FOTI

Strengthening the EU's Cloud & AI Development Act

Step 4: Buy European

How to buy strategically to scale sovereign solutions

A report series by FOTI
November 2026

FOTI

About FOTI

FOTI is a European think tank dedicated to building a prosperous and fair future that harnesses the power of technology.

We help democracies tackle some of the biggest technology challenges of our time. From market concentration and digital sovereignty to platform accountability and industrial policy, we develop practical solutions that strengthen innovation, support challengers and deliver better outcomes for people and societies.

About this series

Strengthening the EU's Cloud & AI Development Act is a report series by FOTI.

Step 4: Buy European: How to buy strategically to scale sovereign solutions
Strengthening the EU's Cloud & AI Development Act
November 2026

Table of contents

01 Executive summary 04

02 Context:
You can't build sovereign supply without public and private demand 05

- Public demand shapes the market, and so far in one direction 06
- Buyers cannot evaluate what they procure 07
- Once there, services are hard to leave – and create vulnerabilities 08
- Buying sovereign is already possible under existing rules 09
- Open source: What public buyers and their providers rely on, and nobody pays for 10
- What CADA does to address this 11

03 CADA's weakness:
As drafted, "Buy European" provisions are too timid to address dependencies 12

04 Our proposed fixes 15

- A. Mandatory contract terms to support sovereignty 16
- B. A decisive European preference and disciplined procurement – for public and private buyers 22

Sources and resources 29

01 / Executive summary

Taxpayers' money built the cloud market Europe now depends on, and it continues to flow in the same direction: towards the incumbents. The Commission acknowledges that the initial growth of today's largest hyperscalers was fuelled by massive public contracts. Today, those incumbents control huge entrenched user bases, stuck there by steep switching costs, technical lock-in, and contracts that public buyers lack the power or expertise to negotiate.

Public buyers are ill-equipped to change that. National audits and data protection reviews reveal public administrations that cannot verify the security or jurisdiction of the cloud services they purchase, rarely execute data protection impact assessments, and possess no contractual exit or reversibility mechanisms. Critical public workloads remain exposed to extraterritorial interference by foreign entities, export controls, or shifting international alignments.

CADA establishes the correct principles: a mandatory baseline assurance level for public bodies, higher tiers for essential public-order tasks, non-price evaluation criteria for Union added value, and an "open source first" principle.

However, as drafted, CADA's procurement provisions are designed not to bite. Purchasing a recognised service does not always equate to buying European. Level 1 admits foreign hyperscalers without modification, covering an estimated 70% of public demand. The sole European preference mechanism in Article 32 is legally barred from being decisive. Derogations under Article 30(4) are open-ended and unmonitored; public buyers receive no knowledge transfer to oversee their suppliers; "open source first" imposes no upstream contribution obligations on commercial vendors; and private operators of essential infrastructure are left entirely exempt.

To fix this, we make six recommendations: mandatory contract terms on knowledge transfer (A.1), exit and reversibility (A.2) and upstream open source contribution (A.3); a Union added value criterion that can decide an award (B.1); disciplined derogations – reasoned, notified, defined, time-limited and reported (B.2); and the same purchase obligation for private operators of essential services (B.3).

02 / Context:

You can't build sovereign supply without public and private demand

Taxpayer money built the cloud market that Europe now relies upon. The Commission confirms this structural reality in its own impact assessment: "the initial growth of today's largest cloud and AI computing service providers was fueled by public contracts. Similar opportunities did not emerge for European providers". But public procurement remains Europe's most powerful economic lever. Whether it succeeds in catalysing domestic supply depends on how the public sector procures: what standards it mandates, whether it possesses the technical capacity to evaluate tenders, whether it can exit existing vendor relationships, and what contributions it requires from commercial contractors.

Public demand shapes the market, and so far in one direction	Page 6
Buyers cannot evaluate what they procure	Page 7
Once there, services are hard to leave – and create vulnerabilities	Page 8
Buying sovereign is already possible under existing rules	Page 9
Open source: What public buyers and their providers rely on, and nobody pays for	Page 10
What CADA does to address this	Page 11

Public demand shapes the market, and so far in one direction

The public sector is a large enough buyer to move the market. Cloud and AI contracts published on the Union's tendering portal were worth EUR 9.2 billion in 2024, up from EUR 2.8 billion in 2021, and the Commission estimates the public sector at around 14% of cloud demand. Moreover, its weight is greater than its share, because public procurement sets primary signals for corporate IT architectures, and procurement standards established for government bodies are routinely mirrored by private operators in regulated industries.

Yet this procurement spend flows, almost exclusively, to three foreign providers. When the Netherlands Court of Audit examined the 1,588 cloud services used by central government, it found that Microsoft, Amazon and Google provided more than half of the Dutch government's cloud services. In June 2026, the Commission reached the preliminary position under competition law that AWS and Microsoft Azure must be designated as gatekeepers under the Digital Markets Act, citing "vast and entrenched user bases" protected by high switching costs and structural lock-in. Every public contract awarded to an entrenched incumbent compounds this market concentration, holding European providers back from achieving economies of scale.

But this weakness is not specific to cloud. Across the single market, the European Court of Auditors found that single-bid tenders across the Single Market surged from 23.5% in 2011 to 41.8% in 2021, concluding that the 2014 Public Procurement Directives have failed to stimulate competition. The primary issue is not excessive foreign competition, but an absence of authentic competition in a public procurement system that defaults to market incumbents.

Buyers cannot evaluate what they procure

Buying strategically presupposes a buyer's ability to judge the offer, negotiate the contract and supervise its performance. Yet most public buyers cannot. The Dutch audit found that some cloud consumers have "too little knowledge of the cloud" and that "this limited knowledge can lead to poor risk analyses and weak risk control"; of the 126 services material to primary government tasks, "no risk assessments were conducted for 84 (67%)", and the ministries "have only limited knowledge of the agreements" they have signed.

Data protection regulators observe identical issues. In a coordinated enforcement action across the European Economic Area examining approximately 100 public bodies, the European Data Protection Board found that only 32 of 86 public cloud consumers had executed a Data Protection Impact Assessment (DPIA). Public buyers routinely accept predetermined standard-form adhesion contracts because public administrations lack the commercial and technical leverage to negotiate modifications. A buyer in that position does not actively choose a provider – it simply accepts the path of least resistance.

Where Member States have funded public alternatives, utilisation has lagged behind capital investment. The French Cour des comptes documented that France's interministerial cloud platforms, Nubo and Pi, absorbed €55 million over nine years yet remain significantly underutilised, even by the founding ministries. The Commission named the cause: "a decline in organisations' overall in-house IT skills, due to higher reliance on managed services provided by private operators". An administration incapable of operating its own infrastructure cannot effectively oversee external commercial vendors. That is the starting point for any "buy sovereign" obligation.

Once there, services are hard to leave – and create vulnerabilities

Once a public body has chosen, it stays. As the OECD's 2025 cloud report emphasises "in the cloud sector, customers rarely switch providers once an initial choice is made". The barriers are technical, financial and organisational, and the Dutch competition authority found them larger for cloud than for other IT services. Public procurement exacerbates this trap: the Dutch Court of Audit revealed that government contracts contain inadequate protections for post-termination data retrieval, transition assistance, and migration to alternative platforms.

The Data Act is the Union's answer to the technical and financial barriers: a right to switch, mandatory contract terms on transition, continuity and the retrieval of data, and the end of switching charges. But it is yet to kick in to full effect. Switching charges are prohibited only from 2027, standard service fees or early termination penalties fall outside the definition, and the interoperability obligations are waiting for specifications that have not yet been published. As such, the Commission concludes that the Data Act's effects on the emergence of European offerings "are at this stage therefore limited and indirect".

A cloud contract can also end due to government actions, without either contractual party choosing it. This is true for foreign providers in Europe or European providers abroad:

- in its twelfth sanctions package on Russia the Union prohibited the supply, "directly or indirectly", of "software for the management of enterprises" to persons established in Russia, with existing contracts to be wound up by 20 March 2024. Even for a European provider, cloud contracts and providing to a foreign legal person can be severed by an act of public law at either end.
- In March 2026 the Finnish Ministry of Justice decided to run the 2027 parliamentary elections on the existing election information system rather than on the new one it had planned to build on the AWS cloud, because "the international political situation has changed".

For critical sectors, this combination of difficult switching with the risk of government shut-off due to geopolitical tensions threatens national security and public order and can only be mitigated by relying on sovereign services and supply chains. It is no longer optional to "buy sovereign" for critical services – it is a core national security need.

Buying sovereign is already possible under existing rules

None of this means that a public buyer *cannot* buy sovereign. In April 2026, the Commission awarded its own sovereign cloud tender, awarding €180 million across six-year framework contracts to serve Union institutions, bodies, and agencies.

To prevent vendor lock-in and enhance systemic resilience, the Commission awarded contracts across multiple consortia: Post Telecom with OVHcloud and Clever Cloud, STACKIT, Scaleway, and Proximus with S3NS, Clarence, and Mistral AI. Bidders were required to satisfy the Commission's Cloud Sovereignty Framework, ensuring operational immunity from third-country supply chain disruption (though we note one of the winning providers, the Proximus / S3NS grouping, is problematic because of its connection to Google Cloud).

This procurement model complies with international legal obligations. While the Union procurement market is bound by the WTO Agreement on Government Procurement (GPA), Recital 64 of CADA affirms that the Union retains the sovereign right under Article III of the GPA to institute measures necessary to protect public order, morals, and national security.

Three months after CADA, the Commission proposed a Public Procurement Act which "enables public buyers to apply European preference requirements", including by "granting evaluation preferences", and "provides a framework for mandatory European preference in sector-specific EU legal acts". CADA should be such such an act; its Union added value criterion is an evaluation preference.

The Commission has shown in its own house that sovereignty can be made a condition of the award; the question is whether CADA, in practice, lets other public buyers do the same.

Open source: What public buyers and their providers rely on, and nobody pays for

The services the public sector buys are built on open source components worth, by the Commission's own study, between EUR 65 and 95 billion a year to the Union's economy – yet maintained by very few people:

- The Harvard-Linux Foundation Census III study revealed that 40% of the most widely used non-npm software packages rely on just one or two developers for more than 80% of all code commits.
- The critical xz-utils supply chain incident of March 2024 (CVE-2024-3094, CVSS 10.0) demonstrated the vulnerability of this model: a single, uncompensated maintainer was targeted by hostile actors to insert an unauthorised backdoor into the OpenSSH authentication pathway, exposing global infrastructure. It became a project that one volunteer could no longer carry alone.

The Commission admitted that open source building blocks "are mostly maintained through…US (and Chinese) big tech providing a massive share of the funding and contributions", Europe's upstream contribution "is uneven and often not matched by structured, long-term maintenance capacity". It commits itself to "public money, public code" for its own stack. Yet, nothing applies that principle to the providers that sell open source-based services to the public sector. They are under no obligation to maintain, or to contribute back to, the projects they sell, and can charge each administration for the same patch while keeping it to themselves.

What CADA does to address this

Article 30 obliges the public sector to buy recognised services. Union entities and public sector bodies must use cloud computing services recognised at least at Union assurance Level 1 (paragraph 2). Contracting authorities whose activities have been identified, through the risk assessment of Article 29, as contributing to the preservation of public order may only procure services recognised at Level 2, 3 or 4 (paragraph 3). Paragraph 4 allows a contracting authority, "on an exceptional basis and where duly justified", to derogate from both obligations on three grounds: no recognised service in the central repository can supply the subject matter, provided this is not the result of "an artificial narrowing down of the parameters" of the procedure; a similar procurement in the previous year attracted no suitable tender; or compliance "would require the contracting authority to procure services at disproportionate cost". The third ground is lettered (a) in the proposal, a typographical error.

Article 31 does not oblige the private sector to buy recognised services. Entities in the sectors of high criticality of the NIS2 Directive that are not public sector bodies "may" carry out assessments similar to those of Article 29, and the Commission may, where duly justified, require them to by delegated act. No provision requires them to buy recognised services.

Article 32 introduces "Union added value". In procurement procedures for innovative cloud computing services and AI systems, contracting authorities must include non-price award criteria evaluating the tenderer's contribution to a European cloud and AI ecosystem: the Union's digital supply chain, technologies developed in the Union, innovation that strengthens security of supply, and delivery through critical hardware designed or manufactured in the Union. The criteria must be linked to the subject matter, not confer unrestricted freedom of choice, be set out in the procurement documents, and be "ancillary and not decisive in the award of the contract" (paragraph 2(d)). Recital 67 adds that the criterion "should not be decisive for award of the contract" and suggests "a maximum weighting of 15 out of 120 points".

Articles 41 to 44 address open source in public administration. The Union and Member States must take measures to "encourage" public bodies to use and reuse open standards and open source components when building their cloud and AI stack (Article 41, headed "open source first"); public bodies that release software under an open source licence must do so through a catalogue connected to a new EU Open Source Solutions Catalogue (Articles 42 and 43); and the Commission sets up a voluntary network of Open Source Programme Offices (first Article 44). Nothing obliges providers of services to contracting authorities to contribute upstream to the open source projects they use to deliver those services.

What happens when a recognised service changes is addressed only on the provider's side. A recognised provider must notify material changes to its auditor and national authority (Article 23), and revocations are published in the central repository for five years (Article 22(3)). Article 29(6) grants a migration period of up to 12 months where a risk assessment requires a change of service. The only migration plans in Annex II concern the provider's own third-country components at Levels 2 and 3.

03 / CADA's weakness:

As drafted, "Buy European" provisions are too timid to address dependencies

The proposal is right to treat public procurement as the main lever for building a European market, and a binding minimum assurance level for the whole public sector is a significant step.

In practice, however, the text limits its effectiveness through restrictive definitions, open-ended derogations, and unaddressed buyer capabilities. The "buy sovereign" effect ends up narrower than it first appears, and the proposal does not create a dynamic through which sovereign purchases would meaningfully reduce costs and improve the services the public sector relies on.

Gaps in CADA

01

Purchasing a recognised service does not equate to buying European.

Level 1, the mandatory minimum, contains no criterion excluding or limiting third-country control of the provider, and the Commission's own assessment is that "US hyperscalers generally all have offerings that would allow them to qualify under Level 1". Levels 2 and 3 remain open to providers under third-country control, subject to safeguards and, at Level 3, to the associated third country decision of Article 18.

The Levels 2 to 3, apply only to activities identified by national risk assessments, which the Commission expects to cover 30% of public use cases, with 10% at Levels 3 and 4.

Measured against the Commission's own tender, this is a step back: the Commission required of itself at least the data sovereignty; on the other hand, CADA requires Level 1 in 70% of cases, a level the Commission says the hyperscalers already meet. Therefore, for most

public demand the framework sends no signal in favour of European providers.

02

Union added value is designed not to bite.

Article 32 is the only European preference mechanism in the text. It applies only to "innovative" cloud services and AI systems, a term the proposal does not define, and the criterion must be "ancillary and not decisive"; recital 67 suggests a maximum of 15 points out of 120. A preference that the law requires to be non-decisive will, by construction, never decide an award. It cannot give European providers the demand, or investors the assurance, that the proposal says it seeks – and it falls short of what the Commission applied to its own purchase.

03

Procurement derogations are unmonitored and too open-ended.

Under Article 30(4), a contracting authority decides alone whether a derogation applies. It needs not notify or justify its decision to any authority, and the decision is not published. The terminology "disproportionate cost" used for derogation is not defined, which invites divergent readings across the Union and disputes between contracting authorities, tenderers and review bodies. The failed-procurement ground sets no condition on the earlier procedure, so that a procedure run with the shortest time limits permitted, or with specifications recognised providers could not meet, is enough to open the derogation for the following year. Nothing limits the duration of a contract concluded under a derogation, and the derogations apply equally to the public order activities for which the highest levels are required. In a European public procurement system where currently four procedures in ten already receive a single bid and one in six is awarded without any call for competition, a derogation that no one reviews will be the path of least resistance.

04

There is no exit for public buyers when a service loses its assurance level.

The provider notifies its auditor and its authority, and the revocation appears in the central repository; the public customer is not notified directly, and Article 30 says nothing about what happens to an existing contract. The 12-month migration period of Article 29(6) applies only when a risk assessment requires migration, not when a recognition is revoked. And the Cloud Sovereignty Framework falls short to protect such cases: the migration plans of Annex II concern the provider's components, at Levels 2 and 3 only; there is no equivalent at Level 1, where the risk of change is highest, or at Level 4, where the protection needed is greatest. The Commission itself expects the migration of public workloads to recognised services at Levels 2 to 4 to require "an anticipation of expenses of EUR 3 to 15 bn".

05

Public buyers are not equipped to judge what they buy, and the proposal does not equip them.

Sovereign procurement requires administrations able to assess and monitor their own supply chain, and we have explained above how far they are from it while CADA ignores it: public bodies that "cannot object meaningfully to the use of sub-processors or to changes of

sub-processors without risking a potentially critical loss of service".

The proposal provides for a common cloud and AI curriculum (Article 4(8)(b); Report 3), but gives public buyers no right to acquire technical knowledge of the service they buy. The technical knowledge of how the service works and of the measures protecting the buyer's sovereignty stays with the provider. Nothing in the proposal provides for a transfer of knowledge from provider to contracting authority that would reduce lock-in, enable in-house verification, or rebuild the competences the administrations have lost.

06

"Open source first" is an aspirational declaration and nothing more.

Article 41 is headed "open source first" but only requires measures to "encourage" its use; recital 84 refers to "obligations to conduct an open-source assessment" which do not appear in the articles. The proposal considers open source only as something public administrations use and release, and ignores the providers that sell open source-based services to them. Without an obligation in public contracts, most providers of cloud and AI services to the public sector will continue to rely on open source projects they do not contribute to, deepening dependencies on components that, on the Commission's own account, rest on "US (and Chinese) big tech" and lack "structured, long-term maintenance capacity"; and they will continue to charge public authorities for patches and updates that they never contribute upstream, inflating the real cost of the services without the administration being able to see it.

07

The exemption for private essential entities is unjustified.

The purchase obligation is justified by the protection of public order yet it applies only to public buyers in the NIS2 sectors. Private operators delivering the same services in the same sectors present the same risk and are covered only by a voluntary assessment. Neither the proposal, nor its recitals, nor the impact assessment explains the difference in treatment; the impact assessment's preferred option "provides measures for the public sector as well as for private sector essential entities", and the Commission costed the assessments of an estimated 25,600 private essential entities at EUR 1.44 billion. The difference also creates uneven conditions where public and private operators compete, for instance in health or energy, since only the public ones bear the cost of compliance. And the boundary is uncertain: whether an entity is a "public sector body" depends on the definition of a body governed by public law, which turns on national practice and has repeatedly had to be settled by the Court of Justice. Obligations placed on the edge of that divide will generate disputes, and a single contract may be worth hundreds of millions of euros.

04 / Our proposed fixes

We put forward six recommendations across two areas. The first introduces mandatory contract terms to ensure sovereign purchasing strengthens both buyers and the supply chain through knowledge transfer, exit and reversibility, and upstream open source contributions. The second reforms the award process by making the Union added value criterion decisive, and ensuring derogations remain strictly exceptional and extending these purchase obligations to private operators of essential services.

A. Mandatory contract terms to support sovereignty

To ensure that contracting authorities procure digital services that do not erode their own digital sovereignty or that of the Union, we suggest that the co-legislators mandate a series of terms that public cloud contracts falling under the Regulation must include. The three recommendations below could take the form of a new article, or a new section of Chapter II, on mandatory contractual terms.

A.1 Knowledge transfer, so that public servants can monitor and oversee the service — Page 17

A.2 Exit, portability and reversibility clauses — Page 19

A.3 Upstream contribution to the open source projects used to deliver the service — Page 21

B. A decisive European preference and disciplined procurement – for public and private buyers

B.1 A Union added value: make the criterion in Article 32(2)(d) decisive — Page 23

B.2 Discipline the derogations with clarifications and procedural oversight — Page 25

B.3 The same purchase obligation for private operators of essential services — Page 28

A. Mandatory contract terms to support sovereignty

A.1 Knowledge transfer, so that public servants can monitor and oversee the service

As it stands, the proposal does nothing to guarantee the contracting authority technical knowledge of how the service works and how its sovereignty is protected. With the adoption of public cloud, national and local administrations have lost the internal capability to oversee, judge and manage the services they buy.

We invite the co-legislators to consider an obligation of knowledge transfer in public cloud contracts above a financial threshold. Without impeding the intellectual property rights of the provider and its subcontractors, the obligation should enable the contracting authority to evaluate the functioning of the services and supply chains it procures, and to maintain the skills and competences it needs not only to procure cloud services but also to use, operate and, when needed, maintain them. We do not consider the obligation implementable for every contract, in particular the smallest; the threshold should identify contracts whose size demonstrates that the contracting authority needs, and can dispose of, the workforce to manage the services it purchases.

Proposed changes:

01 **Threshold (new article 29a on mandatory contract terms).**
Set a threshold for contractual requirements, by reference to the contract value and the number of users, and allow the Commission to adjust it by delegated act.

02 **Knowledge transfer (new article 29a on mandatory contract terms, paragraph 1).**
Require contracts for cloud computing services above a threshold set in the article to include a knowledge transfer plan enabling the contracting authority to understand the architecture of the service, the components and subcontractors used to deliver it, and the measures implementing the criteria of Annex II, without prejudice to intellectual property rights.

03 **Training (new article 29a on mandatory contract terms, paragraph 2).**
Require the provider to deliver, within the contract, training enabling the contracting authority's staff to operate, monitor and, where applicable, migrate the service.

A. Mandatory contract terms to support sovereignty

A.2 Exit, portability and reversibility clauses

The proposal considers migration only after a risk assessment (Article 29(6)) and, for the provider's own components, in the definition of Levels 2 and 3 (Annex II). The only consequence of the revocation of a recognition is removal from the central repository. Given the speed at which supply chains change and cloud providers are acquired by foreign entities, this gap is a risk for public order and national security. We encourage the co-legislators to fill it with a contractual obligation, for all contracts within the scope of the Regulation and at every assurance level, to include exit, portability and reversibility clauses built on the technical elements already defined in the Data Act.

Proposed changes:

01 **Exit clauses (new article 29a on mandatory contract terms, paragraph 3).**
Require every contract for cloud computing services within the scope of this Chapter to include exit, portability and reversibility clauses, at least equivalent to those required by Article 25 of Regulation (EU) 2023/2854, whatever the Union assurance level of the service.

02 **Loss of recognition (Article 30, new paragraph).**
Provide that, where the recognition of a service is revoked or lowered under Article 17(11) or Article 23(3), the contracting authority may terminate the contract without penalty and the provider must support migration within a period not exceeding the 12 months referred to in Article 29(6).

03 **Notification of the customer (Article 23(3)).**
Require the national competent authority to notify contracting authorities using a service whose recognition it amends or revokes, directly or through the central repository.

04 **Migration plans (Annex II, points 1.1 and 4.1, new points).**
Require a documented migration plan at Levels 1 and 4, as already required at Levels 2 and 3.

A. Mandatory contract terms to support sovereignty

A.3 Upstream contribution to the open source projects used to deliver the service

The proposal considers open source use and release by public administrations, but almost entirely ignores the case in which the public sector buys services from private providers relying on open source components, and the behaviour of those providers towards the projects they use. The only references to open source in procurement are the supply chain related obligation of Annex II. Recognising open source as a guarantee of control and transparency is not, in itself, a guarantee of support for the projects used to deliver a service: providers can continue to use projects they do not contribute to, and charge contracting authorities for features, updates and patches they never contribute back.

We consider this a missed opportunity to use public procurement to require contribution to the open source projects used in the delivery of a service, including the patches and updates introduced for the contracting authority. The requirement would improve the quality and security of the projects public administrations rely on every day, and reduce the long-term cost of cloud and AI services by preventing providers from charging several administrations for the same update to a project that is freely available to all. It gives effect, on the supply side, to the “public money, public code” principle the Commission applies to itself.

Proposed changes:

01 **Upstream contribution (new article on mandatory contract terms, paragraph 3).**
Require contracts for cloud computing services within the scope of this Chapter to oblige the provider to contribute upstream, under the project's licence, the modifications, patches and updates it makes to open source components used to deliver the service, unless security or confidentiality constraints duly justified to the contracting authority prevent it.

02 **Transparency of open source use (same paragraph).**
Require the provider to identify, in the software bill of materials made available to the contracting authority, the open source components used and its contributions to them.

03 **Open source first (Article 41).**
Replace "take the necessary measures to encourage" with "ensure that", and add the open source assessment referred to in recital 84 as an obligation on Union entities and public sector bodies before procuring software.

B. A decisive European preference and disciplined procurement – for public and private buyers

B.1 A Union added value: make the criterion in Article 32(2)(d) decisive

Article 32 is the only European preference mechanism in the proposal, and its intent is right: to reward, in European public procurement, the tenderer's contribution to the European economy. The mechanism, however, is designed not to bite. Article 32(2)(d) requires the criteria to be "ancillary and not decisive in the award of the contract", and recital 67 adds that the criterion "should not be decisive for award of the contract" and suggests "a maximum weighting of 15 out of 120 points". A preference that the law requires to be non-decisive will, by construction, never decide an award, and cannot give European providers the demand, or investors the assurance, the proposal says it seeks.

We acknowledge that this is a deliberate choice rather than a drafting oversight – the same formula appears in Article 30(4)(d) of the Chips Act 2.0 proposal – and that it reflects a legitimate concern to preserve the primacy of technical and financial criteria. But that concern is already met by the three other conditions in Article 32(2): the criteria must be linked to the subject matter of the contract, must not confer unrestricted freedom of choice, and must be set out in the procurement documents. These are the ordinary safeguards of Union procurement law. The fourth condition adds nothing to them except the guarantee that the preference will not matter. The Public Procurement Act proposal now provides a horizontal framework in which sector-specific acts may make European preference mandatory; CADA should at least not forbid its own preference from deciding.

Proposed changes:

01 **Award criteria (Article 32(2)(d)).**
Replace “ancillary and not decisive in the award of the contract” with “ancillary to the award criteria linked to the performance of the contract”.

02 **Recital 67.**
Delete the sentence “The criterion relating to European added value should not be decisive …” and the reference to a maximum weighting of 15 out of 120 points.

03 **Consistency (Article 32, new paragraph).**
Provide that the criteria of this Article constitute European preference requirements within the meaning of the Public Procurement Act, once adopted.

B. A decisive European preference and disciplined procurement – for public and private buyers

B.2 Discipline the derogations with clarifications and procedural oversight

Article 30(4) allows contracting authorities to depart from the obligation to procure recognised services on three grounds. Derogations are necessary – the market for recognised services will take time to build – and we do not propose to remove them. But nothing in the text ensures that they remain exceptional: the decision is taken by the contracting authority alone, is neither notified nor published, rests on an undefined notion of cost, and is not limited in time. Left as they are, the derogations are the mechanism by which the obligation will become optional. The five measures below do not narrow the derogations; they make their users accountable.

i. Notification to the national authority. A derogation that no one outside the contracting authority ever sees cannot be exceptional in practice. Any decision relying on Article 30(4) should be taken in a reasoned decision notified to the national competent authority designated under Article 25 – before the procedure is launched where the ground is known in advance, or before the award where it only materialises during the procedure. The contracting authority remains responsible for its decision; the authority should respond within 10 working days, so that procurement timelines are not affected. The purpose is to make the derogation visible to the authority that supervises the framework and to deter its casual use.

ii. Disproportionate cost. The third ground is the one most likely to be invoked, and the one the proposal defines least: it does not say against what baseline the cost is measured, over what period, or on what evidence. The comparison should be made with the best offer meeting the same technical requirements from a non-recognised service, not with the lowest conceivable price; assessed over the whole life of the contract, including the costs of exit and migration and the cost of the sovereignty risk the Regulation is meant to address; and rest on objective and transparent data recorded in the reasoned decision. We caution against importing a fixed numerical presumption such as the one in Article 31(3)(d) of the Chips Act 2.0 proposal, under which cost differences "exceeding 25% of the value of the tender … may be presumed … to be disproportionate".

A threshold set in the abstract, before any evidence on the actual price difference between recognised and non-recognised services exists, risks turning the derogation into the rule; if a figure is thought necessary, it should be set by the Commission once the first years of application have produced the data.

iii. The earlier procedure. The failed-procurement ground should be available only where the earlier procedure gave recognised providers a fair opportunity to tender – in accordance with the minimum time limits for the receipt of tenders in Union procurement law – and did not artificially narrow its parameters.

iv. Duration. Once a contracting authority has derogated, nothing obliges it to return to the recognised market; a contract concluded under a derogation can run for years and be renewed on the same basis long after recognised services have become available. Contracts awarded under any of the three grounds should be of limited duration and not renewable without a fresh verification that no recognised service in the central repository can supply the subject matter. The derogation would thus be what the text says it is: a bridge until the sovereign market can respond.

v. The feedback loop. Each derogation is a documented case in which the sovereign market was unable to supply a public need at a comparable cost. That is precisely the information the risk assessments of Article 29 and the monitoring of Articles 15 and 33 are meant to produce, yet the proposal does not connect them. The national competent authority should compile the derogations notified to it each year and transmit the report to the Commission; Member States should take it into account in their risk assessments, where it will show where the public sector remains dependent on non-recognised services and why; and the Commission should use the aggregated reports to direct the instruments of Titles II and III. Derogation reports thus become the link between the “buy sovereign” and the “build sovereign” parts of the Act (Report 1, recommendation A.1).

Proposed changes:

01 **Reasoned decision and notification (Article 30, new paragraph 5).**
Require any derogation under paragraph 4 to rest on a reasoned decision notified to the national competent authority before the launch of the procedure or, at the latest, before the award; provide that the authority responds within 10 working days; and require the ground relied upon to be indicated in the contract notice or the procurement documents.

02 **Disproportionate cost (Article 30(4), third ground, and new recital after recital 64).**
Specify that disproportionate cost is assessed over the full duration of the contract, including exit and migration costs, by comparison with offers meeting the same requirements, and on the basis of objective and transparent data; correct the lettering of the third ground to (c).

03 **Earlier procedure (Article 30(4)(b)).**
Add that the earlier procurement procedure must have complied with the applicable time limits for the receipt of tenders and must not have artificially narrowed its parameters.

04 **Duration (Article 30(4), new subparagraph).**
Provide that contracts awarded under a derogation are limited in duration and may not be renewed or extended unless the contracting authority has verified, before the renewal, that the conditions of the derogation still apply.

05 **Annual report (Article 30, new paragraph 6).**
Require national competent authorities to report annually to the Commission on the derogations notified to them, and the Commission to publish an aggregated, non-confidential summary.

06 **Use of the reports (Articles 15(1), 29(2) and 33(3)).**
Add a point to each requiring the Commission, Member States and Union entities to take into account the derogations reported under Article 30, and Member States to include the number, grounds and value of derogations in their annual information to the Commission.

B. A decisive European preference and disciplined procurement – for public and private buyers

B.3 The same purchase obligation for private operators of essential services

The purchase obligation of Article 30 is justified, in recitals 50 and 64, by the preservation of public order. That justification does not stop at the boundary between public and private ownership. A hospital, an energy network operator or a water utility presents the same risk of third-country access to data and of service disruption whether it is publicly or privately owned; in many Member States the same service is delivered by both, in competition. Applying the obligation to one and not the other leaves the risk half-addressed, distorts competition between operators in the same sector, and creates legal uncertainty wherever national law places an entity on the border between the two.

We recommend extending the obligation of Article 30(3) to essential entities within the meaning of the NIS2 Directive, for those of their activities that the Member State's risk assessment under Article 29 has identified as contributing to the preservation of public order, at the assurance level that assessment determines. This is a narrower ask than it may appear. It does not extend Level 1 to the whole private sector; it covers only the activities a Member State has itself designated as sensitive, in sectors where the NIS2 Directive already requires those entities to manage supply chain security. The derogations of Article 30(4), as disciplined under recommendation B.2, would apply equally, and a transitional period aligned with the contracting cycle would allow existing contracts to run to term. It completes recommendation B.1 of Report 1, which makes the assessment mandatory for the same entities.

We recognise that the legal basis differs: for public buyers the obligation operates through procurement law and the public order exception of the Agreement on Government Procurement, whereas for private entities it would operate as a security requirement on the operator, in the manner of the NIS2 Directive. That is an argument for drafting the private sector obligation as a distinct provision, not for omitting it.

Proposed changes:

01 **Private sector purchase obligation (new Article 31a).**
Provide that essential entities within the meaning of Directive (EU) 2022/2555 whose activities have been identified under Article 29(1) shall, for those activities, use cloud computing services recognised as having the Union assurance level determined by the risk assessment.

02 **Derogations and transition (new Article 31a, paragraphs 2 and 3).**
Apply the derogations of Article 30(4), as amended, and provide a transitional period for contracts in force at the date of application, aligned with their remaining duration.

03 **Recitals 50 and 64.**
State that the protection of public order requires the same safeguards for the activities identified under Article 29(1) whether they are carried out by public or private operators.

Sources and resources

1. European Commission, 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, 2026/0138 (COD), 3 June 2026. https://ec.europa.eu/newsroom/dae/redirection/document/129111
2. European Commission, Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 502 final, Part 1/2, 3 June 2026, p. 22. https://ec.europa.eu/newsroom/dae/redirection/document/129113
3. European Commission, Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 502 final, Part 2/2 (Annexes), 3 June 2026, Table 19, p. 57. https://ec.europa.eu/newsroom/dae/redirection/document/129114
4. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 71.
5. COM(2026) 502 final (CADA proposal), as above, recital 66, p. 31.
6. Netherlands Court of Audit (Algemene Rekenkamer), Dutch central government in the cloud: Dark clouds looming, report, 15 January 2025, p. 6. https://english.rekenkamer.nl/site/binaries/site-content/collections/documents/2025/01/15/dutch-central-government-in-the-cloud/Dutch+central+government+in+the+cloud.pdf
7. European Commission, "Commission reaches preliminary position that Amazon's and Microsoft's market leading cloud services should be designated under the DMA", press release IP/26/1444, 25 June 2026. https://ec.europa.eu/commission/presscorner/detail/en/ip_26_1444
8. European Court of Auditors, Special report 28/2023: Public procurement in the EU – Less competition for contracts awarded for works, goods and services in the 10 years up to 2021, December 2023, paragraphs 36 and 40. https://www.eca.europa.eu/en/publications/SR-2023-28
9. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 21.
10. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 7.
11. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 38.
12. European Data Protection Board, 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, report adopted on 17 January 2023, Executive summary and sections 1, 3.1 and 3.3, pp. 2, 5, 10 and 14. https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf
13. Cour des comptes, Les enjeux de souveraineté des systèmes d'information civils de l'État, S2025-1479, 31 October 2025. https://www.ccomptes.fr/sites/default/files/2025-10/20251031-S2025-1479-Enjeux-souverainete-des-SI-civils-de-l-Etat.pdf
14. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 23, footnote 76.
15. OECD, Competition in the provision of cloud computing services, OECD Roundtables on Competition Policy Papers, No. 323, OECD Publishing, Paris, 2025 (first released 20 May 2025), p. 26. https://doi.org/10.1787/595859c5-en
16. Netherlands Authority for Consumers and Markets (ACM), Market study into cloud services, 5 September 2022, pp. 5 and 55. https://www.acm.nl/system/files/documents/public-market-study-cloud-services.pdf
17. Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 44.
18. 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), Articles 23, 25 and 29. http://data.europa.eu/eli/reg/2023/2854/oj
19. Regulation (EU) 2023/2854 (Data Act), as above, Article 2, point (36), and Article 29.
20. Regulation (EU) 2023/2854 (Data Act), as above, Article 30(3); SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, p. 207.
21. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, p. 207.
22. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, p. 233.
23. Council Regulation (EU) 2023/2878 of 18 December 2023 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, Article 1, inserting Article 5n(2b) and (4b) into Regulation (EU) No 833/2014. http://data.europa.eu/eli/reg/2023/2878/oj
24. Ministry of Justice of Finland (Oikeusministeriö), "Vuoden 2027 eduskuntavaalit toteutetaan nykyisen vaalitietojärjestelmän avulla" (The 2027 parliamentary elections will be conducted using the current election information system), press release, 24 March 2026. https://valtioneuvosto.fi/-/1410853/vuoden-2027-eduskuntavaalit-toteutetaan-nykyisen-vaalitietojarjestelman-avulla
25. European Commission, "Commission advances cloud sovereignty through strategic procurement", news item, 17 April 2026. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en
26. COM(2026) 502 final (CADA proposal), as above, recital 64, p. 31.
27. European Commission, Proposal for a Regulation of the European Parliament and of the Council on public contracts and concessions (Public Procurement Act), COM(2026) 590 final, 2026/0265 (COD), 9 September 2026 (Council document 12969/26), pp. 3, 13 and 23. https://data.consilium.europa.eu/doc/document/ST-12969-2026-INIT/en/pdf
28. Knut Blind, Mirko Böhm, Paula Grzegorzewska, Andrew Katz, Sachiko Muto, Sivan Pätsch and Torben Schubert (Fraunhofer ISI and OpenForum Europe) for the European Commission, The impact of Open Source Software and Hardware on technological independence, competitiveness and innovation in the EU economy, final study report, September 2021. https://digital-strategy.ec.europa.eu/en/library/study-about-impact-open-source-software-and-hardware-technological-independence-competitiveness-and
29. Frank Nagle, Kate Powell, Richie Zitomer and David A. Wheeler, Census III of Free and Open Source Software, The Linux Foundation and the Laboratory for Innovation Science at Harvard, December 2024, pp. 4 and 24. https://www.linuxfoundation.org/hubfs/lfr_censusiii_120424a.pdf
30. National Institute of Standards and Technology, National Vulnerability Database, CVE-2024-3094 (malicious code in xz versions 5.6.0 and 5.6.1), published 29 March 2024, CVSS base score 10.0. https://nvd.nist.gov/vuln/detail/CVE-2024-3094
31. European Commission, Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy, COM(2026) 503 final, 3 June 2026, pp. 21–22. https://ec.europa.eu/newsroom/dae/redirection/document/129100
32. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 25.
33. COM(2026) 502 final (CADA proposal), as above, p. 62.
34. COM(2026) 502 final (CADA proposal), as above, pp. 62–63.
35. COM(2026) 502 final (CADA proposal), as above, pp. 31–32 and 63.
36. COM(2026) 502 final (CADA proposal), as above, pp. 69–71.
37. COM(2026) 502 final (CADA proposal), as above, p. 57.
38. COM(2026) 502 final (CADA proposal), as above, p. 61.
39. European Commission, Annexes 1 to 3 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, 3 June 2026, pp. 6 and 8. https://ec.europa.eu/newsroom/dae/redirection/document/129112
40. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 40.
41. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, pp. 42 and 46.
42. European Court of Auditors, Special report 28/2023, as above, paragraphs 33 and 36.
43. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, pp. 35 and 130.
44. EDPB, 2022 Coordinated Enforcement Action on the use of cloud-based services by the public sector, as above, section 3.4, p. 15.
45. COM(2026) 502 final (CADA proposal), as above, pp. 36 and 69.
46. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 21 and footnote 84.
47. European Commission, Executive Summary of the Impact Assessment Report accompanying the proposal for a Cloud and AI Development Act, SWD(2026) 503 final, 3 June 2026, p. 2. https://ec.europa.eu/newsroom/dae/redirection/document/129115
48. SWD(2026) 502 final, Part 2/2 (CADA impact assessment, annexes), as above, Table 41, p. 129.
49. COM(2026) 502 final (CADA proposal), as above, Article 2, point (6), p. 39; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), Article 2, points (1) and (2). http://data.europa.eu/eli/dir/2019/1024/oj; Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement, recital 10. http://data.europa.eu/eli/dir/2014/24/oj
50. SWD(2026) 502 final, Part 1/2 (CADA impact assessment), as above, p. 23, footnote 76; Netherlands Court of Audit, Dutch central government in the cloud, 15 January 2025, as above, p. 21.
51. Regulation (EU) 2023/2854 (Data Act), as above, Article 25.
52. COM(2026) 503 final (Communication on European Tech Sovereignty), as above, p. 25.
53. COM(2026) 502 final (CADA proposal), as above, pp. 31–32 and 63.
54. European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework of measures for strengthening the Union's semiconductor ecosystem (Chips Act 2.0), COM(2026) 504 final, 2026/0139 (COD), 3 June 2026, Article 30(4)(d), p. 78. https://ec.europa.eu/newsroom/dae/redirection/document/129104
55. COM(2026) 590 final (Public Procurement Act proposal), as above, p. 13.
56. COM(2026) 504 final (Chips Act 2.0 proposal), as above, Article 31(3)(d), p. 79.
57. Directive 2014/24/EU, as above, Article 27(1).
58. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), Article 21(2), point (d). http://data.europa.eu/eli/dir/2022/2555/oj

FOT/