Cloud and AI Development Act (CADA), Svenskt Näringslivs position och artikelkommentarer

Huvudbudskap

- CADA bör stärka Europas kapacitet och motståndskraft genom att attrahera mer investeringar och innovation till Europa, inte genom att begränsa tillgången till globalt konkurrenskraftiga molntjänster och AI-tjänster.
- Svenskt Näringsliv välkomnar åtgärder för ökad datacenterkapacitet och AI-infrastruktur och är generellt stödjande till förslag som leder till snabbare tillståndsprocesser, men är kritiskt till förslagen om strategiska projekt och accelerationsområden samt till selektiva snabbspår.
- Suveränitets- och säkerhetskrav i CADA ska vara riskbaserade, proportionerliga, teknikneutrala och begränsade till tydligt definierade kritiska användningsfall.
- Offentlig upphandling ska stärka konkurrens, interoperabilitet, valfrihet och resiliens – inte införa ursprungsbaserade preferenser eller Buy European-krav.
- Open source och öppna standarder är viktiga verktyg men får inte bli obligatoriska teknikval eller självändamål.
- CADA måste fullt ut samspela med den kommande revideringen av cybersäkerhetsakten, Cybersecurity Act 2 (CSA2), Data Act, Digital Omnibus, AI Act, direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2), direktivet om kritiska entiteters motståndskraft (CER), Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), Europeisk certifieringsordning för molntjänster (EUCS) och upphandlingsdirektiven för att undvika dubbelreglering eller ny administrativ börda.

1. Sammanfattande position

Svenskt Näringsliv välkomnar kommissionens ambition att stärka Europas kapacitet inom moln, datacenter och AI. Tillgång till konkurrenskraftig beräkningskapacitet är en avgörande förutsättning för AI-utveckling och -användning, produktivitet, innovation och digitalisering i hela näringslivet. Rätt utformad kan CADA bidra till att undanröja flaskhalsar och stärka Europas möjligheter att attrahera investeringar.

Utgångspunkten behöver vara tydlig: CADA ska stärka Europas digitala kapacitet genom bättre investeringsvillkor, snabbare tillståndsprocesser, mer datacenter- och beräkningskapacitet, forskning och utveckling (FoU), kompetens och samordning. Svenskt Näringsliv stödjer dessa delar av förslaget och anser att de vid behov, där det behövs, bör förstärkas.

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 8 553 430 00
svensktnaringsliv.se Orgnr: 802000-1858

Samtidigt anser Svenskt Näringsliv att Sverige och likasinnade medlemsländer bör driva ändringar i de delar som riskerar att motverka konkurrenskraft och öppenhet. Det gäller särskilt: suveränitetsramverket i artikel 16–18 och bilaga II, reglerna om tillitsnivåer och riskbedömningar i artikel 29–31 samt upphandlingsbestämmelserna i artikel 30–32. Dessa krav måste vara teknikneutrala, riskbaserade och proportionerliga. De ska avgränsas till tydligt definierade kritiska användningsfall och får inte leda till handelshinder, generella lokaliserings- eller migrationskrav, ursprungsbaserade preferenser eller indirekta skyldigheter för privata aktörer.

2. Delar i CADA som bör stödjas och utvecklas

2.1 Kapacitet, datacenter och AI-infrastruktur

Det är positivt att CADA identifierar bristen på datacenter- och beräkningskapacitet som ett centralt konkurrenskraftsproblem. För att möta näringslivets behov bör åtgärderna skapa bättre villkor för investeringar, innovation och effektiv användning av moln- och AI-infrastruktur i hela näringslivet, med teknikneutrala regler och nära samverkan med berörda företag.

2.2 Snabbare etableringar och bättre tillståndsprocesser

Svenskt Näringsliv välkomnar förslag som kan förkorta ledtiderna för datacenteretableringar. Effektiva, samordnade och förutsebara tillståndsprocesser är avgörande för investeringar, innovation och konkurrenskraft. Reglerna bör samspela med lösningarna ide särskilda lösningar som införts genom rättsakten om nettonollindustrin (Net-Zero Industry Act, NZIA),) och rättsakten om kritiska råvaror (Critical Raw Materials Act, CRMA) och), samt genom den föreslagna rättsakten om industriell acceleration (Industrial Accelerator Act, IAA). Gemensamma informations- och kontaktpunkter som vägleder företag genom processen kan öka transparensen, förbättra samordningen och korta handläggningstiderna.

Svenskt Näringsliv ställer sig däremot tveksamt till förslaget om att identifiera och prioritera vissa projekt ska identifieras och prioriteras som strategiska. Utgångspunkten bör vara att alla företag bör ha tillgång till effektiva och rättssäkra tillståndsprocesser.

En modell där vissa verksamheter ges företräde riskerar att tränga undan andra investeringar som också är betydelsefulla för samhället och näringslivets utveckling.

Strategiska projekt är dessutom ofta beroende av ett bredare ekosystem av kunder, leverantörer och underleverantörer vars verksamheter också behöver nödvändiga tillstånd.

Vidare är begreppet ”strategiskt projekt” föränderligt och beroende av teknisk utveckling, marknadsförutsättningar och externa händelser. Det finns därför en risk att dagens prioriteringar snabbt blir inaktuella. En selektiv ordning kan också leda till konkurrenssnedvridningar genom att vissa företag eller sektorer ges fördelar som inte motiveras av objektiva och långsiktiga kriterier.

Förslaget om accelerationsområden med förhandsgodkända förutsättningar för etablering väcker också ett antal principiellt viktiga frågor. Det är i nuläget oklart hur förslaget förhåller sig till grundläggande miljörättsliga principer, däribland principen om att förorenaren betalar. Svenskt Näringsliv efterlyser därför ett klargörande av

ansvarsfördelningen mellan staten och verksamhetsutövaren, särskilt när det gäller rättsligt och ekonomiskt ansvar för miljöpåverkan.

Det finns även skäl att ifrågasätta om förslaget i praktiken kommer att leda till kortare tillståndsprocesser. Tillståndsprövningar ska även fortsättningsvis genomföras i enlighet med EU-rättens krav på individuella bedömningar i det enskilda fallet. Det är därför inte självklart att de föreslagna accelerationsområdena kommer att ge de effektivitetsvinster som eftersträvas.

Svenskt Näringsliv anser vidare att de ekonomiska konsekvenserna av förslaget behöver analyseras närmare. Det bör bland annat klargöras om, och i vilken utsträckning, skattebetalarna förväntas bära kostnader för åtgärder som gynnar en avgränsad grupp företag. Det bör också analyseras hur förslaget påverkar konkurrensen och den inre marknadens funktionssätt.

Mot denna bakgrund kan Svenskt Näringsliv i nuläget inte tillstyrka förslaget om accelerationsområden. De rättsliga, ekonomiska och konkurrensmässiga konsekvenserna behöver analyseras och klargöras ytterligare innan ställning kan tas till förslagets lämplighet.

2.3 FoU, innovation och tillämpad AI

Svenskt Näringsliv ser positivt på förslaget till särskilda initiativ för moln- och AI-ledarskap, inklusive *Cloud and AI Leadership Initiatives* och *Grand Challenges*, jfr artikel 3–9.

Initiativen bör inriktas på områden där företag ifrån olika delar av näringslivet kan bygga konkurrenskraftiga styrkepositioner, till exempel AI-tillämpningar inom industri-, tjänste- och kunskapsintensiva verksamheter, avancerad dataanalys, cybersäkerhet, energieffektiv databehandling och kompetensuppbyggnad. Urvalet bör vara transparent, behovsdrivet och öppet för alla företagsstorlekar.

Det behöver säkerställas att villkoren för deltagande, finansiering, rapportering och immaterialrätt måste utformas så att även mindre företag faktiskt kan delta i praktiken, inte bara formellt omfattas.

2.4 Interoperabilitet och standarder

CADA kan bidra till bättre interoperabilitet, portabilitet och öppna standarder, särskilt i de delar som rör gemensamma krav, upphandling och open source, jfr artikel 30–32 och 41–44. Syftet bör vara att minska inlåsning, underlätta leverantörsbyte och stärka resiliensen i både offentliga och privata molnmiljöer.

Särskilt artikel 32 bör därför ändras så att upphandlingskriterierna utgår från objektiva och teknikneutrala kriterier som säkerhet, funktion, interoperabilitet, portabilitet, hållbarhet och möjlighet till leverantörsbyte –, inte från mjukvarans, hårdvarans eller utvecklingens ursprung.

För artikel 41–44 bör det samtidigt tydliggöras att open source och öppna standarder ska främjas som verktyg där det är ändamålsenligt, utan att bli obligatoriska teknikval eller indirekta upphandlingspreferenser.

3. Näringslivets viktigaste förbättringsförslag

#	Prioritet	Berörda delar	Svenskt Näringslivs linje
1	Gör suveränitetskraven riskbaserade	Art. 16–18, Annex II	Krav ska utgå från konkret risk, faktisk kontroll och funktionella skyddsåtgärder. Leverantörer bör inte bedömas som högrisk enbart på grund av ursprung, ägande, jurisdiktion eller etablering i tredjeland, om det inte finns en dokumenterad risk som inte kan hanteras genom likvärdig riskmitigering.
2	Begränsa obligatoriska assurance levels och skydda privata aktörer	Art. 29–31, Annex II	Högre nivåer bör reserveras för mycket kritiska användningsfall. Generella krav för all offentlig molnanvändning bör undvikas och kraven ska inte vare sig direkt eller indirekt utvidgas till privata aktörer. Kommissionen bör inte ges bred befogenhet att genom delegerade akter göra konsekvensanalyser eller riskmitigering obligatoriska för privata företag i NIS2-sektorer.
3	Ändra Union added value	Art. 32	Upphandlingskriterier bör fokusera på säkerhet, funktion, kvalitet, interoperabilitet, portabilitet, hållbarhet och innovation – inte på var mjukvara, hårdvara eller utveckling har sitt ursprung.
4	Stärk investeringsdelarna	Art. 10–15	CADA bör tydligare undanröja praktiska flaskhalsar för datacenteretableringar och AI-infrastruktur, särskilt tillgång till elförsörjning och nätkapacitet, anslutningsprocesser, tillstånd, mark och myndighetssamordning.
5	Bevara teknikneutralitet i open source	Art. 41–44	Open source bör främjas som ett verktyg där det är lämpligt, men valet mellan open source och proprietära lösningar ska avgöras av behov, säkerhet, ansvar, kostnad och funktion.
6	Säkra förenkling och överensstämmelse	Hela förslaget	CADA får inte skapa dubbelreglering i förhållande till CSA2, Data Act, Digital Omnibus, AI Act, NIS2, CER, DORA, CRA eller upphandlingsdirektiven.

4. Centrala sakfrågor

4.1 Digital suveränitet ska förstås som handlingsförmåga – inte självförsörjning

Digital suveränitet bör i CADA förstås som Europas förmåga att hantera konkreta sårbarheter, säkerställa kontinuitet i kritiska funktioner och behålla strategiskt

handlingsutrymme. Det ska inte tolkas som självförsörjning, teknologisk isolering eller en generell ambition att minska alla internationella beroenden. Globala värdekedjor och tekniksamarbeten är tvärtom ofta en förutsättning för innovation, produktivitet och konkurrenskraft.

Det är legitimt att CADA, genom suveränitetsramverket i artikel 16–18 och bilaga II samt riskbedömningarna i artikel 29–31, försöker skapa mer harmoniserade kriterier för att hantera både tekniska och icke-tekniska risker i molnleveranskedjor. Sådan harmonisering kan minska fragmentering mellan medlemsländer och ge företag mer förutsebara villkor. Kriterierna bör dock utgå från konkret risk, faktisk kontroll och användningens kritikalitet – inte från generella antaganden om leverantörers ursprung, ägande, jurisdiktion eller etablering i tredjeland.

Suveränitetsramverket i artikel 16–18 och bilaga II, inklusive de föreslagna risk- och säkerhetsnivåerna, kan vara användbart om det används för att matcha krav mot faktisk risk och hur kritisk användningen är. Högre nivåer bör reserveras för tydligt definierade kritiska användningsfall där konsekvenserna av störningar, obehörig åtkomst eller otillbörlig påverkan är särskilt allvarliga. De bör inte bli generella trösklar för all offentlig molnanvändning eller ett indirekt sätt att styra mot vissa leverantörer, viss lokalisering eller europeiskt ursprung.

Det bör uttryckligen framgå att högre tillitsnivåer (assurance levels) endast får krävas när det finns en tydlig koppling mellan den aktuella molnanvändningen och skyddet av särskilt kritiska samhällsfunktioner, exempelvis försvar, nationell säkerhet, rättsväsende eller andra verksamheter där ett avbrott, otillbörlig påverkan eller obehörig åtkomst skulle få mycket allvarliga konsekvenser.

Riskbedömningen bör utgå från den kritiska funktion som ska upprätthållas och konsekvenserna om funktionen inte längre kan fullgöras. En viss tillitsnivå bör vara en möjlig riskreducerande åtgärd, inte riskbedömningens primära mål eller ett substitut för kontinuitetsplanering, diversifiering och verifierad återställningsförmåga. CADA bör därför avgränsas till att stärka digital kapacitet, investeringar och praktisk resiliens. Suveränitetskrav bör bygga på riskbedömning, proportionalitet och verifierbara skyddsåtgärder, såsom kryptering, åtkomstkontroller, data- och riskklassning, kontraktsstyrning, kontinuitetsplanering, incidenthantering, leverantörsdiversifiering och interoperabilitet.

Regler om cybercertifiering och icke-tekniska risker bör samordnas med CSA2, så att CADA inte skapar parallella eller bredare suveränitetskrav. Leverantörer bör inte uteslutas enbart på grund av ursprung, ägande, jurisdiktion eller etablering i tredjeland, om det inte finns en dokumenterad risk som inte kan hanteras genom likvärdig riskmitigering. En dokumenterad och riskbaserad diversifieringsstrategi, som kan omfatta både europeiska och icke-europeiska leverantörer, bör uttryckligen erkännas som ett sätt att minska koncentrationsrisker och stärka operativ motståndskraft.

Det behöver också säkerställas att samma tekniska eller organisatoriska kontroll inte behöver göras flera gånger enligt olika regelverk, och samordning behöver därför också ske med bland annat EUCS.

4.2 Datacenterkapacitet, energi och tillstånd

Datacenter och molninfrastruktur är en del av Europas digitala ryggrad. De är avgörande för AI, avancerad dataanalys, forskning, cybersäkerhet, näringslivets digitalisering och offentlig sektors modernisering. Europas problem är inte i första hand brist på politiska mål, utan brist på praktiska förutsättningar för investeringar och snabb utbyggnad.

CADA bör därför koncentreras till faktiska flaskhalsar: tillgång till konkurrenskraftig och fossilfri el, elnätskapacitet, anslutningsprocesser, mark, tillstånd, kompetens, FoU, kapital och förutsebara regler. Sverige och Norden har goda förutsättningar att attrahera datacenterinvesteringar, men detta kräver tillräcklig nätkapacitet, konkurrenskraftiga energipriser och effektiva prövningsprocesser.

Som anges ovan är Svenskt Näringsliv tveksamt till förslaget om accelerationsområden och strategiska datacenterprojekt. Om accelerationszoner behålls i förslaget måste de omfatta nödvändig omkringliggande infrastruktur, inte bara själva anläggningen, och förenas med tydlig ansvarsfördelning och objektiva kriterier. Utan elnät, anslutning, planprocesser och myndighetssamordning riskerar CADA:s kapacitetsmål att bli svåra att omsätta i praktiken.

Detta ligger också i linje med kommissionens egen problembild: att långa tillståndsprocesser och begränsad tillgång till energi, mark, vatten och finansiering hindrar utbyggnad av moln- och datacenterkapacitet i Europa.

4.3 Offentlig upphandling – strategiskt verktyg, inte preferenssystem

Offentlig upphandling kan användas mer strategiskt för att stärka innovation, säkerhet, interoperabilitet och resiliens. Samtidigt är upphandling redan ett område där bristande konkurrens, komplicerade krav, och osäker tillämpning och bristande konkurrens ofta leder till få anbud och höga kostnader. CADA bör därför inte införa nya preferenssystem eller parallella upphandlingskrav, utan samspela med den pågående revideringen av EU:s upphandlingsregelverk.

Särskilt artikel 32 om Union added value bör ändras. Kriterier som premierar EU-utvecklad teknik, EU-finansierad FoU eller EU-baserad hårdvara riskerar att i praktiken bli ursprungsbaserade preferenser. Det kan minska konkurrensen, utestänga leverantörer som uppfyller höga säkerhetskrav och leda till dyrare eller sämre lösningar för offentlig sektor.

Även utan ett uttryckligt förbud mot icke-europeiska leverantörer kan kriterier som premierar europeiskt ursprung, EU-baserad utveckling eller EU-finansierad FoU få en utestängande effekt. Upphandlingen riskerar då att styras mot vissa leverantörskategorier i stället för mot objektiva kriterier som säkerhet, funktion, kvalitet, interoperabilitet, resiliens och kostnadseffektivitet. Eventuella begränsningar bör endast kunna motiveras av dokumenterad risk och prövning av om risken kan hanteras genom likvärdig riskmitigering.

Upphandling bör i stället utgå från objektiva och teknikneutrala kriterier: säkerhet, funktionalitet, kontinuitet, interoperabilitet, prestanda, skalbarhet, global räckvidd, portabilitet, hållbarhet, möjlighet till leverantörsbyte, datakontroll, innovation och total kostnad över livscykeln.

4.4 Risk assessments, migrationskrav och privata aktörer

Riskbedömning är rätt princip, men CADA måste undvika generella migrationskrav och/eller breda offentliga suveränitetskrav som spiller över på näringslivet. För många företag är molntjänster integrerade i produkter, utvecklingsmiljöer och globala verksamheter. En påtvingad migration kan därför kräva kostsam omintegration, och parallella system och skapa nya inlåsningseffekter, driftstörningar och fördröjd innovation. Skarpa tidsfrister utan fullständig konsekvensanalys kan därför motverka säkerhet, kontinuitet och konkurrenskraft.

Eventuella krav på migration eller på en viss assurance level bör endast aktualiseras efter en dokumenterad riskbedömning och proportionalitetsprövning. Hänsyn måste tas till teknisk genomförbarhet, affärskontinuitet, kostnader, tillgång till alternativa leverantörer och riskerna med själva migreringen.

Innan krav på migration, leverantörsbegränsningar eller andra ingripande åtgärder införs krävs konsekvensanalys, transparens, realistiska övergångsperioder och en bedömning av påverkan på investeringar, konkurrens och verksamhetskontinuitet. Åtgärder som innebär intrång i äganderätten bör endast komma i fråga vid en dokumenterad, betydande och konkret risk för kritisk verksamhet eller infrastruktur.

Artikel 31, som rör privata aktörer i NIS2-sektorer, bör begränsas. Frivilliga konsekvensanalyser kan vara användbara, men CADA bör inte ge kommissionen en bred delegerad befogenhet att göra sådana analyser eller riskmitigeringsåtgärder obligatoriska för privata aktörer. Sådana krav kan få betydande konsekvenser för investeringar, molnstrategier och verksamhetskontinuitet. De bör därför endast kunna införas genom ordinarie lagstiftningsprocess, efter konsekvensanalys och samråd med berörda företag.

4.5 Open source och öppna standarder

Open source och öppna standarder kan bidra till interoperabilitet, transparens, innovation och minskad inlåsning. Svenskt Näringsliv välkomnar därför åtgärder som gör det enklare att återanvända kod och använda öppna standarder där det är lämpligt.

Samtidigt är open source inte alltid det bästa valet. Valet mellan open source och proprietära lösningar bör grundas på funktion, säkerhet, ansvarsfördelning, underhållsförmåga, kostnad, support och verksamhetsbehov. CADA bör därför tydliggöra teknikneutralitet och undvika att open source blir ett generellt krav eller en indirekt upphandlingspreferens.

Reglerna bör innehålla tydliga skyddsräcken. Open source-krav bör inte omfatta säkerhetskänslig kod, immateriella rättigheter, tredjepartslicenser eller affärshemligheter, och bör inte tillämpas när ansvar för långsiktigt underhåll, support eller säkerhetsuppdateringar inte kan säkerställas.

5. Artikelkommentarer – prioriterad sammanställning

Följande tabell sammanfattar Svenskt Näringslivs centrala artikelkommentarer.

Artiklar	Område	Bedömning	Svenskt Näringslivs linje
1–2	Syfte och definitioner	Förtydliga	Förslaget bör tydligt ange att målet ska nås genom konkurrenskraft, teknikneutralitet, interoperabilitet och riskbaserade krav. Definitioner av leverantörsrisk bör avgränsas till faktisk kontroll och konkret risk och verifierbar exponering för tredjelandslagstiftning som inte kan hanteras genom tekniska, organisatoriska eller avtalsrättsliga skyddsåtgärder. Företag som har verksamhet eller etablering i tredjeland bör inte på den grunden betraktas som högriskleverantörer, om de inte kontrolleras av ett tredjeland eller av en aktör med sådan koppling. Definitioner måste samordnas med Data Act, AI Act, NIS2 och CSA2.
3–9	Cloud and AI Leadership Initiatives	Välkomna med ändringar	Inrikta Cloud and AI Leadership Initiatives och Grand Challenges mot områden där företag från olika delar av näringslivet kan bygga konkurrenskraftiga styrkepositioner med transparent, behovsdrivet urval och öppet deltagande för alla företagsstorlekar.
10–15	Datacenterkapacitet och accelerationsområden	Välkomna med ändringar	Stärk de positiva delarna om datacenter, tillstånd, gemensamma informations- och kontaktpunkter samt kapacitetsövervakning. Selektiva snabbspår och prioritering av strategiska projekt bör undvikas. Koppla åtgärderna uttryckligen till elnät, energi, mark, kompetens och anslutning.
16–18	Union cloud sovereignty framework	Ändra	Gör ramverket strikt riskbaserat och funktionellt. Undvik uteslutningsgrunder baserade på ursprung, ägande, jurisdiktion eller etablering i tredjeland utan dokumenterad risk och prövning av likvärdig riskmitigering. Samordna med CSA2 så att CADA inte skapar parallella eller bredare suveränitetskrav.
19–28	Erkännande, revision och tillsyn	Förtydliga	Säkerställ rättssäkra, snabba och proportionerliga processer. Möjliggör återanvändning av

			befintliga certifieringar och revisioner. Skydda företagshemligheter och säkerhetskänslig information. Tillämpa principer om once only.
29–31	Riskbedömningar och privata aktörer	Ändra	Begränsa krav till mycket kritiska användningsfall. Riskbedömningen bör utgå från den funktion som ska upprätthållas, konsekvenserna av ett avbrott, kritiska beroenden och tillgängliga kontinuitetsåtgärder. Undvik generella migrationskrav. Ta bort eller begränsa kommissionens möjlighet att göra konsekvensanalyser obligatoriska för privata aktörer. Eventuella krav på privata aktörer bör beslutas genom ordinarie lagstiftningsprocess, efter konsekvensanalys och samråd.
30–32	Offentlig upphandling och Union added value	Ändra kraftigt	Upphandling ska vara konkurrensfrämjande, teknikneutral och samspela med revideringen av EU:s upphandlingsregelverk. Ta bort eller begränsa ursprungsbaserade kriterier och ersätt med kriterier för säkerhet, funktion, portabilitet, interoperabilitet, hållbarhet och innovation.
33–40	Innovationsupphandling, EuroCloud Federation och gemensam upphandling	Villkorat stöd	Stöd SME-deltagande och kompetens i upphandling, men undvik kvoter, konkurrenssnedvridning och centraliserad industripolitisk styrning. Säkerställ proportionerliga kvalificerings-, dokumentations- och certifieringskrav samt möjliggör för delkontrakt och återanvändbara bevis.
41–44	Open source	Välkomna med tydligt förbehåll	Främja open source och öppna standarder som verktyg, men behåll teknikneutralitet och tydliga undantag för säkerhet, IP, licenser och underhållsansvar.
45–48	Delegerade akter, kommittéförfarande, översyn och ikraftträdande	Förtydliga och begränsa	Begränsa delegerade befogenheter, särskilt för Annex II. Kräv konsekvensanalys, näringslivskonsultation, transparens, övergångsperioder

			och utvärdering av konkurrens-, SME- och investeringspåverkan.

SVENSKT NÄRINGSLIV

Carolina Brånby och Carola Ekblad