.4 The Sovereignty Paradoxes

The rising share of sovereignty-labelled procurement will likely have an impact on the infrastructure layer. If contracts are increasingly filtered through sovereignty criteria but the infrastructure or software base beneath remains owned by non-EU operators, CADA's Levels 3 and 4 will collide with current procurement structures.

Reading the full text of the sovereignty-flagged award notices shows that at least 13 of the 238 explicitly name a US hyperscaler platform as the product procured, the platform in scope, or the direct supplier. In two of these cases, Microsoft Oy (Finland) and Microsoft Deutschland GmbH (Germany) are the winning contractors. In the remaining cases, the contract document explicitly names a US hyperscaler as the underlying platform or required service environment. These 13 notices are distinct from the 16 lots identified earlier in which a US cloud platform subsidiary registers as the direct winner across the full dataset; the two sets overlap in only two cases.²¹ These 13 cases are certainly an undercount: award notices do not systematically require disclosure of the underlying technology stack, so hyperscaler participation surfaces only where a buyer chooses to publish them.

This interpretation is consistent with the broader market structure: nine out of ten cloud providers supplying European governments are US-headquartered companies, and between 80 and 90 per

²¹ The 238 are contract award notices in the cloud-flagged winner dataset that also contain sovereignty language in their full text, across all nine countries and the 2018–2025 period. The broader sovereignty-language IT procurement universe identified by the TED full-text API also includes pre-award notice types (contract notices, prior information notices) that carry no winner data and are therefore excluded from this search.

cent of cloud services used by European customers are hosted by US-headquartered providers, suggesting that domestic contract winners frequently are system integrators layered on top of the cloud infrastructure.²²

The clearest case visible in the dataset is Finland's Valtori, the central-government IT centre and the single most frequent buyer in the Finnish procurement dataset. Valtori runs a multi-cloud environment on Azure, AWS and Oracle, and procures expert services for each, under competitive frameworks. Five notices document Valtori tendering consultancy services specifically for US hyperscaler environments: AWS cloud expertise services (€5.9 million, six bidders), Oracle Cloud expertise (€6.3 million, five bidders), a combined Azure and AWS consultancy (€2.9 million, three bidders), and a Microsoft CSP cloud-services contract (€5.2 million, nine bidders). Most analytically significant is a sole-source award of €4.7 million for a Microsoft Unified Support Agreement 2024–2026, in which Valtori awarded a direct commercial support contract to Microsoft Oy without competition. This is visible in the procurement record only because Valtori chose to publish it as a standalone award notice.

In Denmark, the European entity of Amazon Web Services won a lot, as the sole bidder, in the central-government standard software purchasing system used by Statens IT. In the Netherlands, Amsterdam's high-trust public cloud procurement, structured under the BIO Beschermingsniveau 2+ security baseline for sensitive personal data, explicitly names Microsoft Azure Sovereign Cloud as the underlying platform; the prime contractor is a Dutch managed services provider, Solvinty B.V. (contract value €14 million, three bidders).

This further illustrates the complexity of cloud services and how nationality-based sovereignty frameworks struggle to achieve the outcome they prefer. In other words, a domestic prime contractor operating on a US hyperscaler platform satisfies one level of sovereignty but cannot achieve the type of outcomes that, on grounds of nationality, achieves technical, operational and legal sovereignty.

CADA's Levels 3 and 4 give practical effect to these aspects through conditions that are structurally incompatible with the arrangements that are already present in European sovereign-cloud procurement. Level 3 prohibits providers and their subcontractors from being subject to third-country control; Level 4 requires that no third-country entity hold effective control over any software component. A national prime contractor delivering with the inclusion of firms subject to non-EU government control is likely to fail on both thresholds. A derogation exists at Level 3 under Article 18, allowing the Commission to certify non-EU countries on a case-by-case basis, but this is designed for exceptional recognition, not as a general mechanism for the layered arrangements currently prevalent.

Commercially documented sovereign-cloud joint ventures confirm that this architecture extends well beyond the procurement record. Bleu (Microsoft Azure and M365, with Capgemini and Orange as co-owning domestic operators, France), Delos (Microsoft Azure and M365, with SAP as

²² Gineikyte-Kanciere, V., Eggert, M., & Skiotyte, G. (2025, December). European software and cyber dependencies (PE 778.576). European Parliament, Policy Department for Transformation, Innovation and Health. https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778576/ECTI_STU%282025%29778576_EN.pdf

founding entity and Arvato Systems as operator, Germany), and S3NS (Google Cloud, with Thales as majority shareholder and operator, France) are some examples. In each of these arrangements a national or European entity is responsible for operating and controlling the service on top of a global hyperscale platform.

The consortium structure is the most developed in Italy. 27 per cent of cloud contracts are awarded to multi-firm RTI 'Raggruppamento Temporaneo di Imprese' groupings – against a nine-country average of 3.3 per cent – reflecting the architecture of large national frameworks such as SPC Cloud and PSN in which state-adjacent primes work on international infrastructure. This pattern is not incidental: Italian public procurement law and the design of major framework agreements actively incentivise RTI formation by distributing technical qualification requirements across consortium members, allowing domestic firms that lack full-stack cloud capability to participate as prime contractors while subcontracting or partnering with hyperscalers for the underlying infrastructure layer.

Taken together, the evidence clearly suggests that European cloud procurement is already a collection of nationally concentrated markets. Sovereignty language, especially the newer framing, is associated with even tighter domestic concentration and with less competition. The paradox is that sovereignty frameworks encourage a market development that is nationalising the contract layer of the market but not the infrastructure layer. Obviously, the infrastructure layer requires capabilities and access to capital-intensive services, and this is the reason that sovereignty certifications accommodate them. If there are nationality-based sovereignty requirements through the entire stack, the market would not just concentrate and nationalise even more. It would seriously reduce serviceability.

There is another dimension to the paradox. If sovereignty requirements specify verifiable operational control – encryption key management, auditable data residency, legal independence from extraterritorial reach – they achieve the same objectives (sovereignty, resilience, risk management and capabilities) that justify the market restrictions. By contrast, when sovereignty requirements are reduced to a nationality filter on the prime contractor without those guarantees, they propel market fragmentation.

These safeguards can be specified concretely and verified independently. Technical controls – client-side encryption, customer-managed encryption keys, confidential-computing environments, workload isolation, and identity and access management – ensure that only authorised customers can access their data even when the underlying infrastructure is operated by an external provider. Operational safeguards – EU-based operational entities, restricted and logged administrative access, security-cleared personnel and auditable procedures – together with contractual protections that bind the provider to EU law and to defined data-access limits, complete the picture.

These are not theoretical constructs: the largest global providers already offer such controls at scale today²³ – including customer-controlled and external key management that leaves the provider unable to read customer data, confidential-computing environments, customer-approval workflows for administrative access, EU data-residency under a defined EU data boundary, and EU-based operating entities staffed by security-cleared European personnel. Recognising these demonstrated safeguards as equivalent or complementary pathways to meet the assurance-level criteria, rather than relying on establishment- and nationality-based proxies, would let public buyers select, combine and switch between the solutions that best fit their needs without sacrificing security or resilience.

Finally, that fragmentation is more European than transatlantic. As the data shows, there is very little intra-EU cross-border competition: sovereignty frameworks entrench the structure of national suppliers and indirectly suppress access by providers from other member states.

4. POLICY RECOMMENDATIONS

There are far better options available that achieve sovereignty defined as security and resilience. Rather than excluding on the basis of nationality and ownership, a sovereignty framework should boost resilience, security, redundancies and increase supply chain diversity, while focusing on risks and mitigation through governance, technical controls, personnel rules, encryption, key management, audit rights, operational separation, and contractual step-in rights from risks that remain inherent in the underlying platform.

CADA's current approach risks replacing that granular analysis with a high-level control test that operates as a de facto exclusion rule but fails to deliver resilience, necessary risk management control, and effective sovereignty. More so, its ambition to exclude certain players from the market will de facto result in lesser choices for European entities and thereby artificially create supply chain scarcity, which is negative from a resilience perspective, especially in light of geopolitical tensions. Finally, the artificial scarcity risks slowing down the digital and AI uptake in Europe and thereby hampering the EU's own digital ambitions, as set out for example in its Digital Decade targets.

These findings point to concrete recommendations for how CADA can strengthen European cloud capacity and resilience without deepening the fragmentation of the single market:

²³ For example, Microsoft completed its EU Data Boundary in February 2025, enabling EU/EFTA-based storage and processing of customer and personal data for its core cloud services, and in June 2025 announced Data Guardian and External Key Management, under which remote administrative access to European systems is approved, monitored and logged exclusively by Europe-resident personnel, and encryption keys can be held entirely outside Microsoft's control. AWS's European Sovereign Cloud, generally available since January 2026, runs on the Nitro System (independently audited by NCC Group) which by design leaves no mechanism for any AWS operator to access customer data or instance memory, and is being transitioned to operation exclusively by EU citizens located in the EU. See: Microsoft. (2025, February 26). Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency [Blog post]. <https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/>; Microsoft. (2025, June 16). Announcing comprehensive sovereign solutions empowering European organizations [Blog post]. <https://blogs.microsoft.com/blog/2025/06/16/announcing-comprehensive-sovereign-solutions-empowering-european-organizations/>; Amazon Web Services. (n.d.). European digital sovereignty FAQ. <https://aws.amazon.com/compliance/europe-digital-sovereignty/faq/>; Cloud Security Alliance. (2026, January 16). AWS launches European Sovereign Cloud: What you need to know and what you need to do [Blog post]. <https://cloudsecurityalliance.org/blog/2026/01/16/aws-launches-european-sovereign-cloud-what-you-need-to-know-and-what-you-need-to-do>

- **Define sovereignty as a demonstrated outcome, not an ownership status.** CADA's aim is secure, resilient, trustworthy cloud for European public bodies. It is best served by criteria that test what a service verifiably does. Four controls can be specified concretely and verified today: customer-held encryption keys under external key management, confidential computing with remote attestation, approved and logged administrative access, and contractually binding auditable data residency. The first two are verifiable cryptographically by the customer, the latter two by independent audit.²⁴ Treating them as equivalent or complementary routes to meeting the Level 3 and 4 criteria, rather than relying on establishment- and nationality-based proxies, would let public buyers select, combine and switch between the solutions that best fit their needs without sacrificing security or resilience.
- **Make the harmonised risk-assessment methodology binding, not indicative.** Article 29(3) already requires the Commission to set the methodology, templates and elements by implementing acts. The weakness is Article 29(4), which allows Member States simply to indicate where they depart from it. Departures should be reasoned, published and time-limited. Without that, twenty-seven national readings of the same assurance levels will reproduce the fragmentation the framework is meant to cure.
- **Make Article 18 recognition objective and predictable.** Recognition of associated third countries is anchored in GDPR adequacy and reciprocal procurement access which are sound foundations. Three changes would make it work: criteria that a partner country can realistically satisfy and demonstrate, an application procedure with defined time limits and a right to reasons. A predictable pathway signals that large-scale investment in European data-centre and AI capacity will be met with stable market access; a discretionary one places precisely that investment at risk.
- **Recognised once, accepted everywhere, with no national requirements on top.** Country-of-origin recognition is CADA's strongest single-market feature: a provider applies once, in its Member State of establishment, and the recognition holds everywhere. But it is a floor, not a ceiling. Nothing in the Regulation prevents contracting authorities from adding national requirements on top of a recognised level, and the review mechanism runs one way – under Articles 17(6) and 17(10), a recognition can be challenged for being too generous, never a national requirement for being too strict. Three changes would close the gap: an explicit clause barring further requirements on recognised services; a review mechanism that works in both directions, so that a provider or the Commission can challenge national

²⁴ The EDPB already treats provider-inaccessible encryption as an effective supplementary measure against third-country access (European Data Protection Board. (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Version 2.0). https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf), and Article 32 of the Data Act requires providers to deploy technical and organisational safeguards to the same end (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), Official Journal of the European Union, L, 2023/2854. <http://data.europa.eu/eli/reg/2023/2854/oj>).

overlays; and a deadline on the Commission's decision under Article 17(10), so that reasoned objections cannot become indefinite delay. Full portability is what would let European systems integrators, cloud operators, cybersecurity firms and managed-service providers compete for the operating-partner layer. The layer at which sovereignty controls are implemented, monitored and audited, and one that today remains nationally scoped.

- **Avoid any extension to the private sector outside of the ordinary legislative procedure.** Under Article 31, entities in Network and Information Security 2 (NIS2) sectors of high criticality may carry out assessments voluntarily, but Article 31(3) allows the Commission to make them mandatory and to specify binding mitigation measures by delegated act. Any such extension should rather follow from a review clause, clear criteria and a full impact assessment. The reduced serviceability and narrower choice documented in this paper would otherwise carry through to the most critical sectors of the European economy.

5. CONCLUSION

A central finding in this paper is that sovereignty frameworks in cloud procurement have nationalised the market for cloud contracts in Europe. Using a novel dataset of 8,725 cloud-related procurement contracts drawn from Tenders Electronic Daily (TED) across nine member states between 2018 and 2025, three findings stand out:

- European cloud procurement was already highly concentrated nationally before sovereignty became a policy objective: roughly 97 per cent of contracts went to domestically registered providers, with negligible intra-EU cross-border competition.
- Sovereignty framings deepen this concentration and narrow competition. Contracts invoking the post-2019 vocabulary reach 100 per cent domestic awards, and the sole-bidder rate rises from 28 per cent where no sovereignty language is present to 46 per cent under the new framing, a contraction of the very optionality that user-level sovereignty requires.
- Domestic winners frequently rely on US hyperscaler infrastructure beneath the prime contractor. Sovereignty attaches to the nationality of the operator, not to the infrastructure layer on which the service depends.

The operator-partner model is necessary for European innovation and growth – and can spur a development that improves European technology strengths. It requires, however, a stronger single market approach to cloud sovereignty than the one currently offered by the CADA. Sovereignty frameworks that inevitably fragment markets in Europe along national lines also dent Europe's capacity to develop a strong cloud ecosystem. If necessary conditions for scale opportunity are weak or weakened, there is less incentive to invest and develop.

Approached in this way, a functional, risk-based sovereignty framework is not only the more legally and economically coherent option; it is also the one that creates the larger opportunity for Europe's own technology ecosystem. Precisely because strict nationality criteria segment the market at national level, a more open model – built on non-discriminatory certification, mutual recognition and demonstrable safeguards – is what would allow European systems integrators, cloud operators, cybersecurity firms and managed-service providers to compete for operating-partner roles across the whole single market, rather than within twenty-seven protected national ones.

ANNEX: METHODOLOGY

A.1 Data

The empirical analysis draws on contract award notices published in Tenders Electronic Daily (TED), the EU's official procurement journal, covering nine member states – France, Germany, the Netherlands, Sweden, Finland, Italy, Denmark, Poland, and Estonia – over 2018–2025. Cloud-relevant lots were identified by two complementary filters: a multilingual keyword match on notice titles and descriptions (covering cloud, IaaS/PaaS/SaaS, data centre, managed service, and related terms across all nine languages), and a match on procurement classification codes specifically designating cloud hosting or data-storage services. Generic IT codes were excluded. Together the two filters produce an analytical sample of 8,725 awarded lots (Table A1).

To detect sovereignty vocabulary – which is not included in the bulk download – a parallel full-text search was run against the TED API using 68 terms covering cloud infrastructure and sovereignty/compliance language in nine national languages. Queries were restricted to IT and software procurement categories to avoid false positives from healthcare, defence, or financial contexts. API results were matched back to the bulk dataset to add winner metadata and contract values for each matched notice.

TABLE A1: DATASET OVERVIEW

Parameter	Value / Description
Source	EU Tenders Electronic Daily (TED), Publications Office of the EU
Coverage period	2018–2025
Countries	France, Germany, Netherlands, Sweden, Finland, Italy, Denmark, Poland, Estonia
Raw notices	~54,000 contract award notices
Analytical sample	8,725 awarded lots (cloud-flagged)
Unit of analysis	Awarded lot (multi-lot notices produce multiple rows)

A.2 Sovereignty Language Classification

Of the 8,725 cloud procurement contracts in the dataset, 238 also contained sovereignty-related language in their published text. Each of these 238 contracts was assigned to one of four groups depending on what kind of sovereignty language it used: NEW (terms that emerged from the post-2019 political debate around cloud sovereignty, such as SecNumCloud or GAIA-X), OLD (references to older national security or data-protection standards that predate that debate, such as IT-Grundschutz or HDS), BOTH (contracts referencing both types), or NONE (cloud contracts with no sovereignty language at all). The NONE group acts as a comparison baseline – it shows what procurement looks like when no sovereignty requirements are imposed. The four groups

were built by reading through individual contracts and assigning terms manually, with some terms moved between categories after closer inspection to ensure consistency.

TABLE A2: SOVEREIGNTY TERM TAXONOMY

Category	Representative terms	Rationale
NEW	SecNumCloud, cloud de confiance, EUCS, GAIA-X, C5-Testat, data residency, Polo Strategico Nazionale, Datensouveränität, datasouvereiniteit, datasuveränitet, suverenność danych, sovranità dei dati	Terms coined or formalised as part of the post-2019 EU cloud sovereignty debate (US CLOUD Act, FISA s.702, ANSSI SecNumCloud v3.2, EUCS)
OLD	IT-Grundschutz, BSI C5, HDS, ANSSI, BIO, NEN 7510, MSB, säkerhetsskydd, Valtori, Katakri, VAHTI, AGID, ACN, Statens IT, third country, extraterritorial, souveraineté, pays tiers	National technical or data-governance certification schemes predating the cloud sovereignty debate
BOTH	Notice contains at least one NEW and one OLD term	Procurement straddling both regimes
NONE	No sovereignty vocabulary found in full notice text	Baseline group for counterfactual domestic winner rates

A.3 Winner Nationality

A lot is classified as having a domestic winner if all winners are registered in the buyer's member state. For consortium awards, every member must be domestic; lots with missing nationality data are excluded. GÉANT – the pan-European research network procuring cloud services on behalf of universities and research institutions across more than 40 countries – is excluded from all domestic winner rate calculations, as its awards are cross-border by design rather than by market outcome.

To assess whether registered nationality overstates domestic concentration, the analysis was re-run under two robustness scenarios. The national strict scenario reclassifies approximately 30 entities where the ultimate parent's nationality differs from the subsidiary's country of registration (e.g. Fujitsu subsidiaries counted as Japanese, CGI as Canadian, Atea as Norwegian). The EU-level scenario counts any EU-headquartered parent as domestic. Registered nationality does overstate domestic concentration, but not enough to change the picture. The national strict scenario lowers the domestic rate by about 10 percentage points for contracts with no sovereignty language (92 to 82 per cent) and for those invoking old compliance frameworks (98 to 87 per cent), and by a similar or larger margin in the small new-framing group. Domestic winners remain the large majority in every category and under every definition.

A.4 Limitations

- Infrastructure disclosure: TED notices do not require disclosure of the underlying technology stack or subcontractor chain. The 13 sovereignty-labelled notices explicitly naming a US hyperscaler are almost certainly an undercount of actual hyperscaler involvement.

- Netherlands exclusion from time series: Dutch procurement data contains a publication-date artefact concentrating a disproportionate share of notices in 2025. The Netherlands is excluded from trend analyses but retained in cross-sectional total.
- Country sample: Nine member states were selected to cover a range of market sizes, geographic regions, and procurement governance models. The findings may not generalise to member states with lower TED publication volumes or different procurement systems.
- Keyword recall: Coverage in lower-volume languages (Estonian, Polish) is somewhat lower than in higher-volume markets, which may slightly understate sovereignty notice counts in those countries.