

Consultation Response - European Pirates

FEEDBACK SUBMISSION

Cloud and AI Development Act | COM(2026) 502

September 2026

Executive Summary

The European Pirate Party (PPEU) recognises that Europe faces a real shortfall in cloud and AI computing capacity, and we support the Cloud and AI Development Act's (CADA) ambition to close that gap through sustainable, well-governed infrastructure. We also welcome its "open source first" language and its attempt to give public bodies a workable notion of sovereign cloud services. Our position, set out in the sections below, is that as currently drafted the Act risks expanding capacity through the same market structure that produced today's dependence on a small number of providers, rather than reshaping that structure. Our five concerns are:

1. The Act facilitates large-scale private investment in data centres without requiring public disclosure of which projects and companies benefit, on what conditions, or what they must deliver in return.
2. The evidence behind the "triple capacity in five to seven years" target is thinner than the scale of the intervention warrants, and the accelerated-permitting toolbox changes where and when environmental scrutiny occurs in ways that, in PPEU's view, need stronger safeguards.
3. The four-level cloud sovereignty framework is built primarily around jurisdiction, ownership, personnel and supply-chain control. It does contain access-control requirements, but these operate by disqualifying non-compliant subcontractors and, in limited cases, hostile third countries; they do not require that a compliant provider's own systems, or a public authority acting through lawful process, be technically unable to read customer data.
4. The Act's own capacity and procurement measures are structured in a way that PPEU believes lets today's hyperscale incumbents qualify relatively easily for the lower sovereignty tiers, while leaving open-source and SME provisions largely voluntary.
5. The Act's green compute ambitions and open-source principles are stated in the recitals but left, in the operative articles, mostly as encouragements rather than obligations.

Our recommendations address each of these concerns in Sections 1 to 5.

Who We Are

The European Pirate Party (PPEU) is a pan-European political party representing Pirate Parties across EU Member States. We are rooted in the defence of digital rights, civil liberties and democratic participation, and we view digital infrastructure as a common good that must serve all citizens.

What We Believe

Our manifesto commits us to the protection of privacy from exploitation by both public and economic actors, to transparency and accountability of public institutions, to open access to publicly funded research and open availability of publicly funded data subject to privacy safeguards, to free and libre open-source software as a means of user control and autonomy, and to democratic participation in public decision-making. Our assessment of CADA in this submission is grounded directly in these commitments.

Why We Are Responding

The Cloud and AI Development Act (COM(2026) 502 final), published on 3 June 2026, is the centrepiece of the Commission's Tech Sovereignty Package. It touches every area where PPEU's voice is most distinct: the concentration of digital infrastructure, the relationship between "security" and surveillance, open-source and public procurement, and the environmental cost of large-scale compute. We support the underlying goal of reducing Europe's dependence on a small number of non-EU cloud providers, currently estimated to control over 70% of the European cloud market. Our concerns, set out below, are about how that goal is being pursued.

Opportunities and Risks

Opportunities

- The Cloud and AI Leadership Initiatives (Title II) direct funding toward energy-efficient data centre technologies, open cloud stacks and open-source foundations, which is the right approach if backed by binding conditions rather than encouragement alone.
- The Euro Cloud Federation (Articles 34 to 36) offers a public-sector alternative to reliance on commercial hyperscalers, through voluntary sharing of public-sector data centre and cloud capacity between Union entities and Member States.
- The "open source first" principle (Articles 41 to 44) and the EU Open-Source Solutions Catalogue give open-source public procurement an institutional home for the first time in a binding cloud instrument.
- The Regulation's five-year review clause (Article 47) and its capacity-gap monitoring duty (Article 15) provide a foothold for future course correction, if strengthened.

Risks

- Private investment facilitation (Title III) creates no general public register identifying which projects and companies receive acceleration-zone status, State aid or strategic-project designation, nor the conditions attached to that support.
- The tripling target and the accelerated permitting toolbox are being deployed at a pace the underlying evidence on grid capacity, water use and environmental impact may not yet support; the European Economic and Social Committee has itself called for mandatory social and environmental impact assessment before acceleration zones are designated.
- On the Commission's own estimates, the two lowest assurance levels cover roughly 90% of public-sector use cases. The public sector represents around 14% of cloud demand, meaning that the sovereignty procurement framework directly concerns only a relatively small share of total cloud demand, while the large private-sector share is not generally subject to the same public-sector procurement requirements. Illustratively, if the public sector accounts for around 14% of total cloud demand and Levels 3 and 4 correspond to around 10% of public-sector needs, that segment represents only around 1.4% of total EU cloud demand, though CADA does not literally reserve that share to EU providers; it is simply the portion of demand where the higher levels are likely to apply.
- Binding obligations on openness, interoperability and SME access are largely replaced with objectives Member States are asked to "pursue" or "consider," with no stated consequence or corrective mechanism where those objectives are not met.

Cross-Cutting Principles

- Public money spent to build or shape digital infrastructure requires public transparency about who benefits and on what terms.
- Deployment speed must not come at the expense of environmental assessment, grid planning or community consultation, and the manifesto's commitment to democratic participation means citizens and civil society should be able to see and contest these assessments, not only technical regulators.

- A framework built to keep data out of the hands of disqualified outsiders is not the same as a framework that limits what a compliant provider or a public authority can do with that data. PPEU's concern is that CADA currently does the first without doing much of the second.
- Concentration risk does not disappear when it moves from non-EU to EU hands. A plural market of SMEs, cooperatives, open-source foundations and public capacity is the goal, not a market of a few large European incumbents replacing a few large foreign ones.

Openness, once stated as a principle in a recital, should be written into the operative text as an obligation, not left as an encouragement.

Section 1: Governance, Investment and Accountability

1.1 Facilitating investment: acceleration zones and strategic projects

CADA's central mechanism for attracting private investment is the data centre acceleration zone (Article 10), paired with a fast-tracked, capped 12-month permitting procedure and an aggregated baseline permit covering the zone as a whole (Article 13). Individual projects can additionally be designated Commission-recognised "strategic projects" (Article 14), unlocking eligibility for the European Competitiveness Fund's competitiveness seal and other Union funding instruments, and potentially State aid under Articles 107 and 108 TFEU where a project meets at least two of five listed criteria, including a strong sustainability or innovation contribution. The Commission's own Call for Evidence identified the barriers this is meant to solve: high construction costs, difficulty accessing energy, water, land and capital, and slow, fragmented national permitting.

1.2 Who decides, and on what terms

Responsibility for identifying acceleration zones and drafting national cloud and AI strategies sits mainly with Member States (Articles 7 and 10), while the Commission's role is confined to monitoring aggregate capacity, demand and the size of the capacity gap (Article 15) and to deciding, by decision, which projects qualify as strategic (Article 14). Neither Article requires public disclosure of the specific companies and projects that receive acceleration-zone status, State aid, or strategic-project designation, nor what obligations those companies take on in return for the advantages granted. The only anti-foreclosure safeguard that exists applies solely inside acceleration zones (Article 11(2)) and addresses speculative resource reservation, not who controls the eventual investment.

1.3 Transparency and public oversight

Formal public accountability is limited to two mechanisms: Member States must supply relevant information to the Commission, and the Regulation as a whole is reviewed and reported to the European Parliament and Council once, five years after entry into force (Article 47). For an instrument expected to triple EU data centre capacity within five to seven years, a single review at the five-year mark means that a substantial part of the deployment period contemplated by the Act will have elapsed before Parliament or Council receive a consolidated public account of who benefited and how. The Commission's own impact assessment recognises that high capital costs are themselves a barrier to new entrants; PPEU's assessment is that this makes it more likely that companies already holding capital, infrastructure and market position will be the primary beneficiaries of accelerated permitting and any State aid attached to it, though the Act does not itself state this outcome.

1.4 Concentration risk: SMEs, cooperatives and open alternatives

The Regulation does gesture toward broader participation. Article 32 lets contracting authorities include non-price "Union added value" criteria in procurement, covering contribution to the European cloud and AI supply chain, integration of Union-funded research and development, security of supply, and use of EU-designed or manufactured hardware where feasible, though these criteria must remain ancillary and not decisive under Article 32(2)(d). Article 33 sets an objective, not an obligation, that Member States pursue a 25% share of cloud and AI procurement of innovation for SMEs, with no specific consequence or corrective mechanism stated where that objective is missed. As Section 4 sets out in more detail, the practical effect PPEU anticipates is that public support measures, faster permits and funding eligibility are open by design to actors who already have capital and infrastructure, while cooperatives, European SMEs and open-source-based providers compete for a residual, discretionary share.

Recommendations

- **R1.1** Require the Commission and national competent authorities to publish, in the central repository already established under Article 22, which specific projects and companies receive acceleration-zone status, strategic-project designation, or State aid support under CADA, together with the criteria applied and the obligations attached.
- **R1.2** Replace the single five-year review (Article 47) with annual public reporting on capacity growth, ownership concentration and the distribution of public support between large incumbents, SMEs, cooperatives and public bodies, alongside the existing capacity-gap monitoring under Article 15.
- **R1.3** Convert the SME procurement objective in Article 33 into a comply-or-explain obligation, requiring Member States that fall short of the 25% target to publish the reasons and corrective measures taken.
- **R1.4** Extend the anti-foreclosure safeguard in Article 11(2) beyond acceleration zones to cover all State-aid-eligible strategic projects designated under Article 14.
- **R1.5** Require any contracting authority or Member State granting acceleration-zone or strategic-project status to publish an assessment of the effect on market concentration before the designation takes effect, not only after the fact through the five-year review.

Section 2: Evidence and Process

2.1 The tripling target and its evidentiary basis

CADA's headline target, to at least triple EU data centre capacity within five to seven years, originates in the Commission's AI Continent Action Plan and was carried forward largely unchanged through the Call for Evidence and into the final proposal. The Call for Evidence and impact assessment identify the barriers behind the capacity gap, including construction costs, energy, water, land and capital access, and fragmented permitting, but PPEU's assessment is that the tripling figure itself functions more as a policy ambition than as a target derived from a published, bottom-up model of EU demand, available land and available clean power. This matters because the entire architecture of Title III, acceleration zones, 12-month permitting and aggregated baseline permits, is calibrated to that number.

2.2 The constraints the Commission itself identifies

The Act's own recitals document real, already-binding physical limits. Recitals 36 to 38 note that data centre deployment is lagging and concentrated in a limited number of hubs, creating higher costs, higher latency for peripheral regions and unequal opportunities across Member States. Grid capacity is treated as a precondition for acceleration zones: Article 10(2) requires Member States to analyse current and future energy needs for each zone, but only "where appropriate," and the resulting analysis feeds into national grid planning rather than functioning as a binding condition on whether a zone is designated at all. The Commission itself, citing IEA estimates, states that EU data centre electricity use stood at around 70 TWh in 2024 and that global data centre electricity consumption is projected to more than double towards 2030, driven primarily by AI and accelerated computing.

2.3 Fast permits and the timing of environmental scrutiny

Article 13 designates every data centre project in an acceleration zone as a "strategic project" for the purposes of the parallel Regulation on speeding up environmental assessments (COM(2025) 984 final), giving it access to that Regulation's dedicated toolbox and a capped 12-month permit-granting procedure. Article 13(3) does require Member States to carry out the necessary environmental assessments, planning procedures and evaluations at zone level before the aggregated baseline permit is issued, so the Act does not remove environmental scrutiny. PPEU's concern is narrower: CADA changes where and when that scrutiny occurs, moving it to the acceleration-zone level and combining it into a single aggregated permit issued before most individual investors and projects within the zone are even known. This is the point in the process where public consultation and challenge are hardest to exercise meaningfully, since the specific project a community would want to comment on may not yet exist.

2.4 Weak ex-ante scrutiny and the case for stronger safeguards

The impact assessment accompanying CADA was submitted to the Regulatory Scrutiny Board on 30 April 2026 and received a positive opinion on 8 May 2026, accompanied by a request for further improvements. The European Economic and Social Committee, in its opinion on the Cloud and AI Development Act (INT/1126), adopted on 23 September 2026, called for mandatory social and environmental impact assessments covering health, employment, electricity and water demand before any acceleration zone is designated, and for stronger conditions attached to grid access. PPEU endorses the EESC's position, and would add a participation dimension to it: a mandatory assessment is only a meaningful safeguard if it is clear who gets to see it, who can comment on it, at what stage, and what information about the proposed infrastructure is made public before the zone, not merely the eventual project, is designated.

Recommendations

- **R2.1** Require the Commission to publish the demand, capacity and environmental modelling underlying the tripling target, updated at least every two years alongside the capacity-gap monitoring already required under Article 15.
- **R2.2** Make the energy needs analysis under Article 10(2) mandatory rather than conditional ("where appropriate"), and require it to be published before, not alongside, zone designation.
- **R2.3** Adopt the EESC's recommendation that social and environmental impact assessments covering health, employment, electricity and water demand be mandatory prerequisites for acceleration-zone designation, and specify a public consultation stage with defined rights to comment before the zone-level aggregated baseline permit is issued.
- **R2.4** Preserve a right for affected communities and civil society to challenge zone-level environmental assessments under Article 13 on the same terms that would apply to an individual project outside an acceleration zone.
- **R2.5** Shorten the single five-year evaluation cycle under Article 47 for the specific purpose of assessing environmental and grid impact, given the pace of deployment the Act itself is designed to produce.

Section 3: Secure Processing Capacity and EU-Based Providers

Sovereign Cloud, Access to Data and Data Ownership

3.1 What the proposal does

Alongside expanding data centre capacity, CADA creates a legal framework for "sovereign" cloud services that public bodies must use for certain activities. Since three non-EU companies control over 70% of the European market, European data and services are, in practice, already dependent on non-EU providers. The core of the proposal is a cloud sovereignty framework (Article 16 and Annex II) built around four levels. Level 1 requires EU establishment, EU-located infrastructure and assets, and EU data residency unless the public body requires otherwise, alongside cybersecurity and subcontractor-transparency conditions. Level 2 adds EU-located personnel, a cybersecurity certification at "substantial" assurance, a prohibition on using service-generated data to train non-EU AI systems, detailed safeguards against third-country control, and software supply-chain transparency including a software bill of materials. Level 3 adds EU citizenship and security-clearance requirements for personnel and, as a default, excludes providers subject to third-country control, subject to a narrow Commission-approved derogation under Article 19. Level 4 removes that derogation entirely and defines "effective control" to include the ability of a non-EU entity to materially influence a software component's technical evolution, maintenance or security remediation, which is broad enough to reach some community-governed open-source projects. Member States must assess which public activities need which level (Article 29), and public buyers must then use services recognised at that level (Article 30).

3.2 Secure from whom

Levels 3 and 4 are designed, among other things, to host EU classified information, and the risk assessments behind them cover national security, defence, justice and law enforcement (Article 29(1)). The lower levels carry weaker access safeguards: Level 1 requires cybersecurity and subcontractor oversight but does not include the explicit requirement, present from Level 2 onward, that third-country access to customer data be actively prevented (Annex II, criterion (g)). Since Level 1 is expected to cover the great majority of ordinary public-sector cloud use, most public-sector data processed under CADA sits at the tier with the least specific access protection built into the framework itself. Recital 63 states that the assurance levels do not affect existing EU rules on cross-border cooperation between authorities. PPEU reads this alongside the Commission's wider ProtectEU work on lawful access to data, which envisages new data retention rules and decryption capability for Europol; we draw this connection as an analytical concern rather than as a stated effect of CADA itself, and we consider that the sovereignty framework should clarify explicitly that stronger European control over infrastructure must not become a route to weakening encryption or creating new avenues for generalised access to customer data.

3.3 What the access-control provisions actually require

Annex III sets out the evidence auditors must gather at Levels 2 to 4. Under audit criterion C (data localisation), auditors must obtain evidence that third parties or subcontractors that do not meet the Annex's conditions are, in no circumstances, technically or operationally able to access, obtain or process customer data without prior authorisation. Where a provider is found to be under third-country control and granted the narrow Level 3 derogation under Article 19, Annex III section 7.2 additionally requires evidence that the provider is unable, legally, technically and operationally, to comply with a third-country request to access customer data, including encrypted data, or to disrupt service continuity. These are genuine access-control obligations, and PPEU's earlier characterisation of the framework as silent on access was too broad. But both provisions work by disqualifying actors who fail the Annex's conditions, non-compliant subcontractors, or a third country exercising control over a provider. Neither requires that a certified, compliant provider's own systems be architected so that the provider itself cannot read customer data, and neither addresses what happens when an EU public authority, rather than a third country, seeks access through lawful process. PPEU's assessment is that the framework's access controls are aimed at keeping data away from disqualified outsiders, not at limiting what a compliant provider or an EU authority can do with it.

3.4 The reCAPTCHA parallel, and who has a say

Our earlier position paper on Google Cloud Fraud Defence and CAPTCHA-based surveillance infrastructure showed that a tool presented as "security" can function as a data-collection system, while the people whose data is collected cannot see or contest what is gathered. PPEU's assessment is that CADA carries a comparable risk at a larger scale: a "Union-assured" label tells citizens their data meets a defined standard of protection against disqualified outsiders, but says little about how a compliant provider or a public authority may use it, and citizens have no mechanism under the Act to see or contest that use, only an assurance that it has been supervised. Data protection is mostly left to the GDPR. Level 1, which the impact assessment expects to cover the great majority of ordinary public-sector cloud use, relies on the provider's own self-assessment (Article 19), with data protection authorities asked only to "cooperate" (Recital 59). The Act also encourages sharing public-sector data and AI models across public bodies (Recital 22) and pooling public cloud capacity through the EuroCloud Federation (Articles 34 and 35); PPEU's concern is that keeping police, border and health data in shared systems creates a real risk of that data being reused beyond the purpose it was collected for, against the GDPR's purpose limitation principle. The "open source first" principle (Articles 41 to 44) and the software transparency rules are a welcome exception to this pattern, since they make security checkable rather than merely asserted.

Recommendations

- **R3.1** Even though Annex III already requires that non-compliant subcontractors, and third-country requesters in the Level 3 derogation scenario, be technically and legally barred from accessing customer data, PPEU recommends that the higher assurance levels go further and require that the certified provider's own architecture prevent it from reading customer data by default, for example through customer-held encryption keys.
- **R3.2** Insert explicit language stating that CADA cannot be used to justify weakening encryption or imposing general data retention obligations.
- **R3.3** Require providers at every assurance level to publish transparency reports on government requests for data, from EU and non-EU authorities alike.
- **R3.4** Extend the independent audit requirement currently reserved for Levels 2 to 4 (Article 20) to Level 1, with published results, rather than leaving the most widely used tier to self-assessment alone (Article 19).

- **R3.5** Require any sharing or pooling of sensitive public-sector datasets, particularly police, border and health data, to have a clearly defined purpose, access controls and a specific legal basis, with a prohibition on secondary use for AI training unless separately authorised.
-

Section 4: Market Structure and Decentralisation

4.1 A gate on ownership, largely unchanged market shares

CADA identifies the right problem and, in PPEU's assessment, targets the wrong variable. Recital 46 names the Union's critical strategic dependencies and concentration risks, and Recital 50 lists vendor and technology lock-in and monopoly pricing among the resulting harms, but both are framed as risks arising from foreign control. The Act's central binding mechanism, the four Union assurance levels (Articles 16 to 30, Annex II), sorts providers by ownership, jurisdiction and control; it does not ask how many providers exist in a given market or how easily a customer can leave one.

The impact assessment indicates that existing hyperscalers may be able to qualify for the lower assurance levels through EU-established operations, while the stricter levels impose substantially greater requirements on ownership, personnel and control. Levels 1 and 2 together are expected to cover roughly 90% of public-sector use cases, and the private market, some 86% of total cloud demand, falls entirely outside the framework's mandatory scope. On the Commission's estimates, Levels 3 and 4 could correspond to around 10% of public-sector cloud needs; given the impact assessment's estimate that the public sector accounts for around 14% of cloud demand, this corresponds illustratively to around 1.4% of total cloud demand, a useful indication of scale rather than a literal reservation of market share to EU providers.

European cloud providers represented by CISPE have warned about "sovereignty washing" where European presence or formal compliance is treated as equivalent to genuine sovereignty. Industry critics such as CCIA have separately warned that the framework risks severe market fragmentation and has raised concerns about the treatment of non-EU providers. The Commission's own impact assessment likewise cautions that, absent clear criteria, incumbents are likely to capture the nascent sovereign market.

4.2 Capacity: faster permits, the same builders

Title III accelerates data centre deployment through acceleration zones, 12-month permits and strategic projects (Articles 10 to 14), without asking who builds. None of the strategic-project criteria in Article 14(1) concerns openness, multi-tenant access or SME participation, so a hyperscaler campus can qualify as readily as a smaller, plural alternative. Four hubs already hold 65% of the EU data centre market, and three hyperscalers are expected to drive 65% of demand growth by 2028. The one anti-foreclosure rule (Article 11(2)) applies only inside acceleration zones. The EuroCloud Federation, letting public bodies share their own capacity, is the closest alternative the Act offers to reliance on commercial hyperscalers, but participation remains entirely voluntary (Articles 34 to 36).

4.3 Targets without obligations

Article 33(4) asks Member States to "pursue" a 25% share of cloud and AI procurement for innovative SMEs, with no specific consequence or corrective mechanism stated where that objective is missed. Article 29(9) requires authorities only to "consider" multi-vendor or multi-cloud strategies. The only SME-specific provision in the sovereignty chapter lets SME self-declarations at Level 1 be recognised automatically without national review (Article 17(3)), at the tier where hyperscalers already compete most effectively. At Levels 2 to 4, providers must fund their own annual independent audits (Article 20), which the Commission itself calls an important cost barrier for SMEs. The "Union added value" criteria in Article 32 prioritise contribution to the European cloud and AI supply chain, integration of Union-funded technology and use of EU-manufactured hardware, without giving equivalent weight to interoperability, portability or open standards, though these criteria must remain ancillary and not decisive under Article 32(2)(d). Combined, PPEU expects concentration to persist in two forms: around foreign incumbents in the mainstream market, and around a small number of large EU firms in the sovereignty niche.

4.4 Open source: encouraged, not required

Recital 81 states plainly that access to source code reduces dependency on a single vendor and limits the risk of vendor lock-in. Yet the Act promotes open source without requiring it. Article 41 only asks Member States to "encourage" open standards and open source. Recital 84 still refers to an "open-source assessment," but no operative Article creates a mandatory obligation to conduct one. Publishing public code also remains voluntary under Article 42.

Sovereignty rules may even work against open source: Level 4 excludes software whose development a non-EU entity can materially influence, defined broadly enough to include the ability to influence a component's technical evolution, maintenance priorities or security remediation (Annex II, criterion 4.1(i)(ii)), a definition that could potentially affect community-governed open-source projects where a non-EU entity has material influence over technical evolution, maintenance or security remediation. This matters because community-governed open-source infrastructure is precisely the kind of reusable alternative to proprietary lock-in that Recital 81 says the Act wants to encourage.

Recommendations

- **R4.1** Add openness, multi-tenant access and SME participation to the strategic-project criteria in Article 14(1), and extend the anti-foreclosure rule in Article 11(2) beyond acceleration zones.
 - **R4.2** Make multi-provider architectures or tested exit plans the default for critical public systems, with a duty to justify single-provider choices under Article 29(9).
 - **R4.3** Back the 25% SME objective in Article 33 with comply-or-explain reporting and mandatory contract lots, including within the Commission's own joint procurement activities (Articles 37 to 40).
 - **R4.4** Add award criteria for open standards, interoperability and portability alongside the existing supply-chain and hardware criteria in Article 32.
 - **R4.5** Convert Article 41 into a genuine open-source-first rule, with a mandatory comparative assessment and a public money, public code obligation, and exempt community-governed foundations from the "effective control" exclusion in Annex II criterion 4.1(i)(ii).
 - **R4.6** Ease SME access to the higher assurance levels through pooled or subsidised audits and multi-year validity of audit results.
-

Section 5: Green Compute, Research and Innovation, and Open Innovation

5.1 Greening compute under the Leadership Initiatives

Title II establishes the Cloud and AI Leadership Initiatives, which fund research into energy- and water-efficient data centre technologies: advanced cooling and waste-heat recovery, quantum computing integration, grid integration and AI-powered server utilisation management, with concrete targets including an average Power Usage Effectiveness of 1.15 and average server utilisation of 50% across the Union (Article 4(1), Annex I, Grand Challenge 1). This is a genuine opportunity: it directs public research funding toward the physical constraints, energy, water and grid integration, that Section 2 identifies as the real bottleneck behind Europe's capacity gap. CADA does connect this to capacity expansion to some degree: Article 14(1) allows a project to be designated a strategic project partly on the basis of highly sustainable or innovative features, or a contribution to grid stability. However, that Article requires only two of five listed criteria to be met, and the other three, essential public-sector functions, EU semiconductor integration, and addressing an identified capacity shortage, do not touch sustainability at all. A project can therefore qualify for accelerated permitting and strategic-project status without adopting any of the technologies the Leadership Initiatives are funding.

5.2 Does tripling capacity fit the Union's climate commitments

The Commission states its objective that data centres be climate-neutral and highly energy-efficient by 2030. CADA's tripling target sits alongside this commitment, and alongside Article 11(1)'s requirement that acceleration zones apply the sustainability key performance indicators set under the Energy Efficiency Directive and its delegated rating scheme, but nothing in the Regulation requires the Commission to report whether aggregate capacity growth under CADA remains compatible with the climate-neutral data centre objective as deployment proceeds. Given that EU data centre electricity use already stood at around 70 TWh in 2024, with global data centre electricity demand projected to more than double by 2030, PPEU's assessment is that a tripling of capacity needs an explicit, monitored link to that climate commitment, not merely a

shared reference to the same underlying rating scheme.

5.3 Open source, again: encouraged but not required

As Section 4 sets out in detail regarding market structure, the same gap between recital and Article undermines the green compute and open-innovation agenda. Recital 15 commits the Leadership Initiatives to fostering open standards, open specifications and open-source software foundations, and to creating a catalogue of software tools to build a one-stop shop for open-source resources. Industry commentary on the parallel EU Open Source Strategy, published alongside CADA, reports a dedicated investment envelope including an Open Source Maintenance Instrument for critical shared infrastructure, though we rely on that commentary only for context, not as authority on what CADA itself legally requires. That funding is worth less than it could be if the procurement obligation that would channel public demand toward the resulting open tools remains, as Section 4 documents, a matter of encouragement under Article 41 rather than a requirement.

5.4 Public money, public code: research funding and reuse

Article 42 requires Union entities and public sector bodies that voluntarily decide to make software available for reuse to do so through the EU Open Source Solutions Catalogue, but the decision to share at all remains voluntary. The Cloud and AI Leadership Initiatives fund research into frontier AI, physical AI, industrial AI and public-sector AI models (Articles 3 and 4), much of it through EuroHPC and Horizon Europe co-funding, without a general default that publicly funded research outputs and models be released under open licences. Our manifesto's commitment to open access for publicly funded research and open availability of publicly funded data supports extending that principle to the software and models this Title funds, even though the manifesto does not use the phrase "public money, public code" itself; we present this as an extension of manifesto principle rather than a direct quotation of it. Left unaddressed, this creates a real risk that public investment ends up embedding dependence on proprietary tools and models built with EU funding but controlled by whichever private partner delivers the research, reproducing the dependency problem CADA is meant to solve through the research budget rather than the procurement budget.

Recommendations

- Require any data centre benefiting from accelerated permitting or strategic-project status under Article 14 to demonstrate adoption of, or a funded pathway toward, the energy and water efficiency technologies and targets supported under Article 4(1) and Annex I, rather than treating research funding and capacity acceleration as unconnected tracks.
- Require the Commission to report, as part of its capacity-gap monitoring under Article 15, whether aggregate data centre capacity growth under CADA remains on track with the Union's climate-neutral-by-2030 data centre objective.
- Adopt the same recommendation as Section 4 (R4.5): convert Article 41 into a binding open-source-first procurement rule so that Open Source Strategy funding and CADA procurement obligations reinforce rather than bypass each other.
- Establish a default, public money, public code requirement for software and models developed with Cloud and AI Leadership Initiative funding, with reuse through the EU Open Source Solutions Catalogue as the default rather than a voluntary option under Article 42.
- Exempt community-governed open-source foundations from the "effective control" exclusion in Annex II criterion 4.1(i)(ii), consistent with Section 4's recommendation (R4.5), so that publicly funded research is not steered away from the open, reusable infrastructure Recital 81 identifies as the way to reduce vendor lock-in.

Conclusion

The European Pirate Party believes that digital infrastructure is a common good, and that expanding Europe's cloud and AI capacity is a legitimate and necessary objective. The rights to privacy, data protection and equal access are fundamental rights, not optional policy preferences, and the institutions that govern Europe's digital infrastructure must remain transparent, accountable and open to public scrutiny as that infrastructure grows.

CADA contains genuine opportunities: its support for green compute research, its EuroCloud Federation as a public-sector alternative, and its open-source-first language all point in the right direction. Our assessment is that, as currently drafted, the Act risks expanding Europe's data centre capacity through much the same concentrated market it says it wants to reduce dependence on; accelerating permits faster than environmental and grid safeguards can be verified; building a sovereignty framework whose access controls are aimed at disqualified outsiders rather than at what a compliant provider or a public authority may do with the data; and leaving its own green and open-source commitments as encouragements rather than obligations.

The areas where we see the greatest opportunity for improvement are clear: requiring public transparency over who benefits from accelerated investment and on what terms; grounding the tripling target and its permitting shortcuts in verified, regularly published evidence and mandatory environmental and social impact assessment with a defined public consultation stage; extending the Act's existing access-control provisions so that they also address what a compliant provider or a public authority may do with customer data, not only who is excluded from it; converting SME, interoperability and open-source provisions from encouragements into obligations; and tying green-compute research funding directly to the capacity expansion it is meant to inform.

References

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, 3 June 2026, including Annexes 1 to 3. <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
2. European Pirate Party Manifesto. <https://europeanpirates.eu/manifesto/>
3. European Commission, *Commission Staff Working Document accompanying the Cloud and AI Development Act (Impact Assessment)*, SWD(2026) 502 final. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502>
4. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). <http://data.europa.eu/eli/reg/2016/679/oj>
5. Charter of Fundamental Rights of the European Union (2012/C 326/02). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT>
6. European Economic and Social Committee, *Opinion on the Cloud and AI Development Act* (INT/1126), adopted 23 September 2026. <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cloud-and-ai-development-act>
7. Computer & Communications Industry Association (CCIA), *Discriminatory EU Cloud and AI Development Act Risks Severe Market Fragmentation*, June 2026. <https://ccianet.org/news/2026/06/discriminatory-eu-cloud-and-ai-development-act-risks-severe-market-fragmentation/>
8. European Commission, *In focus: Data centres – an energy-hungry challenge*, 17 November 2025 (citing International Energy Agency estimates). https://energy.ec.europa.eu/news/focus-data-centres-energy-hungry-challenge-2025-11-17_en
9. European Pirate Party, position paper on Google Cloud Fraud Defence and CAPTCHA-based surveillance infrastructure, 2026 (internal PPEU reference).
10. European Commission, *Cloud computing*, Shaping Europe's digital future. <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing>
11. SUSE, *EU Cloud and AI Development Act: A Major Step for Open Source*, 16 June 2026 (industry commentary, cited for context only). <https://www.suse.com/c/eu-cloud-ai-development-act-open-source-first/>

12. CISPE, *Put Cloud Sovereignty, Resilience, and Fair Competition at the Heart of CADA*, 17 March 2026. <https://www.cispe.cloud/cloud-sovereignty-letter-march-2026>