France Digitale's answer to the Commission's consultation on the Cloud and AI Development Act (CADA) — COM(2026) 502

November 2026

About France Digitale: Founded in 2012, France Digitale is the largest startup association in Europe, bringing together over 2,000 startups, investors and incubators. The association's goal is to enable startups to scale across the EU single market and help build Europe's tech champions.

Introduction

France Digitale welcomes the declared shift of the EU from a reactive to an assertive and proactive approach grounded in technological sovereignty. We subscribe to the definition of tech sovereignty as "staying ahead in critical technologies, lowering our exposure in terms of existing strategic dependencies, and avoiding new dependencies that third countries can weaponise". We agree that tech sovereignty is "grounded in openness, partnership and fair competition".

We welcome the boost of homegrown innovation and industrial capacity at each step of the supply chain of digital technologies, progressing towards a full European technology stack and diversifying suppliers. We agree with digital technology to be "interoperable, portable and based on the widespread adoption of open standards, to ensure that public and private users can choose, switch and scale technological solutions without prohibitive costs".

We support the Tech Sovereignty Package's 360-degree approach: strengthening Europe's ability to develop critical technologies across the entire value chain, from chips, to cloud and AI, while also stimulating demand, particularly through public procurement. Creating a strong market for European technologies is essential for innovative companies to scale and deploy their technologies on the continent. We therefore welcome the Commission's ambition to simplify procurement procedures.

Regarding cloud public procurement, we welcome the Package's gradual approach, providing for a coherent and coordinated European strategy to help the EU cloud ecosystem scale, moving away from fragmented national initiatives. Stability is provided by a single European framework rather than 27 different ones.
This framework responds to a European imperative: to shield against the risks associated with the EU's dependence on non-European technologies and, gradually, to steer the most critical uses towards more sovereign and secure solutions.
A European preference in public procurement should be extended to the entire digital sector. Indeed, public procurement is a powerful lever to stimulate the vibrant European digital ecosystem, enabling our companies to develop and achieve the critical mass needed to compete globally and contribute to social and economic progress for the whole society.

France Digitale represents the entire European tech value chain: European cloud and infrastructure providers, and thousands of European startups and scaleups that build applications, often on non-European infrastructure. CADA and European preference

measures must favour all of them as long as they are European and bring value to our economy and society. We therefore propose that the framework considers three points: (i) if the actor is European. An actor should be considered European when its headquarters are in Europe and it is not directly or indirectly controlled by a third-country entity (within the meaning of decisive influence under Regulation (EC) No 139/2004, so that minority stakes held by non-EU investors do not, in themselves, disqualify a European company), regardless of the nationality of its own suppliers or the existence of non-EU subsidiaries. (ii) the level of assurance that the cloud service offers, which depends on data protection, jurisdictional exposure and control of the technology, and is where criteria for the infrastructure layer belong. (iii) the level required by a given contract, that should be determined by the sensitivity of the data and the use case, so that the highest levels apply only where they are genuinely needed. Keeping these three points separate is how CADA can reward European infrastructure providers without excluding European application providers from public procurement.

I. The Union Assurance Levels framework (Articles 16-28 and Annex II)

1. The four-level structure: sound in principle, but the risk of sovereignty-washing must be addressed

We support the four-level structure, that provides nuance and flexibility for buyers and makes room for market players who have put in place operational measures to strengthen European control.
That said, with a view to a genuinely proactive public policy on strategic autonomy, we believe it is imperative to allow for a clear distinction between genuinely European cloud providers and those relying on technology not controlled within the EU. A preliminary assessment suggests that most providers could achieve Level 3, without European cloud providers being able to truly set themselves apart within that level. This is counterproductive if the aim of CADA is to increase the market share of European cloud providers while bringing clarity and transparency to organisations.
What matters above all is that European cloud providers are able to genuinely differentiate themselves.
In principle, and following the example of DG DIGIT's Cloud Sovereignty Framework, it may be appropriate to allow Level 2 to be achievable by all providers, including hybrid offerings with non-EU services, if they can implement safeguards against unauthorised access to Union data and disruption of service quality or continuity; a Level 3 reserved for European providers that have genuine control over their technology, and a Level 4 requiring full European legal and operational control and an entirely European value chain for certain highly sensitive use cases. The framework must also protect public buyers against the dependency risks created by non-sovereign actors, including joint ventures between European and third-country companies. A service operated by a European entity but jointly controlled by, or technologically dependent on, a third-country partner remains exposed to that partner's jurisdiction, licence decisions and commercial choices. Where a third-country entity exercises decisive influence over a joint venture, within the meaning set out in the introduction, the joint venture should not be eligible for Level 3 or Level 4.
This differentiation regards the infrastructure layer: it should not, in itself, exclude European application providers from contracts that do not genuinely require Level 3 or 4, in line with the distinction set out in the introduction.

Reserving the higher levels for genuinely European providers must not confine them to those levels. Many public contracts will require Level 1 or 2, and European providers must be able to compete for that entire market, not only for the most sensitive use cases. Union added-value criteria should therefore apply in all public tenders covered by CADA, whatever the assurance level required, so that European providers and application developers are rewarded across the whole market rather than in a narrow segment of it.

In addition to that, the criteria relating to added value, or 'European preference', are not sufficiently developed, and their weighting is too low. If the aim of the framework is to provide greater European oversight, the European preference must constitute a genuine industrial policy, enabling the emergence of European champions of excellence in innovation. The text's ambitions fall short in two respects: on the one hand, they are not ambitious enough; on the other, they do not allow for the implementation of a genuine European preference, since the criteria, as they stand, could open the door to non-European players with the means to invest in the EU. In practical terms, this framework risks continuing to favour large players with the capacity for massive investment in Europe.
We believe it is necessary to strengthen the text as follows:

- Public procurement should take European added value into account and mechanisms more conducive to European innovation in cloud computing and AI should be created (see 'joint procurement' and the mechanism for calling for the development of services);
- The added-value criteria should more decisively favour European players, without opening a back door for non-European players;
- Contracting authorities must be granted the flexibility to adjust the weighting of the Union value added criteria based on the specific scope, strategic importance and market context of each tender. The one-size-fits-all approach of the current 15-point cap disregards the diverse needs of contracting authorities. Therefore, we advocate for the removal of the 15-point cap, allowing contracting authorities to determine the weighting of Union value added criteria in their procurement evaluation methodologies.

Broad exceptions would hollow out the sovereignty framework. We call for exceptions under Articles 18 and 30 to be limited to the current Levels 1 and 2, and not to apply to Levels 3 and/or 4. Case-by-case derogations in article 30(4) may cause systematic requests from public buyers and recreate the fragmentation CADA seeks to end. Legitimate transition needs should instead be addressed through a longer default migration window, as set out in Section I.4, and a short, closed list of exceptions in Article 18. That list would cover duly justified extensions for complex migrations and for regulated products subject to sector-specific change procedures.

2. Encryption and resilience: two critical gaps in Annex II

France Digitale's members flag two significant technical omissions in Annex II that could undermine the sovereignty framework's practical credibility.

First, data encryption is absent as a standalone criterion across all four assurance levels, yet it is widely regarded by cloud security professionals as one of the most effective

technical measures for making data practically inaccessible to a foreign entity or jurisdiction, even when it is physically present in EU infrastructure. A foreign-controlled provider can comply with the data-localisation criteria at Level 2 while still leaving customer data accessible to a foreign parent through software backdoors, key-escrow arrangements, or privileged administrative access, none of which the current Annex II criteria explicitly prevent. Encryption at rest and in transit, with key management by a trusted partner or the customer itself, should be added as a technical criterion, at least from Level 2 onwards.

Second, the Annex contains no mention of resilience: there is no requirement for geographic distribution of data-centre infrastructure, redundant connectivity, or defined recovery-time and recovery-point objectives. For critical applications, a cloud service that stores data exclusively in the EU but in a single data centre in one city provides very different operational continuity guarantees than one distributed across multiple sites in multiple Member States and/or geographies. The sovereignty framework will not fulfil its stated purpose of protecting essential public functions if a single incident (technical failure, extreme weather or targeted attack) can take down a certified Level 3 or Level 4 service entirely.

3. Certification validity and periodic review

The CADA certification should be time-limited, for example to three years. There should be periodic and proportionate surveillance reviews, but also early and mandatory reviews in the event of a major change affecting the product or the company's governance. This would ensure that recognition remains a living instrument tracking the actual state of the provider's compliance, rather than a one-time gate that becomes stale.

The audit cycle should be aligned with the certification period and extended from 18 months to three years. This would allow providers to reuse elements from audits - to the extent that it covers equivalent requirements and the same service and components - already under way under existing national schemes, such as SecNumCloud and C5, rather than duplicating assessments at short intervals and significant cost, especially for SMEs and SMCs. It would also give smaller European providers a predictable compliance horizon.

On the other hand, reviewing the criteria every three years (Art. 16(3)) can create uncertainty for companies. To sum up, the criteria should be stable and the certification should be time-limited to 3 years.

4. Migration timelines, transition costs and subcontractor uncertainty

Three practical implementation issues risk making the sovereignty framework unworkable. The first concerns migration timelines. Where existing contracts with non-qualifying providers are in place, a 12-month mandatory migration window does not reflect the 18 to 24 months that migrating a complex public-sector workload realistically requires. A 12-month deadline will either force technically premature migrations that create service instability, or generate waves of derogation requests under Article 30(4) that hollow out the framework's credibility. The default migration window should be set at 24 months, with the possibility of a further extension in duly justified cases involving critical

infrastructure or complex multi-system environments. For regulated products, such as medical-device software under Regulation (EU) 2017/745 (MDR), a change of hosting infrastructure may require a significant-change assessment, re-validation and, where applicable, notified-body involvement, as well as re-certification of the hosting arrangement (e.g., HDS certification in France). Migration timelines should expressly account for these sector-specific procedures.

The second concerns the intersection of CADA's assurance levels with existing national certification requirements such as Germany's BSI C5 and GDPR-specific obligations. The Commission should be required to publish compatibility guidance for major national frameworks within 12 months of CADA's entry into force.

The third concerns Annex III's treatment of subcontractors. As currently drafted, Annex III creates significant uncertainty about the depth to which subcontractors must be audited, how far down the subcontracting chain obligations extend, and what documentary evidence an auditing organisation will require. The Commission should publish, alongside the delegated act updating Annex III, a non-binding interpretive guidance document clarifying the scope of the subcontractor audit trail and establishing a proportionality principle calibrated to the materiality of each subcontractor's role in the provision of the service.

The proposal will create a very large market for audit firms and potentially high costs especially for European SMEs and SMCs. This calls for greater transparency on who audits whom, at what cost and under which methodology. Auditing organisations should be validated on the basis of common EU criteria, with mutual recognition across Member States to prevent « forum shopping » and safeguards for their independence and no conflicts of interest.

5. How AI services fit within the cloud definition and the assurance levels

France Digitale calls on the co-legislators to clarify to what extent AI services fall within the scope of CADA's definition of "cloud computing service" and, consequently, of the Union assurance levels. The proposal is built on a cloud-infrastructure logic, yet public buyers will increasingly procure AI capabilities delivered as a service: access to foundation models via API, inference services, AI development and deployment platforms, and AI agents embedded in business workflows.
As currently drafted, it is unclear:

- whether model access, inference and fine-tuning services are "cloud computing services" in their own right, or only when bundled with the underlying infrastructure;
- how the assurance-level criteria apply when an AI service built by a European provider runs on non-European infrastructure, or when a non-European model is hosted on European infrastructure;
- which layer of the stack (infrastructure, platform, model or application) determines the assurance level of the service as a whole;
- how AI agents, which may call multiple models and third-party services, should be assessed.

Without this clarification, public buyers will either exclude AI services from the framework altogether or apply the strictest level by default, both of which would harm European AI

providers. We therefore ask the co-legislators to specify, in the recitals and in implementing guidance, how each layer of the AI stack is treated under the definition of "cloud computing service" and under the assurance levels.

6. Enforcement: a centralised assessment for the largest providers

The enforcement structure currently envisaged for the cloud sovereignty framework could undermine CADA's objectives. Under the proposal, national authorities would assess cloud providers' assurance levels. This is likely to lead to fragmented implementation, and to assessments shaped by economic or political pressures rather than by sovereignty considerations.

The same risk applies to the scope of the obligations. Member State authorities would also determine which public-sector activities require Levels 2, 3 and 4. A Member State could therefore set a very low bar, allowing non-European hyperscalers to win the vast majority of public contracts, even in areas relevant to national security and sovereignty.

Member States hosting the European headquarters of the largest non-European cloud providers would be responsible for assessing them, while depending heavily on those same companies for investment and tax revenue. This creates strong incentives to under-enforce.

Enforcement may also be distorted by geopolitical pressure. Third-country governments have already threatened tariffs and export restrictions against countries that adopt digital regulations or digital taxes. Individual Member States may be tempted to prioritise avoiding such pressure over Europe's cloud sovereignty goals. The combined economic and political weight of the Union is better placed to withstand it.

Peers' assessments between Member States is insufficient to ensure a coherent enforcement at European level, as it would politicise the process even more. This risk should be addressed through the binding EU framework and common list proposed in Section III.1.

Following the model of the Digital Markets Act and of the Digital Services Act for very large platforms, we suggest that the Commission itself assess the cloud service providers that meet defined size criteria, such as turnover and market capitalisation (Article 17). National authorities would remain competent for all other providers, including SMEs and scaleups, which benefit from proximity and national-language procedures.

II. The EUCS deadlock must be broken: existing national schemes cannot substitute for genuine European harmonisation

France Digitale is concerned by the current state of the European Union Cloud Services certification scheme (EUCS) under the Cybersecurity Act revision. Several Member States have developed their national cloud security certification or qualification frameworks (such as France's SecNumCloud and Germany's C5), which became reference standards for their respective domestic markets. But the existence of national schemes is not a solution to the absence of a European one; it is precisely the problem. A French public body procuring cloud services under SecNumCloud and a German counterpart procuring

under C5 are applying criteria that diverge. The result is that a European cloud provider seeking to serve public-sector customers across multiple Member States must currently qualify under several different national frameworks simultaneously, at significant cost and with no guarantee of mutual recognition.

Meanwhile, the EUCS process at ENISA level has been effectively blocked for years, largely because sovereignty criteria proved politically intractable within the certification framework itself. CADA resolves that political deadlock by relocating sovereignty criteria into procurement law rather than cybersecurity certification, which is the right architectural decision; but it does so by making CADA's higher assurance levels *contingent* on a future EUCS scheme that does not yet exist, leaving Levels 2, 3, and 4 dependent on a fallback cascade of national schemes that are themselves fragmented.

France Digitale calls on the EU Institutions, the Commission in primis, to treat the completion of EUCS as an urgent legislative priority running in parallel with CADA's negotiation, and on co-legislators to set a binding deadline by which the Commission must either have adopted an EUCS scheme under the Cybersecurity Act revision or proposed a legislative amendment specifying a binding Union-wide cybersecurity standard that substitutes for it.

III. Public procurement (Articles 29–33)

1. Risk assessments must be harmonised at European level

Article 29 requires every Member State to conduct its own risk assessment to identify which public-sector activities contribute to the preservation of public order and therefore trigger higher-level procurement obligations. France Digitale regards this architecture as a significant structural flaw that risks reintroducing through the back door the fragmentation that CADA was meant to eliminate. If each Member State applies its own methodology to determine which activities are "public-order-critical", including which sectors, which thresholds and which data categories qualify, European cloud and AI providers will once again face 27 different compliance environments when selling to public bodies across the Union. The history of NIS2 transposition alone demonstrates how quickly a harmonised framework fractures under national implementation.

We call on co-legislators to amend Article 29 so that the Commission's methodology-setting role, currently limited to an implementing act on how assessments are conducted, is elevated to a binding framework that also establishes a common list of data categories and activities that are public-order-critical across all Member States, while ensuring coherence with already existing regulations. It would be preferable to have a common set of practices at European level, or even a common set of use cases, a shared methodology, or at the very least a process to ensure overall consistency across Europe. With regards to audits and the service providers responsible for carrying them out, there will need to be European-wide harmonisation of practices and methods for assessing suppliers.

2. The public sector's duty to lead by example and to give industry the time to follow

France Digitale considers that public administrations have a political and financial duty to procure from European cloud providers: they cannot credibly champion digital sovereignty while continuing to pour public money into the non-European hyperscalers that create the dependency they claim to want to reduce. The risk-assessment and procurement obligations under Articles 29 and 30 are therefore welcomed.

However, this obligation must fall asymmetrically on public bodies, not on the private sector companies. European startups and scaleups that today rely on non-European cloud infrastructure to build and deliver their innovative products should not be compelled to undertake costly and disruptive migrations on an arbitrary calendar, especially when equivalent European services are not yet available across all segments. The obligation to migrate should be structured so that it applies first and most urgently to public bodies themselves, as both a signal of political commitment and a way of generating the demand and revenue that will allow European providers to scale, while transition timelines for private-sector companies remain proportionate, voluntary where appropriate, and accompanied by real financial and technical support mechanisms. Sovereignty in cloud procurement should be built from the demand outward, not imposed downward, especially to innovative companies.

This distinction matters because public buyers and innovative companies do not share the same use cases, constraints or responsibilities. Public administrations manage taxpayers' money and public data: their procurement choices carry a democratic and strategic dimension and directing that spending toward European providers with genuine European added value is both legitimate and necessary. Innovative companies, by contrast, operate under a different primary obligation, that is to pioneer and scale as fast as possible. Forcing startups and scaleups to choose their cloud provider on sovereignty grounds rather than on the basis of technical fit, performance or cost, risks slowing their innovation and growth. CADA should therefore draw a clear and durable line between the procurement obligations that fall on public buyers and the treatment of private-sector companies, for whom sovereignty-aligned choices should be encouraged and supported, but never mandated.

The priority must be to ensure Europe's capacity to build, switch and compete globally. Directing public procurement toward European alternatives where they are competitive is a useful lever, mandating where private firms buy their technology is not. In the current proposal, Article 31(3) would let the Commission extend binding cloud requirements to private companies in critical sectors, including financial and health services, without a real debate and vote. Any extension to private companies needs a full legislative process. Financial services firms are already under comprehensive rules on technology risk and resilience under DORA, in force since January 2025. Similarly, in the health sector, companies are already subject to strict and specific requirements, and rightly so given the sensitivity of the data they process: health-data hosting certification schemes (such as the French HDS certification, which already requires health data to be hosted within the EEA and transparency on the risks of access by third-country authorities), the Medical Device Regulation for medical-device software, the AI Act's high-risk regime for AI-enabled medical devices, NIS2 and the European Health Data Space Regulation. Nonetheless, adding a separate cloud sovereignty obligation on top through a delegated act creates

duplicate requirements and legal uncertainty without additional security gain. Where a sector-specific scheme already addresses data localisation and third-country access, CADA should grant a presumption of conformity with the corresponding assurance level rather than add a new compliance layer.

3. Empower contracting authorities to freely establish the maximum weighting allocated to the Union value added criteria

CADA imposes a cap on the Union value added criteria weighting in public procurement evaluation methodologies, limiting it to a maximum of only 15 out of 120 points. This restrictive threshold undermines the effectiveness of an otherwise commendable initiative by constraining the ability of contracting authorities to prioritise European digital goods and services. In doing so, it fails to provide the necessary leverage to foster the development of a robust and competitive European digital sector aiming to compete globally.

While we acknowledge the intent to uphold the primacy of technical and financial criteria in procurement decisions, we believe that such restriction is counterproductive. Contracting authorities must be granted the flexibility to adjust the weighting of the Union value added criteria based on the specific scope, strategic importance and market context of each tender. The one-size-fits-all approach of the current 15-point cap disregards the diverse needs of contracting authorities. Therefore, we advocate for the removal of the 15-point cap, allowing contracting authorities to determine the weighting of Union value added criteria in their procurement evaluation methodologies.

4. SME procurement target

The award of 25% of public contracts to SMEs is useful for the development of the European innovation ecosystem. It is a much clearer threshold than the value-added criteria mentioned in Article 32 and provides a decisive means of meeting the objective of helping smaller players to grow. Nonetheless, it is key to specify what criteria are taken into account to determine the 25%: whether it is measured by cost, by number of contractual entities, by usage, or on some other basis. It will also be necessary to reassess this threshold in light of practices observed in Member States and to ensure that such an ambitious target does not lead to negative side effects, such as more costly solutions for public procurers or an incentive for certain companies to remain artificially below the SME threshold in order to continue benefiting from the quota rather than growing.

5. Keeping public procurement open to European startups

It is key that CADA does not become a compliance burden that narrows the EU's competitive position. The risk is that all public entities will require the higher level of requirements for the entirety of their activities, thus excluding the majority of European startups from their procurement.
Consider a hospital procuring AI services: rather than conducting risk-specific sovereignty assessments, procurement teams will likely apply the highest sovereignty level uniformly across all vendors and services. This means a low-risk AI service will still require the vendor to meet Level 4 requirements. Multiply this across every hospital, school and public institution in the EU, and you see why European startups could de facto be excluded from public sector procurement. The issue is all the more acute in healthcare, where digital

services such as remote patient monitoring are frequently not procured through classic public tenders but financed through national health-insurance reimbursement, with the hospital acting as the clinical operator. CADA should clarify whether, and how, such arrangements fall within the scope of Articles 29-33, to avoid each hospital adopting its own interpretation.

Beyond the regulatory framework, the EU should:

- **Reshape procurement to favour innovation and startups**: current public sector procurement rules disadvantage European companies, startups and innovation.
- **Support startups in navigating existing law:** strengthen public resources to help companies comply with the EU Digital Rulebook, including legislation like GDPR, the AI Act, etc.

A huge barrier to procuring from European companies is access: startups need the same early visibility with public sector buyers that incumbents already enjoy, and the pre-procurement process must be simplified so that procurement teams across thousands of public bodies can actually engage with innovative firms. Effective procurement reform requires changing how buyers source and evaluate providers rather than adding more compliance layers.

IV. Data centres (Articles 10–15)

The target of tripling the capacity of EU data centres by 2030 is relevant because the EU must demonstrate genuine ambition in this field, both in terms of establishing new infrastructure and expanding existing capacity. Expanding and modernising existing data centres is often faster, cheaper and better accepted locally than building new ones, and should be supported on an equal footing, if not prioritised before the creation of new data centres.
The development of AI and digital applications creates this need, and it is essential that the EU puts in place a plan to support this growth.

Nevertheless, the side effects of deploying data centres in dedicated acceleration zones within each Member State must be anticipated. In particular, accelerating deployment should not mean accelerating dependence:

- The reservation, or even pre-emption, of critical resources (water, electricity, land) by players with considerable financial resources. European measures will need to ensure that European players can continue to develop within the Union and limit the land and electricity speculation that would result. This is an absolutely crucial issue, as data centres are essential to cloud and AI activities: leaving the field open solely to foreign investors would mean excluding European players from the market.
- Fast-track procedures risk benefiting only the players with the greatest financial capacity, and hyperscalers in particular. Access to them should take European value into account, giving priority to projects with a true European added value.
- Local acceptance, given that the rise in local protests is a tangible reality: environmental criteria and transparency standards need to be taken into account.

Energy-efficiency criteria should rely on the existing framework under the Energy Efficiency Directive, including its data-centre reporting scheme, rather than create new CADA-specific requirements.
- Europe's AI and cloud capacities should not rely on very large data centres alone. Frugal AI, meaning models and software that reduce the compute, memory and energy needed for each task, can deliver equivalent results with far fewer resources. CADA should support it alongside infrastructure investment, in line with Section V.
- Operators' freedom to choose their location: decisions on where to set up and how to develop data centres must remain in the hands of the operators themselves.
- Both national and local energy plans need to be put in place to ensure a fair allocation of energy and to avoid excluding European players.

We therefore advocate for:
1. Prioritising European-controlled capacity in Acceleration Zones (Art. 10–13):
- Prioritise projects that demonstrably expand capacity for European-controlled cloud and AI providers or services capable of meeting the two highest assurance levels, as well as projects that deliver Union added value.
- Ensure an effective 12-month deadline covering the full permitting process, with limited grounds for stopping the clock. Maintain links with the Environmental Omnibus to allow joint assessments at acceleration-zone level.
- Ensure acceleration-zone rules also facilitate the expansion of existing data centres, including simplified permitting for extensions and consideration of existing grid and site infrastructure.
- Ensure balanced access to scarce land, power and water across different project sizes, with safeguards preventing individual mega-projects from reserving disproportionate capacity.
- Allocate scarce grid capacity on a "first ready, first served" basis with milestone-based ramp-up periods.

2. Reserve strategic-project status for projects delivering European value (Art. 14):
- Add two additional criteria to the five already proposed in Article 14: (1) compliance with the Energy Efficiency Directive's data centre sustainability indicators; and (2) contribution to Union added value.
- Require strategic data centre projects to meet at least four of the seven criteria, instead of two out of five criteria in the initial proposition.

V. The Cloud and AI Leadership Initiatives (Articles 3–9)

The proposed innovation framework provides a relevant basis for strengthening EU cloud and AI capabilities. However, its effectiveness depends on the degree to which European providers are integrated into national strategies, procurement and funding mechanisms.

On the Centres for AI (Article 5): before this network is mandated, the Commission should clarify how these Centres differ in practice from the AI factories and AI gigafactories already being deployed. We consider that already existing structures should be improved and shown to be effective before creating new ones. Centres for AI could be built as an evolution of existing EDIHs rather than as parallel new entities.

Frontier AI support under Article 9 should also be extended beyond training capacity to include inference, fine-tuning and sovereign cloud infrastructure. Public funding should be aligned with the development of an integrated European AI and cloud ecosystem more broadly.

Quantum technologies can contribute to more efficient cloud and AI infrastructure, notably by helping to optimise the use of resources and data-centre operations. France Digitale therefore supports their inclusion in CADA, in particular in the research initiatives, testbeds and strategic projects foreseen by the text, as well as the development and deployment of quantum and other efficiency-enhancing AI software that reduces compute, energy and data requirements for AI workloads across the Union.

CADA's Leadership Initiatives and procurement rules should also be aligned with the EU Quantum Strategy, and national quantum and AI strategies should be as coherent as possible with the European ambition.

VI. Regulatory consistency and AI agents

In an already dense and complex regulatory landscape, coherence with existing regulations and avoidance of redundant obligations must be ensured.
Numerous legislative pieces pursue complementary objectives, including among others the NIS2 Directive, the Digital Operational Resilience Act (DORA) Regulation, the Cybersecurity Act, the Data Act, the AI Act or the Cyber Resilience Act.
The co-legislators need to avoid creating a parallel compliance regime with duplicative audits, risk assessments, controls, or documentation where they address equivalent risks, thereby imposing unnecessary administrative burden and an increase in regulatory costs.
We call to allow existing audits, certifications, evaluations and evidence to be reused when they cover equivalent requirements, with any additional oversight limited to CADA-specific criteria.

CADA introduces its own definition of an "AI agent" that sits alongside, and differs from, the AI Act's definition of an "AI system." For companies deploying autonomous AI in regulated workflows, two overlapping definitions create uncertainty about which rules apply. CADA should refer to the AI Act rather than add a parallel concept. The same logic runs across the whole package: where a firm already meets GDPR, DORA or the AI Act rules for a given service, CADA should not add a separate compliance layer for the same service.
The treatment of AI agents under the assurance levels should be clarified as set out in Section I.5.

VII. Open source (Article 41)

Open source can strengthen European technological sovereignty by reducing dependence on a small number of dominant, closed non-European vendors. It allows users, businesses and public bodies to inspect, audit and modify code, which improves trust and security. It also strengthens competition, as new market entrants can build on open components without licensing barriers, lowering costs and entry barriers for SMEs and startups.

The measures proposed in the Tech Sovereignty Package, such as the OSS Registry and strengthened Open Source Program Offices, are steps in the right direction, but these should be strengthened in hard law too.

Article 41 merely encourages the use of open-source components and provides broad derogations. We propose turning this encouragement into an obligation for public buyers to examine whether qualified open-source solutions exist. Open-source and proprietary European solutions should compete on equal terms, on the basis of technical fit, performance, cost and Union added value.

VIII. Beyond CADA: complementary instruments and a coordinated European approach

Alongside the CADA regulation, non-regulatory instruments could complement its objectives: coordinated EU public procurement and funding calls for cloud infrastructure; guidelines to contracting authorities supporting open-source cloud and AI infrastructure, together with European actors, as a default for publicly funded software; development of a European reference architecture ("European AI stack") to improve interoperability and reduce fragmentation, and stronger education and skills initiatives for public buyers, to support adoption of European cloud and AI technologies.

CADA will only deliver on its objectives if it is part of a joint approach that combines industrial, innovation and competition policies. If the EU intends to address its external dependencies seriously, these instruments must work hand in hand and be implemented coherently and consistently.

Competition policy is needed to ensure that industrial policy measures are not wasted in markets where dominant firms are protected by anticompetitive practices. Trade policy is needed to protect nascent industries from external shocks and supply-chain disruptions and to secure alternatives to concentrated non-European infrastructure.

Two further pillars are essential: EU Inc, which would allow European companies to raise funds and scale across the Single Market under a single set of rules, and the Savings and Investments Union, to channel European savings towards European growth companies, so that they no longer depend on non-European capital to scale.

Within this framework, a European preference should strengthen the whole European value chain, from infrastructure and cloud providers to the startups and scaleups building applications on top of them. The aim is not to close the European market, but to ensure that European companies can compete on fair terms at global level.

Conclusion and recommendations

France Digitale welcomes CADA as a decisive step towards a coherent European approach to cloud and AI sovereignty. By replacing 27 fragmented national approaches with a single framework, and by using public procurement to create demand for European

technologies, the proposal can help European companies reach the scale they need to compete globally.
To deliver on this ambition, CADA must reward the entire European value chain, from cloud and infrastructure providers to the thousands of startups and scaleups building applications on top of them. This requires keeping three questions distinct: whether an actor is European, what level of assurance a service offers, and what level a given contract genuinely requires.
On this basis, France Digitale calls on the co-legislators to:

- give genuinely European providers a clear way to stand out, by reserving the highest assurance levels to them, closing the door to sovereignty-washing and limiting exceptions;
- make Union added value a real lever across all public tenders;
- ensure the highest levels apply only where data and use cases truly require them, so that European startups are not excluded from public procurement;
- guarantee consistent enforcement across Member States, entrusting the Commission with the assessment of the largest providers;
- keep compliance proportionate and predictable, through stable criteria, longer audit cycles and the reuse of existing certifications and audits;
- steer the expansion of data-centre capacity towards European-controlled projects.

CADA will be all the more effective if it is part of a coordinated European approach, alongside competition and trade policy, EU Inc and the Savings and Investments Union. France Digitale and its members stand ready to work with the co-legislators to make CADA a framework that builds European capability, rather than one that simply certifies it.

Here below are our suggestions to improve the current CADA proposal:

On Union assurance levels (Articles 16-28 and Annex II):

- Clarify and strengthen criteria excluding direct or indirect third-country control (including via joint ventures between EU and third-country companies) from levels 3 and 4.
- Limit exceptions under Articles 18 and 30 to Levels 1 and 2.
- Add encryption at rest and in transit, with key management by a trusted third party or the customer itself, as an explicit criterion from Level 2 onwards.
- Add resilience criteria (geographic distribution, redundancy, recovery objectives) from Level 2 onwards.
- Make certifications time-limited (e.g., three years) with mandatory early review on material change.
- Clarify Annex III's subcontractor audit scope through a proportionality-based interpretive guidance document.
- Strengthen independence and transparency requirements for auditing organisations, which should be validated on the basis of common EU criteria, with mutual recognition across EU Member States.
- Clarify how models, inference, AI platforms and AI agents fall within the definition of "cloud computing service" and how the assurance levels apply to each layer of the AI stack.

- Entrust the Commission with the assessment of cloud service providers meeting defined size and economic-power criteria (turnover, market capitalisation), as for gatekeepers in the DMA and DSA. National authorities will remain competent for other providers.

On EUCS:

- Set a binding deadline for the Commission to either adopt an EUCS scheme or propose a Union-wide statutory substitute.

On public procurement (Articles 29-33):

- Elevate the Article 29 methodology to a binding framework with a common list of public-order-critical data categories and activities.
- Ensure procurement obligations fall asymmetrically on public bodies first, with voluntary and time-supported transitions for the private sector. In this case, set the default migration window at 24 months and ensure guidance and support for this transition, taking into account sector-specific change-management procedures for regulated products.
- Remove the 15-point cap, allowing contracting authorities to determine the weighting of Union value added criteria in their procurement evaluation methodologies.
- Specify the measurement basis for the 25% SME procurement target and monitor it with genuine accountability mechanisms.
- Define Union added-value criteria more precisely and mandate Commission guidelines for their consistent application.
- Require any extension of cloud sovereignty obligations to private companies to go through a full legislative process.
- Grant a presumption of conformity with the relevant assurance level to services already certified under sector-specific schemes addressing data localisation and third-country access (e.g. health-data hosting certification).

On open source (Article 41):

- The encouragement set out in Article 41 should be turned into an obligation for public buyers to examine whether qualified open-source solutions, or proprietary European solutions, exist.

On data centres (Articles 10-15):

- Harmonise permitting frameworks with binding EU-level minimum standards.
- Ensure strategic data-centre classification gives greater weight to European sovereignty and already existing sustainability criteria, by prioritising European-controlled capacity in Acceleration Zones (Art. 10–13) and by adding (1) compliance with the Energy Efficiency Directive's data centre sustainability indicators and (2) contribution to Union added value in Article 14.
- Ensure an effective 12-month deadline covering the full permitting process.
- Protect access to critical resources for European providers and link accelerated permitting to demonstrable European industrial benefit.

- Support the expansion of existing data centres on an equal footing with new builds, and support frugal AI alongside infrastructure investment.

On the Leadership Initiatives (Articles 3-9):

- Require Centres for AI to be built as an evolution of existing structures, not as parallel ones.
- Ensure Cloud and AI Leadership Initiatives explicitly support European providers across the full cloud stack.
- Extend frontier AI support to inference, fine-tuning and sovereign cloud infrastructure.

On regulatory consistency:

- Cross-refer CADA's definition of AI agents to the ones in the AI Act, do not restate them.
- Where firms already comply with GDPR, DORA, the AI Act, or sector-specific health rules (MDR, health-data hosting certification), for a given service, CADA should not impose a separate compliance layer for the same service.
- Allow existing audits, certifications, evaluations and evidence to be reused when they cover equivalent requirements, with any additional oversight limited to CADA-specific criteria