
Remiss av Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)50

Om Axis Communications och varför vi väljer att svara på denna remiss

Axis Communications är ett svenskt teknikföretag med huvudkontor i Lund. Axis uppfann världens första nätverkskamera 1996 och är i dag en global teknikledare inom intelligent video, ljud och passerkontroll med verksamhet i över 50 länder.

Öppen källkod, interoperabilitet och internationellt samarbete är sedan länge viktiga delar i vår innovationsmodell. Våra produkter bygger sedan 1990-talet i stor utsträckning på öppen programvara och vår AXIS 2100 betraktas som den första massproducerade produkten i världen baserad på embedded Linux.

Som ett av Sveriges mest forsknings- och utvecklingsintensiva teknikföretag utvecklar vi avancerad mjukvara, egenutvecklade systemkretsar, AI-baserad analys och molnbaserade funktioner för hantering, drift och integration. Vi är därmed både utvecklare och användare av den digitala infrastruktur som omfattas av kommissionens nya förslag. Våra lösningar används dessutom av myndigheter, kommuner, verksamheter inom kritisk infrastruktur i hela Europa. Detta ger oss en konkret och praktisk förståelse för de beroende- och säkerhetsfrågor som förordningen ämnar adressera, men också de utmaningar och andra effekter som det nuvarande förslaget kan innebära.

Inledande kommentarer

Axis Communications välkomnar kommissionens ambition att stärka Europas konkurrenskraft, motståndskraft och teknologiska kapacitet inom moln och artificiell intelligens. Frågor om teknisk rådighet, säker tillgång till digital infrastruktur och förmågan att upprätthålla samhällsviktiga funktioner kommer att bli allt viktigare för Europas långsiktiga konkurrenskraft och säkerhet. Vi anser att europeisk teknisk suveränitet bör byggas genom konkurrenskraft, innovation, investeringar, öppna standarder, internationella partnerskap och diversifiering. Offentlig sektor måste även fortsättningsvis kunna välja lösningar utifrån funktionalitet, säkerhet, prestanda och kostnad. Ett regelverk som i praktiken begränsar tekniska val, skapar detaljstyrning eller leder till kostsam duplicering av befintliga lösningar riskerar att motverka sitt eget syfte

genom att försvaga Europas innovationskraft och europeiska företags globala konkurrenskraft.

Vi menar att förslaget i sin nuvarande utformning riskerar att skapa betydande osäkerhet för de företag, myndigheter och samhällsaktörer som i dag driver Europas digitala utveckling. Offentlig sektor, näringsliv och industri har genomfört omfattande investeringar i molnbaserade arkitekturer, digitala tjänster och AI-lösningar. Detta har skett i linje med EU:s egen digitaliseringspolitik och i en situation där likvärdiga europeiska alternativ till de ledande globala molnplattformarna i många fall inte har funnits tillgängliga.

Om kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)50 (på engelska kallad Cloud and AI Development Act, här framöver förkortad till CADA) i praktiken förändrar förutsättningarna för användningen av dessa plattformar innan konkurrenskraftiga alternativ finns på plats riskerar detta att skapa osäkerhet kring redan genomförda investeringar, försvåra fortsatt digitalisering och minska Europas attraktionskraft som plats för teknikutveckling och innovation.

För medlemsstater som Sverige kan effekterna bli särskilt betydande. Sverige har under lång tid varit en av Europas mest digitaliserade ekonomier och skiljer sig från många andra medlemsstater genom vår höga grad av molnanvändning, en stark exportorienterad tekniksektor och ett omfattande beroende av digitala lösningar inom både offentlig verksamhet och industrin. Det finns därför en risk att ett regelverk som syftar till att stärka Europas konkurrenskraft i praktiken får oproportionerliga konsekvenser för de medlemsstater som kommit längst i sin digitala omställning.

Avslutningsvis riskerar förslaget i praktiken att påverka långt fler aktörer än de direkta adressaterna. Det är därför viktigt att förslagets effekter också analyseras utifrån hela den digitala värdekedjan och inte enbart utifrån marknaden för molntjänster.

Våra synpunkter beskrivs mer utförligt nedan:

1. Förslagets tillämpningsområde behöver förtydligas

Förslaget bygger på samma definition av "cloud computing service" som används i NIS2. Samtidigt anges i skäl 10 att även fjärrlevererad åtkomst till AI-system kan omfattas. Kombinationen av dessa skrivningar skapar betydande osäkerhet för företag som utvecklar uppkopplade produkter där hårdvara, mjukvara, AI och molnfunktionalitet utgör delar av samma sammanhängande lösning.

För traditionella molnleverantörer kan avgränsningen vara relativt okomplicerad. För företag som utvecklar uppkopplade produkter är situationen annorlunda eftersom moderna tekniska lösningar ofta bygger på en kombination av fysisk hårdvara, lokal mjukvara, molnbaserad enhetshantering, fjärruppdateringar, analysfunktioner och AI-tjänster. Det är i dag oklart när sådana funktioner ska betraktas som en integrerad del av produkten och när de ska anses utgöra en självständig molntjänst i CADA:s mening. Denna fråga får särskild betydelse genom artikel 30, där tillämpningen av UAL-systemet kopplas till offentlig upphandling. Definitionen blir därmed inte enbart en klassificeringsfråga utan en fråga om marknadstillträde.

Förslagets definition av molntjänster är i nuvarande form mycket bred och kan omfatta såväl infrastruktur- och plattformstjänster som programvara som tillhandahålls som tjänst. Detta gör det svårt att i praktiken avgöra var gränsen går mellan en molntjänst och molnbaserade funktioner som utgör en integrerad eller kompletterande del av en produkt eller tjänst. För svenska teknikföretag som utvecklar uppkopplade produkter, AI-lösningar och andra tjänster med molnbaserade hanteringslager är denna avgränsning mycket viktig.

Vi ser en risk att olika medlemsstater kan komma att tolka gränsdragningen på olika sätt. En sådan utveckling skulle skapa osäkerhet för både leverantörer och upphandlande myndigheter samt riskera att motverka målet om en harmoniserad digital inre marknad. För företag som utvecklar uppkopplade produkter kan osäkerheten också påverka investeringsbeslut, produktutveckling och val av teknisk arkitektur långt innan regelverket börjar tillämpas.

Förordningen bör förtydliga gränsdragningen mellan fristående molntjänster och molnfunktioner som utgör en integrerad eller accessorisk del av en fysisk eller digital produkt. Reglernas omfattning bör stå i proportion till tjänstens faktiska kritikalitet och roll i den övergripande lösningen. Särskilt viktigt är att undvika att produktnära molnfunktioner automatiskt omfattas av samma krav som storskaliga molntjänster om de inte medför motsvarande riskprofil.

2. Krav och kapacitet måste utvecklas i takt med varandra

Utbyggnaden av europeisk kapacitet och införandet av nya regulatoriska krav måste ske i takt. Vi ser en risk att förslaget i sin nuvarande utformning bygger upp nya krav på efterfrågesidan innan det finns ett tillräckligt utbud av tjänster av tillräcklig förmåga som kan uppfylla dem.

CADA innehåller flera åtgärder som syftar till att stärka den europeiska marknadens kapacitet på sikt. Samtidigt införs genom artiklarna 29 och 30 krav på användning av erkända molntjänster inom offentlig sektor. Förslaget bygger därmed parallellt upp ett nytt system för bedömning, erkännande och offentlig upphandling samtidigt som marknaden förväntas utveckla tjänster som kan uppfylla dessa krav. Det finns en uppenbar risk att efterfrågan på högre UAL-nivåer uppstår betydligt snabbare än utbudet av kvalificerade tjänster, särskilt inom områden där europeiska alternativ fortfarande är under utveckling.

Detta gäller särskilt samspelet mellan artikel 22 och artikel 30. Artikel 30 förutsätter att det finns ett tillräckligt utbud av erkända tjänster som kan användas vid offentlig upphandling, medan artikel 22 inrättar det register där dessa tjänster ska föras upp. Det är dock i dag oklart i vilken omfattning erkända tjänster kommer att finnas registrerade när reglerna börjar tillämpas. Osäkerheten förstärks av att förslaget hänvisar till certifieringsmekanismer som ännu inte är fullt utvecklade eller harmoniserade på EU-nivå

Axis noterar att artikel 30.4 innehåller möjligheter att i undantagsfall frångå kraven på erkända tjänster, bland annat när lämpliga alternativ saknas eller när tillämpningen skulle medföra oproportionerliga kostnader. Dessa undantag är viktiga men löser enligt vår bedömning inte ett potentiellt strukturellt problem med otillräckligt utbud. Om ett

stort antal upphandlande myndigheter samtidigt behöver förlita sig på undantagsbestämmelser därför att marknaden ännu inte kan erbjuda tjänster på den tillitsnivå som efterfrågas, bör detta betraktas som ett tecken på att reglernas tillämpning inte är tillräckligt samordnad med marknadens faktiska mognad.

Vi ser här en uppenbar risk för ökad fragmentering inom den inre marknaden. Om medlemsstaterna ställs inför situationer där de formella kraven inte kan mötas av tillgängliga tjänster kommer olika nationella lösningar och undantag sannolikt att utvecklas. Resultatet riskerar då att bli olika tillämpning i olika medlemsstater, vilket motverkar förslaget ambition om harmonisering och ökar komplexiteten för europeiska företag. Förordningen bör därför säkerställa att utbud finns innan nya användarkrav börjar tillämpas.

För offentlig sektor och de företag som levererar digitala lösningar till denna riskerar detta att skapa betydande osäkerhet, högre kostnader och försenade upphandlingar. Detta riskerar att bli särskilt problematiskt inom säkerhetskritiska områden där val av teknik direkt påverkar förmågan att förebygga, upptäcka och hantera säkerhetshot. En ordning som begränsar tillgången till marknadsledande säkerhetslösningar innan fullgoda alternativ finns riskerar att försvaga, snarare än stärka, Europas motståndskraft.

Ambitionen att stärka europeisk suveränitet måste gå hand i hand med målet att upprätthålla högsta möjliga säkerhetsnivå för offentliga aktörer och medborgare. Tillämpningen av artikel 30 bör villkoras av att kommissionen kan visa att det finns ett tillräckligt och konkurrenskraftigt utbud av erkända tjänster för den aktuella tillitsnivån. Alternativt bör delar av tillämpningen kopplas till att ett gemensamt europeiskt certifieringssystem är fullt operativt. Grundprincipen bör vara att marknaden först måste kunna möta efterfrågan innan nya rättsliga krav börjar gälla.

3. Kraven måste åtföljas av realistiska övergångsperioder

Axis anser att förslaget kraftigt underskattar den tid som krävs för att genomföra de komplexa förändringar som de nya kraven innebär. Förslaget utgår i flera delar från att verksamheter relativt snabbt kommer att kunna anpassa sina lösningar till de nya kraven. För moderna digitala system är detta sällan fallet. Att ersätta eller migrera molnbaserade lösningar handlar i praktiken inte om ett leverantörsbyte utan om omfattande transformationsprojekt som påverkar arkitektur, integrationer, säkerhetsfunktioner, AI-modeller och verksamhetsprocesser. För offentlig sektor kan sådana projekt sträcka sig över flera år och kräva betydande investeringar. Detsamma gäller för de leverantörer som kan behöva anpassa produktarkitekturer, utvecklingsprocesser och underliggande infrastruktur för att möta de nya kraven.

Förslaget i sin nuvarande form behandlar migrering och anpassning som huvudsakligen upphandlingsmässiga eller administrativa frågor, när de i själva verket handlar om tekniskt komplexa förändringsprojekt med betydande operativa risker.

Denna problematik blir särskilt tydlig i artikel 29.6. Om en riskbedömning innebär att en verksamhet måste migrera till en annan molntjänst ska detta enligt förslaget ske inom en skäligen övergångsperiod som inte får överstiga tolv månader. Detta är en mycket kort tidsram. För komplexa och verksamhetskritiska system kan en sådan absolut och snäv tidsgräns vara svår för att förena med teknisk genomförbarhet, säker migrering,

nödvändiga integrationer, testning och krav på kontinuitet. En alltför kort migreringsperiod riskerar i sig skapa nya operativa och säkerhetsmässiga risker. En övergångsperiod på tre till fem år skulle vara mer realistisk för att kunna säkerställa en säker och ordnad omställning.

Riskerna detta innebär förstärks ytterligare av att flera av de centrala mekanismer som CADA bygger på samtidigt fortfarande är under utveckling. Det gäller bland annat tillgången till erkända tjänster på olika tillitsnivåer och samspelet med framtida europeiska certifieringssystem. Om skyldigheter börjar tillämpas innan dessa förutsättningar finns på plats riskerar verksamheter att hamna i en situation där kraven är tydliga men de praktiska möjligheterna att uppfylla dem är begränsade.

Övergångsperioder bör utformas med hänsyn till den faktiska tid som krävs för säker migrering av komplexa system och anpassning av befintliga produkter och tjänster. Den absoluta tolv månadersgränsen i artikel 29.6 bör omprövas eller kompletteras med möjlighet till längre övergångstid när teknisk komplexitet, säkerhet eller verksamhetskontinuitet motiverar detta.

4. Digital suveränitet bör utgå från faktisk teknisk och operativ kontroll

Axis delar kommissionens bedömning att Europa behöver minska sårbara beroenden och stärka sin tekniska rådighet inom digital infrastruktur. Samtidigt anser vi att förslaget ger ägarstruktur, etableringsland och juridisk hemvist en alltför framträdande roll i förhållande till den faktiska tekniska och operativa kontrollen över en tjänst. Dessa faktorer är relevanta i en riskbedömning, men de ger inte ensamma en rättvisande bild av var den faktiska rådigheten över teknik, data och säkerhetsfunktioner ligger. Europas digitala ekosystem är djupt integrerat i globala värdekedjor för mjukvara, halvledare, molntjänster och artificiell intelligens. Detsamma gäller programvaruförsörjningskedjor, där moderna digitala produkter regelmässigt bygger på en kombination av egenutvecklad programvara, kommersiella komponenter och öppen källkod. Den centrala frågan bör därför inte vara en komponents geografiska ursprung, utan om leverantören har tillräcklig insyn, kontroll och förmåga att identifiera och hantera risker genom hela produktens livscykel.

För moderna digitala tjänster avgörs den faktiska rådigheten i hög grad av var tekniken utvecklas och underhålls, vem som kontrollerar källkod, programvaruuppdateringar, data och kryptografiska nycklar samt vem som har administrativ åtkomst och faktisk möjlighet att påverka eller stänga ned tjänsten. Ett företag kan formellt vara etablerat inom EU men samtidigt vara beroende av kritiska komponenter, utvecklingsresurser eller leveranskedjor utanför unionen. Omvänt kan ett företag med utomeuropeiska ägarintressen ha forskning, utveckling, säkerhetsfunktioner, personal och operativ kontroll koncentrerade till Europa. En bedömning som ensidigt utgår från ägande eller jurisdiktion riskerar därför att ge en missvisande bild av den faktiska risken. Detta blir särskilt tydligt i artikel 18, där kommissionen ges möjlighet att identifiera tredjeländer vars kontrollerade leverantörer kan kvalificera sig för högre tillitsnivåer. Axis anser att frågor om leverantörer som bedöms utgöra en hög och dokumenterad säkerhetsrisk för unionen bör hanteras genom en gemensam och transparent EU-process. Om säkerhetspolitiska eller geopolitiska skäl motiverar begränsningar av vissa leverantörers marknadstillträde bör sådana beslut fattas centralt på unionsnivå efter en dokumenterad riskbedömning. Detta skulle bidra till en mer harmoniserad tillämpning,

stärka rättssäkerheten och minska risken för olika nationella bedömningar som fragmenterar den inre marknaden.

En mer träffsäker modell vore att betrakta ägarstruktur och jurisdiktion som en del av den samlade riskbilden snarare än som avgörande kriterier i sig. Bedömningen bör kompletteras med faktorer som teknisk rådighet, operativ kontroll, beroenden till externa leverantörer, kontroll över uppdateringar och säkerhetsfunktioner samt möjligheten att upprätthålla tjänsten vid störningar eller förändrade geopolitiska förutsättningar. En sådan ansats skulle ge en mer rättvisande bild av faktisk digital suveränitet samtidigt som den bättre speglar hur moderna teknik- och molnekosystem fungerar i praktiken. En sådan ordning skulle också göra det möjligt för UAL-systemet att i större utsträckning fokusera på teknisk säkerhet, motståndskraft och faktisk operativ kontroll.

Ett ytterligare problem är att CADA:s tillitsnivåer bygger på en annan logik än befintlig europeisk resiliens- och cybersäkerhetslagstiftning. Medan NIS2- och CER-regelverken utgår från verksamhetens funktion, kritikalitet och faktiska riskbild, utgår CADA i högre grad från leverantörens ursprung, kontrollstruktur och jurisdiktion. Utan ett tydligare samspel mellan dessa regelverk riskerar företag och myndigheter att möta parallella och delvis motstridiga modeller för riskhantering, vilket kan skapa osäkerhet om vilka kriterier som ska väga tyngst vid bedömningar av säkerhet och motståndskraft. Axis anser därför att CADA så långt som möjligt bör bygga vidare på den risk- och förmågebaserade ansats som redan etablerats genom NIS2 och CER.

Förordningen bör i högre grad harmonisera med den risk- och förmågebaserade metodik som redan etablerats genom NIS2 och CER. Bedömningar enligt CADA bör i större utsträckning utgå från faktisk teknisk och operativ kontroll. Ägarstruktur och jurisdiktion bör ses som viktiga riskfaktorer, men vägas samman med faktorer såsom kontroll över källkod, programvaruuppdateringar, administrativ åtkomst, krypteringsnycklar, driftmiljöer och den faktiska förmågan att upprätthålla tjänstens funktion och säkerhet över tid. Om säkerhetspolitiska eller geopolitiska skäl motiverar begränsningar av vissa leverantörer bör sådana beslut fattas genom en gemensam och transparent process på EU-nivå, grundad på en dokumenterad riskbedömning och tydliga rättssäkerhetsgarantier.

5. Portabilitet och interoperabilitet bör främjas på ett proportionerligt sätt

Axis välkomnar åtgärder som stärker interoperabilitet, öppna standarder och möjligheten att flytta data mellan olika miljöer. Sådana åtgärder kan bidra till ökad motståndskraft, minskad inlåsning och en mer konkurrenskraftig digital marknad. Samtidigt är det viktigt att skilja mellan dataportabilitet och teknisk portabilitet. Att användare kan exportera och flytta sina data mellan olika tjänster är i många fall både rimligt och önskvärt. Att däremot kräva att avancerade digitala tjänster ska kunna flyttas mellan olika plattformar utan betydande kostnader, anpassningar eller funktionella kompromisser är en betydligt mer komplex fråga.

Moderna moln- och AI-tjänster bygger ofta på djupt integrerade tekniska miljöer där funktionalitet, prestanda, säkerhet och skalbarhet är nära sammankopplade med den underliggande infrastrukturen. Krav på långtgående teknisk portabilitet kan därför medföra betydande utvecklingskostnader, ökad komplexitet och i vissa fall begränsa

möjligheten att utnyttja avancerade funktioner eller säkerhetslösningar. Detta riskerar att minska incitamenten för innovation och försvaga Europas konkurrenskraft inom strategiskt viktiga teknikområden.

För företag som utvecklar avancerade produkter och tjänster kan omfattande portabilitetskrav innebära att resurser flyttas från forskning, produktutveckling och cybersäkerhet till arbete med att upprätthålla kompatibilitet mellan flera olika tekniska miljöer. Ett sådant krav riskerar därmed att hämma innovation snarare än att främja den. Vi ser även en risk att portabilitet ges en alltför framträdande roll i offentlig upphandling utan att vägas mot andra viktiga kriterier. För myndigheter, kommuner och regioner måste säkerhet, funktionalitet, prestanda, innovationsförmåga och totalkostnad fortsatt vara centrala utgångspunkter. Den mest ändamålsenliga lösningen bör inte väljas bort enbart därför att den är enklare att flytta från i framtiden. Axis menar därför att portabilitet bör betraktas som ett verktyg för att minska omotiverad inlåsning, inte som ett mål i sig. I många fall kan öppna standarder, gemensamma gränssnitt, väldokumenterade API:er och effektiva möjligheter till dataexport ge större nytta än krav på full teknisk flyttbarhet mellan olika plattformar.

Förordningen bör tydligare skilja mellan dataportabilitet och teknisk portabilitet. Krav på teknisk portabilitet bör endast införas när de är tydligt motiverade, riskbaserade och proportionerliga. Mot bakgrund av artikel 29 bör det förtydligas att migrationskrav normalt kan uppfyllas genom dataportabilitet, öppna standarder, väldokumenterade gränssnitt och dokumenterade migrationsmekanismer, utan att detta förutsätter full teknisk kompatibilitet mellan olika plattformar.

6. Skyddet för immateriella rättigheter, källkod och leverantörskedjor behöver stärkas

Vissa delar av förslagets gransknings- och dokumentationskrav riskerar att få betydande konsekvenser för immateriella rättigheter och globala leverantörskedjor. De mest långtgående kraven återfinns i Annex III, särskilt punkt 9, där omfattande dokumentation av programvaruförsörjningskedjan krävs. Punkt 9.4(b) innebär dessutom att den granskade leverantören ska säkerställa att den oberoende revisorn ges rätt att få tillgång till och granska relevant källkod samt tillhörande dokumentation.

Moderna digitala produkter bygger på komplexa kombinationer av egenutvecklad programvara, kommersiella tredjepartskomponenter och öppen källkod. För många leverantörer är det varken tekniskt eller avtalsmässigt möjligt att säkerställa att externa granskare kan ges tillgång till och revisionsrätt avseende all relevant källkod i de komponenter som ingår i en produkt eller tjänst. Leverantören äger i många fall inte själv dessa komponenter och kan sakna såväl faktisk tillgång till källkoden som avtalsmässig rätt att göra den tillgänglig för tredje part.

Det är inte heller realistiskt att förutsätta kontroll över den framtida utvecklingen av alla relevanta programvarukomponenter. Praktiskt taget alla avancerade digitala system bygger på globala beroenden i form av operativsystem, bibliotek, verktygskedjor, utvecklingsverktyg och open-source-projekt. Den relevanta frågan bör därför vara om leverantören har tillräcklig insyn och faktisk förmåga att identifiera risker, underhålla kritiska komponenter och vid behov ersätta eller begränsa beroenden, snarare än var en

komponent ursprungligen har utvecklats eller vem som i framtiden kan komma att bidra till dess utveckling.

Mot denna bakgrund ser vi en risk att kraven i praktiken sprids genom hela leverantörskedjan. En komponentleverantör eller mjukvaruutvecklare som aldrig själv avser att få en tjänst erkänd enligt CADA kan ändå möta krav på källkodsåtkomst, revisionsrättigheter eller utökad dokumentation därför att en kund längre upp i värdekedjan omfattas av regelverket. Om sådana krav måste säkras avtalsvägen kan effekterna därmed omfatta ett betydligt större antal aktörer än de som formellt omfattas av förordningen. Detta riskerar att skapa osäkerhet för såväl europeiska som internationella teknikleverantörer och kan minska viljan att tillhandahålla avancerade komponenter på den europeiska marknaden om skyddet för immateriella rättigheter, företagshemligheter och tredjepartsrättigheter uppfattas som otillräckligt.

Krav som utgår från att varje komponent har en tydligt identifierbar kontrollstruktur, jurisdiktion eller alternativ leverantör är också svåra att tillämpa på öppen källkod. Det är välkommet att kommissionen uttryckligen lyfter fram öppen källkod som ett verktyg för europeisk teknisk suveränitet, konkurrenskraft och säkerhet. De konkreta kraven i UAL-systemet behöver dock utformas så att de är förenliga med hur öppna programvaruekosystem faktiskt fungerar. Open-source-programvara utvecklas ofta i globala och decentraliserade projekt där det inte finns någon enskild leverantör som kontrollerar utveckling, underhåll eller framtida bidrag. Projekt kan förvaltas av internationella communities eller stiftelser och har utvecklare, infrastruktur och beroenden i flera jurisdiktioner. Annex II ställer för UAL 2–4 särskilda krav på dokumenterade kontroller när programvara under open-source-licens används. Annex III går längre och förutsätter bland annat riskhantering av open-source-beroenden, identifiering av alternativa lösningar och planer för att kunna byta till dessa samt mekanismer för att hantera förändringar i kontrollen över open-source-projekt. Sådana krav behöver vara riskbaserade och proportionerliga och utformas så att de inte skapar osäkerhet kring användningen av etablerade och väl underhållna open-source-komponenter.

Tillgång till källkod innebär inte heller i sig operativt oberoende eller digital suveränitet. Att självständigt kunna underhålla, vidareutveckla och drifva ett komplext system kräver kompetens, resurser och organisatorisk förmåga som går långt utöver själva tillgången till källkoden. Även här bör bedömningar av teknisk rådighet utgå från den faktiska förmågan att upprätthålla tjänstens funktion, säkerhet och långsiktiga utveckling, inte från tillgång till källkod som sådan.

Avslutningsvis vill vi lyfta artikel 20.3 som innehåller sekretess- och tystnadspliktskrav för den oberoende revisorn. Samtidigt framgår att dessa krav inte får hindra revisionens genomförande. Detta skapar osäkerhet kring hur skyddet för företagshemligheter, tredjepartsrättigheter och immateriella tillgångar kommer att fungera i praktiken. Här menar vi att säkerhetsgranskning i första hand bör inriktas på att verifiera identifierade risker. I många fall kan motsvarande säkerhetsnytta uppnås genom mindre ingripande åtgärder såsom teknisk dokumentation, säkerhetsrevisioner, SBOM eller verifiering av processer och kontroller.

Krav på tillgång till och revision av källkod bör begränsas till de delar av en tjänst där sådan insyn är nödvändig för att bedöma eller verifiera en specifik och identifierad risk. Åtkomsten bör vara strikt proportionerlig och avgränsad till den information som krävs för det aktuella ändamålet. Förordningen bör även tydliggöra att leverantörer inte kan åläggas att lämna ut källkod som tillhör tredje part eller som de saknar rättslig eller faktisk möjlighet att tillhandahålla. Samtidigt bör starka och tydliga skydd säkerställas för företagshemligheter, immateriella rättigheter och andra konfidentiella uppgifter som delas inom ramen för granskningsförfaranden.

Regelverket bör dessutom skilja mellan faktiska säkerhets- och beroenderisker och de globala och decentraliserade utvecklingsmodeller som präglar många open source-projekt. Förordningen bör undvika att skapa incitament att ersätta eller begränsa användningen av open source-lösningar utan en tydligt motiverad och riskbaserad grund.

7. Samma säkerhetsarbete ska inte behöva dokumenteras flera gånger

Nya regler måste samspela med den omfattande cybersäkerhets- och digitaliseringslagstiftning som redan införts på EU-nivå under de senaste åren. Många företag arbetar redan i dag med omfattande krav på riskhantering, dokumentation, leverantörskedjor, produktsäkerhet och teknisk efterlevnad enligt bland annat NIS2, CRA, AI Act, GDPR, Data Act och i vissa sektorer även DORA. Flera av de uppgifter som efterfrågas inom ramen för CADA överlappar i stor utsträckning den information som företag redan behöver ta fram enligt andra unionsrättsliga regelverk. Exempelvis efterfrågar Annex III i flera delar information om programvaruberoenden, utvecklingsprocesser, leverantörskedjor och SBOM:er som redan i dag dokumenteras enligt andra unionsrättsliga regelverk, särskilt CRA.

Problemet är i sig inte nödvändigtvis att kraven är identiska utan att företag riskerar att behöva beskriva, verifiera och rapportera samma tekniska verklighet flera gånger i olika processer, format och granskningsystem. Detta innebär betydande administrativa kostnader utan att nödvändigtvis bidra till ökad säkerhet. Särskilt problematiskt blir detta om olika regelverk utvecklar separata krav på i grunden samma information, men med mindre skillnader i metodik eller format.

Vi menar därför att CADA i större utsträckning bör bygga vidare på befintliga europeiska regelverk och certifieringsstrukturer. Där en leverantör redan har visat att ett visst krav är uppfyllt enligt annan unionslagstiftning bör detta som huvudregel kunna återanvändas även inom ramen för CADA. Ett sådant synsätt skulle minska administrativa kostnader, förenkla efterlevnaden och bidra till ett mer sammanhållet europeiskt regelverk utan att sänka säkerhetsnivån.

Principen "produce once, use many times" bör genomsyra CADA. Dokumentation, riskanalyser, säkerhetsbedömningar och annan evidens som redan tagits fram och verifierats enligt annan relevant EU-lagstiftning bör kunna återanvändas när den visar samma eller likvärdiga förhållanden. Förordningen bör uttryckligen uppmuntra återanvändning av befintlig dokumentation och undvika uppbyggnaden av parallella dokumentations- och granskningsregimer.

8. Förslagets effekter kommer sannolikt att sträcka sig utanför offentlig sektor och detta bör konsekvensbedömas

CADA beskrivs ofta som ett regelverk för offentlig upphandling och användningen av moln- och AI-tjänster inom offentlig sektor. Digitala marknader fungerar sällan så att krav stannar hos de aktörer som formellt omfattas av regleringen och vi menar att det finns goda skäl att anta att de faktiska effekterna av CADA kommer att bli betydligt bredare. Erfarenheter från annan EU-lagstiftning, exempelvis NIS2, visar att krav som införs för offentlig eller särskilt reglerade verksamheter ofta sprids genom leverantörskedjor, upphandlingsvillkor och marknadspraxis. Företag som inte direkt omfattas av lagstiftningen påverkas därmed indirekt genom kundkrav.

Denna utveckling är inte enbart en möjlig konsekvens av förslaget utan förutses också i viss utsträckning av kommissionen: I skäl 66 konstateras att offentlig upphandling ofta fungerar som en signal för marknadens utveckling och att krav på specifika tillitsnivåer i offentlig sektor sannolikt kommer att påverka efterfrågan även hos privata aktörer, särskilt i reglerade branscher. Förslaget bygger därmed uttryckligen på antagandet att UAL-systemet över tid kommer att få effekter långt utanför den offentliga sektorn.

Denna risk för spridningseffekter förstärks ytterligare av artikel 31.3, som ger kommissionen möjlighet att genom delegerade akter göra motsvarande riskbedömningar obligatoriska även för privata aktörer i sektorer av hög kritikalitet. Sammantaget innebär detta att UAL-systemet på sikt kan komma att påverka användningen av moln- och AI-tjänster i betydligt större delar av ekonomin än vad som framgår av förslagets formella tillämpningsområde.

Detta blir särskilt relevant inom digital infrastruktur och cybersäkerhet, där offentliga och privata aktörer i stor utsträckning använder samma teknik, leverantörer och lösningar. När myndigheter börjar ställa krav på vissa tillitsnivåer, certifieringar eller leverantörsegenskaper uppstår ofta motsvarande förväntningar i privata verksamheter med höga säkerhetskrav. För svenska teknikföretag kan detta få betydande konsekvenser. Många levererar samtidigt till offentlig sektor och till privata verksamheter inom energi, industri och transport.

Ytterst handlar detta om marknadstillträde. Även om regelverket formellt riktas mot offentlig sektor kan det i praktiken komma att forma konkurrensvillkoren för stora delar av den europeiska teknikmarknaden. Axis anser därför att konsekvenserna för privata aktörer, innovation, konkurrenskraft och investeringar bör analyseras mer ingående än vad som gjorts hittills. Annars finns en risk att betydande marknadseffekter uppstår utan att de har analyserats fullt ut.

Konsekvenserna för den privata sektorn bör analyseras betydligt mer ingående innan förordningen antas. Särskilt viktigt är att eventuella framtida utvidgningar till privata verksamheter föregås av egna konsekvensbedömningar. Förordningen bör också utformas så att UAL-systemet inte i praktiken utvecklas till en generell marknadsstandard med betydande effekter på marknadstillträde och konkurrens utan att detta först har prövats genom ordinarie lagstiftningsprocess.

9. UAL 1 bör utgöra europeisk basnivå

Att skapa ett gemensamt europeiskt system för bedömning och erkännande av moln- och AI-tjänster är klokt. En förutsättning för att ett sådant system ska fungera är dock

att det är enkelt att tillämpa, förutsägbart för leverantörer och harmoniserat inom hela unionen.

Vi ser en risk att UAL 1 i praktiken blir mer administrativt betungande än vad som framstår av förslaget. UAL 1 bygger på en självbedömning och en EU-försäkran om överensstämmelse från leverantören. För små och medelstora företag innehåller artikel 17.3 en särskild ordning där en sådan försäkran erkänns direkt och automatiskt i samtliga medlemsstater utan föregående erkännande av den nationella behöriga myndigheten. För andra leverantörer gäller däremot det ordinarie erkännandeförfarandet enligt artikel 17, med nationell bedömning och efterföljande granskning av övriga medlemsstater.

Axis har svårt att se de sakliga skälen till varför principen om ömsesidigt erkännande ska vara beroende av ett företags storlek och hur detta skapar mervärde ur säkerhets- eller tillsynsperspektiv. En sådan modell riskerar att skapa onödiga ledtider, ökad administration och leda till olika tillämpning mellan medlemsstater. Den riskerar också att motverka ett av grundsyftena med den inre marknaden, nämligen att en tjänst som lagligen erkänts i en medlemsstat ska kunna erbjudas i hela unionen utan ytterligare administrativa hinder. Från ett svenskt perspektiv är detta särskilt viktigt. Många svenska teknikföretag verkar på en europeisk marknad från första dagen och är beroende av snabba och förutsägbara processer för att kunna introducera nya tjänster och lösningar.

En korrekt utfärdad deklaration om överensstämmelse för UAL 1 bör medföra automatiskt ömsesidigt erkännande i hela unionen, oavsett företags storlek. Nationell tillsyn och kontroll bör fortsatt kunna ske i efterhand, men den grundläggande principen bör vara att UAL 1 utgör en verklig europeisk basnivå.

10. Kostnaden och komplexiteten med migrering riskerar att underskattas

Att kunna ersätta en leverantör och minska kritiska beroenden är en viktig del av en robust digital infrastruktur. Samtidigt måste CADA ta hänsyn till den praktiska verkligheten för moderna digitala miljöer. Förslaget innebär bland annat att medlemsstater och unionsorgan ska överväga multi-vendor- och multi-cloud-strategier samt att riskbedömningar i vissa fall kan leda till krav på migration till en annan molntjänst.

Som framhållits ovan innebär dataportabilitet inte nödvändigtvis att komplexa system kan flyttas mellan olika plattformar utan omfattande tekniska anpassningar. Moderna digitala lösningar bygger ofta på djupt integrerade miljöer där lokala system, molntjänster, AI-funktionalitet och tredjepartsintegrationer samverkar. Att byta plattform eller upprätthålla parallella miljöer kan därför kräva omfattande omarkitekturering, testning och anpassning, med betydande kostnader samt operativa och säkerhetsmässiga risker som följd.

Denna problematik blir särskilt tydlig i artikel 29.6. Om en riskbedömning leder till krav på migration ska övergången enligt förslaget genomföras inom en period som inte får överstiga tolv månader. För komplexa och verksamhetskritiska system kan en sådan absolut tidsgräns vara svår att förena med teknisk genomförbarhet, nödvändig testning,

säker migrering och krav på verksamhetskontinuitet. En alltför kort migreringsperiod riskerar dessutom att skapa nya operativa och säkerhetsmässiga risker. Tolv månader framstår också som en begränsad tidsram i förhållande till de tekniska och regulatoriska processer som ofta krävs inom området. Vissa certifierings- och granskningsförfaranden kan exempelvis ta flera år att genomföra. En generell maxtid riskerar därför att bli oproportionerlig i förhållande till de faktiska förutsättningarna för en säker och ordnad migration.

Konsekvenserna sträcker sig dessutom bortom användarna av molntjänster. Leverantörer av digitala produkter och tjänster kan påverkas om möjligheten att delta i offentlig upphandling i praktiken blir beroende av vilken molninfrastruktur deras lösningar använder. Det kan skapa behov av parallella lösningar eller omfattande tekniska anpassningar för att bibehålla marknadstillträde. Även offentlig sektor kan påverkas genom ökade migrationskostnader och begränsad tillgång till den teknik som bäst möter verksamhetens behov under en övergångsperiod.

Den fortsatta behandlingen av CADA bör utgå från en realistisk bedömning av de tekniska, operativa och ekonomiska konsekvenserna av migrering. Den absoluta tolv månadersgränsen i artikel 29.6 bör omprövas eller kompletteras med möjlighet till längre övergångsperioder när teknisk komplexitet, säkerhetskrav eller verksamhetskontinuitet motiverar detta. Bedömningar av migration, multi-vendor- och multi-cloud-strategier bör vara riskbaserade och proportionerliga samt väga den förväntade resiliensnyttan mot konsekvenserna för säkerhet, funktionalitet, kostnader och innovation.

11. Offentlig sektor måste även fortsättningsvis ha tillgång till den mest ändamålsenliga tekniken

I dag utgör moln- och AI-tjänster en viktig del av den digitala infrastrukturen inom såväl offentlig sektor som många säkerhets- och industrikritiska verksamheter, ofta som en del av hybridmiljöer där molnlösningar samverkar med lokala system. För många av dessa verksamheter är tillgången till den mest ändamålsenliga och avancerade tekniken en förutsättning för att kunna upprätthålla hög säkerhet, operativ förmåga och motståndskraft. Om tillgången till sådana teknologier begränsas innan funktionellt likvärdiga alternativ finns tillgängliga riskerar offentlig sektor att få sämre förutsättningar att välja de lösningar som bäst möter verksamhetens behov. Detta kan i sin tur påverka säkerhet, effektivitet och operativ förmåga hos de aktörer som ansvarar för att skydda samhällsviktiga funktioner.

Detta är särskilt viktigt i en tid då myndigheter, kommuner och regioner möter ett alltmer komplext cyberhotlandskap och samtidigt förväntas stärka sin digitala motståndskraft. Regelverket bör därför utformas på ett sätt som stärker Europas säkerhet utan att under en övergångsperiod begränsa tillgången till teknik som redan i dag bidrar till att skydda samhällsviktig verksamhet.

Axis anser därför att det är viktigt att skilja mellan två mål som inte nödvändigtvis uppnås genom samma åtgärder. Att bygga upp europeisk kapacitet och stärka Europas tekniska rådighet är ett legitimt och viktigt industripolitiskt mål. Att säkerställa att offentlig sektor har tillgång till de mest ändamålsenliga lösningarna för att skydda

medborgare och samhällsfunktioner är ett annat. I många fall kan dessa mål förstärka varandra, men under en övergångsperiod kan det också uppstå målkonflikter.

CADA bör säkerställa att ambitionen att stärka Europas tekniska rådighet inte sker på bekostnad av offentlig sektors tillgång till den teknik som bäst uppfyller krav på säkerhet, funktionalitet och operativ förmåga. Vid tillämpningen av artiklarna 29 och 30 bör särskild hänsyn tas till verksamheter med höga krav på cybersäkerhet och verksamhetskcontinuitet.

Om funktionellt likvärdiga alternativ saknas bör offentliga aktörer kunna använda den lösning som ger högst säkerhetsnivå och bäst stöd för verksamhetens uppdrag. Begränsningar av tillgången till befintliga lösningar bör endast införas när de bygger på tydligt identifierade risker och en dokumenterad proportionalitet mellan säkerhetsnytta och samhällsekonomisk kostnad.

12. Konsekvensanalysen underskattar effekterna för teknikindustrin

Axis anser att den konsekvensanalys som ligger till grund för förslaget inte fullt ut fångar hur moderna digitala produkter och tjänster utvecklas och levereras. Analysen fokuserar i stor utsträckning på marknaden för molntjänster och relationen mellan användare och molnleverantörer. Däremot ges relativt begränsat utrymme åt de företag vars produkter och tjänster bygger på molninfrastruktur utan att själva vara traditionella molntjänster.

I praktiken utvecklas stora delar av dagens säkerhetslösningar, AI-applikationer, industriella system och uppkopplade produkter i komplexa ekosystem där flera olika leverantörer samverkar. Effekter som uppstår på infrastrukturnivå får därför konsekvenser långt upp i värdekedjan. Axis ser också att konsekvensanalysen i begränsad utsträckning behandlar de kostnader och tekniska utmaningar som uppstår när företag behöver anpassa befintliga produkter, tjänster eller affärsmodeller till nya krav.

Nuvarande förslag bör kompletteras med en mer omfattande analys av effekterna för europeiska teknikföretag, särskilt företag som utvecklar uppkopplade produkter, AI-lösningar och digitala tjänster där molnfunktionalitet utgör en integrerad del av erbjudandet.

Axis Communications AB
Lund, oktober 2026