



Beslut

Datum	Diarienummer	Ärendetyp
2026-09-30	26FMV5569	1.3
		Sida
		1(12)

Regeringskansliet
Finansdepartementet

Er referens
Christina Knutsson
Hamrén

Ert datum	Er beteckning
2026-07-10	Fi2026/01676

Svar på remiss av Europeiska kommissionens förslag till *förordning om utveckling av moln och AI KOM* *(2026)502*

Ärendet

Regeringskansliet (Finansdepartementet) har genom remiss den 10 juli 2026 bett Försvarets Materielverk (FMV) att senast den 2 oktober 2026 inkomma med synpunkter på Europeiska kommissionens förslag till *förordning om utveckling av moln och AI KOM (2026)502*.

Generell kommentar

FMV har tagit del av fakta-PM från Finansdepartementet och håller med om många synpunkter som framkommer där. FMV instämmer i behovet och är positiv till ambitionen att stärka EU:s kapacitet, konkurrenskraft, och digitala suveränitet inom moln- och AI-området. Ett riskbaserat förhållningsätt där informationsvärderingen är central är positivt. Instämmer i det som framkommer i Fakta-PM att cybersäkerhet ska beaktas i det fortsatta arbetet. Bra att satsa på öppen källkod. Viktigt att det finns metoder för att utvärdera sådana modeller samt att medlemsstaterna fortsatt har rådighet över dessa frågor, särskilt avseende säkerhetskänslig verksamhet.

Förslaget till förordning är synnerligen långtgående och ger kommissionen befogenheter som påverkar medlemsstaters självbestämmande. FMV anser att den rättsliga grunden för förslaget kan ifrågasättas. Förslaget minskar medlemsstaters bestämmande över nationella säkerhetsintressen. Artikel 4.1 FEU anger att i enlighet med artikel 5 ska varje befogenhet som inte tilldelats unionen i fördragen tillhöra medlemsstaterna. Artikel 4.2 FEU anger vidare att unionen ska respektera medlemsstaternas likhet inför fördragen samt deras nationella identitet som kommer till uttryck i deras politiska och konstitutionella grundstrukturer samt medlemsstaternas väsentliga statliga funktioner, särskilt avseende syftet att hävda deras territoriella integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. Det anges vidare att *i synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstat eget ansvar*.

FMV

Försvarets materielverk

115 88 Stockholm

Besöksadress: Banérgatan 62

Tel: 08-782 40 00

Fax: 08-667 57 99

registrator@fmv.se

www.fmv.se

Org.nr: 202100-0340

VAT nr: SE202100-0340-01

Det finns en stor osäkerhet avseende vilka uppgifter som kommissionen kommer att begära in eftersom kommissionen ska anta genomförandeakter där de ska fastställa den metod som ska tillämpas vid riskbedömningar, mallar som ska användas och faktorer som medlemsstaterna ska beakta vid genomförande av riskbedömningar. Uppgifter kan vara säkerhetsskyddsklassificerade och det är svårt att förstå varför kommissionen har behov av dessa uppgifter. På en aggregerad nivå riskerar dessa uppgifter att vara mycket känsliga även i det fallet att de var för sig inte skulle utgöra säkerhetsskyddsklassificerade uppgifter.

Förslaget om ömsesidigt erkännanden kan påverka medlemsstaternas rådighet över frågor kopplat till suveränitet och nationell säkerhet. Medlemsstater ska ha möjlighet att ställa hårdare krav på exempelvis cybersäkerhet. Vidare ska medlemsstaterna ha rådighet över vilka tjänster som ska nyttjas och kravställande utifrån Sveriges roll som allierad i Nato.

Utgångspunkten är att upphandlingsregelverket ska göras enklare och inte mer komplicerat. Ambition om att förenkla regelverket för offentlig upphandling riskerar att motverkas av att nya politiska mål och upphandlingsrelaterade krav successivt införs genom sektorsspecifik lagstiftning. För upphandlande myndigheter i medlemsstaterna innebär detta att de inte enbart behöver förhålla sig till det direktivstyrd upphandlingsregelverket, utan även identifiera, tolka och tillämpa de särskilda krav som följer av olika sektorsspecifika rättsakter. Ett sådant regelverk riskerar att öka såväl den administrativa bördan som den rättsliga osäkerheten för de upphandlande myndigheterna. Regelverket blir svårt att överblicka.

EU önskar en gradvis/fördjupad överstatlig styrning av medlemsstaternas offentliga upphandling vilket kan kritiseras ur ett nationellt självbestämmandeperspektiv. EU:s roll (i många fall) verkar inte längre handla om att säkerställa konkurrens och den inre marknadens funktion inom offentlig upphandling, utan också av att styra politiska mål som upphandlingarna ska bidra till.

Det kan vidare ifrågasättas om kommissionen har den kompetens och kapacitet som krävs för att fullgöra de uppgifter avseende offentlig upphandling som enligt förslaget läggs på kommissionen. Möjligheten för medlemsstaterna att använda kommissionen för att genomföra upphandlingar, och därigenom omfattas av de undantag från upphandlingsregelverket som följer av förslaget, är konstruerat som ett incitament för medlemsstaterna att använda sig av kommissionens upphandlingsmöjligheter som en praktisk förenkling. Samtidigt innebär ordningen att delar av medlemsstaternas upphandlingsverksamhet flyttas till unionsnivå.

Om upphandlingar i större utsträckning genomförs centralt av kommissionen kan medlemsstaterna få mindre praktisk erfarenhet av att själva utforma krav, bedöma marknaden och genomföra upphandlingar inom de berörda områdena. Detta kan i sin tur skapa ett ökat beroende av kommissionen och bidra till en självförstärkande centralisering över tid. Det är i detta sammanhang särskilt relevant att kommissionen enligt förslaget inte endast ges möjlighet att genomföra upphandlingar på medlemsstaternas uttryckliga begäran, utan även att på eget initiativ inleda upphandlingsförfaranden som är öppna för deltagande medlemsstater.

Såsom konstateras i fakta-PM kräver nya datacenter för moln- och AI-tjänster stora mängder energi, vilket förutsätter investeringar i elnät och elproduktion men kan också innebära prioriteringar om elen inte räcker till. Det är därför viktigt att *styrning av el till prioriterade elanvändare*

vid bristsituationer (Styrel) omhändertas och att medlemsstaterna fortsatt har rådighet över elförsörjningen.

Granskningskommentarer

Artiklarna 10-15: Accelerationszoner för datacenter – europeisk strategisk nytta

Ramverket för accelerationszoner för datacenter i artiklarna 10–15 kan skapa ett potentiellt policygap mellan CADA:s mål att öka datacenterkapaciteten i unionen och dess bredare mål att stärka Europas teknologiska suveränitet, motståndskraft/resiliens och strategiska autonomi.

Artiklarna 10–13 är utformade för att underlätta utbyggnaden av datacenter genom utsedda accelerationszoner, gemensamma informationspunkter, förenklade administrativa förfaranden och ett aggregerat grundtillstånd (aggregated baseline permit). Bestämmelserna förefaller inte kräva att operatören eller ägaren av ett datacenter är europeiskt ägd eller kontrollerad. Artikel 14 fastställer ytterligare kriterier för att vissa projekt ska kunna utses till strategiska projekt, bland annat bidrag till samhällsviktiga funktioner, hållbarhet, elsystemets stabilitet, integrering av teknik som konstruerats eller tillverkats i unionen samt hantering av lokala kapacitetsbrister. Inget av dessa kriterier kräver dock uttryckligen en bedömning av projektets bidrag till europeisk strategisk autonomi, europeisk kontroll över kritisk infrastruktur eller minskat beroende av leverantörer från tredjeland.

Detta kan leda till att accelerationsramverket framgångsrikt ökar den fysiska datacenter- och beräkningskapaciteten inom unionen utan att nödvändigtvis ge en proportionerlig ökning av Europas strategiska förmåga eller teknologiska suveränitet. En leverantör från tredjeland skulle kunna utveckla och driva infrastruktur inom en accelerationszon och dra nytta av de tillhörande infrastruktur- och tillståndsfördelarna, förutsatt att de tillämpliga kriterierna är uppfyllda. Sådana investeringar kan naturligtvis ge betydande fördelar för unionen, bland annat investeringar, sysselsättning, skatteintäkter, infrastrukturutveckling och ytterligare beräkningskapacitet. Frågan gäller däremot om regelverket i tillräcklig utsträckning skiljer mellan kapacitet som är lokaliserad inom unionen och kapacitet som påtagligt stärker unionens strategiska autonomi.

Denna skillnad är särskilt relevant eftersom CADA självt identifierar beroendet av ett begränsat antal icke-europeiska moln- och AI-leverantörer som ett strategiskt problem. Förslagets ramverk för monitorering (monitoring framework, artikel 7 och artikel 15 – se specifikt LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT 1.3.4 objective 3C) behandlar även andelen installerad datacenter / kapacitet i EU som ägs av europeiska leverantörer som en indikator för att mäta minskat beroende av icke-europeiska moln- och AI-databehandlingstjänster. Artikel 32 visar dessutom att CADA kan bedöma bredare europeisk strategisk nytta genom faktorer såsom bidrag till Europas moln- och AI-ekosystem, integrering av unionsteknik och försörjningstrygghet. Motsvarande överväganden är inte tydligt integrerade i ramverket för accelerationszoner.

Fysisk utbyggnad av ytterligare kapacitet inom unionen eliminerar därför inte nödvändigtvis ägarrelaterade, operativa, teknologiska, leveranskedjerelaterade eller jurisdiktionella beroenden av aktörer i tredjeland. Ramverket förefaller i högre grad mäta ökningen av kapacitet som är lokaliserad i Europa än i vilken utsträckning denna kapacitet stärker europeisk kontroll, försörjningstrygghet och operativ autonomi.

FMV anser därför att det bör övervägas om ramverket för accelerationszoner bör innehålla

ytterligare behörighets- eller prioriteringskriterier som beaktar europeisk strategisk nytta, såsom europeiskt ägande eller kontroll, bidrag till europeisk moln-/AI-förmåga, minskat beroende av tredjeland, försörjningstrygghet eller åtaganden avseende tillgängligheten till eller användningen av den resulterande beräkningskapaciteten för europeiska strategiska ändamål. Som ett minimum bör förslaget klargöra hur kapacitetsmålen är avsedda att samspela med målen om autonomi/suveränitet när en icke-europeisk leverantör utvecklar och driver infrastruktur inom unionen.

Artikel 16 och Annex II–III: Undantagande av hårdvara från unionens ramverk (Union cloud computing sovereignty framework) / assurancesramverk för cloud computing suveränitet

Unionens ramverk, som fastställs genom artikel 16 och Annex II–III, ger en jämförelsevis detaljerad bedömning av autonomi- och suveränitetsrelaterade risker förknippade med molnbaserade databehandlingstjänster. Kriterierna omfattar bland annat leverantörens etablering och kontroll, tredjelandsjurisdiktion, lokaliseringen av/platsen för infrastruktur och personal, operativt stöd, programvaruberoenden, tillgång till källkod, fjärrmanipulering, programvaruförteckningar (Software Bills of Materials, SBOM), underleverantörer och beroenden i leveranskedjan.

Annex II skiljer dock uttryckligen mellan programvara och hårdvara och placerar själva hårdvaran utanför tillämpningsområdet för assurancesbedömningen i Annex II–III. En molnbaserad databehandlingstjänst kan därför potentiellt uppfylla en hög unionsassuransnivå samtidigt som den fortfarande är väsentligt beroende av processorer, acceleratorer, nätverksutrustning, lagringssystem eller annan kritisk hårdvara som har konstruerats, tillverkats eller levererats från tredjeland. Hårdvarans lokalisering inom unionen samt programvara eller fast programvara som är kopplad till tjänsten kan omfattas av relevanta krav, men detta framstår inte som likvärdigt med en bedömning av det strategiska beroendet av den fysiska tekniken eller dess fortsatta försörjning.

Denna skillnad är anmärkningsvärd eftersom CADA på andra ställen erkänner hårdvaruberoende som relevant för europeisk teknologisk autonomi. Förslaget främjar processorer och acceleratorer som konstruerats eller tillverkats i unionen och identifierar uttryckligen, enligt artikel 32, användning av europeisk teknik och försörjningstrygghet som relevanta överväganden. Hårdvaruberoenden kan även hanteras genom andra unionsinstrument för cybersäkerhet eller leveranskedjor. Trots detta skapar undantaget en potentiell diskrepans mellan omfattningen av CADA:s högsta nivåer för unionens (suveränitets) assurance och det bredare begreppet teknologisk suveränitet som uttrycks på andra ställen i förordningen.

Frågan är särskilt relevant för försvar, nationell säkerhet och andra mycket kritiska arbetslaster (workloads). Den operativa kontrollen över en tjänst kan vara europeisk samtidigt som möjligheten att bygga ut, ersätta eller vidmakthålla kritisk databehandlingsinfrastruktur är beroende av teknik vars tillverkning, leverans eller export kontrolleras utanför unionen. Ett krav på enbart EU-hårdvara skulle sannolikt vara oproportionerligt och kanske inte spegla dagens tekniska realiteter, men väsentliga hårdvaruberoenden är fortfarande relevanta för suveränitet och försörjningstrygghet.

FMV anser därför att det bör övervägas om de högre unionsassuransnivåerna bör omfatta en bedömning av väsentliga beroenden av kritisk hårdvara och deras konsekvenser för försörjningstrygghet och operativ autonomi. Alternativt bör CADA klargöra varför hårdvara är

undantagen från bedömningen av 'suveränitetsassurans' / unionens assurancesnivåer och hur hårdvarurelaterade beroenden som hanteras genom andra unionsinstrument är avsedda att samspela med erkännande på unionens assurancesnivå 3 och 4.

Artikel 16 och Annex II–III: Kontroll över kryptografiska nycklar och dataskydd

Kontroll över kryptografiska nycklar och dataskydd

Unionens ramverk (Union cloud computing sovereignty framework) / assurancesramverk för cloud computing suveränitet fastställer detaljerade krav avseende lokalisering och kontroll av kunddata, infrastruktur, personal, drift och programvaruberoenden. Annex II–III förefaller dock inte innehålla uttryckliga krav på kryptografiskt skydd av kunddata eller, i synnerhet, ägande, förvaring och kontroll av kryptografiska nycklar.

Den cybersäkerhetscertifiering som krävs för de högre unionsassurancesnivåerna kan behandla kryptering och nyckelhantering som tekniska cybersäkerhetsfrågor. Säker nyckelhantering innebär dock inte nödvändigtvis att det finns effektiv kontroll över själva nycklarna. Om en molnleverantör, underleverantör eller annan extern aktör behåller teknisk eller rättslig åtkomst till kryptografiska nycklar kan data som lagras och behandlas inom unionen fortfarande vara åtkomliga för en extern part trots de lokaliserings- och organisatoriska skyddsåtgärder som CADA fastställer.

Denna skillnad är särskilt relevant för unionens assurancesnivåer 3 och 4 och för försvar, nationell säkerhet och andra mycket kritiska arbetslaster. Effektiv kontroll över känslig/säkerhetskänslig data är beroende av inte bara på var data lagras och behandlas, utan även på vem som kan generera, få åtkomst till, återställa, rotera, exportera, revokera eller på annat sätt utöva kontroll över de kryptografiska nycklar som krävs för dekryptering. Lokaliseringen och administrationen av infrastruktur för nyckelhantering, inklusive hårdvarusäkerhetsmoduler (HSM), kan därför ha direkt betydelse för tredjelandsjurisdiktion, operativ autonomi och skydd mot extern åtkomst.

FMV anser därför att det bör övervägas om de högre unionsassurancesnivåerna bör innehålla uttryckliga krav avseende kontroll över kryptografiska nycklar, inklusive lämpliga krav på ägande eller förvaring av nycklar, leverantörers och underleverantörers åtkomst, lokalisering och administration av infrastruktur för nyckelhantering, arrangemang för säkerhetskopiering och återställning samt exponering för tredjelandsjurisdiktion. CADA bör även klargöra hur dessa krav är avsedda att samspela med de tekniska kryptografiska kontroller och kontroller för nyckelhantering som fastställs genom europeiska cybersäkerhetscertifieringsordningar.

Artiklarna 23–28: Konsekvens i gränsöverskridande tillsyn och verkställighet

Konsekvens i gränsöverskridande tillsyn och verkställighet

Artiklarna 23–28 fastställer ett flerskiktat ramverk för att upprätthålla, utöva tillsyn över och verkställa unionsassurancesnivåer efter erkännande, inklusive leverantörers anmälan av väsentliga förändringar, sanktioner, tillsyns- och utredningsbefogenheter, ömsesidigt bistånd och gränsöverskridande samarbete. Tillsammans med den årliga revisionsöversynen enligt artikel 20 ger dessa bestämmelser viktiga skydd för att säkerställa att erkända assurancesnivåer fortsatt är giltiga.

Inom detta ramverk tilldelar artikel 25(4) exklusiv verkställighetsbehörighet (enforcement competence) till den medlemsstat där leverantören har sitt huvudsakliga etableringsställe, medan artikel 28 gör det möjligt för behöriga myndigheter i andra medlemsstater samt kommissionen att begära en bedömning och lämpliga utrednings- eller verkställighetsåtgärder (enforcement measures).

när det finns skäl att misstänka att en erkänd (recognised) tjänst inte längre uppfyller de tillämpliga kraven i Annex II.

Artikel 28 kräver att den behöriga myndigheten i etableringsstaten vederbörligen beaktar sådana begäranden och inom två månader meddelar sin bedömning samt de åtgärder som har vidtagits eller planeras. Artikel 28 förefaller dock inte fastställa någon ytterligare mekanism för eskalering eller tvistlösning när den begärande myndigheten eller kommissionen i väsentlig grad inte delar etableringsmyndighetens bedömning eller svar.

Detta kan skapa en potentiell inkonsekvens mellan unionsomfattande erkännande och i huvudsak nationell verkställighet (national enforcement). En erkänd molnbaserad databehandlingstjänst kan användas i hela unionen, även för mycket kritisk verksamhet, medan den fortsatta giltigheten av dess assurancesnivå i slutändan kan bero på tillsynsbedömningen och verkställighetsmetoden hos en enda nationell behörig myndighet. Frågan kan vara särskilt relevant för försvar, nationell säkerhet och andra mycket kritiska användningsfall där medlemsstater kan identifiera olika hotexponeringar eller suveränitetsrelaterade farhågor.

Detta är särskilt anmärkningsvärt eftersom det inledande erkännandeförfarandet enligt artikel 17 ger andra medlemsstater möjlighet att invända mot ett föreslaget beslut om erkännande. Någon jämförbar mekanism förefaller inte finnas för att lösa meningsskiljaktigheter om huruvida samma unionskrav för assurance fortsatt är uppfyllda efter erkännandet.

FMV anser därför att det bör övervägas om artikel 28 bör innehålla en mekanism för att lösa väsentliga meningsskiljaktigheter mellan behöriga myndigheter om det fortsatta uppfyllandet av unionens assuranceskrav, inklusive en lämplig eskaleringsmekanism när sådana meningsskiljaktigheter inte kan lösas mellan de berörda myndigheterna. Detta skulle kunna bidra till att säkerställa att en assurancesnivås unionsomfattande giltighet stöds av en lika sammanhängande mekanism för att lösa meningsskiljaktigheter om dess fortsatta giltighet.

Artikel 29: Risker avseende riktighet och manipulation vid fastställandet av lämplig unionsassurancesnivå

Artikel 29 fastställer den riskbaserade process genom vilken medlemsstater och unionsorgan fastställer lämplig unionsassurancesnivå för verksamheter som omfattar mycket kritiska sektorer och funktioner, inklusive försvar och nationell säkerhet. Bedömningen beaktar uttryckligen faktorer som de berörda uppgifternas känslighet, kritikalitet och omfattning, risken för olaglig åtkomst till data från myndigheter i tredjeland samt risken för och konsekvenserna av avbrott i den molnbaserade databehandlingstjänsten.

Dessa faktorer ger en uttrycklig grund för att beakta risker som i stora drag motsvarar konfidentialitet/kontroll över data och tjänstens tillgänglighet. Artikel 29 förefaller däremot inte med motsvarande tydlighet identifiera risken för obehörig eller oupptäckt ändring eller manipulation av data, behandling eller utdata. Detta ska inte tolkas som att CADA saknar skydd för uppgifters riktighet. Annex II–III innehåller ett antal tekniska och organisatoriska krav som är relevanta för riktighet, bland annat åtkomstbegränsningar, kontroller av programvara och leveranskedjor, möjlighet till granskning av källkod, bevisning kopplad till förändringar samt skydd mot fjärrmanipulering eller störning.

Den mer avgränsade frågan är att risker avseende riktighet eller manipulation inte förefaller vara uttryckligen inkluderade bland de minimifaktorer som används för att avgöra vilken nivå av unionens assurancesnivåer som en mycket kritisk verksamhet kräver. För vissa arbetslaster, särskilt inom försvar, underrättelserelaterad verksamhet, brottsbekämpning, kritisk infrastruktur och AI-stödda beslutssystem, kan en motståndare eller ett externt beroende orsaka allvarliga konsekvenser utan att vare sig få åtkomst till skyddad information eller göra tjänsten otillgänglig. Manipulation av data, bearbetningslogik eller utdata medan tjänsten fortfarande fungerar kan i sig utgöra en betydande suveränitets- och operativ risk.

FMV anser därför att det bör övervägas. Överväg att uttryckligen inkludera risken för och den potentiella effekten av obehörig eller oupptäckt ändring eller manipulation av data, behandling eller utdata bland de minimifaktorer som bedöms enligt artikel 29 vid fastställandet av lämplig unionsassurancesnivå, särskilt när sådana risker kan uppstå till följd av kontroll från tredjeland, tekniskt beroende eller privilegierad åtkomst.

Artikel 30(4): Undantag från krav på viss unionsassurancesnivå vid offentlig upphandling **Undantag från krav på viss unionsassurancesnivå vid offentlig upphandling**

Artiklarna 29 och 30 fastställer en riskbaserad mekanism enligt vilken medlemsstater och unionsorgan fastställer lämplig unionsassurancesnivå för offentliga molntjänster, inklusive tjänster som stödjer försvar, nationell säkerhet och andra mycket kritiska verksamheter. Om en riskbedömning identifierar ett krav på unionsassurancesnivå 2, 3 eller 4 kräver artikel 30 i allmänhet upphandling av en molnbaserad databehandlingstjänst som har erkänts på motsvarande nivå.

Artikel 30(4) medger emellertid undantag från dessa krav under exceptionella och vederbörligen motiverade omständigheter, bland annat när ingen lämplig erkänd (recognised) tjänst finns tillgänglig eller när efterlevnad av den erforderliga assurancesnivån skulle medföra oproportionerliga kostnader.

Detta skapar en potentiell spänning inom det riskbaserade ramverket. En högre assurancesnivå kan ha valts enligt artikel 29 eftersom verksamheten innebär betydande suveränitets- eller operativa risker. Ett undantag enligt artikel 30(4) kan därför leda till upphandling av en tjänst som inte visar de suveränitetsegenskaper som tidigare har bedömts vara lämpliga för verksamheten.

Den flexibilitet som artikel 30(4) medger kan vara nödvändig för att hantera marknadstillgång, proportionalitet och kontinuitet i offentliga tjänster. Detta kan dock vara särskilt känsligt för försvar, nationell säkerhet och andra mycket kritiska verksamheter, där konsekvenserna av att acceptera en lägre unionsassurancesnivå kan vara betydande. CADA bör inte nödvändigtvis föreskriva detaljerade kompenserande säkerhetsåtgärder eller förfaranden för riskacceptans i sådana fall, eftersom dessa lämpligen kan hanteras inom medlemsstaternas eller sektorsspecifika ramverk. Förordningen bör dock bevara den logiska kopplingen mellan den risk som identifierats enligt artikel 29 och beslutet att göra undantag från motsvarande assuranceskrav.

FMV anser därför att det bör övervägas att klargöra att användningen av ett undantag enligt artikel 30(4) inte undanröjer behovet av att på lämpligt sätt bedöma och hantera de suveränitetsrisker som identifierats enligt artikel 29, särskilt när den berörda verksamheten avser försvar, nationell säkerhet eller en annan mycket kritisk funktion.

Artikel 31: Omfattningen av mekanismen för konsekvensbedömning i privat sektor och beroenden inom försvarsindustrin

Artikel 31 utvidgar delar av ramverket för bedömning av konsekvenser och suveränitetsrisker till vissa privata aktörer. Dess tillämpningsområde är dock kopplat till aktörer som omfattas av Annex I till direktiv (EU) 2022/2555, nätverks- och informationssäkerhetsdirektivet 2 (NIS2). Detta skiljer sig från artikel 29:s ramverk för offentlig sektor, som uttryckligen behandlar försvar, nationell säkerhet och andra mycket kritiska statliga funktioner utöver de relevanta NIS2-sektorerna.

Som en följd av detta förefaller ett privat företag inte omfattas av artikel 31 enbart på grund av att det har en strategiskt viktig roll i den europeiska försvarsindustriella basen. Vissa försvarsföretag kan oberoende av detta omfattas av NIS2 Annex I på grund av andra verksamheter eller sektorsklassificeringar, men försvarsindustriell betydelse är inte i sig en uppenbar utlösande faktor för artikel 31.

Detta kan innebära att vissa privata aktörer vars beroende av moln- eller AI-tjänster har betydande konsekvenser för försvarsförmåga, försörjningstrygghet eller europeisk strategisk autonomi hamnar utanför mekanismen. Försvarsleveranskedjor är i stor utsträckning beroende av privata tillverkare, ingenjörsföretag, teknikleverantörer och specialiserade underleverantörer, och betydande moln- eller AI-beroenden hos sådana aktörer kan få konsekvenser som sträcker sig utöver det enskilda företaget.

Samtidigt skulle en urskillningslös utvidgning av artikel 31 till hela försvarsindustrin sannolikt vara oproportionerlig och kunna överlappa med nationella säkerhets- och försvarssäkerhetsregelverk. Frågan är därför inte om varje försvarsföretag bör omfattas, utan om den nuvarande tröskeln i NIS2 Annex I i tillräcklig grad fångar strategiskt betydelsefulla beroenden i privat sektor som är relevanta för CADA:s autonomimål.

FMV anser därför att det bör övervägas. Överväg om tillämpningsområdet för artikel 31 i tillräcklig grad omfattar privata aktörer vars beroende av molnbaserade databehandlings- eller AI-tjänster kan skapa väsentliga risker för europeisk försvarsförmåga, försörjningstrygghet eller strategisk autonomi. Vid behov skulle förordningen kunna tillhandahålla en riskbaserad mekanism för att hantera sådana aktörer utan att automatiskt utvidga hela ramverket i artikel 31 till försvarsindustrin som helhet.

Artiklarna 34–35: Förhållandet mellan EuroCloud-federationen och unionens assurancesnivåer

Artiklarna 34–35 etablerar EuroCloud-federationen som en mekanism genom vilken unionsorgan och offentliga organ kan dela offentligt ägda eller kontrollerade datacenter- och molnresurser. Modellen skiljer sig medvetet från konventionell kommersiell upphandling. Artikel 35 kräver att den delande aktören upprätthåller det erforderliga offentliga ägandet eller den offentliga kontrollen och genomför lämpliga tekniska, operativa och organisatoriska åtgärder för att säkerställa att den delade tjänsten är säker och motståndskraftig.

Detta ger betydelsefulla skyddsåtgärder och modellen med offentlig kontroll bidrar i sig till suveränitet. Artikel 35 förefaller dock inte uttryckligen ange hur tjänster som erhålls genom EuroCloud-federationen förhåller sig till ramverket för unionens assurancesnivåer enligt artiklarna 16 och 29–30. Detta blir särskilt relevant eftersom delningsarrangemanget (sharing arrangement) är

utformat som samarbete mellan offentliga aktörer snarare än ett vanligt upphandlingsförfarande.

Enligt artiklarna 29–30 kan en offentlig myndighet som upphandlar en molnbaserad databehandlingstjänst för en mycket kritisk verksamhet, efter en riskbedömning, vara skyldig att använda en tjänst som har erkänts på unionsassuransnivå 2, 3 eller 4. Om motsvarande molnkapacitet i stället erhålls genom EuroCloud-federationen förefaller artikel 35 förlita sig på sina egna krav avseende säkerhet, motståndskraft och offentlig kontroll utan att tydligt ange om den assuransnivå som följer av riskbedömningen enligt artikel 29 också måste uppfyllas.

Frågan är inte nödvändigtvis att EuroCloud ger ett svagare skydd. En offentligt kontrollerad federation kan i vissa avseenden ge mycket starka suveränitets- och autonomiegenskaper. Snarare är förhållandet mellan två separata assuransmekanismer inte tillräckligt transparent. Skillnaden är särskilt betydelsefull för försvar, nationell säkerhet och andra mycket kritiska funktioner, där en offentlig myndighet bör kunna avgöra om ett krav enligt artikel 29 på exempelvis unionsassuransnivå 4 fortfarande gäller när molnkapacitet erhålls genom delning mellan offentliga aktörer i stället för kommersiell upphandling.

FMV anser därför att det bör övervägas att klargöra förhållandet mellan artiklarna 34–35 och ramverket för unionens assuransnivåer. CADA bör särskilt klargöra om en EuroCloud-tjänst som stödjer en verksamhet som bedömts enligt artikel 29 måste uppfylla motsvarande unionsassuransnivå eller på annat sätt visa en likvärdig suveränitetsassurans som är lämplig i förhållande till den identifierade risken.

Artikel 37, artikel 16, Annex II–III och skäl 10: Unionens assuransnivåer för AI-system som upphandlas genom det gemensamma upphandlingsramverket

Artikel 37 gör det möjligt för kommissionen att genomföra gemensamma upphandlingsaktiviteter för datacentertjänster, molnbaserade databehandlingstjänster, programvara och AI-system. Samtidigt är unionens assuransramverk enligt artikel 16 och Annex II–III särskilt utformat för molnbaserade databehandlingstjänster.

Skäl 10 klargör att när ett AI-system nås genom en molnbaserad databehandlingstjänst är det endast leveransen och tillgängliggörandet av AI-systemet som utgör en del av molntjänsten, medan själva AI-systemet och dess underliggande modell är undantagna från definitionens tillämpningsområde. Ett erkännande av en molntjänst på en viss unionsassuransnivå fastställer följaktligen inte i sig motsvarande suveränitetsegenskaper för ett AI-system eller en underliggande modell som används på tjänsten.

Detta kan skapa ett potentiellt assuransgap när AI-system upphandlas för mycket kritiska verksamheter inom offentlig sektor. En molntjänst kan uppfylla en hög unionsassuransnivå samtidigt som AI-systemet eller modellen som körs på infrastrukturen introducerar separata strategiska beroenden avseende exempelvis ägande eller kontroll, proprietär modellteknik, modelluppdateringar, externa gränssnitt, kritiska beroenden av tredjeland, exponering i leveranskedjan eller möjligheten för en extern leverantör att påverka systemets fortsatta drift eller beteende.

Skillnaden kan vara särskilt relevant för försvar, nationell säkerhet och andra mycket kritiska funktioner, där suveräniteten hos värdmiljön i sig kanske inte är tillräcklig för att säkerställa operativ autonomi, försörjningstrygghet eller betrodd kontroll över hela den AI-baserade

förmågan. En värdmiljö med hög grad av suveränitetsassurans kan inte i sig eliminera strategiska beroenden som introduceras i applikations- eller modellaget.

Artikel 32 hanterar delvis frågor om strategiska beroenden vid innovativ AI-upphandling genom tilldelningskriterier som avser mervärde för unionen, europeisk teknik och försörjningstrygghet. Dessa upphandlingsöverväganden förefaller dock inte utgöra en assuransmekanism som är likvärdig med de unionsassuransnivåer som har fastställts för molnbaserade databehandlingstjänster.

FMV anser därför att det bör övervägas om CADA tydligare bör klargöra hur suveränitetsrisker och strategiska beroenden som är förknippade med AI-system och deras underliggande modeller ska bedömas när sådana system upphandlas för mycket kritiska verksamheter inom offentlig sektor. Som ett minimum bör förordningen klargöra att erkännande av den underliggande molnbaserade databehandlingstjänstens suveränitet inte i sig fastställer suveräniteten hos det AI-system eller den underliggande modell som används på tjänsten.

Skäl 62 och artiklarna 16–30: Unionens assuransnivåer och ackreditering för säkerhetsskyddsklassificerad information

Skäl 62 anger att unionens assuransnivåer 3 och 4 bör stödja säker lagring av säkerhetsskyddsklassificerade EU-uppgifter. Motsvarande krav i Annex II innehåller flera kontroller som är direkt relevanta för känsliga och klassificerade arbetslaster, bland annat krav avseende etablering och kontroll, personal, unionsmedborgarskap, säkerhetsklarering där så är lämpligt, lokalisering av drift och support, underleverantörer, cybersäkerhetsassurans samt begränsningar kopplade till beroenden av tredjeland.

Dessa krav kan utgöra en viktig grund för autonomi- och suveränitetsassurans för molntjänster som är avsedda att stödja klassificerade eller försvarsrelaterade funktioner. Ett erkännande enligt CADA-ramverket är dock fortfarande en bedömning mot unionens kriterier för suveränitet hos molnbaserade databehandlingstjänster. Det förefaller inte i sig utgöra en fullständig säkerhetsackreditering eller auktorisation för behandling av säkerhetsskyddsklassificerade EU-uppgifter eller nationellt säkerhetsskyddsklassificerade uppgifter. Sådana miljöer kan, beroende på användningsfallet, omfattas av ytterligare krav avseende fysisk säkerhet, personalsäkerhet, kryptografiskt skydd, kommunikationssäkerhet, informationsassurans, ackreditering och hantering av säkerhetsskyddsklassificerade uppgifter enligt unions-, Nato- eller nationella ramverk.

Formuleringen i skäl 62 kan därför skapa en risk för övertolkning av vad ett erkännande på unionsassuransnivå 3 eller 4 faktiskt innebär. En upphandlande myndighet eller leverantör bör särskilt inte dra slutsatsen att ett erkännande på någon av dessa nivåer automatiskt medger behandling av säkerhetsskyddsklassificerade uppgifter enbart därför att molntjänstens autonomi- och suveränitetsegenskaper uppfyller CADA.

Detta är särskilt viktigt för användare inom försvar och nationell säkerhet, för vilka skillnaden mellan suveränitetsassurans och säkerhetsackreditering av ett specifikt klassificerat system eller en specifik arbetslast (workload) är operativt betydelsefull.

FMV anser därför att det bör övervägas att klargöra att ett erkännande på unionsassuransnivå 3 eller 4 kan stödja de autonomi- och suveränitetskrav som gäller för klassificerade arbetslaster, men

att det inte i sig utgör en auktorisation eller säkerhetsackreditering för behandling av säkerhetsskyddsklassificerade EU-uppgifter eller nationellt säkerhetsskyddsklassificerade uppgifter och inte ersätter tillämpliga unions- eller medlemsstatskrav för säkerhetsskyddsklassificerad information.

Redaktionella och språkliga kommentarer

Sida 15(2)

FMV uppmärksammar felstavningen “necessary frameowrk”.

Artikel 2

FMV uppmärksammar att numreringen av definitionerna förefaller hoppa från punkt (22) till punkt (25), medan punkterna (23) och (24) saknas. Numreringen bör verifieras och korrigeras, inklusive eventuella interna hänvisningar som påverkas av de saknade punkterna.

Artikel 4.1 d

FMV uppmärksammar mellanslagsfel “theirflexibility”.

Annex II, nivå 3, kriterium (g), och motsvarande avsnitt 7.2 (c) i Annex III

FMV uppmärksammar att annex II, unionsassuransnivå 3, kriterium (g), förefaller felaktigt hänvisa till en genomförandeakt enligt artikel 19, medan mekanismen för att fastställa ett associerat tredjeland regleras i artikel 18. Samma felaktiga hänvisning till artikel 19 förekommer även i motsvarande beviskriterium i Annex III. Båda hänvisningarna bör därför korrigeras konsekvent.

Artikel 30(4)

FMV uppmärksammar att bokstavsbeteckningen för undantagsgrunderna förefaller innehålla en dubblerad punkt (a), efter punkt (b) följd av ytterligare en punkt (a). Den tredje grunden bör ses över och förefaller behöva numreras om till punkt (c).

Artikel 37(1)

FMV uppmärksammar mellanslagsfel “forUnion entitiesand”.

Artikel 38(9)

FMV uppmärksammar att skrivningen Regulation (EU, Euratom) 2014/2509 ska korrigeras till Regulation (EU, Euratom) 2024/2509.

Artikel 40(5)

FMV uppmärksammar fel i att punkten inleds med “5. ”

Artiklarna 44–45 / Allmänt

FMV uppmärksammar felaktig numrering av bestämmelsen om delegering. Avdelning IV, kapitel V avslutas med artikel 44, ”Nätverk av programkontor för öppen källkod”. Avdelning V inleds därefter med en andra bestämmelse som också är numrerad artikel 44, ”Utövande av delegeringen”, följd direkt av artikel 46. Artikel 45 saknas således i den normativa texten. I motiveringen anges bestämmelsen om utövande av delegerade befogenheter som artikel 45, och artiklarna 6.4, 16.2, 20.9, 21.1 och 31.3 hänvisar också till delegerade akter som ska antas i enlighet



BESLUT

Datum	Diarienummer	Ärendetyp
2026-09-30	26FMV5569	1.3
		Sida
		12(12)

med artikel 45. Den andra artikel 44 i avdelning V förefaller därför vara felnumrerad och bör vara artikel 45.

Artikel 47(3)

FMV uppmärksammar att "to Commission shall take into account..." rimligen bör lyda "the Commission shall take into account...".

Annex / Allmän redaktionell granskning

FMV uppmärksammar att annexen innehåller ett antal ytterligare stavnings-, mellanslags- och formateringsfel. I stället för att skapa en separat granskningspost för varje uppenbart skrivfel bör dessa samlas i en rekommendation om en heltäckande juridisk-språklig och redaktionell genomgång av den normativa texten och Annexen före antagandet.

Beredning av ärendet

I den slutliga handläggningen har chef för Lednings- och ekonomistabens enhet för EU- och Nato-samarbete, Mikael Ericsson, samt Tobias Koppel, Karin Adamsson Anna Lundborg Regnér deltagit. Den sistnämnda har varit föredragande.

Försvarets materielverk

Henrik Gaunitz
Chef Lednings- och ekonomistaben

Sändlista

Finansdepartementet (fi.remissvar@regeringskansliet.se med kopia till fi.ofa.dis.remissor@regeringskansliet.se).

Kopia till

Lednings- och ekonomistaben
Marknad och inköp
Infrastrukturstaben
Juridik- och säkerhetsstab
Ledningssystemmateriel
Arkiv