

AI Swedens remissvar Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM (2026) 502

AI Sweden är Sveriges nationella center för tillämpad artificiell intelligens. Vårt uppdrag är att accelerera användningen av AI till förmån för vårt samhälle, vår konkurrenskraft och för alla som bor i Sverige. Vi har en bred finansiering, är inte vinstdrivande, och samarbetar med våra över 190 partner från både privat och offentlig sektor samt akademi. AI Sweden driver europeiska flaggskeppsprojekt som utvecklingen av en transparent och öppen europeisk språkmodell (OpenEuroLLM), och tillsammans med över 120 offentliga aktörer utvecklar vi en prototyp för en gemensam digital assistent för den offentliga sektorn (Svea). Tillsammans med Nationellt cybersäkerhetscenter och Försvarsmakten utforskar vi sätt att öka Sveriges nationella förmåga att möta AI-drivna cyberhot.

AI Sweden välkomnar Europeiska kommissionens helhetsgrepp kring suveränitet som presenteras i meddelandet som åtföljer förordningen om moln- och AI-utveckling (CADA). Kommissionen belyser betydelsen av att analysera hela AI-stacken och dess värdekedja, en bild som AI Sweden delar. De grundläggande förmågorna och horisontella möjliggörarna i hela samhället är avgörande för att framgångsrikt kunna hantera det breda ekosystemperspektiv som krävs för att uppnå verklig europeisk suveränitet. Utöver den tekniska kapaciteten måste Europa även integrera AI-kompetens i hela utbildnings- och yrkeskedjan – från grundskola, via högre utbildning, till arbetslivet. Därtill behöver vi mobilisera betydande riskkapital och strukturella investeringar för att kunna minska beroenden och stimulera tillväxt.

Vi vill också understryka att det redan idag finns tjänster och leverantörer från EU, och AI Sweden är övertygade om att ännu fler europeiska alternativ kommer att växa fram innan den föreslagna lagstiftningen träder i kraft. Med våra kommentarer hoppas vi kunna bidra med ökad teknisk förståelse och dela med oss av våra erfarenheter inom AI för att stödja europeiska aktörer, öka användningen av ansvarsfull AI och samarbeta med tillförlitliga partners.

1. Undvik särskilda formuleringar kring AI-agenter

CADA föreslår nya formuleringar kring AI-agenter. AI Sweden vill betona att AI-agenter redan omfattas av definitionen av AI-system och banbrytande AI samt regleras genom AI-förordningen. Med tanke på den snabba utvecklingstakten inom AI har vi tidigare uppmanat lagstiftare att avstå från att hänvisa till specifik teknik eller specifika användningsområden för AI, såsom promptning. Sådan lagstiftning riskerar att snabbt bli föråldrad varför en mer teknikneutral ansats är att föredra. Detta gäller även för moln- och AI-ledarskapsinitiativen. Vi förordar därför att de specifika delarna om AI Agenter utgår då dessa även omfattas av banbrytande AI.

- ~~Artikel 2.5 AI-agent: ett AI-system, eller en samordnad uppsättning AI-system, som med en viss grad av autonomi kan uppfatta och agera på sin miljö och vid behov använder verktyg för att uppnå specifika mål och anpassa sig till föränderliga input och sammanhang.~~
- ~~Artikel 3.2.f: Stödja utvecklingen av avancerade plattformar för storskalig utbyggnad av AI-agenter (operativt mål 6).~~
- ~~Artikel 4.6 Inom ramen för operativt mål 6 ska moln- och AI-ledarskapsinitiativen~~
 - ~~a) stödja utvecklingen av avancerade resilienta och säkra plattformar för utveckling, införande och orkestrering av avancerade AI-agenter i stor skala;~~
 - ~~b) underlätta utvecklingen av riktade test- och experimentmetoder för avancerade AI-agenter och orkestrering av dem under hela deras livscykel.~~

2. Beräkningskapacitet, energi och datacenter

2.1 Beakta olika typer av beräkningskapacitet

AI Sweden delar helt uppfattningen att det är centralt att åtgärda Europas underskott av beräkningskapacitet för att säkra suveränitet och konkurrenskraft. För att kunna utforma effektiva politiska åtgärder behöver dock en åtskillnad mellan de olika typer av beräkningskapacitet göras. Dessa inkluderar kapacitet för modellträning, inferens, fysisk AI, kvantteknik och inte enbart kantdatorteknik, vilket för närvarande görs i artikel 15.1 a.

Beräkningskapacitet för inferens används för operationalisering och drift av AI-tjänster, vilket är en förutsättning för en storskalig upptagning och användning av AI. Även om marknaden, åtminstone till stor del, kan driva kapacitetsutbyggnaden av datacenter för inferens, utgör regulatoriska hinder som långa tillståndsprocesser en flaskhals.

Beräkningskapacitet för träning av stora språkmodeller (LLM) kräver specialiserad datorkraft i en betydligt större skala än för inferens. Detta görs genom en dator som kopplar samman tiotusentals AI-chip för att bilda en enda, sammanhängande beräkningsmotor. För att träna en stor språkmodell krävs det att alla dessa AI-chip kan kommunicera extremt snabbt med varandra vilket kräver särskild teknisk design och arkitektur när dessa datacenter byggs.

Behovet av statligt stöd är betydande när det gäller datacenter för träning vilket görs genom så kallade superdatorer, AI-fabriker och AI-gigafabriker. Om EU menar allvar med att utveckla suveräna och konkurrenskraftiga stora språkmodeller måste tillräcklig beräkningskapacitet för träning säkras inom våra gränser. Att förlita sig på att träna europeiska modeller i USA kan inte vara ett alternativ om vi vill minska våra strategiska beroenden. Tillgång till adekvat beräkningskapacitet för AI-träning har visat sig vara ett stort hinder i initiativ som OpenEuroLLM. Följaktligen måste tillgången för europeiska flaggskeppsprojekt, vilka kräver massiv beräkningskapacitet, prioriteras vid byggandet av datacenter utformade för AI-träning.

På motsvarande sätt skiljer sig beräkningskraft för fysisk AI, kvantteknik och edge AI, åt när det gäller skala, arkitektonisk utformning, geografisk närhet och acceptabel latens (tiden mellan att användaren trycker på enter och det mottagna svaret). Om bevakning av dessa olika typer av beräkningskapacitet inte differentieras kommer vi inte att kunna investera i den mest kritiska typen av beräkningskapacitet. I takt med att AI-tekniken utvecklas kommer även behoven att ändras varför det är viktigt att följa utvecklingen. AI Sweden uppmanar därför kommissionen att identifiera och bevaka olika typer av beräkningskapacitet som finns tillgängliga i unionen. Genom att inte specificera de särskilda typerna av beräkningskapacitet i artikeln, utan endast exemplifiera detta i skälen, uppnås teknikneutralitet och flexibilitet eftersom dessa typer också kan komma att förändras framgent.

- Skäl 44: För att främja den strategiska utbyggnaden av datacentralkapacitet i hela unionen bör kommissionen bevaka den tillgängliga beräkningskapaciteten **för exempelvis AI-träning, inferens, fysisk AI, kvantteknik, samt edge AI** och volymen av efterfrågan på datacentralkapacitet och identifiera storleken på kapacitetsbristen runt om i unionen. Kommissionen får använda denna bevakning som underlag för sina eventuella rekommendationer. För att vägleda medlemsstaterna när det gäller att påskynda utbyggnaden av datacentralkapacitet får kommissionen, när så är lämpligt, rekommendera åtgärder för att ta itu med den identifierade kapacitetsbristen i unionen. I enlighet med policyprogrammet för det digitala decenniet 2030 bör kommissionen också

se över målen för det digitala decenniet för att återspegla den tekniska, ekonomiska och samhällsliga utvecklingen och hur unionens prioriteringar har förändrats i detta avseende.

- Artikel 15.1.a.: den **olika typer av** beräkningskapacitet som är tillgängliga i unionen, ~~inbegripet kändatorkapacitet,~~

2.2. Accelerationszoner

AI Sweden välkomnar förslag om kortare tillståndprocesser men ifrågasätter om detta bör göras genom införandet av dedikerade accelerationszoner eller om åtgärder som förkortade tillståndprocesser mer generellt hade varit att föredra. Om accelerationszoner införs, ställer vi oss frågande till om en tidsram på maximalt tolv månader verkligen är nödvändig för tillståndsförfarandet för datacenterprojekt inom dessa zoner. Vi förespråkar att denna tidsram kortas ned till sex eller nio månader för att påskynda utbyggnaden av olika typer av beräkningskapacitet. Om dessa snabbzoner införs är också en fråga om alla aktörer ska kunna dra nytta av dessa eller om den snabbare tillståndprocessen i första hand ska kunna nyttjas av europeiska aktörer.

Slutligen är det oklart för AI Sweden vad som avses med "datacenter med högt värde" i artikel 7, varför vi föreslår att detta antingen förtydligas eller stryks.

- Om accelerationszoner införs förslår vi att Artikel 13.5. ändras till : [...] Tillståndsförfarandet för datacentralprojekt som byggs ut i accelerationszoner för datacentraler får inte räckta längre än ~~tot~~ **sex [eller nio]** månader från den tidpunkt då en övergripande ansökan har lämnats in **av en datacentralsoperatör etablerad i en medlemsstat.** [...]
- Artikel 7.2.d.: Förtydliga vad som avses med "datacentraler med högt värde" eller låt denna del utgå.

2.3 Strategiska datacenterprojekt

För att effektivt stimulera det europeiska ekosystemet och undvika att subventionera utländsk marknadsdominans med hjälp av europeiska offentliga medel, borde huvudaktörerna i de strategiska datacenterprojekt som avses i artikel 14 vara europeiska. Samtidigt som vi säkerställer att den strategiska kontrollen och ägandet av dessa projekt förblir europeiska, måste vi upprätthålla en pragmatisk inställning till internationella partnerskap. Att uppnå teknisk suveränitet får inte innebära inte teknisk isolering.

AI Sweden rekommenderar därför att behörighetskraven för huvudsökanden till dessa strategiska projekt uttryckligen knyts till de kriterierna för etablering, ägande och kontroll som fastställs för den 4e tillsnivån i bilaga II. Genom att endast

tillämpa detta krav på huvudsökanden möjliggörs också deltagande av aktörer från tredjeländer. Detta säkerställer att europeiska strategiska projekt kan dra nytta av oundgänglig utländsk teknik genom teknikleverantörer eller konsortiepartner.

Att säkerställa ägandet och kontrollen över fysisk infrastruktur är bara den ena sidan av suveränitetsekvationen; Europa måste i lika hög grad säkra den beräkningskapacitet som dessa datacenter genererar. Den tekniska suveräniteten riskerar att undergrävas om europeiska offentliga medel och regulatoriska fördelar används för att bygga ut infrastruktur som i slutändan ökar eller bibehåller våra tekniska sårbarheter.

Även när europeiska aktörer idag bygger datacenter, köps beräkningskraften ofta av aktörer utanför EU. Privata aktörer måste naturligtvis ha full kommersiell frihet att sälja sina tjänster till en global kundkrets, men för aktörer som erhåller EU-finansiering, till exempel genom strategiska datacenterprojekt, är det rimligt att det strategiska värdet och resultatet i första hand tillfaller Europeiska unionen. AI Sweden föreslår därför att merparten av beräkningskapaciteten öronmärks för europeiska aktörer.

- Artikel 14.1: Kommissionen får genom ett beslut utse datacentralprojekt, **där huvudsökanden uppfyller de kriterier för etablering och kontroll som fastställs i bilaga II för unionens tillitsnivå 4**, som valts ut genom öppna inbjudningar att anmäla intresse och som uppfyller minst två av följande kriterier till strategiska projekt:
- Artikel 14.1.a: Genom projektet inrättas och drivs infrastruktur som direkt stöder och förbättrar viktiga funktioner inom den offentliga sektorn, inbegripet forskning och utbildning, hälso- och sjukvård samt allmän säkerhet och trygghet **där majoriteten av dess beräkningskapacitet tillfaller aktörer etablerade i en medlemsstat.**

2.4 Energi och socioekonomiska krav för etablering av datacenter

AI Sweden delar till fullo kommissionens uppfattning att AI har en enorm potential att kartlägga, prognostisera, säkra och optimera elförbrukningen i energisystemet. Den snabba ökningen av AI-användning och utbyggnaden av datacenter ökar drastiskt den totala efterfrågan på el. För att tillgodose efterfrågan kommer det inte bara att krävas en massiv utbyggnad av befintligt elnät, utan även en utbyggnad av produktion av ren energi på plats, bakom mätaren eller genom samlokalisering.

Vidare är det viktigt att öka incitamenten för datacenter att införa flexibilitet på efterfrågesidan och tillhandahålla stödtjänster till nätet. Till exempel kan datacenter åta sig dynamisk lastnedkoppling vid akuta påfrestningar på elnätet, till exempel vid infrastrukturskador eller oväntade brister i baslastproduktionen. På så sätt kan datacenter omvandlas till aktiva nätbalansera tillgångar. Det är därför välkommet att samlokalisering av stora anläggningar för produktion och lagring av ren energi kan utses till strategiska datacenterprojekt genom artikel 14.1.c. Detta stimulerar datacenter till att bygga ut och investera i fossilfri energiförsörjning.

Ur ett svenskt perspektiv ser vi hur både nationella och globala aktörer redan har eller planerar att etablera datacenter i Sverige. I samband med detta förekommer det att kommuner ställer specifika socioekonomiska krav på de som etablerar datacenter för att säkerställa att etableringarna bidrar till nationella, regionala och lokala intressen – i linje med den nu föreslagna artikel 7.2 d. Kraven kan inbegripa arbetstillfällen, infrastrukturinvesteringar, AI-inriktade utbildningsinitiativ eller dedikerade beräkningsallokeringar för offentlig sektor. AI Sweden välkomnar dessa typ av krav. Att behandla el som en strategisk bristvara värnar lokala och nationella intressen samtidigt som det kan öka den allmänna acceptansen för utbyggnaden av datacenter. Det är också viktigt att framhålla att datacenteretableringar bidrar till den nödvändiga beräkningskapaciteten som krävs för AI-inferens, vilket är avgörande för att driva ekonomisk tillväxt, höja kvaliteten inom offentlig sektorn och öka vår konkurrenskraft.

3. Krav och fördelar för banbrytande AI-projekt

Enligt det nuvarande förslaget krävs det medverkan från minst tre medlemsstater för att ett projekt ska kunna klassificeras som ett prioriterat projekt för banbrytande AI. AI Sweden ifrågasätter grunderna för denna tröskel. Ur vårt perspektiv bör ett projekt utvärderas utifrån dess innovationsnivå och förmåga, snarare än utifrån antalet deltagande medlemsstater. Utifrån samma logik bör bildandet av ett konsortium inte vara en förutsättning för behörighet. Även om vi har förståelse för att det underliggande syftet med förslaget kan vara att främja gränsöverskridande samarbete och kunskapsutbyte, riskerar en sådan begränsning att bli kontraproduktiv. Ett högkvalitativt och innovativt projekt med ursprung i en enda medlemsstat bör också kunna beviljas denna status.

Som AI Sweden uppfattar förslaget, är den främsta fördelen med att erkännas som ett banbrytande AI-projekt, att man tilldelas beräkningskapacitet. Vi ställer oss något frågande till huruvida detta är tillräckligt. Med den nuvarande formuleringen finns det en betydande risk att få aktörer kommer att ansöka, och att de som erhåller statusen ändå inte erhåller den nödvändiga beräkningskapaciteten. AI

Sweden understryker därför att banbrytande AI-projekt både ges öronmärkt finansiering och garanterad tillgång till beräkningskapacitet. En uppdelning mellan finansiellt stöd och beräkningsresurser i två separata processer riskerar att avsevärt försena projektens arbete, vilket till exempel varit fallet för OpenEuroLLM.

Den dedikerade beräkningskapacitet som banbrytande AI-projekt ska erhålla är vagt formulerad där medlemsstaterna och unionen ska sträva efter att tillhandahålla tillräckliga AI-beräkningsresurser. Utan garanterad tillgång till beräkningskapacitet riskerar erkännandet av banbrytande AI-projekt att förlora sin praktiska betydelse. AI Sweden föreslår därför att artikel 9 justeras för att säkerställa att EU och dess medlemsstater avsevärt utökar sin kapacitet – och därmed omsätter politiska åtaganden i konkreta åtgärder.

Utifrån AI Swedens erfarenhet är det framförallt offentlig sektor som har svårigheter att erhålla nödvändig beräkningskraft för inferens till marknadspris och som behöver stöd för detta. Därför föreslår vi att detta tydligare prioriteras i artikel 9.3. Även flera initiativ som baseras på öppen källkod har utmaningar att säkra nödvändig beräkningskraft (för både träning och inferens) till marknadspris då de har svårare att nå kommersiell lönsamhet. Därför rekommenderar vi att även dessa initiativ erhåller prioriterad tillgång till beräkningskraft som ett komplement till EU:s “open source first principle”.

- Artikel 8.b.: Projektet genomförs av ett europeiskt konsortium för digital infrastruktur som inrättats i enlighet med beslut (EU) 2022/2481 eller en annan rättslig enhet som är berättigad till finansiering enligt unionsrätten, ~~och minst tre medlemsstater deltar i projektet.~~
- Artikel 9.1: Unionen och medlemsstaterna ska säkerställa att tillräckliga AI-resurser från deras beräkningskapacitet anslås för att stödja utvecklingen av prioriterade projekt för banbrytande AI som uppfyller kriterierna i artikel 8 ~~inom ramen för tillgänglig kapacitet.~~
- Artikel 9.2: Unionen ska åtminstone matcha de AI-resurser som medlemsstaterna bidrar med till prioriterade projekt för banbrytande AI ~~den utsträckning som tillräcklig AI-kapacitet finns tillgänglig inom ramen för unionens andel av åtkomsttiden till europeiska högpresterande datorsystem.~~
- Artikel 9.3: Unionen och medlemsstaterna ska ~~sträva efter att tillhandahålla tillräckligt med beräkningsresurser för industriell AI-innovation, fysisk AI och AI-projekt inom den offentliga sektorn~~ **och för projekt som bygger på öppen källkod.**

4. AI Centrum

AI Sweden välkomnar starkt inrättandet av erfarenhets- och accelerationscentrum för AI i artikel 5, eftersom dessa kommer att spela en avgörande roll för att påskynda användningen av AI i hela det europeiska ekosystemet.

5. Suveränitetsregelverket, revision och migrering

Som en inledande kommentar vill AI Sweden betona svårigheten i att till fullo utvärdera de föreslagna kriterierna för unionens fyra tillitsnivåer utan vetskap om vilka specifika verksamheter inom offentlig sektor som kommer att knytas till respektive nivå. Vi vill också understryka behovet av en enhetlig och harmoniserad ansats över hela EU när det gäller hur medlemsstater genomför riskbedömningar och när de fastställer lämplig tillitsnivå.

5.1 Utvidga undantag för tillitsnivå 1 till scale-ups

AI Sweden välkomnar undantaget som görs för små och medelstora företag i artikel 17.3 avseende unionsassuransnivå 1. För att främja europeisk tillväxt och undvika att bestraffa framgångsrika scaleups, bör detta undantag emellertid uttryckligen vidgas till att även omfatta små midcapföretag (SMCs).

- Artikel 17.3: [...] Genom undantag från det första stycket ska den EU-försäkran om överensstämmelse som utfärdats enligt artikel 19.2 av molntjänstleverantörer som är små och medelstora företag **inklusive SMCs** erkännas direkt och automatiskt i alla medlemsstater utan att den utvärderande nationella behöriga myndigheten först behöver erkänna dem.

5.2 Riskbedömningar

AI Sweden stödjer det underliggande syftet med artikel 29, som kräver att medlemsstaterna genomför riskbedömningar för att fastställa lämpliga tillitsnivåer för verksamheter inom offentlig sektor. Även om detta ansvar vilar på medlemsstaten kommer det att kräva att offentliga aktörer involveras. Här önskar vi belysa de stora utmaningar som uppstår när decentraliserade offentliga aktörer behöver göra komplexa juridiska bedömningar. Varje dag ser vi hur upphandlande myndigheter, från små kommuner till stora statliga myndigheter, kämpar med att utvärdera risker kopplade till juridik, teknik och efterlevnad särskilt vid överlappande regelverk (som GDPR, AI-förordningen och NIS2 utöver nationella regleringar som OSL).

Bristen på en gemensam och centraliserad juridisk bedömning och tolkning leder till att kommuner och myndigheter drar motstridiga slutsatser i likartade rättsfrågor; exempelvis huruvida GDPR tillåter användning av AI-transkribering inom

socialtjänsten, eller huruvida molntjänster är tillåtna. Rädslan för att göra fel bedömningar på grund av legala osäkerheter riskerar att leda till att AI-tjänster helt väljs bort. Det är också enormt resurskrävande att varje aktör måste göra sin egen bedömning särskilt då både offentliga resurser och kompetensen för dessa bedömningar är mycket knapp. Befintliga mekanismer, såsom regulatoriska sandlådor, är i grunden värdefulla men är för närvarande alldeles för långsamma i förhållande till den snabba tekniska utvecklingen.

Följaktligen kan behovet av att kommissionen utfärdar metoder och mallar genom genomförandeakter enligt artikel 29.3, samt tillhandahåller centralt samordnad vägledning kring kartläggningen (skäl 63), inte nog understrykas och bör förstärkas. Europeiska kommissionen bör, i nära samordning med medlemsstaternas tillsynsmyndigheter (t.ex. dataskyddsmyndigheter och Enisa), tillhandahålla centralt samordnade och godkända klassificeringar av användningsfall. Offentliga aktörer skulle då kunna förlita sig på standardiserade grundbedömningar för allmänna verksamheter som omfattas av CADA.

- Skäl 63: [...] För att säkerställa ett harmoniserat genomförande i hela unionen bör kommissionen, i samarbete med **medlemsstaterna och** relevanta myndigheter, tillhandahålla centralt samordnad vägledning om sammanpassningen och **användningsfall** av unionsassuransnivåer och informationskategorier, med beaktande av känsligheten, kritikaliteten och omfattningen hos de uppgifter som behandlas i molnmiljön, systembetydelsen av de upphandlande myndigheternas verksamhet och de tillämpliga skyldigheter som följer av unionsrätten. [...]

5.3 Introducera en engångsprincip för riskbedömningar

Även om CADA bygger på GDPR och NIS2 skapar regelverket ett ytterligare lager för att hantera suveränitetsrisker, vilket ökar regelbördan och kostnader för regelefterlevnad. För att hantera detta, föreslår AI Sweden att en "engångsprincip" (fill in once-paradigm) för riskbedömningar införs där harmonisering sker mellan GDPR, AI-förordningen och CADA samt domänspecifika lagstiftningar däribland NIS2, DORA och MDR.

Till och med svenska globala bolag med betydande regulatoriska resurser, pressas idag hårt av de överlappande och resurskrävande riskbedömningar som måste göras. Något som också betonas i studien om moln och AI (Cloud & AI Study). För att implementera en enskild AI-tjänst kan en organisation behöva genomföra en konsekvensbedömning avseende dataskydd (DPIA), en konsekvensbedömning vid överföring (TIA), en intresseavvägning (LIA), en konsekvensbedömning avseende grundläggande rättigheter (FRIA), en riskbedömning för högrisk AI, i tillägg till den nu ytterligare föreslagna riskbedömningen.

När dessa riskbedömningar görs tvingas organisationer att duplicera teknisk information i flera isolerade regulatoriska stuprör. Även om de specifika rättsliga frågorna i dessa ramverk skiljer sig åt, är en stor del av den grundläggande tekniska informationen likartad. AI Sweden förespråkar därför en övergång till ett paradigm som bygger på en engångsprincip. Detta skulle till exempel kunna uppnås genom en harmonisering av riskbedömningarna mellan de olika regelverken eller genom att införa mallar som kan underlätta.

- Inför en ”engångsprincip” (fill in once-paradigm) för riskbedömningar för GDPR, AI-förordningen och CADA samt domänspecifika lagstiftningar däribland NIS2, DORA och MDR.

5.4 Utfasningsstrategi för migrering

Inledningsvis vill AI Sweden ta tillfället i akt att lyfta fram att Sverige och Europa redan idag har ett stort antal molntjänstleverantörer. Ett axplock av dessa är Intric, Evroc, Cleura, Safespring, Elastx, Redpill Linpro, Binero och Oderland samt de mest välkända OHVCloud, Scaleway och T-Systems. Det finns också svenska datacenteretablerare som bland annat inkluderar Bahnhof, GleSYS, Berget och Airon. Vi står alltså inte utan egna alternativ och AI Sweden är övertygade om att dessa aktörer kommer kunna växa innan CADA träder i kraft samt att vi också kommer att se nya aktörer etablera sig.

Trots dessa aktörer, kan vi inte bortse från det beroende som vi har idag varför det är rimligt att möjliggöra för vissa tredjeländer att leverera tjänster även under tillitsnivå 3. För att bedöma huruvida kraven i artikel 18 är väl avvägda och verkligen motsvarar befintliga risker har vi tillämpat CIA-triaden som ramverk för cybersäkerhetsbedömning. Denna bedömning syftar till att säkerställa konfidentialitet, riktighet och tillgänglighet. Dessa faktorer är avgörande för att skydda känsliga uppgifter mot obehörig åtkomst, säkerställa att informationen är korrekt, aktuell och oförändrad samt att det finns ett skydd för driftskontinuitet. Vår slutsats är att kraven i 18.1 a–d är inriktade på relevanta risker avseende konfidentialitet, riktighet och tillgänglighet (se bilaga för bedömningen i sin helhet). Villkoren i 18.1 e och f utgör å andra sidan snarare makroekonomiska suveränitets- och handelsvillkor.

Vi tror dock att kraven i Artikel 18 och för respektive tillitsnivå tillsammans med det strikta migreringskravet om 12 månader i Artikel 29.6 kan bli svårt att uppfylla. I stället för att sänka kraven i Artikel 18 föreslår vi att en utfasningsstrategi läggs till i artikel 26. Kravet på migrering bör endast utlösas när en likvärdig europeisk lösning finns tillgänglig. Eftersom CADA redan har en revisionsmekanism på plats, kan utfasning-smekanismen knytas till registreringen i det centrala registret i artikel 22.

- Artikel 26: Om riskbedömningen kräver migrering till en annan molntjänst ska medlemsstaten eller unionsenheten migrera inom en rimlig övergångsperiod som inte får överstiga tolv månader, med beaktande av den tekniska genomförbarheten, tjänstens kontinuitet och de krav på dataportabilitet som är tillämpliga på sådan migrering. **Detta förutsätter att det finns en likvärdig, erkänd molntjänstleverantör i det centrala registret.**

5.5 Om artikel 18 inte är uppfylld

Mot bakgrund av Schrems I och II-fallen rekommenderar AI Sweden att formuleringen i artikel 18.2 ändras till ”inte uppfyller, eller inte längre uppfyller”. Att endast förlita sig på den nuvarande formuleringen ”inte längre uppfyller” förutsätter att ett tredjeland *de facto* har uppfyllt kriterierna i 18.1 vid tiden för det ursprungliga beslutet. Som EU-domstolen har visat kan det dock i efterhand visa sig att rättslig grund för en tredjelandsöverföring *aldrig* har varit uppfylld. Genom denna redaktionella förändring undviks eventuellt juridiskt vakuum om liknande slutsatser nås framgent.

- Artikel 18.2: Om tillgänglig information visar att tredjelandet inte **uppfyller eller inte** längre uppfyller kraven i punkt 1 ska kommissionen återkalla, ändra eller tillfälligt upphäva det beslut som avses i punkt 1.

5.6 Revision och erkännande av molntjänstleverantörer

För att suveränitetsramverket ska bli framgångsrikt måste revisionsprocessen för tillitsnivå 2 och uppåt vara enkel, förutsägbar och strikt proportionerlig. AI Sweden välkomnar därför att det i Artikel 20.4 betonas att revisionsföretag ska vara helt oberoende och fria från intressekonflikter med molntjänstleverantören.

Det finns dock en överhängande risk att revisionsförfarandet blir ett betydande administrativt och ekonomiskt hinder, inte minst för små och medelstora företag. Kostnaden för revision måste vara hanterbar även för mindre aktörer såväl som de krav som ställs enligt Bilaga III och den dokumentation/bevisning som krävs för att kraven ska anses vara uppfyllda. AI Sweden ifrågasätter huruvida de omfattande krav och bevisning som krävs i Bilaga III är strikt nödvändig för tillitsnivå två. Det är allt för långtgående att ”Revisorer får inhämta all ytterligare information som behövs för att säkerställa en heltäckande och korrekt bedömning av efterlevnaden av de revisioner som utförts.” Kraven i Bilaga III framstår i dagsläget som alltför omfattande. Vi föreslår därför att en tydligare åtskillnad görs i de krav och den dokumentation som krävs beroende på vilken tillitsnivå som revisionen sker för.

För att förhindra att revisioner drar ut på tiden och hämmar innovationstillväxt skulle fasta tidsbegränsningar för själva revisionsprocessen kunna fastställas. AI

Sweden vill också understryka vikten av erforderlig kompetens hos tredjepartsrevisorerna. Det kan också förekomma tillfällen när offentliga aktörer med säkerhetskänslig verksamhet agerar som leverantörer varför det kan ifrågasättas om det då är lämpligt att privata aktörer utför revision.

När det gäller artikel 17.5 och erkännande av molntjänstleverantörer betonar AI Sweden att det är avgörande att tidsfristen på 60 dagar för den utvärderande nationella behöriga myndigheten efterföljs och inte blir föremål för godtyckliga förlängningar. Det måste beaktas att molntjänstleverantören för tillitsnivåer två till fyra då redan har genomgått en omfattande tredjepartsrevision. Den efterföljande erkännandeprocessen måste därför vara ytterst skyndsam och smidig för att förhindra regulatoriska flaskhalsar, i synnerhet för mindre aktörer vars tid till marknaden (time-to-market) är kritisk.

- Artikel 20.9: Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 för att komplettera denna förordning genom att fastställa regler för utförandet av revisioner av stegen i förfarandet, **tidsbegränsningar för genomförandet av revisioner, särskilda åtgärder för att begränsa revisionskostnader för små och medelstora företag**, regler för revisionsföretag och deras tekniska kompetens, revisionsmetoder och mallar för revisionsberättelserna.
- Artikel 21.1: För att utarbeta revisionsberättelsen och revisionsuttalandet ska revisionsföretaget bedöma om den granskade tjänsten uppfyller kriterierna i bilaga II på grundval av de revisionsbevis som anges i bilaga III. **Vid begäran om sådan bevisning ska revisionsföretaget anpassa den krävda dokumentationens omfattning till den specifika unionsassuransnivå som ansöks om.** Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 45 för att ändra bilaga III genom att fastställa de bevis som krävs för att bedöma revisionskriterierna enligt bilaga II.

6. Offentlig upphandling

AI Sweden delar kommissionens uppfattning att multi-cloud och multi-vendor strategier kan vara som ett bra sätt för att minska risker och motverka inlåsnings effekter hos enskilda leverantörer. Det måste emellertid betonas att det kan vara dyrt och tekniskt komplicerat att utforma, implementera och underhålla sådana lösningar, vilket också understryks i konsekvensbedömningen. Detta gäller i synnerhet för mindre kommuner och myndigheter. Följaktligen bör inte en multi-cloud eller multi-vendor strategi anses vara en obligatorisk standard eller en one-size-fits-all lösning.

AI Sweden understryker vikten av Artikel 33.2 och att underlätta för små och medelstora företag i offentliga upphandlingar. Vi vill särskilt välkomna och betona vikten av att dela in upphandlingen i flera olika sär viktigt då svenska och europeiska aktörer sällan har möjlighet att erbjuda samma heltäckande erbjudanden som större globala aktörer. Däremot kan de ha möjlighet att leverera inom vissa delar, applikationer, lösningar eller specialiserade komponenter i AI- och molnstacken. Det bör dock framhållas att från upphandlande aktörers perspektiv är införandet av multi-cloud, multi-vendor strategier och dela upp upphandlingar i olika delar mer komplext än att teckna avtal med en enda global leverantör. Detta medför tydliga utmaningar när det gäller interoperabilitet, kompatibilitet med äldre system och hur dessa interagerar med varandra.

För att överkomma dessa svårigheter kan konsortium med flera mindre europeiska aktörer bildas med en utpekad projektledare som ansvarar för integration mellan de olika projektdeltagarna. Att tillåta europeiska aktörer att samarbeta och gemensamt lämna anbud på upphandlingar ger det europeiska ekosystemet förutsättningar att erhålla offentliga upphandlingar vilka utgör en betydande marknad. Samtidigt underlättar konsortiebildning med en huvudansvarig aktör för den upphandlande myndigheten. Därför föreslår vi smärre förtydliganden i artikel 33.2 för att lyfta fram möjligheten till konsortiebildning.

Vidare krävs en större medvetenhet kring hur anbudsspecifikationer och krav vid upphandlingar utformas, för att säkerställa att de inte oavsiktligt hindrar europeiska aktörer samt små och medelstora företag från att delta eller vinna upphandlingen. Det är också avgörande att medlemsstaterna prioriterar kunskapsspridning och systematisk delning av best-practices för hur offentliga aktörer kan underlätta för europeiska aktörer vid upphandlingar.

I lagstiftningsförslaget anges i artikel 32.1 att det är tillåtet för upphandlande myndigheter att använda tilldelningskriterier som inte rör pris för att gynna ett europeiskt moln- och AI-ekosystem. Att enbart tillåta detta kommer inte att vara tillräckligt för att öka den europeiska efterfrågan. Följaktligen föreslår vi ett tillägg om att en europeisk preferens aktivt ska främjas.

- Artikel 32.1: I offentliga upphandlingsförfaranden för innovativa molntjänster och AI-system ska upphandlande myndigheter, som en del av kvalitetsutvärderingen av anbudet, inkludera tilldelningskriterier som inte rör pris och som gör det möjligt för dem att utvärdera **och aktivt främja** anbudsgivarens bidrag till utvecklingen av ett europeiskt moln- och AI-ekosystem.
- Artikel 33.2: Medlemsstaterna ska vidta lämpliga åtgärder för att säkerställa att den övervakning och rapportering som avses i punkt 1 aktivt används för

att identifiera hinder för små och medelstora företags deltagande i upphandlingsförfaranden, förbättra små och medelstora företags tillträde till upphandlingsmarknader, stödja utformningen av förenklade och proportionella upphandlingsstrategier som lämpar sig för små och medelstora företag, inbegripet uppdelning i delar **samt genom konsortium**, när så är lämpligt, samt främja små och medelstora företags deltagande i det innovationsförfarande som föreskrivs i direktiv 2014/24/EU och förkommersiell upphandling av molntjänster och AI-system.

7. Öppen källkod

7.1 Modeller med helt öppen källkod och stängda öppna modeller

AI Sweden välkomnar initiativ och satsningar kring öppen källkod. Språkmodeller baserade på öppen källkod är en viktig pusselbit för att säkra Europas teknologiska suveränitet och konkurrenskraft då de förhindrar leverantörsinlåsning och gör det möjligt för aktörer att bygga vidare på, anpassa och granska tekniken. I detta avseende är det grundläggande att skilja mellan olika grader av öppenhet för språkmodeller. En modell där endast dess vikter offentliggörs bör inte behandlas som likvärdig med en modell som även har transparens och återanvändbarhet genom hela utvecklingskedjan – från data som modellen tränats på och vilka träningsmetoder, utvärderingsparametrar och benchmarks som har nyttjats.

Utvecklare som använder modeller med öppen källkod som saknar transparens kring data som har använts för träning, riskerar att bygga vidare på en modell som kan ha tränats på personuppgifter som använts i strid med GDPR eller på upphovsrättsligt skyddat material som man inte haft rätt till. Modeller som endast har öppenhet kring modellvikter är inte heller alltid transparenta med de metoder som används för deras säkerhetsanpassning (safety alignment), vilket medför risker för inbyggd censur, bias eller otillräckliga skyddsräcken (guardrails).

AI Sweden föreslår därför att åtskillnad görs mellan helt öppna modeller och stängda öppna modeller.

- Artikel 41: Unionen och medlemsstaterna ska vidta nödvändiga åtgärder för att uppmuntra unionsenheter och offentliga myndigheter att använda och underlätta vidareutnyttjande av öppna standarder och komponenter som släpps ut med en öppen källkodslicens när de bygger sitt moln- och AI-ekosystem eller sin moln- och AI-stack, med beaktande av funktioner, inbegripet säkerhet, **transparens kring träningsdata och metoder för**

säkerhetsanpassning, totala kostnader och andra relevanta, vederbörligen motiverade objektiva kriterier.

7.2 EU:s strategi för öppen källkod

AI Sweden välkomnar det helhetsgrepp som tas i EU:s strategi för öppen källkod, i synnerhet insikten om att teknisk suveränitet kräver kapacitet genom hela tekniskstacken vilket också inkluderar tillgången på halvledare, beräkningskapacitet, mjukvaruutveckling och AI-modeller.

Vi vill dock ytterligare betona vikten av data. Utan tillgång till stora, högkvalitativa och rättsligt användbara dataset kommer Europa ha svårt att bygga konkurrenskraftig och genuint öppen AI-kapacitet. Data bör därför behandlas som ett strategiskt infrastrukturlager jämsides med beräkningskraft, molninfrastruktur, programvara och modeller.

Svårigheterna rör inte bara tillgången till data, utan även dess användbarhet för AI-utveckling. Även om vi i Europa har betydande mängder offentlig, vetenskaplig, kulturell och språkliga data, betyder tillgången inte per automatik att den kan användas på ett effektivt sätt. Rättslig osäkerhet, oklara licensvillkor, fragmenterad åtkomst, otillräcklig dokumentation och ursprungsinformation gör det svårt att veta vilken data och information som verkligen får nyttjas. Därtill krävs omfattande resurser för att extrahera, filtrera och kvalitetssäkra data. Europeisk policy för öppen källkod bör därför göra en tydligare åtskillnad mellan att tillgängliggöra data och att skapa dataset som lagligen och i praktiken kan användas, delas och vidareutnyttjas för AI. AI Sweden vill därför se mer investeringar för insamling, förberedelse, dokumentation och underhåll av högkvalitativa data för flera europeiska språk och domäner för att säkerställa att de europeiska gemensamma europeiska dataområdena också fungerar rent praktiskt.

9. Grand challenges

9.1 Grand challenge 7

Även om AI Sweden är tveksam till särskilda formuleringar i själva rättsakten kring AI Agenter, är det fullt rimligt och välkommet med en grand challenge för denna teknik. Som många är medvetna om, medför autonoma AI-agenter en ny riskprofil. Säkerheten behöver numera både hanteras mot yttre hot, och på en intern processnivå genom organisatoriska riktlinjer för operativ styrning, behörighetsgränser och kvalitetsvalidering.

Vi föreslår därför att en säkerhetsdimension utökas i utmaningen. Detta skulle kunna omfatta dynamisk kvalitetsvalidering, processspecifika skyddsräcken (guardrails) för behörighet, rättslig och etisk anpassning (alignment) samt systemisk robusthet för att minska riskerna vid autonomt agerande. Därtill kan operativa ramverk kräva att agenter i klartext genererar den stegvisa logik som använts för att fatta ett beslut innan agenter tillåts utföra själva åtgärden för att säkerställa att mänsklig översyn är möjligt. Detta etablerar också en standardiserad loggning för att spåra agentens aktivitet vilket gör det möjligt för realtidsbaserade detektionssystem, i likhet med de som idag används för skadliga virus eller kod, att reagera.

- [...] Fokus kommer att ligga på att i) utforska innovativa tekniska paradigmer som gör att flera AI-agenter kan samarbeta effektivt och överträffa kapaciteten hos fristående system, samtidigt som strikta säkerhetsstandarder upprätthålls, ~~och~~ ii) skapa motståndskraftiga, molnbaserade öppna plattformar för storskalig hantering av AI-agenter **och (iii) inrätta ramverk och operativa riktlinjer för ett säkert användande av autonoma AI-agentsystem.** [...]

9.1 Grand challenge 8

Det är ytterst välkommet med en utmaning för offentlig sektor där stora effektivitets- och kvalitetsvinster finns. Vi rekommenderar dock ett fokus på att finjustera och träna befintliga AI-modeller för den offentliga sektorn, snarare än att skapa helt egna modeller då detta är mycket komplicerat och resurskrävande. För att finjustera och träna befintliga modeller skulle EU kunna spela en viktig roll för kunskapsspridande och delning av bästa möjliga metoder för dataannotering (dvs den process där rådata märks och kategoriseras för att därefter kunna användas av utvecklare) varför vi föreslår att detta läggs till i utmaningen.

Här skulle man även kunna komplettera de gemensamma europeiska dataområdena genom att använda den enorma mängd tillgängliga data från offentliga sektor som inte är känslig såsom lagstiftning, riktlinjer, vägledningar, tillsynsrapporter, administrativa förfaranden och offentliga beslutsprotokoll. Genom att systematiskt aggregera och strukturera öppna data kan information omvandlas till maskinläsbara dataset av hög kvalitet.

Vi vill också lyfta fram att skapandet av moduler och komponenter, såsom RAG-lösningar, kan vara lika viktigt, eller till och med viktigare, än ett helt system eller en hel modell.

- Utveckla AI-modeller, **moduler och komponenter** och AI-system som bygger på högkvalitativa data från **för** den offentliga sektorn ~~och~~ **som** är inriktade

på kritiska områden (t.ex. hälso- och sjukvård, offentlig förvaltning, lagstiftning och krishantering samt offentliga tjänster).

Fokus kommer att ligga på lösningar för offentliga tjänster som förväntas ha en stor positiv inverkan på de mest kritiska offentliga tjänsterna och som delas på olika nivåer av den offentliga sektorns organisationer.

Ett mål kommer att vara att möjliggöra datadelning, **finjustera** och **träna** ~~utveckling av banbrytande~~ modeller i alla nationella offentliga tjänster för att öka effekterna på unionens offentliga sektor överlag (**inkluderat gränsöverskridande samordning av dataannotering för finjustering av specialiserade modeller**), även på områden där känsliga uppgifter hanteras. Ramar för sekretesskydd (däribland federerad träning och generering av syntetiska data med hög tillförlitlighet), som gör det möjligt att träna modeller utan att äventyra konfidentialiteten hos underliggande datauppsättningar, samt åtgärder för att påskynda en bred spridning av sådana ~~modeller~~ **tekniker**, även på regional och lokal nivå, kommer också att bidra till att uppnå detta mål.

Bilaga

Tillämpning av CIA-triaden avseende artikel 18

18.1 Konfidentialitet – Skydd mot obehörig åtkomst och utlämnande

Krav som säkerställer att tredjeland inte kan framtvinga utlämnande av data eller kringgå europeiska sekretess- och konfidentialitetsstandarder.

18.1.a. Beslut om adekvat skyddsnivå (GDPR)

Garanterar att lagstiftningen i tredjeland förbjuder oproportionerlig övervakning av och obehörig åtkomst till europeiska personuppgifter. Detta utgör den fundamentala skyddsåtgärden för att upprätthålla personuppgifters konfidentialitet vid internationella dataöverföringar.

18.1.b Efterlevnad av dataförordningen (Data Act)

Skyddar data som inte utgör personuppgifter inklusive företagshemligheter. Kravet förhindrar utländska myndigheter från att utnyttja extraterritoriell lagstiftning (exempelvis amerikanska CLOUD Act eller kinesisk nationell säkerhetslagstiftning) för att tvinga molntjänstleverantörer att bevilja obehörig åtkomst till europeisk data.

2. Tillgänglighet – Operativ resiliens och kontinuitet

Krav avsedda att skydda europeisk infrastruktur mot politiskt eller rättsligt motiverade driftstörningar.

18.1.c & d. Förbud mot framtvingade avbrott och sanktioner

Förhindrar tredjeland från att stänga ned, degradera eller strypa tjänster för europeiska aktörer, samt från att verkställa embargoliknande blockader av molninfrastruktur.

3. Riktighet (Integrity) – Skydd mot manipulation

Krav som säkerställer att systemarkitektur, säkerhetsfunktioner och data förblir okomprometterade och uppfyller högsta tekniska standard (state-of-the-art).

Artikel 181.d. Förbud mot restriktioner av spetsteknologi

Förhindrar utländska stater från att inskränka molntjänstleverantörers förmåga att implementera den senaste teknologin exempelvis genom att föreskriva svagare krypteringsstandarder, fördröja säkerhetsuppdateringar eller införa krav på inbyggda bakdörrar.

Villkoren i artikel 18.1 e och f utgör inte tekniska säkerhetsåtgärder inom ramen för informationssäkerhetens CIA-triad, utan verkar snarare som makroekonomiska suveränitets- och handelsvillkor: