



Finansdepartementet

Ert tjänsteställe, handläggare

Avdelningen för offentlig förvaltning,
Enheten för digital infrastruktur och säkerhet

Vårt tjänsteställe, handläggare

Madeleine Nilsson

Ert datum

2026-07-10

Vårt föregående datum

Er beteckning

Fi2026/01676

Vår föregående beteckning

Försvarsmaktens yttrande över Finansdepartementets remiss av Europeiska kommissionens förslag till förordning om utveckling av moln och AI KOM(2026)502

Sammanfattning

Försvarsmakten ställer sig positiv till en EU-gemensam strategi för att stimulera forskning, utveckling och innovation för att uppnå en högre grad av suveränitet inom moln- och AI-området. Det är av vikt att Sverige deltar aktivt i det EU-gemensamma arbetet i dessa frågor för att bevaka landets intressen och dra fördelar av frukterna som arbetet resulterar i. Förslaget aktualiserar flera frågor av betydelse för försvarsförmågan.

Det är av största vikt att det inte skapas ett regelverk som i praktiken inskränker handlingsfriheten när det gäller försvar och nationell säkerhet. Styrande för teknikval behöver ytterst vara den militära förmågan, hur snabbt den kan införas och om den kan upprätthållas i kris och krig. Försvarsmakten avstyrker därför förslaget i de delar det kan antas begränsa den militära förmågeutvecklingen. Realistiska tidsplaner och undantag för militär verksamhet kommer att vara avgörande för att uppfylla operativa krav och interoperabilitet inom Nato.

Försvarsmakten delar många av de synpunkter som lyfts fram i Finansdepartementets Faktapromemoria 2025/26:FPM99, exempelvis att Sverige behöver rådighet över data och system samtidigt som fördelarna med samarbete med partners tillvaratas, att en eventuell reglering måste bygga på tydliga konsekvensanalyser utifrån existerande behov av åtgärder samt att regler, processer och strukturer måste utformas så att konsekvenserna är proportionerliga. Försvarsmakten delar bedömningen att medlemsstaternas ansvar

(MNI)

Postadress

Försvarsmakten

107 85 Stockholm

Besöksadress

Lidingövägen 24

Telefon

08-788 75 00

Telefax

08-788 77 78

E-post, Internet

exp-hkv@mil.se

www.forsvarsmakten.se



för verksamheter inom försvarsområdet och säkerhetskänslig verksamhet måste värnas. Försvarsmakten delar även bedömningen att det är viktigt att värna de upphandlande myndigheternas handlingsutrymme.

Försvarsmakten bedömer sammanfattningsvis att kommissionens fortsatta arbete med förordningen tydligare måste förankras i rådande tekniska, regulatoriska, ekonomiska och säkerhetspolitiska förutsättningar. Särskilt bör handlingsfrihet för nationell säkerhet och militärt försvar och relationen till allierade och partners säkerställas.

Om behovet av suveränitet och rådighet

Rådighet och suveränitet behöver för det militära försvaret definieras utifrån militär kontroll och handlingsfrihet, inbegripet att snabbt kunna anskaffa, integrera och vidmakthålla teknik som krävs för nationell och kollektiv försvarsförmåga. Försvaret behöver kunna ta hänsyn till interoperabilitet inom Nato, befintliga system, tidskritiska förmågebehov och tillgång till spetsteknik. Försvarets faktiska rådighet behöver även inkludera drift, vidareutveckling, kostnadsbild och ersättningsmöjligheter.

Försvarsmakten är beroende av avancerad teknik och tekniskt samarbete med allierade och partners. Framväxande och kritisk teknik, som IKT/AI, kvantteknik och halvledare, är väsentlig för den militära förmågeutvecklingen. Försvarsmakten har behov av både ny och befintlig teknik i vidmakthållande och utveckling av den militära förmågan. Handlingsfrihet och tillgången till teknik måste vägas mot möjligheten till självförsörjning. Från Försvarsmaktens perspektiv är det därför angeläget att en eventuell reglering utformas så att teknologisk autonomi stärks utan att tillgång till relevant teknik begränsas. Ett förslag är att överse möjligheten att stärka ambitionen avseende ömsesidiga beroenden.

Kommissionen utgår från att beroende av leverantörer som står under kontroll av tredje land kan innebära risker. Försvarsmakten påtalar att även om en aktör uppfyller förordningens krav på europeisk etablering kan den faktiska rådigheten för beställaren vara begränsad. Det är i slutändan leverantörer som kan ha avgörande inflytande över utvecklingsprioriteringar, produktlivscykler, prissättning, licensvillkor och funktionalitet. I ljuset av det skulle en vidareutveckling av förslaget om EuroCloud Federation kunna vara att stärka förutsättningarna för offentligt kontrollerade digitala basförmågor som strategiskt alternativ till kommersiellt dominerade system.

Datacenterkapacitet utgör endast en del av den digitala suveräniteten. Som kommissionen också beskriver ligger de stora teknikföretagens styrka i sammanhängande ekosystem av infrastruktur, plattformar och mjukvara samt i innovations- och investeringskraft och affärsmodeller med kraftig inlåsningsseffekt. Försvarsmakten anser att risken för fortsatta beroenden och



strukturella inlåsningseffekter tydligare bör adresseras i det fortsatta arbetet med förordningen.

Krav vid offentlig upphandling av molntjänster

Försvarsmakten ser inga behov av ytterligare reglering på upphandlingsområdet. Försvarsmakten vill särskilt understryka att nya regleringar inte får riskera möjligheten att utforma och genomföra upphandlingar utifrån operativa behov. I förordningen bör tydligt säkerställas att medlemsstaterna behåller handlingsfrihet inom försvarsområdet och att nya krav inte blir ett hinder för att snabbt anskaffa, integrera och vidmakthålla teknik som krävs för nationell och kollektiv försvarsförmåga. Det bör gälla även tillämpningen av ickeprisbaserade tilldelningskriterier, såsom t.ex. i vilken utsträckning leverantörer bidrar till utvecklingen av ett europeiskt moln- och AI-ekosystem. Sådana hänsyn bör inom försvarsområdet vara en möjlighet, inte en skyldighet.

Försvarsmakten noterar att det i motiveringen till förslaget anges att den föreslagna förordningen kompletterar upphandlingsdirektiven. Det framgår dock inte hur det förhåller sig till försvars- och säkerhetsupphandlingsdirektivet som i svensk rätt genomförts i lagen om upphandling på försvars- och säkerhetsområdet. Det är därmed oklart om kraven (i föreslagen artikel 30) ska tillämpas även vid upphandling som genomförts enligt det regelverket och hur de i så fall förhåller sig till de säkerhetsskyddskrav som redan ställts där. Detta bör förtydligas i det fortsatta arbetet med förordningen.

Försvarsmakten avstyrker förslaget att medlemsstaterna ska lämna rapporter till kommissionen som innehåller riskbedömningar och information om användning och planerad användning av molntjänster bl.a. inom försvaret. Det behöver närmare analyseras vad kommissionens roll och uppgift bör vara i förhållande till medlemsstaterna med utgångspunkt i det nationella självbestämmandet i frågor som rör försvar och nationell säkerhet.

Det framgår inte av förslaget hur riskbedömningarna ska förhålla sig till de säkerhetsskyddsanalyser som redan görs enligt nationell säkerhetsskyddslagstiftning. Om de två processerna ska genomföras parallellt utan samordning innebär det ett dubbelarbete utan motsvarande säkerhetsvinst, eftersom det i praktiken handlar om överlappande förhållanden.

Vid ett införande av en ny förordning måste övergångsregler formuleras utifrån en realistisk tidsplan. För verksamhet som omfattas av säkerhetsskyddsregelverket är ledtiderna för leverantörsbyte väsentligt längre än för annan verksamhet, eftersom även säkerhetsprövning, ackreditering och migrering av skyddad information ingår.



Ramverk för tillitsnivåer för molntjänster

Ett gemensamt ramverk med fastställda kriterier och där ett erkännande av en medlemsstat gäller i hela unionen skulle på en generell nivå kunna innebära lättnader i administrationen, bidra till tydlighet för leverantörerna och förenkla upphandlingen av aktuella tjänster. Försvarsmakten avstyrker inte förslaget i grunden.

Totalförsvaret behöver kunna upprätthålla eller ersätta kritisk funktionalitet även under störda förhållanden. Tillitsnivåerna innehåller flera krav som är relevanta i detta avseende. Försvarsmakten föreslår dock att dessa kompletteras med tydligare fokus på styrning av kritiska teknikleverantörer, med beredskapskrav kopplat till kontinuitet, ersättningsmöjligheter och kontroll.

Det bör säkerställas att medlemsstaterna ges ett reellt inflytande när det gäller vilka krav som ska ställas för de olika tillitsnivåerna och innan ett tredjeland erkänns ha tillräckliga skyddsåtgärder. Nationella förhållanden och nationella bedömningar avseende hotbild m.m. kan skilja sig åt mellan medlemsstaterna och i förhållande till den medlemsstat som erkänner en leverantör. Försvarsmakten måste för sin verksamhet göra en egen bedömning i varje enskilt fall. Det kan ifrågasättas om verksamhetsutövare över huvud taget ska vara bundna av gjorda erkännanden. I vart fall bör i förordningen tydligt regleras undantag för verksamhet som rör försvar och nationell säkerhet.

Enligt förslaget ska en leverantör vara skyldig att anmäla väsentliga förändringar som kan påverka tillitsnivån som har erkänts, exempelvis ägarförändring. Försvarsmakten anser att detta är av stor vikt. Det framgår dock inte vad som gäller för en tjänst som redan är i drift när tillitsnivån för leverantören sänks. För säkerhetsskyddad verksamhet är det av vikt att det klargörs eftersom ett omedelbart avbrott sällan är möjligt medan fortsatt drift på en otillräcklig nivå inte heller är godtagbar. Verksamhetsutövaren behöver veta vilket handlingsutrymme som finns och inom vilken tid åtgärder ska vidtas.

Varje medlemsstat ska utse en eller flera behöriga myndigheter som ska ansvara för att pröva ansökningar och utöva tillsyn enligt förordningen, men det framgår inte om säkerhetsskyddad verksamhet ska hanteras av samma myndighet som annan verksamhet inom offentlig sektor. Försvarsmakten anser att det bör framgå uttryckligen i förordningen att medlemsstaterna får utse en särskild behörig myndighet för säkerhetsskyddad verksamhet.

Inrättande av accelerationszoner för datacenter och strategiska datacenterprojekt

Försvarsmakten är positiv till ambitionen att öka datacenterkapaciteten inom EU. Det måste i detta avseende göras en noggrann konsekvensanalys och avvägningar av olika intressen rörande bl.a. miljö, ekonomi och näring precis som regeringen påpekar i Faktapromemorian. För Försvarsmaktens del är det särskilt viktigt att



myndigheten fortsatt har möjlighet att bevaka sina intressen på det sätt som följer av miljöbalkens bestämmelser, bl.a. genom riksintressebevakning och möjlighet att ta aktiv del i tillstånds- och lovprocesser. Om datacenterprojekt ska anses vara av riksintresse så är det viktigt att bestämmelsen i 3 kap. 10 § miljöbalken, enligt vilken försvarsintresset ska ges företräde vid avvägningen mellan olika icke förenliga ändamål, alltså ska gälla.

Datacenter kan vara kritisk infrastruktur där störningar snabbt kan få konsekvenser. Försvarsmakten anser därför att förslaget i den del det avser kommissionens ambition att kraftigt öka antalet datacenter bör kompletteras med en samlad säkerhetsskyddsanalys inbegripet risken för antagonistiska eller militära angrepp. Särskilt datacenter knutna till de högsta tillitsnivåerna bör betraktas som skyddsobjekt.

Åtgärder för att främja användningen av öppen källkod och öppna standarder inom EU:s moln- och AI-ekosystem.

Något uttryckligt undantag för säkerhetsskyddsklassificerat material anges inte. Försvarsmakten utgår ifrån att kraven inte ska omfatta sådan programvara. Detta behöver tydliggöras i det fortsatta arbetet.

.....

I beredningen av detta ärende har deltagit utvecklingsstrateg Elsa Lindstedt och strategisk samordnare Tommy Söder.

Detta remissyttrande har beslutats av chefsjurist Kerstin Bynander. I den slutliga handläggningen har som föredragande försvarsjurist Madeleine Nilsson deltagit.

Bynander, Kerstin

Chefsjurist

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

**Sändlista**

Regeringskansliet
med kopia till

fi.remissvar@regeringskansliet.se
fi.ofa.dis.remisser@regeringskansliet.se

Inom myndigheten för kännedom

MUST SÄKK SÄKS

FST CYBER

FST STRA