

Finansdepartementet

fi.remissvar@regeringskansliet.se

fi.ofa.dis.remisser@regeringskansliet.se

REMISSVAR AVSEENDE EUROPEISKA KOMMISSIONENS FÖRSLAG TILL FÖRORDNING OM UTVECKLING AV MOLN OCH AI KOM(2026)502

Microsoft Aktiebolag, i fortsättningen Microsoft, välkomnar möjligheten att lämna synpunkter på Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)502 (härefter CADA). Microsoft är ett globalt teknikföretag som tillhandahåller moln-, AI- och produktivitetstjänster till såväl offentlig som privat sektor i Sverige och EU, och som investerar i digital infrastruktur i Europa. Vi har ett starkt intresse av att CADA utvecklas på ett sätt som kombinerar rättssäkerhet, innovationsförmåga och praktisk genomförbarhet, i linje med förordningens syfte.

Övergripande bedömning

Microsoft stöder EU:s ambition att stärka unionens ekonomiska säkerhet, resiliens och strategiska autonomi. Vi anser att dessa mål bäst uppnås genom en funktionell och riskbaserad modell för suveränitet, där proportionerliga tekniska, operativa och rättsliga skyddsåtgärder bedöms, snarare än genom exkluderande kriterier som bygger på nationalitet eller geografiskt ursprung.

Microsoft välkomnar CADA som ett viktigt steg mot den infrastruktur som Europas AI-ambitioner förutsätter, och menar att förslaget kan stärkas ytterligare för att ge större rättslig tydlighet i hela unionen och stödja robusta strategier för hållbara datacenterinvesteringar. Microsoft stöder EU:s mål att bygga ut ytterligare datacenterkapacitet och avser att fortsätta investera i den infrastruktur som AI-utvecklingen i Europa kräver.

Microsoft noterar att regeringen i faktagruppmemoriet¹ om förslaget framhåller att regelverket bör vara proportionerligt och teknikneutralt, inte medföra större begränsningar eller kostnader än nödvändigt, inte öka regelbördan eller hämma innovation för medlemsstater eller företag, samt att fördelarna med globalt samarbete med internationella partner ska tillvaratas. Dessa utgångspunkter ligger nära de principer som Microsoft förordar nedan.

Datacenterkapacitet – tillståndprocesser och nätanslutning

¹ Förordning om utveckling av moln och AI 2025/26:FPM99

Tillgång till accelerationsområden bör knytas till hållbarhetsindikatorerna i EU:s klassificeringssystem för datacenter

Microsoft välkomnar den vikt som CADA fäster vid datacentrens hållbara prestanda och drift, inte minst genom det bredare ramverk som kommissionen utvecklar för att vägleda sektorns tillväxt. Samtidigt hade vi välkomnat en starkare harmonisering på EU-nivå genom att tillgången till accelerationsområden förankras i EU:s klassificeringssystem för datacenter (EU data center rating scheme) i stället för i EU:s rapporteringsreglering. Klassificeringssystemet är det lämpligare instrumentet för att erkänna och belöna drift i absolut framkant, vilket ytterst är den standard som bör premieras i accelerationsområdena.

För att stärka tillståndsramverkets effektivitet och skapa ett verkligt incitament för hållbara investeringar bör tillgången till områdena därför kopplas till de hållbarhetsindikatorer för datacenter som ingår i det klassificeringssystem som kommissionen nu utvecklar. Utan en sådan ansats riskerar medlemsstaterna att tillämpa olika nyckeltal hämtade från rapporteringsregleringen, inklusive indikatorer som inte är centrala för hållbarhetsprestanda. En förankring i ett gemensamt klassificeringssystem skulle istället stödja ett mer harmoniserat ramverk, stärka lika villkor på den inre marknaden och ändå låta medlemsstaterna identifiera nyckeltal som är anpassade till deras klimat och lokala förhållanden, med utgångspunkt i en gemensam uppsättning hållbarhetsindikatorer som erkänns på unionsnivå.

Accelerationsområden bör knytas till nätanslutning genom principen first ready, first served

En helhetssyn på utbyggnad av datacenter och molntjänster måste ta hänsyn till att infrastrukturkapacitet inte bara beror på snabba tillståndsprocesser, utan också på förutsägbar tillgång till energi och nätanslutning i tid. Microsoft välkomnar CADA:s målsättning att påskynda tillståndsgivningen för datacenterprojekt i utpekade accelerationsområden (artikel 10–11). Ramverkets effektivitet kommer dock ytterst att bero på om dessa områden också kan erbjuda en tydlig och tillförlitlig väg till nätanslutning. Accelerationsområden bör därför ha en bekräftad realistisk möjlighet till nätanslutning inom en förutsägbar tidsram. Utan en sådan koppling riskerar accelerationsområdena att förenkla administrativa förfaranden utan att möjliggöra den faktiska utbyggnaden.

CADA bör därför tydligare ange att ansökningar om nätanslutning i accelerationsområden bedöms och tilldelas enligt principen *first ready, first served* (FRFS) i stället för en renodlad *first come, first served*-ordning (FCFS). Därmed prioriteras projekt som kan visa verklig mognad och förmåga att genomföras. Microsoft anser att icke-bindande vägledning inte är tillräcklig, utan att en uppsättning objektiva och teknikneutrala kriterier och processteg bör föras in i EU-rätten för att stödja en mer enhetlig och harmoniserad tolkning av FRFS-principen mellan medlemsstaterna.

Två element bör särskilt adresseras. För det första behövs tydlighet om vilken bevisning som krävs för att visa projektmognad, genom större precision om vilka typer av underlag

som kan lämnas in, vilket minskar den administrativa bördan för både sökande och nätägare. För det andra behövs en stegvis, s.k. grindad, ansats för att säkerställa transparens, förutsägbarhet och investeringstrygghet, där ansökningar avancerar i anslutningskön genom en strukturerad process i flera steg. En sådan ordning motverkar spekulativa reservationer av begränsad nätkapacitet och bör tillämpas både på nya ansökningar och på befintliga anslutningsköer.

Microsoft noterar i detta sammanhang att regeringen framhåller att utbyggnaden av datacenter förutsätter investeringar i elnät och elproduktion och att beslut om accelerationsområden och strategiska projekt bör föregås av analyser ur flera perspektiv. En harmoniserad FRFS-ordning bidrar till att den begränsade nätkapaciteten tilldelas de projekt som faktiskt är redo att genomföras.

Det samlade grundtillståndets rättsliga verkan och omfattning bör förtydligas

Microsoft stöder målsättningen att inrätta ett samlat grundtillstånd (aggregated baseline permit) och en tolv månaders tidsfrist för tillståndprocessen för datacenterprojekt i accelerationsområden (artikel 13), liksom utpekandet av gemensamma informations- och kontaktpunkter (artikel 12). För att ramverket ska ge verklig rättssäkerhet och acceleration bör förordningen förtydliga grundtillståndets rättsverkan, omfattning och funktion. Tillståndet bör utgöra ett enda förvaltningsbeslut, samordnat genom den gemensamma informations- och kontaktpunkten och bindande för samtliga berörda behöriga myndigheter.

Tillståndets omfattning bör harmoniseras genom en positiv lista över vilka tillstånd som täcks, inklusive planfrågor, byggnation, miljö, vatten, spillvärmeåtervinning och nätanslutning. För att undvika fragmentering bör förordningen fastställa en harmoniserad och uttömmande uppsättning ansökningskrav samt definiera när en ansökan ska anses fullständig, vilket är den tidpunkt då tolv månadersfristen börjar löpa.

Tillståndet bör vidare ges på grundval av tydligt definierade rampparametrar, (exempelvis anläggningens markanspråk, vattenanvändning och intervall för kyllosningar), fastställda i en delegerad akt, så att projekt kan rymma teknikutveckling och etappvis utbyggnad utan att tillståndprocessen behöver öppnas på nytt. Förändringar inom den godkända ramen bör endast kräva anmälan, medan tillståndets giltighet, förlängning, överlåtbarhet och överklagande bör omfattas av tydliga och förutsägbara regler. Slutligen bör förordningen bekräfta att projekt som omfattas av undantag från miljöbedömning enligt miljöomnibusen inte behöver upprepa dessa bedömningar inom ramen för grundtillståndsförfarandet.

Strategiska projekt bör omfattas av samma tillståndsförenklingar

Enligt förslaget kan kommissionen genom beslut utse datacenterprojekt till strategiska projekt om de uppfyller minst två av de angivna kriterierna (artikel 14). En sådan utnämning underlättar enligt vår förståelse tillgången till offentliga stödåtgärder och EU:s finansieringsinstrument. Bestämmelsen anger dock inte tydligt att dessa projekt

också ska omfattas av det förenklade tillståndsförfarande som följer av förordningen om att påskynda miljöbedömningar inom miljöomnibusen.

Avsaknaden av sådan tydlighet riskerar att undergräva ett av de syften kommissionen vill uppnå, och som ingår bland kriterierna för att utses till strategiskt projekt, nämligen att åtgärda betydande brist på beräkningskapacitet i områden där sådan brist har identifierats. Microsoft anser därför att kommissionen bör förtydliga att utnämningen till strategiskt projekt ger rätt att dra nytta av förenklingarna i förordningen om att påskynda miljöbedömningar. Det undviker att utnämningen får flera olika innebörder och ger strategiska datacenterprojekt samma tillståndsförenklingar som andra projekt som utses till strategiska – även utanför accelerationsområden – enligt annan relevant unionslagstiftning, såsom den föreslagna rättsakten om industriell acceleration (Industrial Accelerator Act, IAA). Tillgång till tillståndsförenklingarna skulle säkerställa att utnämningen leder till konkreta fördelar för den faktiska utbyggnaden, och inte enbart till finansiella fördelar eller tillgång till finansieringsinstrument.

Behåll ambitionen i miljöomnibusen och använd AI i tillståndprocesserna

Förordningen² om att påskynda miljöbedömningar är ett nyckelinstrument för hela det nya tillståndsrामverk som kommissionen bygger genom sektorslagstiftning. Miljöbedömningen är ofta den del av tillståndprocessen som kräver flera steg, inklusive förprövning och samråd, och som är särskilt utdragen för storskaliga projekt. Miljöomnibusen sätter fasta tidsramar för miljöbedömningens faser och inför tyst godkännande för projekt som bedöms strategiska. Om ambitionsnivån i den förordningen sänks skulle de datacenterprojekt som utses till strategiska enligt CADA inte kunna dra nytta av verktygslådan i dess bilaga, och den gemensamma informations- och kontaktpunkten skulle inte få samordna, underlätta, följa upp och dela information om miljöbedömningar. Microsoft uppmanar därför lagstiftarna att säkerställa att ambitionen i förordningen om att påskynda miljöbedömningar upprätthålls.

Microsoft anser vidare att varken miljöomnibusen eller CADA fullt ut tar tillvara AI-systemens potential att förbättra administrativt beslutsfattande. Sådana system kan stödja förvaltningar i att lösa interna flaskhalsar och höja kunskapsnivån. Vi uppmuntrar därför kommissionen att integrera användningen av AI-system, såsom de definieras i AI-förordningen, både i artikel 10 i förordningen om att påskynda miljöbedömningar och i CADA:s bestämmelser om administrativa förfaranden och tillståndsgivning (artikel 13.5).

Autonomipelaren – ramverket för tillitsnivåer för molntjänster

CADA:s ramverk för moln- och AI-suveränitet (Union cloud sovereignty framework, artikel 16–18 och bilaga II) bygger på fyra tillitsnivåer (assurance levels), som

² Förslag till Europaparlamentets och rådets förordning om att påskynda miljöbedömningar, COM(2025) 984

tillsammans med riskbedömningarna i artikel 29–31 avgör vilka molntjänster offentliga aktörer får upphandla. Microsoft stöder målet att stärka Europas ekonomiska säkerhet, resiliens och strategiska autonomi, och lämnar nedan synpunkter på hur ramverket bör utformas för att fungera i praktiken.

En genuint riskbaserad ansats i stället för generella suveränitetskrav

Suveränitetskrav bör vara riskbaserade, proportionerliga och teknikneutrala samt stå i proportion till användningens känslighet, och inte ställas generellt. Kritiska tillämpningar i offentlig sektor kan kräva högre tillitsnivåer, medan mindre känsliga användningsområden bör behålla flexibilitet. Det är därför väsentligt att den uppsättning särskilt kritiska användningsfall inom offentlig sektor som utlöser högre krav inte bara definieras snävt utan också begränsas strikt, för att undvika otillbörlig diskriminering och för att upprätthålla EU:s åtaganden enligt WTO:s avtal om offentlig upphandling (GPA).

Ramverkets nuvarande schablonmässiga utformning, där samma tillitsnivå tillämpas oavsett användning och för samtliga kriterier, skapar två skilda problem. För det första varierar risken beroende på arbetslast, och kraven bör därför bedömas för varje enskild tillämpning snarare än åläggas en organisation som helhet. För det andra kan den tillitsnivå som behövs skilja sig åt mellan olika suveränitetsdimensioner för samma kund eller arbetslast; en kund kan exempelvis behöva mycket hög tillitsnivå avseende cybersäkerhet men en lägre nivå avseende datalokalisering. Ett krav på att välja en enda tillitsnivå för samtliga kriterier förhindrar en sådan nödvändig kalibrering. Microsoft förordar därför en modulär ansats som gör det möjligt att tillämpa olika tillitsnivåer för olika kriterier – såsom cybersäkerhet, operativ kontroll, datalagring inom EU och datalokalisering – utifrån den specifika riskprofilen för varje tillämpning. Utan en sådan kalibrering riskerar rutinmässig offentlig molnanvändning, exempelvis personalsystem, plattformar för medborgarkommunikation och icke-känslig analys, att genom en alltför extensiv riskbedömning föras upp i högre tillitsnivåer. Det skulle begränsa antalet tillgängliga leverantörer, höja kostnaderna och fördröja digitaliseringen av offentliga tjänster.

Bevara öppna och konkurrensutsatta molnmarknader

CADA bör stärka europeisk digital förmåga, inte skydda europeiska leverantörer från konkurrens genom ursprungsbaserade preferenser i upphandling. Microsoft ser en risk i att krav på geografiskt ursprung, om de tolkas som generella lokaliseringskrav, minimikrav på inhemskt innehåll eller Buy European-krav, oavsiktligt motverkar Europas egna mål. Sådana ansatser riskerar att minska konkurrens och innovation, begränsa valfriheten för offentliga aktörer, höja upphandlingskostnader, fördröja tillgången till den senaste tekniken och cybersäkerhetsförmågan samt skapa friktion mot internationella handelsåtaganden. De kan också leda till fragmentering inom den inre marknaden om medlemsstaterna tillämpar reglerna olika.

Ett mer ändamålsenligt alternativ är att prioritera förmågor som är skapade *med* Europa snarare än tillverkade i Europa. Det innebär fokus på starkt dataskydd och efterlevnad

av dataskyddsförordningen, robust cybersäkerhet med EU-baserad drift och hotbevakning, möjlighet till datalagring inom EU, transparenta och granskningsbara leveranskedjor samt uthålliga investeringar i forskning, infrastruktur och kompetens i EU. Förhandlingarna om CADA ger ett direkt tillfälle att förhindra bestämmelser som oavsiktligt kan få protektionistiska effekter och stå i strid med åtagandena enligt WTO:s GPA. D9+-deklarationen från Luxemburg i juni 2026 efterlyser redan digital suveränitet som eftersträvas på ett öppet sätt, där kritiska beroenden minskar och europeisk digital kapacitet ökar samtidigt som en öppen och pragmatisk hållning behålls som erkänner internationella partnerskaps strategiska roll, med fokus på riskbaserade ansatser och interoperabilitet. Microsoft uppmuntrar till att denna ansats tydligt återspeglas i ramverket.

Erkänn tekniska och operativa skyddsåtgärder som giltiga suveränitetsinstrument

Suveränitet kan och bör uppnås genom verifierbara skyddsåtgärder, såsom kryptering, datalagring inom EU och operativa kontroller, snarare än genom bolagsnationalitet eller hårdvarans geografiska ursprung. Till de tekniska kontrollerna hör kryptering på klientsidan, kundhanterade krypteringsnycklar, konfidentiella beräkningsmiljöer, isolering av arbetslaster samt identitets- och behörighetshantering, det vill säga mekanismer som säkerställer att endast behöriga kunder kan komma åt sina data även när infrastrukturen drivs av en extern leverantör. Till de operativa skyddsåtgärderna hör EU-baserade driftsenheter, begränsad administrativ åtkomst, säkerhetsprövad personal och granskningsbara driftsrutiner, och till de avtalsmässiga skydden hör åtaganden som skyddar kunddata mot obehörig åtkomst och säkerställer efterlevnad av EU-rätten.

Digital suveränitet bör inte likställas med exkluderande eller konstlade lokaliseringskriterier. Den bygger i stället på användarnas förmåga att välja, kombinera och byta mellan de tekniker och lösningar som bäst motsvarar deras behov. Restriktiva ansatser riskerar att medföra betydande ekonomiska kostnader och kan i förlängningen försvaga säkerhet och innovationsförmåga. Kriterierna för CADA:s tillitsnivåer bör därför uttryckligen erkänna påvisade tekniska och operativa skyddsåtgärder som likvärdiga eller kompletterande vägar att uppfylla suveränitetskraven, och därmed minska det nuvarande beroendet av etablering och nationalitet som indirekta mått.

Samordna cybersäkerhetskraven med befintlig EU-lagstiftning

CADA:s kriterier för cybersäkerhet och programvarans leveranskedja bör genomföras genom, och harmoniseras med, EU:s befintliga ramverk – cyberresiliensakten (CRA), NIS2 och de europeiska certifieringsordningarna för cybersäkerhet – i stället för att skapa en parallell och delvis motstridig uppsättning skyldigheter. De relevanta certifieringsordningarna (EUCC och den kommande EUCS) är ännu inte tillgängliga för molntjänstleverantörer, samtidigt som kriterierna för programvarans leveranskedja, sårbarhetsrapportering och öppen källkod i stor utsträckning motsvarar krav som redan hanteras inom ramen för CRA. Att införa krav innan dessa ordningar är på plats, eller i termer som avviker från CRA, skapar dubbelreglering, rättsosäkerhet och fragmenterade nationella krav.

Microsoft förordar därför att tillgången till europeiska cybersäkerhetscertifieringar påskyndas och att dessa harmoniseras mellan NIS2, CRA och CADA. I avvaktan på att certifieringarna finns tillgängliga bör väsentligen likvärdiga alternativ, såsom en bedömning av överensstämmelse enligt CRA, godtas som likvärdiga.

Precisera begreppet allmän ordning

Begreppet att bidra till upprätthållandet av allmän ordning, som utlöser skyldigheten att använda molntjänster på en högre tillitsnivå än den grundläggande, är inte definierat i CADA och saknar en enhetlig definition i unionsrätten. Det riskerar därför att tolkas olika mellan medlemsstaterna. Risken är påtaglig att tröskeln tolkas extensivt och att ett brett spektrum av ordinarie offentliga funktioner dras in i kraven för högre tillitsnivåer. CADA inför också en suveränitetsriskbedömning som avgör vilka molntjänster offentliga aktörer får använda (artikel 29–31); den centrala farhågan är att dessa bedömningar gradvis utvidgar antalet användningsområden som kräver höga tillitsnivåer och därmed begränsar konkurrensen.

CADA bör tydligt ange vilka verksamheter som kan motivera högre tillitsnivåer, och fastställa tydliga och bindande kriterier som begränsar omfattningen av de verksamheter med relevans för allmän ordning som kräver högre tillitsnivåer, så att verklig flexibilitet bevaras för huvuddelen av den offentliga sektorns molnanvändning. Microsoft förordar antingen en definierad förteckning över de verksamheter inom offentlig sektor som utlöser högre tillitsnivåer, eller en gemensam metodik från kommissionen som sätter en genuint hög tröskel för relevans för allmän ordning, begränsad till de mest kritiska användningsfallen inom försvar, brottsbekämpning, gränsförvaltning och liknande. En odefinierad standard inbjuder till fragmentering på den inre marknaden och riskerar att bli det instrument genom vilket ramverket sträcker sig långt utöver sitt avsedda syfte.

Microsoft noterar att regeringen i faktrapromemorian understryker att medlemsstaternas ansvar för bedömningar av säkerhetskrav inom exempelvis försvarsområdet måste värnas och att kommissionens befogenheter bör vara tydligt avgränsade och proportionerliga. En precis avgränsning av begreppet allmän ordning bidrar till både tydlighet för medlemsstaterna och förutsägbarhet för leverantörer.

Mekanismen för erkännande av tredjeländer bör vara genomförbar och icke-diskriminerande

Vägen till tillitsnivå 3 för leverantörer från betrodda tredjeländer måste vara praktiskt framkomlig, regelbaserad och förenlig med befintliga adekvansramverk. Som förslaget är utformat är nivå 3 i praktiken stängd för leverantörer under tredjelandskontroll, om inte kommissionen fattar ett positivt beslut om att det aktuella tredjelandet erbjuder tillräckliga skyddsåtgärder (artikel 18). Mekanismen förutsätter kumulativa villkor, bland annat ett beslut om adekvat skyddsnivå enligt dataskyddsförordningen, avsaknad av åtgärder som möjliggör motstridig kontroll eller olaglig dataåtkomst, öppet marknadstillträde och ömsesidigt tillträde till offentlig upphandling för EU-kontrollerade molntjänster. Microsoft anser att detta förfarande bör vara transparent, regelbaserat

och skyndsamt, och närmare anpassat till EU:s befintliga ramverk för adekvans enligt dataskyddsförordningen samt till dataförordningen. Villkor som går utöver adekvanskriteriet bör därför ses över. Mekanismen bör aktiveras omgående och objektivt när villkoren är uppfyllda, i stället för att kunna användas som ett politiskt påtryckningsmedel. En förutsägbar väg till erkännande skulle ge en stark signal till molntjänstleverantörer utanför EU om att storskaliga investeringar i europeisk infrastruktur möts av stabilt och tillförlitligt marknadstillträde, vilket i sin tur understödjer just den utbyggnad av datacenter- och AI-kapacitet som CADA syftar till att påskynda.

Säkerställ ett harmoniserat genomförande mellan medlemsstaterna

Metodik för CADA:s suveränitetsriskbedömning bör fastställas centralt och tillämpas enhetligt, så att det inte uppstår ett lapptäcke av nationella trösklar. Enligt förslaget genomför medlemsstaterna egna bedömningar medan kommissionen fastställer metodik och mallar genom genomförandeakter och kan åsidosätta en medlemsstats valda suveränitetsrisknivå. Även med denna säkerhetsventil är risken betydande att medlemsstaterna tolkar metodiken olika, vilket fragmenterar den inre marknaden och skapar rättsosäkerhet för leverantörer som verkar över gränserna.

Tydliga trösklar och utvärderingskriterier är avgörande för ett konsekvent genomförande hos offentliga upphandlare, och minskad subjektivitet ökar transparens och förutsägbarhet för både upphandlande myndigheter och leverantörer. Microsoft förordar därför en obligatorisk och enhetlig mall för riskbedömning med begränsat nationellt handlingsutrymme, samt ett centralt register hos kommissionen över erkända tjänster som underhålls aktivt och är allmänt tillgängligt.

Undvik en oproportionerlig utvidgning till privat sektor

CADA:s suveränitetsramverk bör förbli strikt inriktat på offentlig sektor och inte spridas till privata aktörer som omfattas av NIS2 genom delegerade akter. Även om skyldigheterna i CADA riktar sig till offentlig sektor uppmuntras privata aktörer i NIS2:s bilaga I att genomföra liknande bedömningar, och förslaget ger kommissionen möjlighet att ålägga verksamheter av hög kritikalitet sådana skyldigheter genom delegerade akter utan tydliga skäl eller objektiva kriterier (artikel 31).

En utvidgning av skyldigheten att upphandla enligt CADA:s suveränitetsramverk till NIS2-reglerade privata områden skulle utgöra en betydande och oproportionerlig utvidgning av ramverket som saknar motivering. Varje utvidgning utanför offentlig sektor bör därför ske genom det ordinarie lagstiftningsförfarandet med stöd av en översynsklausul, på grundval av tydliga kriterier och en gedigen konsekvensanalys, i stället för genom delegerade akter. En strykning av artikel 31.3 bör därför övervägas.

Offentlig upphandling av moln- och AI-tjänster

Offentlig upphandling bör i första hand säkerställa tillgång till avancerad och säker teknik för att driva digitaliseringen av EU:s ekonomi och offentliga sektor, i enlighet med målen i det digitala decenniet. Tilldelningskriterier bör vara objektiva och teknikneutrala och leda till val av lösningar som är hållbara och erbjuder ett högt cybersäkerhetsskydd, och de bör möjliggöra att små och medelstora företag fullt ut kan delta i upphandlingar. Microsoft noterar att kriterierna om europeiskt mervärde (Union added value, artikel 32) och den europeiska preferens i offentlig upphandling för strategiska sektorer och tekniker som konkurrenskraftskompassen föreslår i praktiken kan verka som ursprungsbaserade preferenser. Oavsett hur en sådan preferens definieras begränsar den i sig myndigheternas val och hindrar dem från att använda ett brett utbud av innovativa och säkra produkter till rimliga priser.

Framtida regelverk, riktlinjer och upphandlingsverktyg bör därför stödja större valfrihet för kunderna, främja en öppen och konkurrensutsatt marknad och vara förenliga med internationella standarder. Myndigheter och kunder bör kunna välja bland en mångfald av molntjänstleverantörer utifrån sina behov och utifrån objektiva och riskbaserade kriterier såsom styrning, riskhantering, säkerhet, transparens och prestanda. En sådan ansats hjälper europeiska offentliga köpare att fatta informerade beslut samtidigt som oavsiktliga konsekvenser i form av minskad leverantörs mångfald, högre kostnader, minskad resiliens eller innovation undviks.

Microsoft noterar att regeringen i faktagruppromemorian avser verka för tydliga bestämmelser som är enkla att tillämpa även för små upphandlande myndigheter, att minimera den administrativa bördan och att värna myndigheternas handlingsutrymme vid valet av tilldelningskriterier, samt att förslaget om tilldelningskriterier för europeiskt mervärde kräver fortsatt analys. Microsofts synpunkter ovan är avsedda att bidra till den analysen.

Avslutande kommentar

CADA:s ramverk för moln- och AI-suveränitet ger möjlighet att etablera en framtidsinriktad modell för digital suveränitet som balanserar strategisk autonomi med öppenhet, förutsatt att den byggs på riskproportionerliga kriterier, tekniska och operativa skyddsåtgärder, transparent styrning och ett harmoniserat genomförande. Microsoft avser att fortsätta stödja Europas digitala framtid genom investeringar i infrastruktur, suveräna molnlösningar och partnerskap inom det europeiska ekosystemet, och bidrar gärna med ytterligare underlag i den fortsatta beredningen.

Microsoft Aktiebolag genom

Frida Orring, Samhällspolitisk chef