

Confederation of Swedish Enterprise on the European Commission's proposal for a regulation on cloud and AI development, CADA

OKTOBER 2026

The Confederation of Swedish Enterprise presents the following views on the European Commission's proposal for a Cloud and AI Development Act (CADA).

Key messages

- CADA should strengthen Europe's capacity and resilience by attracting more investment and innovation to Europe, not by restricting access to globally competitive cloud and AI services.
- The Confederation of Swedish Enterprise welcomes measures to increase data centre capacity and AI infrastructure and is generally supportive of proposals that lead to shorter and more efficient permitting procedures, but is critical of the proposals on strategic projects and acceleration areas and of selective fast-track procedures.
- Sovereignty and security requirements in CADA must be risk-based, proportionate, technology-neutral and limited to clearly defined critical use cases.
- Public procurement must strengthen competition, interoperability, freedom of choice and resilience – not introduce origin-based preferences or Buy European requirements.
- Open source and open standards are important tools but must not become mandatory technology choices or ends in themselves.
- CADA must be fully aligned with the proposed revised Cybersecurity Act (CSA2), the Data Act, the Digital Omnibus, the AI Act, the Directive on measures for a high common level of cybersecurity across the Union (NIS2), the Critical Entities Resilience Directive (CER), the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the ongoing revision of the EU public procurement framework, in order to avoid regulatory duplication and additional administrative burdens.

1. Summary position

The Confederation of Swedish Enterprise welcomes the Commission's ambition to strengthen Europe's capacity in cloud, data centres and AI. Access to competitive computing capacity is a crucial prerequisite for AI development and use, productivity, innovation and digitalisation across business. If properly designed, CADA can help remove bottlenecks and strengthen Europe's ability to attract investment.

The starting point needs to be clear: CADA must strengthen Europe's digital capacity through better investment conditions, faster permitting processes, more data centre and computing capacity, research and development (R&D), skills and coordination. The Confederation of Swedish Enterprise supports these parts of the proposal and believes they should be strengthened where needed.

At the same time, the Confederation of Swedish Enterprise considers it essential to address provisions that risk undermining European competitiveness, openness and access to global technologies and markets. This applies in particular to the sovereignty framework in Articles 16–18 and Annex II, the rules on assurance levels and risk assessments in Articles 29–31, and the procurement provisions in Articles 30–32.

These provisions must be technology-neutral, risk-based and proportionate. Any additional requirements should be strictly limited to clearly defined critical use cases where they are justified by a concrete and demonstrable risk. They must not result in trade barriers, general localisation or migration requirements, preferences based on the origin of providers or technologies, or indirect obligations for private actors.

2. Parts of CADA that should be supported and developed

2.1 Capacity, data centres and AI infrastructure

It is positive that CADA identifies the shortage of data centre and computing capacity as a key competitiveness problem. To meet the needs of the business sector, the measures should create better conditions for investment, innovation and efficient use of cloud and AI infrastructure across the business sector, through technology-neutral rules developed in close cooperation with the companies concerned.

A competitive European AI ecosystem requires investment across the entire AI stack, including applications, models, data, computing capacity, connectivity and other underlying digital infrastructure. CADA should therefore not have an overly narrow focus on large data centres, but ensure good investment conditions throughout the digital value chain.

2.2 Faster establishment and better permitting processes

The Confederation of Swedish Enterprise welcomes proposals that can shorten lead times for establishing data centres. Efficient, coordinated and predictable permitting processes are crucial for investment, innovation and competitiveness. The rules should be aligned with the specific solutions introduced through the Net-Zero Industry Act

(NZIA) and the Critical Raw Materials Act (CRMA), as well as through the proposed Industrial Accelerator Act (IAA). Single points of contact and information that guide companies through the process can increase transparency, improve coordination and shorten processing times.

However, the Confederation of Swedish Enterprise is sceptical of the proposal that certain projects should be identified and prioritised as strategic. The starting point should be that all companies have access to efficient and legally sound and predictable permitting procedures. A model in which certain activities are given priority risks crowding out other investments that are also important for society and for the development of the business sector.

Moreover, strategic projects often depend on a broader ecosystem of customers, suppliers and subcontractors whose operations also require the necessary permits.

Furthermore, the concept of a "strategic project" is changeable and depends on technological developments, market conditions and external events. There is therefore a risk that today's priorities quickly become outdated. A selective system may also lead to distortions of competition by giving certain companies or sectors advantages that are not justified by objective and long-term criteria.

The proposal on acceleration areas with pre-approved conditions for establishment also raises a number of important questions of principle. It is currently unclear how the proposal relates to fundamental principles of environmental law, including the polluter pays principle. The Confederation of Swedish Enterprise therefore calls for clarification of the division of responsibility between the state and the operator, particularly with regard to legal and financial liability for environmental impact.

There is also reason to question whether the proposal will in practice lead to shorter permitting processes. Permit assessments must continue to be carried out in accordance with the requirements of EU law for an individual assessment in each case. It is therefore not self-evident that the proposed acceleration areas will deliver the efficiency gains sought.

The Confederation of Swedish Enterprise also believes that the economic consequences of the proposal need to be analysed more closely. Among other things, it should be clarified whether, and to what extent, taxpayers are expected to bear the costs of measures that benefit a limited group of companies. It should also be analysed how the proposal affects competition and the functioning of the internal market.

Against this background, the Confederation of Swedish Enterprise cannot currently endorse the proposal on acceleration areas. The legal, economic and competitive consequences need to be further analysed and clarified before a position can be taken on whether the proposal is appropriate.

2.3 R&D, innovation and applied AI

The Confederation of Swedish Enterprise welcomes the proposal for specific initiatives for cloud and AI leadership, including Cloud and AI Leadership Initiatives and Grand Challenges, cf. Articles 3–9.

The initiatives should be directed towards areas where companies from different parts of the business sector can build competitive areas of strength, for example AI applications in industrial, service and knowledge-intensive activities, advanced data analytics, cybersecurity, energy-efficient data processing and skills development. The selection should be transparent, needs-driven and open to companies of all sizes.

It must be ensured that the conditions for participation, funding, reporting and intellectual property rights are designed so that smaller companies can actually participate in practice, not merely be formally covered.

The initiatives should in particular help bridge the gap between research, innovation and commercial scale-up. Funding and participation conditions should be designed so that innovative companies can develop and scale their solutions in Europe, rather than having to establish their first commercial growth in other markets.

2.4 Interoperability and standards

CADA can contribute to better interoperability, portability and open standards, particularly in the parts concerning common requirements, public procurement and open-source software, cf. Articles 30–32 and 41–44. The aim should be to reduce lock-in, facilitate switching between providers and strengthen resilience in both public and private cloud environments.

Article 32 in particular should therefore be amended so that procurement criteria are based on objective and technology-neutral criteria such as security, functionality, interoperability, portability, sustainability and the ability to switch providers, not on where the software, hardware or development originates.

For Articles 41–44, it should at the same time be clarified that open source and open standards are to be promoted as tools where appropriate, without becoming mandatory technology choices or indirect procurement preferences.

3. The business sector's most important proposals for improvement

	PRIORITY	PARTS CONCERNED	THE CONFEDERATION OF SWEDISH ENTERPRISE'S POSITION
1	Make sovereignty requirements risk-based	Art. 16–18, Annex II	The requirements must be based on concrete risk and actual control. A provider should not be regarded as high-risk solely because of links to a third country if the risks can be managed with equivalent safeguards.
2	Limit mandatory assurance levels and protect private actors	Art. 29–31, Annex II	Higher assurance levels should be reserved for highly critical use cases. General requirements for all public cloud use should be avoided, and the requirements must not be extended, directly or indirectly, to private actors. The Commission should not be given broad powers through delegated acts to make impact assessments or risk mitigation measures mandatory for private companies in NIS2 sectors.
3	Amend Union added value	Art. 32	Procurement criteria should focus on security, functionality, quality, interoperability, portability, sustainability and innovation – not on where software, hardware or development originates.
4	Strengthen the investment provisions	Art. 10–15	CADA should more clearly remove practical bottlenecks for establishing data centres and AI infrastructure, in particular access to electricity supply and grid capacity, connection processes, permits, land and coordination between authorities.
5	Preserve technology neutrality in open source	Art. 41–44	Open-source solutions should be encouraged where they offer clear benefits. However, the choice between open-source and proprietary solutions must be based on the specific needs of each use case, including security, accountability, functionality and total cost of ownership.
6	Ensure simplification and consistency	The entire proposal	CADA must not create duplicate regulation in relation to CSA2, the Data Act, the Digital Omnibus, the AI Act, NIS2, CER, DORA, CRA or the proposed Public Procurement Act.

4. Key issues

4.1 Digital sovereignty should be understood as capacity to act – not self-sufficiency

In CADA, digital sovereignty should be understood as Europe's ability to manage concrete vulnerabilities, ensure continuity of critical functions and retain strategic room for manoeuvre. It must not be interpreted as self-sufficiency, technological isolation or a general ambition to reduce all international dependencies. On the contrary, global value chains and technology cooperation are often a prerequisite for innovation, productivity and competitiveness.

It is legitimate for CADA, through the sovereignty framework in Articles 16–18 and Annex II and the risk assessments in Articles 29–31, to seek to create more harmonised criteria for managing both technical and non-technical risks in cloud supply chains. Such harmonisation can reduce fragmentation between Member States and give companies more predictable conditions. The criteria should, however, be based on concrete risk, actual control and the criticality of the use case– not on general assumptions about providers' origin, ownership, jurisdiction or establishment in a third country.

The sovereignty framework in Articles 16–18 and Annex II, including the proposed assurance levels, can provide a useful basis for aligning requirements with concrete risks and the criticality of the use case. Higher assurance levels should be reserved for clearly defined, highly critical use cases where the potential consequences of disruption, unauthorised access or undue influence are particularly serious. They must not become general requirements for all public-sector cloud use or be used indirectly to favour certain providers, impose localisation requirements or give preference to solutions based on European origin.

Higher assurance levels should only be required where there is a clear link between the cloud use in question and the protection of particularly critical societal functions. This could include defence, national security, the judiciary or other activities where disruption, unauthorised access or undue influence could have particularly serious consequences.

The risk assessment should be based on the critical function to be maintained and the consequences if the function can no longer be performed. A given assurance level should be one possible risk-mitigation measure, not the primary objective of the risk assessment or a substitute for continuity planning, diversification and verified recovery capability. CADA should therefore be limited to strengthening digital capacity, investment and practical resilience. Sovereignty requirements should be based on risk assessment, proportionality and verifiable safeguards, such as encryption, access controls, data and risk classification, contract governance, continuity planning, incident management, supplier diversification and interoperability.

Rules on cyber certification and non-technical risks should be coordinated with CSA2, so that CADA does not create parallel or broader sovereignty requirements. Providers should not be excluded solely on the basis of origin, ownership, jurisdiction or establishment in a third country, unless there is a documented risk that cannot be managed

through equivalent risk mitigation measures. A documented and risk-based diversification strategy, which may include both European and non-European providers, should be expressly recognised as a way of reducing concentration risks and strengthening operational resilience.

The same technical or organisational control should not have to be assessed repeatedly under different regulatory frameworks. CADA should therefore be coordinated with the EUCS and follow a clear 'once only' principle.

At the same time, the scope and key definitions of CADA need to be clearly delimited. An overly broad definition of cloud and computing services risks covering significantly more services and products than traditional cloud infrastructure, for example SaaS services, connected products and Edge AI solutions. It must also be clarified how third-party components, open source and different forms of effective and operational control are to be assessed.

The practical and economic implications of certification and audits also need to be analysed. If individual services must be certified separately, the costs may be considerable, while limited access to qualified and independent auditors risks creating bottlenecks. Existing certifications, audits and other evidence should therefore be reusable in line with a clear 'once only' principle.

4.2 Data centre capacity, energy and permits

Data centres and cloud infrastructure are part of Europe's digital backbone. They are crucial for AI, advanced data analytics, research, cybersecurity, the digitalisation of the business sector and the modernisation of the public sector. Europe's problem is not primarily a lack of political goals, but a lack of practical conditions for investment and rapid expansion.

CADA should therefore focus on actual bottlenecks: access to competitive and fossil-free electricity, grid capacity, connection processes, land, permits, skills, R&D, capital and predictable rules. Sweden and the Nordic region are well placed to attract data centre investment, but this requires sufficient grid capacity, competitive energy prices and efficient permitting processes.

As stated above, the Confederation of Swedish Enterprise is sceptical of the proposal on acceleration areas and strategic data centre projects. If acceleration zones are retained in the proposal, they must include the necessary surrounding infrastructure, not just the facility itself, and be combined with a clear division of responsibility and objective criteria. Without electricity grids, connections, planning processes and coordination between authorities, CADA's capacity targets risk being difficult to implement in practice.

This is consistent with the Commission's own finding that lengthy permitting processes and limited access to energy, land, water and financing are hindering the expansion of cloud and data centre capacity in Europe.

4.3 Public procurement – a strategic tool, not a preference system

Public procurement can play a strategic role to strengthen innovation, security, interoperability and resilience. At the same time, procurement is already an area where limited competition, complicated requirements and uncertain application often lead to few bids and high costs. CADA should therefore not introduce new preference systems or parallel procurement requirements, but be aligned with the ongoing revision of the EU procurement framework.

Article 32 on Union added value in particular should be amended. Criteria that favour EU-developed technology, EU-funded R&D or EU-based hardware risk becoming origin-based preferences in practice. This could reduce competition, exclude providers that meet high security requirements and lead to more expensive or poorer solutions for the public sector.

Even without an explicit ban on non-European providers, criteria that favour European origin, EU-based development or EU-funded R&D can have an exclusionary effect. Procurement then risks being steered towards certain categories of providers instead of towards objective criteria such as security, functionality, quality, interoperability, resilience and cost-effectiveness. Any restrictions should only be justifiable on the basis of documented risk and an assessment of whether the risk can be managed through equivalent risk mitigation.

Procurement should instead be based on objective and technology-neutral criteria: security, functionality, continuity, interoperability, performance, scalability, global reach, portability, sustainability, the ability to switch providers, data control, innovation and total life-cycle cost.

4.4 Risk assessments, migration requirements and private actors

Risk assessment is the right principle, but CADA must avoid general migration requirements or broad sovereignty requirements for the public sector that spill over onto the business sector. For many companies, cloud services are integrated into products, development environments and global operations. It is also important to distinguish between data portability and the migration of an entire technical infrastructure. The fact that data can be moved does not mean that applications, integrations, security solutions and underlying infrastructure can be migrated within the same timeframe. Forced migration may require extensive development and engineering work, costly reintegration and parallel systems, and may create new lock-in effects, operational disruptions and delayed innovation. Strict deadlines without a full impact assessment may therefore undermine security, continuity and competitiveness.

Any requirements for migration or for a particular assurance level should only be considered after a documented risk assessment and proportionality test. Account must be taken of technical feasibility, business continuity, costs, the availability of alternative providers and the risks of the migration itself.

Transition periods must reflect the actual technical complexity of the migration and cannot be set through a general deadline that applies to all services and use cases.

Before migration requirements, supplier restrictions or other far-reaching measures are introduced, they should be subject to an impact assessment, transparency requirements and realistic transition periods. Their effects on investment, competition and business continuity must also be assessed.

Any localisation requirements must also take into account the need for cross-border processing of security and telemetry data. Such data may be necessary to identify global cyber threats and stop attacks before they reach European operations. Requirements that create European data silos therefore risk, in some cases, weakening rather than strengthening cybersecurity.

Measures that interfere with property rights should only be considered in the event of a documented, significant and concrete risk to critical operations or infrastructure.

Article 31, which concerns private actors in NIS2 sectors, should be limited. Voluntary impact assessments can be useful, but CADA should not give the Commission a broad delegated power to make such assessments or risk mitigation measures mandatory for private actors. Such requirements may have significant consequences for investment, cloud strategies and business continuity. They should therefore only be possible to introduce through the ordinary legislative procedure, following an impact assessment and consultation with the businesses concerned.

The impact assessment must also cover indirect effects in supply chains. Experience from other regulatory frameworks shows that requirements formally directed at public or specially regulated actors are often passed on contractually to suppliers and sub-contractors. CADA should therefore be designed so that higher assurance levels and sovereignty requirements do not become informal standard requirements for private actors that are not covered by the provisions.

4.5 Open source and open standards

Open source and open standards can contribute to interoperability, transparency, innovation and reduced lock-in. The Confederation of Swedish Enterprise therefore welcomes measures that make it easier to reuse code and use open standards where appropriate.

At the same time, open source is not always the best choice. The choice between open source and proprietary solutions should be based on functionality, security, the allocation of responsibilities, maintainability, cost, support and operational needs. CADA should therefore clarify technology neutrality and avoid open source becoming a general requirement or an indirect procurement preference.

Clear safeguards are also needed. Open source requirements should not cover security-sensitive code, intellectual property, third-party licences or trade secrets, and should not apply where responsibility for long-term maintenance, support or security updates cannot be ensured.

5. Article-by-article comments

– prioritised overview

The following table summarises the Confederation of Swedish Enterprise's key article-by-article comments.

ARTICLES	AREA	ASSESSMENT	THE CONFEDERATION OF SWEDISH ENTERPRISE'S POSITION
1–2	Purpose and definitions	Clarify	The proposal should promote competitiveness, technology neutrality and interoperability and be based on risk-based requirements. Supplier risk must be assessed on the basis of concrete and verifiable risk and actual control. Links to a third country must not in themselves result in a provider being classified as high-risk, if the risks can be managed through technical, organisational or contractual safeguards. The scope should be delimited so that connected products and services are not covered merely because they use cloud infrastructure. The definitions should be coordinated with the Data Act, the AI Act, NIS2 and CSA2.
3–9	Cloud and AI Leadership Initiatives	Welcome with amendments	Direct Cloud and AI Leadership Initiatives and Grand Challenges towards areas where companies from different parts of the business sector can build areas of competitive strength, with transparent, needs-driven selection and open participation for companies of all sizes.
10–15	Data centre capacity and acceleration areas	Welcome with amendments	Strengthen the positive parts on data centres, permits, single points of contact and information, and capacity monitoring. Selective fast tracks and prioritisation of strategic projects should be avoided. Link the measures explicitly to electricity grids, energy, land, skills and grid connections.
16–18	Union cloud sovereignty framework	Amend	Make the framework strictly risk-based and functional. Avoid grounds for exclusion based on origin, ownership, jurisdiction or establishment in a third country without documented risk and an assessment of equivalent risk mitigation. Coordinate with CSA2 so that CADA does not create parallel or broader sovereignty requirements.
19–28	Recognition, auditing and supervision	Clarify	Ensure legally sound, swift and proportionate processes. Analyse costs and access to qualified and independent auditors. Enable the reuse of existing certifications, audits and other evidence in line with a clear once-only principle. Protect trade secrets and security-sensitive information.

29–31	Risk assessments and private actors	Amend	Limit requirements to highly critical use cases. The risk assessment should be based on the function to be maintained, the consequences of a disruption, critical dependencies and available continuity measures. Avoid general migration requirements and ensure realistic, risk-based transition periods that take into account the difference between moving data and migrating technical infrastructure. Remove or limit the Commission's ability to make impact assessments mandatory for private actors. Any requirements on private actors should be decided through the ordinary legislative procedure, following an impact assessment and stakeholder consultation.
30–32	Public procurement and Union added value	Amend substantially	Procurement must promote competition, be technology-neutral and be aligned with the revision of the EU procurement framework. Remove or limit origin-based criteria and replace them with criteria for security, functionality, portability, interoperability, sustainability and innovation.
33–40	Innovation procurement, EuroCloud Federation & joint procurement	Conditional support	Support SME participation and procurement skills, but avoid quotas, distortions of competition and centralised industrial-policy steering. Ensure proportionate qualification, documentation and certification requirements and enable the use of lots and the reuse of evidence.
41–44	Open source	Welcome with clear reservations	Promote open source and open standards as tools, but maintain technology neutrality and clear exceptions for security, IP, licences and maintenance responsibility.
45–48	Delegated acts, committee procedure, review and entry into force, and application.	Clarify and limit	Limit delegated powers, in particular for Annex II. Require impact assessment, consultation with businesses, transparency, transition periods and evaluation of the impact on competition, SMEs and investment.

CONFEDERATION OF SWEDISH ENTERPRISE

Contact: Carola Ekblad carola.ekblad@svensktnaringsliv.se