

YTTRANDE
Fi2026/01676

Till Finansdepartementet:
fi.remissvar@regeringskansliet.se
Med kopia till:
fi.ofa.dis.remisser@gov.se

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

Säkerhets- och försvarsföretagen (SOFF) tackar för möjligheten att yttra sig. SOFF är en branschförening för företag inom säkerhets- och försvarsområdet med verksamhet i Sverige. SOFF har idag 500 medlemsföretag som har verksamhet inom försvar, samhällssäkerhet och cybersäkerhet.

Sammanfattning

SOFF stöder ambitionen att stärka Europas moln- och AI-förmåga och minska kritiska beroenden. Förordningen kan – beroende på hur den slutligt utformas – skapa en konkret möjlighet för Europa att stärka rådigheten över säkerhetskänsliga data och digitala tjänster, samt särskilt kritiska funktioner och minskaberoenden som medför oacceptabla risker för säkerhet eller kontinuitet. En tydlig reglering kan också ge europeiska myndigheter mandat och incitament att aktivt efterfråga europeiska lösningar som uppfyller tydliga säkerhets- och kontinuitetskrav. Samtidigt understryker SOFF vikten av att förordningen inte utformas på ett sätt som i praktiken minskar försvarsförmågan och strategiskt viktiga samarbeten.

Förordningen bör främja konkurrens, innovation och handlingsfrihet genom teknikneutrala och proportionerliga krav, verifierbar kontinuitet och praktiska möjligheter till leverantörsbyte när så krävs för att säkerställa funktion. Europeiska och svenska alternativ behöver ges möjlighet att växa, samtidigt som tillgång till teknik och interoperabilitet med allierade väpnas. För särskilt kritiska funktioner kan långtgående krav på *rättslig* och *operativ* kontroll vara motiverade. Tillämpningsområde och övergångsregler behöver förtydligas, och genomförandet bör samordnas med befintliga regelverk.

En gemensam europeisk certifieringsram

SOFF välkomnar ambitionen om unionsomfattande erkännande. Samtidigt riskerar nationella bedömningar, skilda administrativa förutsättningar och möjligheten till invändningar från andra medlemsstater att leda till långa processer och varierande

tillämpning. Det behövs därför gemensamma bedömningsmetoder, tydliga tidsfrister och tillräcklig kompetens och förmåga hos de nationella myndigheterna.

Tillämpningsområde, harmonisering och dubbelreglering

Föreningen noterar också att nationella certifieringsbeslut kan leda till olika tillämpning mellan medlemsstater och därmed underminera förtroendet för systemet.

Tillämpningsområdet behöver förtydligas för molnbaserade produkter, privata kommunikationsnät och lösningar där molntjänster, lokal beräkning, edge-funktioner och operativa system samverkar. Det bör framgå vilken tjänst och vilket leverantörsled som omfattas av respektive krav, så att kraven inte oavsiktligt utsträcks till hela system eller .

Otydlighet skapar bristande förutsebarhet för teknikföretag som erbjuder exempelvis uppkopplade produkter och samhällskritiska tjänster. Företagen får svårt att avgöra vilka delar av erbjudandet som omfattas, vilka krav som gäller och hur efterlevnaden ska visas. Det kan leda till olika nationella tolkningar, dubbla eller överlappande krav, högre dokumentations- och anpassningskostnader samt att produkter som i grunden inte är molntjänster ändå dras in i regelverket. Definitionen behöver därför knytas till tydligt angivna tjänstekategorier och användningsfall samt avgränsas utifrån faktisk funktion, kritikalitet och risk.

En leverantör som bygger sin tjänst på en redan bedömd infrastrukturtjänst bör kunna återanvända relevant och aktuell granskningsbevisning. Ansvarsfördelningen mellan infrastruktur-, plattforms- och programvaruleverantörer måste samtidigt vara tydlig. Återanvändningen bör avse de kontroller som den underliggande bedömningen täcker, medan integrationen och den samlade tjänstens risker behöver bedömas särskilt.

SOFF vill även understryka vikten av att undvika dubbelreglering som kan medföra parallella riskbedömningar samt separata certifieringar, revisioner och uppföljningar. Kraven i förordningen bör samordnas med befintliga ramverk — särskilt NIS2-direktivet, CER-direktivet och det kommande europeiska certifieringsschemat för molntjänster (EUCS). Certifikat och revisioner bör dessutom kunna åberopas som bevis på efterlevnad av krav på informations- och cybersäkerhet även i andra regelverk, såsom NIS2 och Cyberresiliensakten (CRA).

Säkerhet, sekretess och förtroende

Erkännandeförfarandet kan innebära att en leverantörs underliggande tekniska bevisning cirkuleras till ansvarig myndighet i alla medlemsstater som i sin tur kan ha olika säkerhetsnivåer och sekretessregler. Det skapar en riskexponering som ramverket är avsett att förhindra. SOFF anser att hanteringen av säkerhetskänslig teknisk dokumentation och företagshemligheter i förförande förslaget måste omgärdas av tydliga och enhetliga sekretesskrav och att spridningen av sådan information bör begränsas till vad som är nödvändigt i det enskilda fallet.

Kostnad och ersättning

Det bör tydliggöras hur rätten till ersättning enligt artikel 24.3 ska tillämpas när privata aktörer använder erkända tjänster. Att klargöra denna punkt är avgörande för att certifieringsramverket ska bli fullt användbart för den privata sektorn. SOFF noterar också att företag åläggs att, på egen bekostnad svara för både tredjepartsrevision enligt artikel 20 och cybersäkerhetscertifiering enligt bilaga II, vilket medför ökade kostnader för företagen till nackdel för konkurrenskraften.

Cybersäkerhetscertifiering enligt EUCS

I bilaga II artikel 2.1 (e), 3.1 (e) och 4.1 (e) anges att för att en molntjänst ska erkännas på säkerhetsnivå 2 – 4 så ska molntjänsten erhålla ett cybersäkerhetscertifikat. SOFF understryker att övergångsbestämmelserna behöver ge företagen tillräcklig tid att anpassa verksamheten och genomföra certifiering efter att EUCS:s slutliga krav har fastställts och certifiering finns tillgänglig i praktiken. Detta är viktigt för att säkerställa tillgången till certifierade molntjänster för svenska säkerhets- och försvarsföretag samt deras kunder inom totalförsvaret.

Kriterier för att erkännas som leverantör av tjänster på säkerhetsnivå 1 – 4

SOFF välkomnar etableringen av ett ramverk för unionens molntjänstsuveränitet i bilaga II till förordningen. Det finns ett behov av ett enhetligt ramverk för hela EU för att bedöma molntjänsters suveränitetsegenskaper, för att undvika divergerande system.

Bilaga II fastställer kriterier som leverantörer av molntjänster måste uppfylla för att erkännas som leverantör på unionens olika säkerhetsnivåer. Den är till stor del inriktad på egenskaper hos leverantörer (exempelvis var data lagras, var personal finns m.m.). Även om de faktorerna är viktiga, utgör de i sig ingen garanti för att verksamheten kommer att fortsätta fungera om en störning inträffar. Andra faktorer som kan inverka på förmågan att upprätthålla funktion relaterar till kartläggning av andra beroenden än sådana kopplade till suveränitet (jfr nedan), möjlighet till återställning eller alternativa sätt för drift.

Följande frågor behöver dock förtydligas eller utvecklas:

- Enligt förslaget ska bilaga II, där kriterierna för säkerhetsnivåer fastställs, ses över minst var 18:e månad och kan ändras av Europeiska kommissionen genom delegerade akter. SOFF ser behov av regelbunden översyn av kriterierna. Förändringar bör föregås av samråd med näringslivet och en konsekvensbedömning samt förenas med proportionerliga övergångsregler. Företagens behov av förutsägbarhet bör vägas mot behovet att skyndsamt hantera nya säkerhetsrisker.
- Det bör tydliggöras hur kraven tillämpas på integrerade AI-funktioner, externa modeller och tilläggstjänster, inklusive deras dataflöden, uppdateringar och underleverantörer. Bedömningen bör omfatta kontrollen över tjänstens drift och



SOFF

Säkerhets- och
försvarsföretagen

dataanvändning samt kontinuiteten. Förordningens krav på migrationsplanering bör kompletteras med tydliga krav på kundens praktiska möjlighet att fortsätta verksamheten vid ägarförändringar, ändrade licensvillkor eller indragen tjänsteleverans. Det bör framgå hur nödvändiga data, konfigurationer, dokumentation och nyttjanderättigheter kan göras tillgängliga för fortsatt drift eller leverantörsbyte. Kraven bör samordnas med dataförordningens regler om byte av databehandlingstjänst.

- Kraven på datalokalisering bör tillämpas utifrån informationens skyddsvärde, hur kritisk tjänsten är samt relevant rättslig risk. SOFF noterar också att en lagrad datakopia inom EU sällan ensamt kan betraktas som tillräcklig för kontinuitet. Kontinuitet kräver också att det finns möjlighet att återuppta tjänsten och använda informationen.

Riskbedömningen i artikel 29

Riskbedömningen enligt den föreslagna artikel 29 lyfter vissa beroenden, men adresserar inte fullt ut verksamhetens beroenden.

SOFF anser att riskbedömningen bör tydligare beakta hur identifierade beroenden påverkar förmågan att upprätthålla kritiska funktioner. Den bör omfatta beroenden till kommunikation, elförsörjning, identitets- och behörighetssystem, programvara, licenser, uppdateringar, underleverantörer och kompetens. Även gemensamma beroenden bakom till synes oberoende leverantörer bör identifieras. Relevanta resultat från riskbedömningar enligt andra tillämpliga regelverk bör återanvändas. Metodiken bör tydliggöra hur dessa resultat påverkar valet av nivå och bedömningen av tjänsteavbrott, så att parallella bedömningar av samma risker undviks.

För kritiska funktioner bör verksamheten fastställa acceptabel avbrotts tid och dataförlust samt verifiera återställning och alternativa driftsätt genom återkommande tester. Bedömningen bör omfatta scenarier med långvariga leveransavbrott, exportrestriktioner, bortfall av tekniskt stöd och förändrade geopolitiska förutsättningar. Kraven bör anpassas till funktionens betydelse och konsekvenserna av bortfall.

SOFF understryker att förekomsten av ett beroende inte i sig innebär att risken är oacceptabel. Bedömningen bör utgå från beroendets kritiska nivå, sannolikheten för störning, möjliga konsekvenser och vilka riskreducerande åtgärder som finns. För samhällsbärande funktioner bör ett beroende inte accepteras om en extern aktör kan avbryta tjänsten och verksamheten saknar verifierad förmåga att upprätthålla funktionen inom fastställda avbrottsgränser.

Hårdvara ligger utanför kriteriernas tillämpningsområde i bilaga II och III, men kan utgöra ett kritiskt beroende för tjänstens funktion. Riskbedömningen bör därför omfatta relevanta hårdvaruberoenden, inklusive tillgång till reservdelar, underhåll och uppdateringar, med proportionerliga krav på kontroll och alternativa försörjningsvägar. Bedömningen bör

inriktas på försörjningsrisker under tjänstens livslängd och inte innebära ett generellt krav på europeiskt ursprung.

Föreningen noterar att Europeiska kommissionen ges vissa långtgående rättigheter som bör utredas närmre ur ett säkerhets- och försvarsperspektiv. Till exempel ger artikel 29.5 kommissionen möjlighet att anta implementeringsakter om den anser att en medlemsstats bedömning av säkerhetsnivå är felaktig. Ett annat exempel är att artikel 29.8 ger kommissionen en långtgående rätt att begära information från leverantörer och att skyddet för företagshemligheter och säkerhetskänsliga uppgifter vid sådana informationskrav behöver förtydligas. Utifrån ett säkerhets- och försvarsperspektiv framhåller SOFF vikten av att förordningen säkerställer nödvändigt nationellt handlingsutrymme. Det bör klargöras hur kommissionens befogenheter enligt artiklarna 29.3 och 29.5 förhåller sig till medlemsstaternas ansvar för nationell säkerhet och deras militära operativa behov.

Enligt artikel 29.6 ska en medlemsstat, om riskbedömningen kräver en övergång till en annan molntjänst, genomföra övergången inom tolv månader. Kravet gäller oberoende av om övergången föranletts av medlemsstatens egen bedömning eller av en bedömning som kommissionen ålägger enligt artikel 29.5. SOFF noterar att tidsperioden kan vara utmanande för komplexa säkerhetskritiska system och det bör införas en möjlighet till motiverad förlängning.

Konsekvensbedömning av privata aktörer

SOFF ser positivt på att privata aktörer kan använda en gemensam metodik för att bedöma beroenden och risker. Kraven bör vara riskbaserade och proportionerliga samt samordnas med bland annat NIS2, CER och sektorsspecifik lagstiftning, så att dubbelreglering undviks.

SOFF vill särskilt uppmärksamma att kommissionen enligt artikel 31 kan utvidga obligatoriska krav till privata aktörer i samhällsviktiga sektorer (t.ex. energi, hälsa, telekom och finans) genom delegerade akter. En sådan utvidgning berör breda delar av SOFF:s medlemskrets och bör föregås av en fullständig konsekvensbedömning och samråd med berörda branscher, samt vara riskbaserad och proportionerlig.

Digital suveränitet och motståndskraft

Inriktande principer för suveränitet och motståndskraft

SOFF stöder ambitionen att stärka Europas förmåga inom molntjänster och AI samt minska kritiska och svårersättliga beroenden. Konkurrenskraftiga europeiska alternativ – däribland svenska lösningar – kan bidra till större valfrihet, försörjningstrygghet och långsiktig handlingsfrihet. Offentlig efterfrågan bör ge sådana lösningar möjlighet att prövas, införas och växa utifrån tydliga verksamhetsbehov och verifierbara krav.

Kravställningen bör samtidigt vara teknikneutral och proportionerlig. Den bör öppna marknaden för fler konkurrenskraftiga leverantörer och minska befintlig inlåsning. Samtidigt bör kundernas möjligheter att kombinera och byta tjänster stärkas när europeiska

alternativ växer. Europeisk förmågeutveckling och tillgång till teknik och samarbete med allierade behöver därför utvecklas tillsammans. Förordningen bör säkerställa att Sverige och övriga medlemsstater kan upprätthålla interoperabilitet enligt överenskomna Nato-standarder, genomföra säkert informationsutbyte och fullgöra sina åtaganden inom Nato med hänsyn till de operativa behov som följer av alliansens kollektiva försvar.

Kravställningen bör tillgodose operativa behov både i dag och på längre sikt, samtidigt som kritiska sårbarheter minskas. Samarbete och ömsesidiga beroenden inom EU och Nato kan stärka försörjningsförmågan och tillgången till avancerad teknik. Även beroenden inom denna krets behöver dock bedömas utifrån koncentration, alternativa försörjningsvägar och risken för ändrade nationella prioriteringar eller restriktioner. För vissa särskilt kritiska funktioner kan Sverige behöva säkerställa tillgång inom landet till driftförmåga, kompetens, underhåll och återställning under en dimensionerande störning. Omfattningen bör följa av totalförsvarets behov och tydliga krav på uthållighet.

Ägande, jurisdiktion och avgörande inflytande över leverantören är relevanta faktorer att beakta i en riskbedömning, men måste bedömas tillsammans med andra faktorer som exempelvis cybersäkerhet, kontinuitet och möjligheten att byta leverantör. Tekniska, organisatoriska och avtalsmässiga skyddsåtgärder bör tillgodoräknas i den utsträckning i den utsträckning som det kan verifieras att de minskar de identifierade riskerna. Kryptering och kundkontrollerade nycklar bör tillgodoräknas för den verifierade minskningen av risken för obehörig åtkomst. Risker för indragna licenser eller avbruten tjänsteleverans behöver hanteras med kompletterande åtgärder.

För särskilt kritiska funktioner kan därför mer långtgående krav på rättslig och operativ kontroll vara motiverade. Sådana krav bör knytas till identifierade risker och det skydd som behöver uppnås.

Suveränitetsskalan i förslaget antyder att en högre nivå alltid är säkrare och mer tillförlitlig än en lägre nivå. Samtidigt anger de ingående kriterierna för varje nivå olika riskdimensioner (t.ex. datalokalisering, jurisdiktion, teknisk säkerhet m.m.). En sammanvägd nivå kan dölja information om att en lösning är stark i en dimension men svag i en annan, vilket kan leda till felaktiga upphandlingsbeslut.

Sammanfattningsvis förespråkar SOFF en balanserad kravställning som kombinerar ett starkt engagemang för europeisk molnkapacitet över tid med bibehållen flexibilitet i teknik- och leverantörsväl utifrån verksamhetens skyddsbehov – för att tillgodose Europas försvars- och säkerhetsbehov samtidigt som den europeiska kapaciteten fortsätter att utvecklas. Kravställningen bör beakta både kortsiktiga och långsiktiga perspektiv. SOFF anser att digital suveränitet bör förstås som förmågan att upprätthålla handlingsfrihet, kontrollera kritiska beroenden och säkerställa kontinuitet även vid störningar eller förändrade geopolitiska förutsättningar. Detta förutsätter inte nationell eller europeisk självtillräcklighet. Beroenden kan hanteras genom en kombination av europeiska och allierade försörjningskedjor, diversifiering, öppna gränssnitt, portabla data, modulära arkitekturer samt tekniska, rättsliga och avtalsmässiga kontrollmekanismer. Vilka

beroenden som kan accepteras måste avgöras utifrån användningsfallets skyddsbehov och möjligheten att upprätthålla funktionen vid avbrott.

Kommentarer avseende vissa artiklar

Det bör tydliggöras att krav enligt artiklarna 29 och 30 ska knytas till identifierade aktiviteter och användningsfall. Försvarsanknytning bör inte ensamt medföra att samtliga tjänster hos en myndighet hänförs till högsta tillitsnivån. Administrativa och operativa tjänster kan ha olika skyddsbehov, samtidigt som beroenden mellan dem måste beaktas.

SOFF konstaterar till exempel att artikel 30.3 innebär att de försvarsaktiviteter som identifierats enligt artikel 29.1 enbart kan upphandla tjänster som möter säkerhetsnivå 2 – 4. SOFF noterar därutöver att kombinationen av artikel 30.3 och metodiken i artikel 29.3 — som styr de mest kritiska verksamheterna, uttryckligen inbegripet försvar, mot den högsta säkerhetsnivån — i praktiken riskerar att göra nivå 4 till förvald utgångspunkt för försvarsarbetslaster.

Förslaget anger inte att all försvarsrelaterad användning av molntjänster ska omfattas av den högsta suveränitetsnivån, nivå 4. Samtidigt saknas en tydlig definition av vilka försvarsaktiviteter som ska betraktas som kritiska. För att skapa förutsebarhet för både myndigheter och företag behöver den kommande metodiken tydligare avgränsa vilka typer av verksamheter som omfattas av nivå 4 och vilka som kan hanteras på nivå 2 eller 3.

Om begreppet försvarsverksamhet ges en alltför bred tolkning kan konsekvensen bli att mycket stora delar av den civila verksamhet som bedrivs av försvarsmyndigheter och försvarsföretag indirekt omfattas av nivå 4. Det skulle riskera att begränsa tillgången till kommersiellt tillgängliga digitala tjänster, minska interoperabiliteten med internationella partners och öka kostnaderna för såväl myndigheter som leverantörer. En mer tydlig definition av vilka försvarsrelaterade aktiviteter som ska betraktas som kritiska är därför viktig för att säkerställa att kraven blir proportionerliga och riskbaserade.

Om nivå 4 tillämpas brett på, eller blir förvald utgångspunkt, för all försvarsverksamhet behöver konsekvenserna för tillgången till lämpliga tjänster, redundans och allierad interoperabilitet analyseras för berörda användningsfall. Analysen bör samtidigt belysa riskerna med leverantörskoncentration och kritiska beroenden samt möjligheterna att utveckla konkurrenskraftig europeisk förmåga.

Tilldelningskriterierna som åsyftas i artikel 32 måste vara transparenta, proportionerliga och möjliga att verifiera. De bör bedöma det faktiska bidraget till europeisk kompetens, forskning, innovation, försörjningstrygghet och industriell kapacitet, inte enbart leverantörens ägande eller säte. Föreningen understryker också vikten av att företag oberoende av storlek ska kunna tillgodoräkna sig utveckling och investeringar som sker inom Europa.



SOFF
Säkerhets- och
försvarsföretagen

Datacenter och totalförsvarets behov

Vid utbyggnaden av datacenterförmågor bör totalförsvarets behov av fysisk motståndskraft, geografisk redundans, robust elförsörjning och alternativa kommunikationsvägar beaktas. Lokalisering och koncentration bör bedömas utifrån risken för gemensamma bortfall. Kraven bör vara funktionsbaserade och ge utrymme för olika tekniska lösningar. Möjligheter till värmeåtervinning och samspel med energisystemet bör tillvaratas där de är ändamålsenliga och förenliga med verksamhetens kontinuitetskrav. Planeringen bör även beakta relevanta folkrättsliga hänsyn, exempelvis distinktionsprincipen och proportionalitetsprincipen i den internationella humanitära rätten. Behovet av separation mellan civila och militära funktioner bör särskilt bedömas utifrån den militära och civila verksamhetens skyddsbehov och riskerna för civila funktioner i varje enskilt fall.

Öppna standarder och källkod

SOFF välkomnar att förslaget främjar öppna standarder, interoperabilitet samt delning och återanvändning av programvara.

Öppna och internationellt vedertagna standarder, dokumenterade gränssnitt, portabla data och modulära arkitekturer stärker konkurrensen, underlättar leverantörsbyten och minskar risken för inlåsning.

Öppen källkod kan vidare bidra till transparens och långsiktig handlingsfrihet, men bör inte betraktas som ett mål i sig eller som en garanti för säkerhet. Valet mellan öppen och proprietär programvara bör grundas på verksamhetens behov och en bedömning av säkerhet, försörjningskedja, förvaltning, licensvillkor, totalkostnad och nödvändiga immateriella rättigheter.

För säkerhetskänslig verksamhet måste källkod, företagshemligheter och teknisk information kunna skyddas. Krav på öppenhet och återanvändning bör därför vara proportionerliga och inte innebära att leverantörers skyddsvärda information eller immateriella rättigheter behöver offentliggöras.

Yttrandet har beretts av föreningens medlemsgrupper för Digitalt försvar och Cyberförsvar.

Stockholm den 2 oktober 2026.

För föreningen,

Robert Limmergård