

Finansdepartementet

fi.remissvar@regeringskansliet.se

**Remissvar avseende
Europeiska kommissionens förslag till Cloud and AI Development Act (CADA), en rättsakt om utveckling av moln
och AI KOM(2026)502**

Amazon Web Services ('AWS') tackar för möjligheten att yttra sig över Finansdepartementets remiss av Europeiska kommissionens förslag till Cloud and AI Development Act ('CADA').

AWS stöder förslaget mål att öka Europas moln- och AI-kapacitet, påskynda investeringar i datacenter och stärka motståndskraften i kritisk digital infrastruktur. Delar av det föreslagna ramverket för autonomi riskerar dock att begränsa tillgången till säkra molntjänster med god kapacitet utan att förslaget visar ett tydligt samband mellan begränsningen och den risk den ska hantera. Reglerna för hur medlemsstaterna ska genomföra avdelning III behöver också bli tydligare om mekanismen för att attrahera investeringar ska bli effektiv och enhetlig.

Innan EU antar nya regler med betydande marknadspåverkan bör nyligen antagna regler få verka och utvärderas på medellång till lång sikt. EU:s dataförordning, som tillämpas sedan september 2025, förbjuder exempelvis redan avgifter vid byte av leverantör, begränsar uppsägningstiderna och fastställer tidsramar för övergången. Den hanterar alltså redan de hinder för leverantörbyte som förslaget pekar på. Förslaget saknar också en bedömning av kostnaderna för nationella budgetar, innovation eller små och medelstora företag, eller av hur det påverkar det uttalade målet att attrahera 200 miljarder euro i privata investeringar. Begränsningar som grundas på nationalitet riskerar att motverka detta mål.

Frågan berör direkt Sveriges ambition att tillhöra världens tio ledande AI-nationer. Det kräver säker och motståndskraftig digital infrastruktur, tillgång till avancerad moln- och AI-teknik samt förutsägbara villkor för långsiktiga investeringar.

AWS har gjort betydande investeringar i svensk molninfrastruktur. AWS Europe (Stockholm) Region lanserades 2018 och drivs genom datacenterkluster i Eskilstuna, Katrineholm och Västerås. Mellan 2017 och 2025 investerade AWS mer än 39 miljarder kronor med anknytning till regionen, inklusive kapitalinvesteringar och driftskostnader.

AWS bidrar också till Sveriges digitala kompetens och innovationsmiljö för nystartade företag. Sedan 2017 har AWS utbildat fler än 60 000 personer i Sverige i molnkompetens. Sedan 2011 har fler än 2 400 svenska nystartade företag använt AWS för att utveckla, lansera och skala upp sina lösningar.

Andelen svenska företag som använder AI har ökat från 35 procent till 48 procent under det senaste året. Det visar undersökningen Unlocking Sweden's AI Potential 2026, som Strand Partners har gjort på uppdrag av AWS. Sverige ligger ändå under det europeiska genomsnittet på 54 procent, och bara 26 procent av de svenska företag som använder AI uppger att de använder avancerade eller genomgripande AI-tillämpningar. Fler svenska organisationer behöver alltså gå från att pröva AI till att använda tekniken på djupet. Proportionerlig och förutsägbar reglering gör den övergången lättare. Svenska företag ser tillgången till globala teknikleverantörer som viktig: 87 procent anser att den är viktig för innovation och 90 procent att den är viktig för att snabbt kunna skala upp.

AWS rekommenderar att regeringen driver en riskbaserad och teknikneutral linje i förhandlingarna i rådet. Kraven bör utgå från den säkerhet, motståndskraft, kontinuitet och kundkontroll som en leverantör kan visa. Leverantörens nationalitet eller enskilda komponenters ursprung bör inte i sig vara avgörande. Begränsningar bör bara komma i fråga när en specifik och dokumenterad risk har identifierats, till exempel att ett tredjelands lagstiftning medger åtkomst till data eller ingripanden i tjänsten utan rättsliga skyddsåtgärder, och risken inte kan hanteras genom mindre ingripande åtgärder.

AWS rekommenderar att regeringen:

1. Stöder ett transparent och proportionerligt ramverk för den offentliga sektorns riskbedömning och riskreducering enligt artiklarna 29–30. Ramverket bör erkänna alternativa skyddsåtgärder, medge motiverade förlängningar vid komplexa migreringar och begränsa kommissionens befogenhet att ersätta nationella bedömningar.

2. Verkar för en översyn av nivåerna 3 och 4 inom Union Assurance Levels ('UAL'), systemet för unionens tillitsnivåer, så att båda nivåerna grundas på granskningsbara tekniska och organisatoriska kontroller för säkerhet, operativ autonomi, kontinuitet och kundkontroll i stället för på leverantörens nationalitet.
3. Stöder ett förutsägbart ramverk för erkännande av associerade tredjeländer enligt artikel 18. Tredjeländer som är parter i WTO:s avtal om offentlig upphandling ('GPA') och omfattas av ett EU-beslut om adekvat skyddsnivå bör som huvudregel erkännas på UAL 3, med förbehåll för lämpliga skyddsåtgärder. Övriga tredjeländer bör bedömas genom ett objektiva och tidsbegränsat förfarande som ger leverantörerna rättslig förutsägbarhet.
4. Verkar för att artikel 31 utgår. En eventuell utvidgning av obligatoriska krav till privata företag bör ske genom det ordinarie lagstiftningsförfarandet, inte genom delegerade akter. En sådan utvidgning bör förutsätta belägg för en väsentlig risk, samråd med berörda sektorer och en bedömning av samspelet med befintlig EU-lagstiftning.
5. Verkar för praktiskt genomförbara och harmoniserade regler för investeringar i datacenter. Bestämmelserna om accelerationszoner bör tydliggöra tidsfristerna för tillståndsgivning, säkerställa förutsägbara hållbarhetskrav och fastställa operativa regler för fördelning av begränsad nätkapacitet.

Artiklarna 29–30: riskbedömning och riskreducering

AWS stöder principen att säkerhetskrav bör återspegla den offentliga verksamhetens känslighet och konsekvenserna av en säkerhetsincident eller ett avbrott i tjänsten.

Olika arbetslaster i den offentliga sektorn medför olika risker. En tjänst som används för att publicera allmän information behöver inte samma skyddsåtgärder som en tjänst som behandlar känsliga personuppgifter eller stöder den kontinuerliga driften av en samhällsviktig offentlig tjänst. Ramverket bör därför skilja mellan risker för konfidentialitet, riktighet, tillgänglighet och operativ kontinuitet.

Artiklarna 29 och 30 kopplar resultatet av riskbedömningen till en av unionens fyra tillitsnivåer. En upphandlande myndighet skulle sedan bara få använda molntjänster som har erkänts på den nivån.

Artikel 29 kräver uttryckligen att medlemsstater och unionsorgan överväger om en strategi med flera leverantörer eller flera molnmiljöer är lämplig. Artikel 30 medger dock inte tydligt att sådana åtgärder, eller andra tekniska, avtalsbaserade och operativa skyddsåtgärder, är ett annat sätt att uppfylla kraven när en viss tillitsnivå väl har fastställts.

Artikel 30 innehåller begränsade undantag när erkända tjänster inte är tillgängliga, en tidigare upphandling har misslyckats eller efterlevnaden skulle medföra oproportionerliga kostnader. Inget av undantagen låter en upphandlande myndighet visa att ett likvärdigt skydd har uppnåtts genom andra skyddsåtgärder.

En svensk myndighet kan exempelvis minska konfidentialitetsriskerna genom att behålla kontrollen över krypteringsnycklar och förhindra att leverantören får tillgång till okrypterade kunddata. Kontinuitetsrisker kan hanteras genom geografisk redundans, säkerhetskopiering, testade återställningsplaner och avtalsbaserade kontinuitetsåtaganden. Beroendet av en enda leverantör kan minskas genom arbetslasternas portabilitet, planering för utträde och lösningar med flera leverantörer. Så arbetar marknaden redan: 85 procent av de nordiska företagen uppger att de kombinerar teknikleverantörer från olika regioner, och 80 procent anser att möjligheten att välja och byta mellan leverantörer av AI-teknik är viktig för deras användning av AI.¹

En leverantör som är etablerad i EU kan fortfarande vara utsatt för cyberangrepp, tekniska fel, störningar i leveranskedjan eller ekonomiska svårigheter. En leverantör med anknytning till ett tredjeland kan ha möjlighet att visa en långtgående teknisk separering, effektiv kundkontroll, operativ kontinuitet och oberoende granskade säkerhetsåtgärder.

¹ Strand Partners, Unlocking the Nordics' AI Potential 2026, på uppdrag av Amazon Web Services, s. 6.

Bedömningen bör därför utgå från hur tjänsten utformas, kontrolleras och drivs. Leverantörsbegränsningar kan vara motiverade, men bara när mindre ingripande skyddsåtgärder inte räcker för att hantera en specifik och dokumenterad risk.

Artikel 30 bör erkänna alternativa skyddsåtgärder

Artikel 30 bör ge upphandlande myndigheter möjlighet att visa att en identifierad risk har minskats tillräckligt genom tekniska, avtalsbaserade eller operativa åtgärder. Leverantörsbegränsningar bör inte krävas när åtgärderna ger den säkerhet och kontinuitet som behövs.

Myndigheterna skulle därmed inte få fritt fram att bortse från ramverket för unionens tillitsnivåer. Den upphandlande myndigheten bör vara skyldig att dokumentera den identifierade risken, de valda skyddsåtgärderna och varför åtgärderna räcker för att hantera risken.

Leverantörsbegränsningar bör fortfarande kunna användas när risken kräver det, men de bör inte vara den enda godtagbara formen av riskreducering.

AWS rekommenderar att regeringen verkar för att artikel 30 erkänner följande:

- kundkontrollerad kryptering och nyckelhantering;
- teknisk separering och begränsad operatörsåtkomst;
- avtalsbaserade kontinuitetsåtaganden och bindande servicenivåer;
- testade planer för utträde, portabilitet och återställning;
- lösningar med flera leverantörer eller flera molnmiljöer; och
- geografisk redundans och säkerhetskopieringsmiljöer.

Svenska myndigheter skulle då behålla ansvaret för säkerheten och kunna välja de åtgärder som passar deras verksamhet och tekniska miljö bäst.

Verksamheter som inte är känsliga bör inte omfattas av lokaliseringskrav eller leverantörsbegränsningar

En stor andel av arbetslasterna i den offentliga sektorn, såsom publicering av allmän information, administrativa uppgifter som inte utgör personuppgifter och liknande verksamheter med låg risk, medför inte sådana konfidentialitets- eller kontinuitetsrisker att leverantörsbegränsningar eller krav på exklusiv datalokalisering är motiverade. Ramverket bör säga det uttryckligen för den lägsta nivån.

AWS rekommenderar att regeringen verkar för att den lägsta tillitsnivån inte innebär några begränsningar som grundas på leverantörens nationalitet. Där krav på datalokalisering gäller bör det räcka att en kopia av relevanta data finns inom EU. Data ska inte behöva lagras uteslutande där. Omfattningen av eventuella lokaliseringskrav bör också definieras tydligt, särskilt om de omfattar härledda operativa metadata, så att svenska myndigheter och deras leverantörer vet vad som gäller och kan planera därefter.

Begränsningarna förbehålls då verksamheter där uppgifternas känslighet eller tjänstens kritiska betydelse faktiskt motiverar dem. Det följer den proportionalitetsprincip som genomsyrar artiklarna 29 och 30.

Tidsfristen för migrering bör värna säkerhet och kontinuitet

När en riskbedömning kräver migrering till en annan molntjänst föreskriver artikel 29.6 en rimlig övergångsperiod på högst 12 månader, med hänsyn till teknisk genomförbarhet, tjänstens kontinuitet och dataportabilitet.

För stora eller kritiska offentliga miljöer räcker 12 månader inte alltid. En migrering kan kräva en ny upphandling, teknisk omutveckling, dataöverföring, säkerhetstester, personalutbildning och en period av parallell drift. Tidsåtgången beror på miljöns omfattning, applikationernas komplexitet och konsekvenserna av ett avbrott i tjänsten.

En påskyndad migrering kan i sig skapa säkerhets- och kontinuitetsrisker. System kan flyttas innan testerna är slutförda, myndigheter kan tvingas godta en tjänst som inte fullt ut uppfyller deras operativa krav, eller övergången kan avbryta en samhällsviktig offentlig funktion.

AWS rekommenderar att regeringen verkar för att tidsfristen ska kunna förlängas, när det är objektivt motiverat, vid komplexa eller kontinuitetskritiska migreringar. En förlängning bör förutsätta en dokumenterad migreringsplan, en förklaring till varför det inte är tekniskt eller operativt genomförbart att slutföra migreringen inom 12 månader samt lämpliga tillfälliga skyddsåtgärder för de berörda arbetslasterna. En sådan förlängning skulle ge praktisk verkan åt de kriterier för genomförbarhet och kontinuitet som redan anges i artikel 29.6 när bedömningen visar att 12 månader är otillräckligt.

Övergångsperioden blir då inget obegränsat undantag, och svenska myndigheter kan genomföra känsliga migreringar säkert och ordnat.

Metoden bör ingå i lagstiftningsramverket

Enligt artikel 29.3 ska kommissionen, efter att förordningen har trätt i kraft, anta viktiga delar av den metod som avgör vilken tillitsnivå som gäller. Det sker genom genomförandeakter, utan att Europaparlamentet och rådet tar ställning.

Metoden avgör vilka offentliga verksamheter som hänförs till respektive nivå, vilka molntjänster som får användas och om befintliga lösningar behöver ändras. Det är en sakfråga med direkta konsekvenser för svenska myndigheter.

Offentliga upphandlingar och projekt för övergång till molntjänster planeras över flera år. Investeringar i moln- och datacenterinfrastruktur görs med ännu längre tidshorisonter. Myndigheter och leverantörer behöver förstå de tillämpliga kraven innan de gör tekniska och ekonomiska åtaganden.

AWS rekommenderar att regeringen verkar för att riskbedömningsmetodens huvudsakliga delar tas in i förordningen eller i en bilaga som behandlas av Europaparlamentet och rådet.

Metoden bör:

- identifiera risker för konfidentialitet, riktighet, tillgänglighet och kontinuitet samt bedöma deras sannolikhet och konsekvenser, med åtskillnad mellan verksamheter och arbetslaster med olika grad av känslighet;
- erkänna tekniska, avtalsbaserade och operativa skyddsåtgärder samt medge att arbetslaster och systemkomponenter bedöms separat när en effektiv teknisk segmentering är möjlig; och
- kräva ett tydligt samband mellan den identifierade risken och den införda begränsningen, och endast begränsa vilka leverantörer som får anlitas när mindre ingripande åtgärder inte kan ge ett tillräckligt skydd.

Kommissionens ingripanden i nationella bedömningar bör begränsas

En gemensam europeisk metod behövs för att undvika att liknande offentliga verksamheter tilldelas olika tillitsnivåer i olika medlemsstater. Samtidigt måste Sverige själv kunna bedöma hur känsliga de svenska offentliga verksamheterna är och vilka risker de möter.

Enligt artikel 29.5 får kommissionen anta en genomförandeakt som anger vilken av unionens tillitsnivåer som krävs för en verksamhet i den offentliga sektorn, om kommissionen anser att den nivå som en medlemsstat har valt inte är lämplig eller inte i tillräcklig grad tillgodoser hänsynen till allmän ordning.

Kommissionen bör inte kunna ersätta en svensk bedömning enbart därför att den själv skulle ha dragit en annan slutsats.

AWS rekommenderar att regeringen verkar för att begränsa denna befogenhet till fall där det finns en specifik och dokumenterad risk, med stöd av ett motiverat beslut och en proportionalitetsbedömning.

Det främjar en enhetlig tillämpning inom EU och låter medlemsstaterna behålla ansvaret för att bedöma sina offentliga verksamheter.

UAL 3, UAL 4 och bilaga II: kraven bör grundas på granskningsbara kontroller, inte på leverantörens nationalitet

AWS rekommenderar att regeringen verkar för en översyn av UAL 3 och UAL 4, så att båda nivåerna grundas på granskningsbara tekniska och organisatoriska kontroller för säkerhet, operativ autonomi, kontinuitet och kundkontroll i stället för på leverantörens nationalitet.

Frågan är central för svenska myndigheter. UAL 3 och UAL 4 avgör vilka tjänster som får användas för de mest känsliga offentliga verksamheterna, bland annat inom försvar, rättsväsende och brottsbekämpning. Om kraven utesluter tjänster av andra skäl än säkerhet får myndigheterna färre alternativ just där kraven på skydd, motståndskraft och återställningsförmåga är som högst.

UAL 4 förenar krav om kontroll från tredjeländer med omfattande krav på programvarukomponenter och produkter som används i den granskade tjänsten.

Alla moderna molntjänster, oavsett om leverantören är europeisk eller inte, bygger på operativsystemslager, programvarubibliotek, säkerhetsverktyg och komponenter med öppen källkod som utvecklas och underhålls globalt.

Ett internationellt programvaruberoende är inte i sig en säkerhets- eller kontinuitetsrisk. Frågan är om den berörda komponenten eller tredje parten kan få tillgång till kunddata, ändra säkerhetskontroller, avbryta en kritisk funktion eller förhindra att tjänsten fungerar.

En brett utformad prövning av kontrollförhållanden kan därför utesluta en tjänst även när den berörda programvarukomponenten inte har någon väsentlig inverkan på den granskade tjänstens säkerhet eller kontinuitet. En sådan prövning kan också vara svår för leverantörer, granskare och myndigheter att tillämpa konsekvent, eftersom molntjänster och deras programvarukomponenter utvecklas och uppdateras kontinuerligt.

För svenska myndigheter skulle ett begränsat utbud av tillåtna tjänster kunna försvaga konkurrensen och göra det svårare att upprätthålla teknisk och operativ redundans. Det skulle slå hårdast mot känsliga arbetslaster som utsätts för kvalificerade cyberhot och kräver avancerad säkerhet, hotinformation och återställningsförmåga.

En tjänst bör därför bara uteslutas om den berörda komponenten eller relationen skapar en faktisk risk. En anknytning till ett tredjeland är i sig inte avgörande.

Sverige bör verka för en resultatbaserad modell för UAL 3 och UAL 4 som kräver att leverantörer visar:

- effektiv kundkontroll över data och kryptering;
- strikta kontroller av administratörs- och operatörsåtkomst;
- teknisk och organisatorisk separering;
- säkra och oberoende granskade processer för programvaruutveckling och uppdatering;
- hantering av risker i programvarans leveranskedja som kan påverka tjänsten väsentligt;
- testade lösningar för kontinuitet och återställning;
- geografisk och operativ motståndskraft; och
- avskilda eller fränkopplade driftmodeller när arbetslastens känslighet kräver det.

Kraven på leveranskedjan bör innehålla ett väsentlighetskriterium. Ett beroende bör betraktas som väsentligt när den berörda komponenten eller tredje parten kan få tillgång till kunddata, ändra säkerhetskontroller, avbryta en kritisk funktion eller förhindra att tjänsten fungerar. Komponenter som saknar dessa möjligheter bör inte automatiskt omfattas av samma krav.

Ramverket bör också medge likvärdiga skyddsåtgärder när en leverantör inte kan avlägsna en programvarukomponent men kan visa att komponenten är isolerad, omfattas av säkra processer för utveckling och uppdatering och inte kan komma åt data eller påverka kritisk drift.

Denna inriktning skulle ge svenska myndigheter ett strikt och granskningsbart skydd utan en brett utformad prövning av kontrollförhållanden som kan vara svår att tillämpa konsekvent i komplexa och föränderliga leveranskedjor för programvara.

Artikel 18: erkännande av associerade tredjeländer

Artikel 18 fastställer villkoren och mekanismen för erkännande av associerade tredjeländer. Erkännandet avgör om molntjänster som står under kontroll från det erkända landet får granskas mot kriterierna för UAL 3. Bestämmelsen innehåller sex kumulativa kriterier som rör adekvat skyddsnivå för personuppgifter, statlig kontroll, tjänstens kontinuitet, tillgång till teknik, marknadens öppenhet och ömsesidigt tillträde till offentlig upphandling.

Förslaget fastställer ingen bindande tidsplan för att inleda eller slutföra bedömningen. Det ger inte heller berörda länder eller leverantörer möjlighet att formellt kräva att kommissionen inleder förfarandet.

Detta kan skapa osäkerhet för svenska myndigheter om en tjänst kommer att få användas i en kommande upphandling. Det kan också göra det svårare att attrahera långsiktiga investeringar i datacenter och digital kompetens, eftersom sådana beslut fattas flera år i förväg.

Flera av kriterierna i artikel 18 gäller om tredjelandet har regler som kan kräva tillgång till data, påverka tjänstens kontinuitet, införa restriktiva åtgärder eller begränsa tillhandahållandet av teknik.

Demokratiska rättsordningar har lagstiftning om myndigheters tillgång till information, sanktioner och exportkontroller. Förekomsten av sådan lagstiftning bör inte i sig hindra ett erkännande. Bedömningen bör också beakta de begränsningar och skyddsåtgärder som reglerar hur dessa befogenheter får utövas.

Hit hör krav på att en befogenhet bara får utövas med rättslig grund, för ett definierat ändamål och när det är nödvändigt och proportionerligt. Bedömningen bör också beakta oberoende tillsyn, domstolsprövning, effektiva rättsmedel och leverantörens möjlighet att bestrida ett olagligt eller oproportionerligt föreläggande.

AWS rekommenderar att regeringen verkar för att erkännandet bygger på bedömningar som EU redan har gjort. Tredjeländer som omfattas av ett EU-beslut om adekvat skyddsnivå och är parter i WTO:s avtal om offentlig upphandling (GPA) bör som huvudregel erkännas på UAL 3. Ordningen skulle gälla lika för alla länder som uppfyller villkoren och undvika att EU prövar samma frågor två gånger.

Ett erkännande som huvudregel bör vara förenat med tydligt definierade skyddsåtgärder och en befogenhet att tillfälligt upphäva erkännandet om ett land inte längre uppfyller kriterierna i artikel 18.

Artikel 31: obligatoriska krav på den privata sektorn kräver fullständig lagstiftningsprövning

Artikel 31 ger privata företag som är verksamma i sektorer som omfattas av bilaga I till NIS2-direktivet möjlighet att genomföra konsekvensbedömningar som liknar den offentliga sektorns riskbedömningar enligt artikel 29.

Artikel 31.3 ger också kommissionen möjlighet att, under angivna omständigheter och efter samråd med medlemsstaterna, anta delegerade akter som kräver att sådana privata företag genomför en konsekvensbedömning och vidtar föreskrivna riskreducerande åtgärder.

I Sverige kan det gälla företag inom energi, transport, bankverksamhet, hälso- och sjukvård samt digital infrastruktur.

De praktiska konsekvenserna kan bli betydande. Ett företag skulle kunna behöva ompröva sin molnmiljö, omförhandla avtal, flytta data och applikationer eller omforma system som har utvecklats under flera år. För kritiska tjänster kan en påskyndad migrering i sig skapa säkerhets- eller kontinuitetsrisker.

Företag i de berörda sektorerna omfattas redan av EU-krav rörande cybersäkerhet, operativ motståndskraft och risker i leveranskedjan. Ytterligare skyldigheter enligt CADA skulle kunna skapa överlappande bedömningar, rapporteringsskyldigheter och riskreduceringskrav vid sidan av NIS2, DORA, dataförordningen och annan EU-lagstiftning. Dataförordningen kräver redan att molnleverantörer vidtar tekniska, rättsliga och organisatoriska åtgärder mot att tredjeländers myndigheter får olaglig tillgång till icke-personuppgifter som lagras i EU (artikel 32). Den ger också företagen rätt att byta leverantör och flytta sina data. De risker som artikel 31 tar sikte på hanteras alltså redan i stor utsträckning.

Innan ytterligare krav införs bör kommissionen visa vilken risk som inte redan hanteras, varför den befintliga lagstiftningen är otillräcklig och vilken särskild säkerhetsnytta den föreslagna åtgärden skulle ge.

Artikel 31.3 hänvisar till särskilda omständigheter, vederbörlig motivering och samråd med medlemsstaterna. Villkoren anger inte tydligt vilka trösklar för väsentlighet eller nödvändighet som ska gälla. De innehåller inte heller något uttryckligt krav på samråd med de företag och sektorer som skulle bära de praktiska konsekvenserna.

Europaparlamentet och rådet kan invända mot delegerade akter, men inte ändra dem. Det ordinarie lagstiftningsförfarandet ger både rätt att ändra och en fullständig behandling.

AWS rekommenderar att regeringen verkar för att artikel 31 utgår. En eventuell utvidgning av kraven till privata företag bör ske genom det ordinarie lagstiftningsförfarandet i stället för genom delegerade akter.

Sverige bör också verka för att ett sådant lagstiftningsförslag endast läggs fram när:

- en specifik och väsentlig risk har identifierats;
- kommissionen har visat att risken inte hanteras tillräckligt genom befintlig lagstiftning;
- samråd har skett med de berörda sektorerna;
- kostnaderna, säkerhetsnyttan och effekterna på konkurrensen har bedömts;
- samspelet med NIS2, DORA och andra tillämpliga krav har undersökts;
- de riskreducerande åtgärderna är proportionerliga i förhållande till den berörda verksamhetens känslighet och kritiska betydelse; och
- övergångsperioderna återspeglar de berörda systemens tekniska komplexitet och kontinuitetskrav.

Svenska företag bör inte vara skyldiga att omstrukturera kritiska teknikmiljöer utan ett påvisat säkerhetsbehov, ett tydligt samband mellan den identifierade risken och den införda åtgärden samt en realistisk genomförandeperiod.

Tillståndsgivning för datacenter, hållbarhet och tillgång till elnätet

AWS välkomnar de föreslagna accelerationszonerna för datacenter, de gemensamma kontaktpunkterna och tidsfristerna för tillståndsgivning. Dessa åtgärder kan stärka Sveriges förmåga att attrahera investeringar i den moln- och AI-infrastruktur som behövs för att stödja digitalisering och en bredare användning av AI.

Uttekandet av accelerationszoner bör återspegla den faktiska efterfrågan

Accelerationszoner kan locka effektiv digital infrastruktur, men bara om kriterierna för utpekande enligt artikel 10 är harmoniserade, efterfrågestyrda och förankrade i hur verksamheten faktiskt bedrivs. Tre strukturella skyddsmekanismer behövs.

För det första bör accelerationszonerna påskynda projekt som uppfyller kriterierna utan att fördröja tillståndsgivningen för projekt utanför de utpekade områdena. Projekt utanför zonerna måste även fortsättningsvis ha tydliga och förutsägbara tidsramar och få del av de fördelar som föreslås i Environmental Omnibus.

För det andra riskerar en koncentration av projekt till snävt avgränsade zoner att driva upp markpriserna. Medlemsstaterna bör därför vidta åtgärder mot spekulation. För det tredje krävs ett reellt samråd med datacenteroperatörer när zonerna pekas ut, så att besluten överensstämmer med den faktiska efterfrågan på marknaden och den operativa genomförbarheten.

AWS har följande synpunkter på de enskilda kriterierna för utpekande.

- Zonernas lokalisering och dimensionering bör återspegla den faktiska efterfrågan genom att beakta kundtäthet, närhet till arbetslaster, sammankoppling med befintlig digital infrastruktur och tillgång till kvalificerad arbetskraft, inte enbart geografiska förhållanden.
- Tillgången till elnätet kräver framförhållning i planeringen. Kapaciteten bör fördelas efter principen att det projekt som är redo först får kapacitet först, med företräde för operatörer som kan visa att deras projekt är redo att genomföras. Utan en samordnad utbyggnad av elnätet blir zonerna bara streck på kartan.
- Kriteriet om produktion på plats bör vara teknikneutralt och tillgodoräkna verifierade inköp av fossilfri el, däribland elköpsavtal ('PPA') för produktion utanför anläggningen. Sammantaget kan sådana avtal ge jämförbar nytta för klimatet och elnätets motståndskraft.
- En prioritering av tidigare exploaterad mark bör kombineras med påskyndade saneringsförfaranden, särskilda tillståndsteam och en gemensam kontaktpunkt. Markföreningar förlänger normalt ett projekt med 18–36 månader.

- Slutligen bör hållbarhetsbedömningen uttryckligen omfatta vatten, eftersom kylningen kan ta lokala vattenresurser i anspråk. Bedömningen bör bland annat beakta tillgången till vatten för industriell användning och hållbara investeringar inom det större avrinningsområdet.

Fullständiga ansökningar och tidsfrister för tillståndsgivning

Den föreslagna tillståndsfristen på 12 månader börjar löpa när en fullständig ansökan har lämnats in. Artikel 13 definierar inte vad som utgör en fullständig ansökan.

Tidsfristens praktiska värde beror därför på om de sökande kan avgöra vilka uppgifter som krävs och hur snabbt den ansvariga myndigheten måste bedöma ansökan.

Om kraven är otydliga kan en sökande mötas av upprepade begäranden om kompletteringar innan den formella tidsfristen börjar löpa. Den totala processen kan då förbli lång, även om den del som formellt omfattas av tidsfristen begränsas till 12 månader.

AWS rekommenderar att regeringen stöder bestämmelser som kräver:

- en offentligt tillgänglig checklista som beskriver vilka uppgifter som krävs för en fullständig ansökan;
- en fast tidsfrist inom vilken den ansvariga myndigheten måste bekräfta att ansökan är fullständig eller begära kompletteringar;
- en samlad begäran som omfattar alla uppgifter som myndigheten rimligen kan identifiera i det skedet;
- en motivering för varje senare begäran om ytterligare uppgifter;
- en bindande handlägningsplan som anger vilka myndigheter som är involverade, vilka milstolpar som gäller och vilka tidsfrister respektive myndighet ska följa; och
- effektiv samordning genom den gemensamma kontaktpunkten.

En gemensam kontaktpunkt bör göra mer än att hänvisa sökande till olika myndigheter. Den bör vara tillgänglig för alla datacenterprojekt, oavsett om de är belägna i en accelerationszon, och vara skyldig att fastställa en bindande handlägningsplan med milstolpar och tidsfrister för respektive myndighet. Den bör samordna begäranden om uppgifter, minska dubbelarbete mellan myndigheter och ha befogenhet att ingripa och fatta nödvändiga beslut när myndigheter överskrider tidsfristerna, lösa konflikter mellan myndigheter och föra olösta frågor vidare.

Hållbarhetskraven bör vara harmoniserade och förutsägbara

När medlemsstaterna fastställer hållbarhetskrav för datacenter i accelerationszoner kräver artikel 11.1 att de använder de centrala prestandaindikatorer som anges i delegerad förordning (EU) 2024/1364 enligt direktiv (EU) 2023/1791, bilaga II, punkterna a–n. Uppsättningen indikatorer är alltså redan föreskriven. Bestämmelsen fastställer dock inte någon harmoniserad metod för att välja bland dessa indikatorer, kombinera dem eller fastställa de tröskelvärden som ett datacenter måste uppfylla.

Det kan leda till väsentligt olika villkor mellan medlemsstaterna. En datacenteroperatör som utformar infrastruktur för flera europeiska marknader kan behöva uppfylla olika kombinationer av indikatorer och olika prestandatrösklar i varje rättsordning.

AWS rekommenderar att regeringen stöder en harmoniserad ordning som grundas på gemensamma indikatorer för energi- och vattneffektivitet, beräkningsmetoder och jämförbara prestandaklasser som utvecklas inom EU:s klassificeringssystem för datacenter. Medlemsstaterna bör fastställa de tröskelvärden för prestandaklasser som är lämpliga utifrån deras lokala miljöprioriteringar, men de underliggande definitionerna, beräkningsmetoderna och rapporteringsreglerna bör vara enhetliga.

Befintlig rapportering enligt energieffektivitetsdirektivet och dess delegerade förordning bör räcka för att uppfylla motsvarande rapporteringsskyldigheter enligt CADA. Operatörer bör inte vara skyldiga att rapportera samma underliggande uppgifter genom parallella system med olika format eller metoder.

Reglerna om nätkapacitet bör vara operativt tillämpbara

Förslaget kräver redan att medlemsstaterna beaktar nuvarande och framtida nätkapacitet när de pekar ut accelerationszoner. Det kräver också att fördelningen och användningen av resurser inom dessa zoner sker på rättvisa, rimliga och icke-diskriminerande villkor och syftar till att förhindra spekulativa reservationer.

Dessa principer bör omsättas i operativa regler för situationer där flera projekt konkurrerar om begränsad nätkapacitet.

Otydliga fördelningsregler gör det svårt att bedöma om en föreslagen etableringsplats är genomförbar. De kan också låsa knapp kapacitet för projekt som inte är tillräckligt mogna för att gå vidare, samtidigt som mer utvecklade projekt inte kan få en anslutning.

AWS rekommenderar att regeringen verkar för att reglerna om fördelning av begränsad nätkapacitet inom accelerationszoner tar hänsyn till:

- projektets mognad och tekniska genomförbarhet;
- bindande investeringsåtaganden;
- milstolpar som ett projekt måste uppnå för att behålla sin tilldelning;
- hanteringen av kapacitet som har reserverats för projekt som inte genomförs.

Dessa kriterier bör inte garantera kapacitet åt en viss leverantör eller kategori av operatörer. De bör säkerställa att tilldelningsbesluten är transparenta och icke-diskriminerande och kan prioritera projekt som realistiskt kan genomföras. Icke-diskriminerande villkor måste definieras tillräckligt precist för att skydda tillträde på konkurrensmässiga villkor utan att missgynna storskalighet, långsiktig planering eller modeller för etappvis utbyggnad.

Ramverket bör också förbli teknikneutralt när ett projekts bidrag till energisystemet bedöms. Relevanta bidrag kan omfatta produktion på plats, verifierade elköpsavtal (PPA) för produktion utanför anläggningen, energilagring, efterfrågefleksibilitet och andra åtgärder som stöder elnätets stabilitet eller tillför koldioxidfri elproduktion.

Tydliga tillståndskrav, förutsägbara hållbarhetskriterier och operativa regler för tilldelning av nätkapacitet skulle stärka Sveriges förmåga att attrahera långsiktiga investeringar i moln- och AI-infrastruktur.

Slutsats

Regeringen bör därför driva en riskbaserad och teknikneutral linje i rådsförhandlingarna och stödja högt ställda och granskningsbara krav på säkerhet, motståndskraft, operativ kontinuitet och kundkontroll. Leverantörens nationalitet och enskilda komponenters ursprung får inte ersätta en bedömning av hur en tjänst utformas, kontrolleras och drivs.

En riskbaserad och teknikneutral inriktning skulle skydda känsliga svenska verksamheter och samtidigt upprätthålla konkurrensen, tillgången till avancerad teknik och de förutsättningar som krävs för fortsatta investeringar i svensk moln- och AI-infrastruktur.

För Amazon Web Services:

Christa Torm

Samhällspolitisk chef, Norden och Baltikum

Amazon Web Services (AWS)