

REMISSYTTRANDE

2026-10-01

FRA beteckning

Dnr 2026FRA1618-2

Finansdepartementet

Er handläggare

Ert datum

Er beteckning

FRA handläggare
Viktor Berg

2026-07-10

Fi2026/01676

FRA föreg. datum

FRA föreg. beteckning

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

Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på förslaget till förordning. De inledande synpunkterna rör myndighetens verksamhet generellt och den avslutande delen rör myndighetens uppdrag att förebygga, upptäcka och hantera cyberhot.

Förordningens tillämpningsområde

FRA välkomnar ambitionen att stärka den digitala suveräniteten inom EU och minska beroendet av tredjeland vad gäller moln- och AI-tjänster.

Förslaget bygger dock på förutsättningen att det finns, eller snart kommer att finnas, europeiska alternativ till de aktörer i tredjeland som idag dominerar marknaden på området. Det kan ifrågasättas om det finns europeiska aktörer som i närtid kommer kunna leverera motsvarande kapacitet, skalbarhet och säkerhet.

I regeringens faktapromemoria om förslaget¹ anges som preliminär svensk ståndpunkt bl.a. att regeringen anser att medlemsstaternas ansvar för bedömningar av säkerhetskrav för verksamheter inom exempelvis försvarsområdet och annan säkerhetskänslig verksamhet, måste värnas. Vidare anser regeringen att det är viktigt att kommissionens

¹ 2025/26:FPM99, s. 12.

eventuella befogenheter på området är tydligt avgränsade och proportionerliga och att medlemsstaternas handlingsutrymme säkerställs.

FRA delar till fullo denna uppfattning. Den föreslagna förordningen riskerar att begränsa FRA:s möjligheter till digitalisering och därmed utvecklingen av myndighetens förmågor. Det vore till skada för myndighetens verksamhet och i förlängningen Sveriges nationella säkerhet. FRA anser därför att det i den föreslagna förordningen måste föras in en avgränsning av tillämpningsområdet på så sätt att det anges att förordningen inte gäller verksamhet och åtgärder till skydd för medlemsstaternas nationella säkerhet. En sådan avgränsning skulle också vara i linje med artikel 4.2 i fördraget om Europeiska unionen, som slår fast att den nationella säkerheten är varje medlemsstats eget ansvar.

Ramverk för tillitsnivåer för molntjänster och krav vid offentlig upphandling av molntjänster (Title IV, Chapter I, *Cloud computing sovereignty framework*, Chapter II, Section 1, *Public procurement*, och Annex II, *Criteria for union assurance levels*)

För att avgränsa vilka offentliga verksamheter som omfattas av kravet på riskbedömning i artikel 29.1 a används begreppet ”verksamhet med betydelse för att upprätthålla allmän ordning”. Begreppet definieras inte i förordningen och det är svårt att avgöra vilka verksamheter som omfattas. Avgränsningen får stor praktisk betydelse eftersom verksamheter som träffas av artikel 29.1 endast ska få upphandla molntjänster med tillitsnivå 2, 3 eller 4, enligt artikel 30.3.

Även kraven för de olika tillitsnivåerna är i vissa delar otydliga. Ett exempel är att det i bilaga II, avsnitt 1.1 e anges att molntjänstleverantören ska visa att tjänsten uppfyller ”state-of-the-art cybersecurity standards” men inte vad som avses med detta. Det föreslås också att kommissionen ska få justera kraven genom delegerade akter.

Detta gör det sammantaget svårt att förutse vilken påverkan förslaget i dessa delar skulle ha. FRA:s bedömning är dock att få leverantörer av molntjänster idag kan leva upp till kraven som ställs i bilaga II, särskilt på de högre tillitsnivåerna, vilket innebär att urvalet av tänkbara leverantörer kommer att minska. Vidare finns det ofta behov av att kunna beakta och prioritera andra intressen vid upphandlingar inom försvars- och säkerhetsområdet än de som angetts i förordningen, såsom intressen kopplade till leverans- och försörjningstrygghet samt kompatibilitet mellan olika system.

För FRA:s del skulle kraven i det föreslagna ramverket – givet att myndigheten omfattas av dem – innebära att såväl vissa befintliga och planerade åtgärder inom försvars- underrättelseverksamheten, bl.a. vissa internationella samarbeten, omöjliggörs.

Utöver det generella undantaget för nationell säkerhet enligt ovan bör det därför i artikel 29.1 förtydligas att kravet på riskbedömning i artikel 29.1 a inte omfattar verksamhet som bedrivs för nationell säkerhet.

Inrättande av accelerationszoner för datacenter (Title III, Chapter I, *Data centre acceleration zones*)

Kommissionen föreslår att varje medlemsstat ska utse särskilda områden, s.k. accelerationszoner, där det ska bli enklare och gå snabbare att etablera datacenter, för att påskynda utbyggnaden av datacenter i unionen. Vid bedömningen av lämpliga platser ska medlemsstaterna bland annat beakta tillgången till mark, energi och elektronisk kommunikation samt möjligheterna att använda spillvärme och befintlig infrastruktur. Förslaget innehåller även kortare tillståndprocesser och möjlighet att ge vissa datacenter ställning som strategiska projekt.

Datacenter utgör en central del av den digitala infrastruktur som offentlig och samhällsviktig verksamhet är beroende av. Lokaliseringen påverkar bland annat anläggningarnas fysiska skydd, tillgång till energi och elektronisk kommunikation samt möjligheten att upprätthålla verksamheten vid kris och höjd beredskap. Samtidigt kan den här typen av anläggningar väcka frågor om elektromagnetisk kompatibilitet (EMC) eftersom de riskerar att störa eller på andra sätt påverka befintliga anläggningar som används inom totalförsvaret, bl.a. för signalspaning.

Artiklarna 10 och 13 bör därför kompletteras med krav på att totalförsvarets intressen beaktas vid lokalisering, tillståndsprövning och utpekande av strategiska datacenterprojekt. Bedömningen bör omfatta fysisk säkerhet, geografisk spridning, redundans, energiförsörjning, elektronisk kommunikation. Det bör även framgå att de skyndsamma tillståndprocesserna inte får begränsa möjligheten att genomföra nödvändiga säkerhetsbedömningar eller minska totalförsvarets inflytande vad gäller EMC-frågor.

Cybersäkerhet

FRA har, främst genom den verksamhet som bedrivs av det nationella cybersäkerhetscenter (NCSC) som finns inom myndigheten, i uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Ur detta perspektiv har myndigheten följande synpunkter på förslaget till förordning.

Cybersäkerhet i utvecklingssatsningarna

Förslaget innehåller vissa hänvisningar till cybersäkerhet. Artikel 4.2 behandlar säkra och motståndskraftiga molnlösningar, artikel 4.3 anger cybersäkerhet som ett strategiskt

område för avancerad AI och artikel 4.6 behandlar säkra plattformar för AI agenter. Cybersäkerhet framgår däremot inte som ett genomgående mål för utvecklings-satsningarna.

Den nuvarande utformningen innebär att cybersäkerhet främst behandlas inom vissa särskilt utpekade teknikområden. De omfattande investeringar som ska göras i datacenter, molntjänster och AI-system kommer samtidigt att skapa tekniska lösningar och beroenden som kommer bestå under lång tid. Säkerheten behöver därför finnas med redan när tekniken utvecklas och införs.

Det behöver också vara tydligt att satsningarna kan stödja AI-projekt som har till huvudsakligt syfte att stärka cybersäkerheten. Det kan exempelvis handla om lösningar för att förebygga, upptäcka, analysera och hantera cyberhot och cyberincidenter. Möjligheten till sådant stöd bör inte vara begränsad till projekt inom avancerad AI enligt artikel 4.3.

Cybersäkerhet bör därför läggas till som ett genomgående mål för utvecklingssatsningarna i artiklarna 3 och 4. Det bör framgå att säkerhet och motståndskraft ska byggas in från början i de tekniker, infrastrukturer och AI-system som utvecklas med stöd av initiativen.

Det bör även uttryckligen anges att stöd kan lämnas till AI-projekt som stärker cybersäkerheten, oavsett vilket av de operativa målen projektet i övrigt hänför sig till. Detta skulle säkerställa att cybersäkerhet behandlas både som ett grundläggande krav på den teknik som utvecklas och som ett eget strategiskt användningsområde för AI.

NCC:erna bör vara AI-centrum för cybersäkerhet

De nationella samordningscentren för cybersäkerhet (NCC) har redan i uppdrag att stödja forskning, innovation och införande av ny cybersäkerhetsteknik, särskilt hos små och medelstora företag. Nätverket av nationella samordningscenter för forskning och innovation på cybersäkerhetsområdet (NCC-nätverket) utgör därmed en redan etablerad struktur för att genomföra ett operativt mål om AI för cybersäkerhetsändamål. Uppdraget ligger alltså nära de uppgifter som de föreslagna centrumen för AI ska ha. Att skapa parallella strukturer framstår inte som ändamålsenligt.

Det bör därför anges i artikel 5 att de nationella samordningscentrumen enligt förordning (EU) 2021/887 ska kunna utses till eller ingå i de centrum för AI som ansvarar för genomförandet av detta operativa mål. I andra hand bör det anges i skälen att medlemsstaterna bör använda de nationella samordningscentrumen för detta ändamål.

Däriigenom kan deras befintliga kompetens, kontaktytor och stödstrukturer tas till vara utan att parallella organisationer byggs upp.

AI i det nationella cybersäkerhetsarbetet

I artikel 7.2 anges vilka frågor som de nationella moln- och AI-strategierna minst ska omfatta. Där ingår åtgärder för bl.a. införande av moln- och AI-tjänster, datacenterkapacitet, beräkningsinfrastruktur, offentlig upphandling, teknisk suveränitet och tillgång till data. Cybersäkerhet nämns däremot inte uttryckligen som en obligatorisk del av strategierna.

På motsvarande sätt anges det inte uttryckligen i kraven på de nationella cybersäkerhetsstrategierna enligt NIS 2-direktivet² hur strategierna ska omhänderta AI och teknikens betydelse för cybersäkerheten. Förslaget säkerställer därmed inte att kopplingen mellan AI och cybersäkerhet tas om hand inom medlemsstaternas strategiska arbete.

Det finns en risk att åtgärder för att öka användningen av moln- och AI-tjänster kan planeras utan ett genomgående cybersäkerhetsperspektiv, samtidigt som de nationella cybersäkerhetsstrategierna inte är anpassade till hur AI förändrar cyberhot, sårbarheter, tekniska beroenden och incidenthantering. Detsamma gäller möjligheten att använda AI för att stärka cybersäkerhetsförmågan.

Det bör därför säkerställas i förordningen att kopplingen mellan AI och cybersäkerhet blir en obligatorisk del av medlemsstaternas strategiska arbete. Kravet bör i första hand införas som en uttrycklig och obligatorisk del av de nationella moln- och AI-strategierna enligt artikel 7. Om kravet i stället knyts till medlemsstaternas nationella cybersäkerhetsstrategier bör ett motsvarande bindande krav införas i förordningen.

Övergångstid vid byte av molntjänst

Om en riskbedömning medför att en molntjänst behöver tillhandahållas utifrån en högre tillitsnivå och en verksamhetsutövare identifierar att den molntjänst man nu nyttjar inte kan uppnå den tillitsnivån så behöver verksamhetsutövaren byta molntjänst. Bytet ska enligt artikel 29.6 genomföras inom en skälig övergångsperiod som inte får överstiga tolv månader. Vid fastställandet av perioden ska hänsyn tas till bytets tekniska genomförbarhet, tjänstekontinuiteten och möjligheten att överföra data.

² Direktiv (EU) 2022/2555.

Även om bestämmelsen anger att dessa omständigheter ska beaktas kan de enligt förslaget aldrig motivera en längre övergångsperiod än tolv månader. För komplexa och samhällsviktiga verksamheter kan ett byte kräva omfattande anpassningar av system, data, integrationer, behörigheter, säkerhetsfunktioner och avtal med underleverantörer.

Kontinuitet och säker ändringshantering är centrala delar av cybersäkerhetsarbetet. Omfattande förändringar i komplexa informationssystem medför i sig en förhöjd risk för incidenter. En alltför snabb övergång kan bland annat leda till driftstörningar, felaktiga inställningar, dataförlust eller brister i säkerhetsövervakningen. Den absoluta tidsgränsen kan därmed motverka bestämmelsens säkerhetssyfte. Det bör därför vara möjligt att förlänga övergångsperioden med anledning av exempelvis behovet av kontinuitet.

I artikel 29.6 bör det därför medges en längre övergångsperiod när ett byte inte kan genomföras inom tolv månader utan betydande risker för cybersäkerheten eller tjänstekontinuiteten. Behovet av en längre övergångsperiod bör grundas på en dokumenterad bedömning av verksamhetens kritiska funktioner, systemens komplexitet och de säkerhetsrisker som följer av bytet.

Tolv månader kan kvarstå som utgångspunkt, men bör alltså inte utgöra en absolut tidsgräns. En längre övergångsperiod bör förenas med en plan för bytet och lämpliga åtgärder för att hantera riskerna under övergångstiden. Därmed kan bytet genomföras under kontrollerade former utan att verksamheten ges möjlighet att fortsätta använda en olämplig tjänst på obestämd tid.

Risk för monoberoenden

Enligt artikel 30 ska vissa offentliga verksamheter endast upphandla molntjänster som har erkänts på den tillitsnivå som följer av verksamhetens riskbedömning. I artikel 29.9 anges att verksamheterna ska överväga om en strategi med flera leverantörer eller flera molntjänster är lämplig.

Om endast ett fåtal leverantörer kan uppfylla både verksamheternas behov och kraven för de högre tillitsnivåerna kan situationer där många organisationer i ett land, eller inom en sektor, har ett beroende till samma digitala produkt (information, mjukvara, hårdvara eller tjänst), s.k. monoberoenden³, uppstå. Regler som är avsedda att minska kritiska beroenden kan därmed i stället skapa eller förstärka monoberoenden.

³ Se Myndigheten för civilt försvar, Metodik för strategisk cybersäkerhetsanalys, 2026, s. 39. Se även motsvarande definition i EU ICT Supply Chain Security Toolbox [ICT supply chain security: EU adopts a toolbox to mitigate risks | Shaping Europe's digital future](#).

Att använda flera leverantörer eller molntjänster minskar inte nödvändigtvis denna risk. Olika tjänster kan vara beroende av samma underliggande infrastruktur, programvara eller underleverantörer. En störning eller säkerhetsincident hos en sådan aktör kan därför påverka flera tjänster samtidigt.

Det bör därför anges i artiklarna 3 och 4 att utvecklingssatsningarna ska bidra till att bredda utbudet av sinsemellan oberoende och utbytbara molntjänster som kan erkännas på de högre tillitsnivåerna. På detta sätt kan satsningarna förbättra möjligheterna att undvika monoberoenden i tjänsternas underliggande infrastruktur och leveranskedjor.

Det bör vidare förtydligas i artikel 29.9 att riskbedömningen ska omfatta monoberoenden till infrastruktur, programvara och underleverantörer. Bedömningen bör utgå från den faktiska möjligheten att byta eller kombinera leverantörer och inte enbart från antalet tjänster eller leverantörer.

Ägarförändringar som påverkar en molntjänsts tillitsnivå

I det föreslagna ramverket för tillitsnivåer för molntjänster ställs det för tillitsnivå 3 och 4 särskilda krav på att leverantören och relevanta underleverantörer inte står under kontroll av ett tredjeland eller av en aktör etablerad i ett tredjeland. En försäljning eller annan förändring av ägandet av en leverantör eller underleverantör kan därför medföra att kraven för tillitsnivån inte längre uppfylls.

I artikel 23 regleras hur sådana förändringar ska hanteras när leverantören har fått kännedom om dem, men inte att en planerad ägarförändring ska anmälas och bedömas innan den genomförs. Planerade ägarförändringar kan samtidigt omfattas av förordningen om granskning av utländska investeringar⁴. Det anges dock inte hur en möjlig påverkan på tillitsnivån ska föras in i den prövningen. Om tillitsnivån sänks eller återkallas först efter att en försäljning har slutförts kan offentliga och samhällsviktiga verksamheter tvingas byta molntjänstleverantör, med de kostnader samt risker för säkerhet och kontinuitet som ett sådant byte medför. I vissa fall kan det vara närmast praktiskt omöjligt att byta leverantör.

Det bör därför förtydligas hur planerade förändringar av ägande eller kontroll som kan påverka en molntjänsts tillitsnivå förhåller sig till EU:s regelverk för granskning av utländska direktinvesteringar. Risken för att en transaktion medför att en tjänst förlorar en högre tillitsnivå bör kunna beaktas vid bedömningen av transaktionens konsekvenser för säkerhet och allmän ordning. Om risken inte kan hanteras genom villkor bör ägarförändringen kunna förhindras med stöd av det regelverket.

⁴ Förordning (EU) 2026/1386.

Harmoniserade sanktionsavgifter

Enligt artikel 24 ska medlemsstaterna fastställa sanktionerna för överträdelser av bestämmelserna om tillsitsnivåer. Sanktionerna ska vara effektiva, proportionerliga och avskräckande, men förordningen anger inte några gemensamma nivåer för sanktionsavgifter. Leverantörens årsomsättning inom unionen är endast en av flera omständigheter som ska beaktas.

Av artikel 25.4 följer att den medlemsstat där leverantören har sitt huvudsakliga säte exklusiv behörighet att utöva tillsyn. Det innebär att samma överträdelse kan mötas av väsentligt olika sanktioner beroende på var leverantören är etablerad. Det skapar en risk för att leverantörer söker sig till medlemsstater med mindre ingripande sanktionssystem och för en konkurrens mellan medlemsstaterna om att erbjuda mindre sträng tillsyn och lägre sanktionsavgifter.

Eftersom en tillsitsnivå erkänns i hela unionen påverkar en otillräcklig nationell tillsyn även verksamheter i andra medlemsstater. För stora internationella leverantörer kan låga nationella sanktionsavgifter dessutom sakna avskräckande verkan.

Förordningen bör därför innehålla ett harmoniserat system för sanktionsavgifter efter förebild av förordningen om artificiell intelligens⁵ och cyberresiliensförordningen⁶, med gemensamma högsta nivåer och tydliga kategorier utifrån överträdelsens allvar.

De högsta sanktionsavgifterna bör bestämmas som ett fast belopp eller som en andel av leverantörens totala globala årsomsättning. Den enskilda avgiften bör fortsatt bestämmas med hänsyn till bland annat överträdelsens allvar och varaktighet samt leverantörens storlek.

Ansvarig myndighet för de nationella riskbedömningarna

Enligt artikel 29 ska medlemsstaterna genomföra nationella riskbedömningar, uppdatera dem regelbundet och rapportera resultaten till kommissionen. Det anges däremot inte vilken nationell aktör som ska ansvara för att bedömningarna genomförs.

För att säkerställa kontinuitet i riskbedömningarna bör det anges att varje medlemsstat ska utse en ansvarig myndighet för de nationella riskbedömningarna. Myndigheten bör ha det samlade ansvaret för att genomföra eller samordna bedömningarna, hålla dem aktuella och rapportera resultaten till kommissionen. Bedömningarna bör tas fram i

⁵ Förordning (EU) 2024/1689.

⁶ Förordning (EU) 2024/2847.

samverkan med berörda sektorsmyndigheter, cybersäkerhetsmyndigheter, säkerhetsmyndigheter och offentliga verksamheter. Uppgiften bör kunna ges till en befintlig myndighet.

I detta ärende har generaldirektören Björn Lyrvall beslutat. I den slutliga handläggningen har även överdirektören Maria Diamant, chefsjuristen Michaela Dráb, avdelningschefen John Billow (avd. NCSC), enhetschefen Jessica Öhlund Andersson (C JUR:s kansli/Rättsenhet 2) och handläggaren Olof Wijkmark (avd. NCSC) deltagit. Juristen Viktor Berg har varit föredragande.

Försvarets radioanstalt

Björn Lyrvall

Viktor Berg

Sändlista

Externt

Försvarsdepartementet/EFU

Försvarsdepartementet/ECH

Försvarsdepartementet/Rättssekretariatet

Internt FRA

GD

ÖD

C JUR

Bitr. C JUR

C GD:s stab

C KOM

C PS

AC

C JUR:s kansli/C Rätts 1

C JUR:s kansli/C Rätts 2