Totalförsvarets forskningsinstitut

Datum
2026-10-15

Diarienummer
FOI-2026-1811

Klimat- och näringslivsdepartementet

Er referens
KN2026/01835

Vår handläggare
Karin Nygren

Remissvar gällande *Europeiska kommissionens förslag till en förordning om innovation*

Sammanfattning av FOI:s synpunkter

Den korta remisstiden har inneburit begränsad möjlighet att på djupet analysera konsekvenserna av Europeiska kommissionens förslag till en förordning om innovation. Givet det och utifrån de utgångspunkter myndigheten har att beakta har Totalförsvarets forskningsinstitut (FOI) följande synpunkter.

FOI välkomnar ambitionen att stärka innovationsförmågan inom Unionen. Myndigheten instämmer i behovet av att öka förmågan att utveckla och kommersialisera innovativa lösningar. Det gäller även för försvar och säkerhet.

FOI menar att de huvudsakliga problem som förordningen identifierar är reella men att de föreslagna lösningarna riskerar att bli kontraproduktiva. De riskerar att skapa en omfattande byråkrati, utmaningar ur flera säkerhetsperspektiv samt försvåra tillgången till unik och verksamsamhetskritisk spetskompetens.

Även om köp av varor och tjänster mellan myndigheter under regeringen inte omfattas av ramverket, ser FOI att förslagen kan försvåra för andra staters myndigheter samt för EU- och Natoinstitutioner att lägga uppdrag på FOI. Förslaget till förordning försvårar även möjligheterna för FOI och andra myndigheter att lägga uppdrag avseende forskning och utveckling som inte faller under lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS). Detta eftersom forskningsundantaget i nuvarande lagstiftning tas bort. Forskning och utveckling kan inte jämföras med varor och tjänster som upphandlas. FOI avråder därför från det nya förslaget.

FOI
164 90 STOCKHOLM
08-55 50 30 00
Orgnr: 202100-5182
registrator@foi.se
www.foi.se

FOI:s synpunkter

FOI anser att de två huvudsakliga problem som förordningen identifierar är reella. Det är svårt att få privat finansiering av högriskprojekt i tidiga skeden och det är svårt för företag att skala upp på grund av finansiella, regulatoriska och marknadsmässiga begränsningar.

FOI menar dock att de lösningar som presenteras, ett ramverk för upphandling av forskning och utveckling, ett gemensamt ramverk för värdering av immateriella tillgångar, ett EUIPO-kompetenscentrum för IP-baserad finansiering samt en EU-omfattande digital plattform, riskerar att bli kontraproduktiva. Detta genom att introducera en omfattande byråkratisk process, även i fall där det endast är en eller ett fåtal leverantörer som kan komma i fråga av kompetens- eller säkerhetsskäl. Detta gäller inte minst i områden som gränsar till försvar och säkerhet, men inte strikt träffas av undantagen i 2009/81/EC. Parallellt med värdet av att stärka innovationsförmågan inom EU genom att stimulera marknad och samarbeten för innovation på ett unionsövergripande plan utgör undantagsregler för FoU en viktig möjlighet för enskilda upphandlande myndigheter – särskilt inom sektorn för försvar och säkerhet – att säkra unik och verksamhetskritisk spetskompetens.

Forskning och utveckling skapar möjligheter att blicka in i framtiden och finna lösningar på problem och svar på frågor som ännu ej är kända. Det innebär att upphandling inom FoU i väsentligt högre grad än inom andra områden medför utmaningar vid kravställning, liksom vid utvärdering av anbud. Sådan upphandling skulle dessutom ställa särskilda krav på specialistkompetens hos en beställare inom det aktuella området, vilka kan vara utmanande att efterleva.

FOI menar att förslaget i denna mening snarare kan låsa än gynna en effektiv innovation.

Från svensk sida är det viktigt att understryka att köp av varor och tjänster *mellan* myndigheter under regeringen inte omfattas av det upphandlingsrättsliga regelverket och därmed inte av förslaget till förordning (se högsta förvaltningsdomstolens avgörande HFD 2021 Ref 35). Detta innebär att svenska myndigheter under regeringen kan lägga uppdrag på varandra avseende forskning och utveckling. För FOI som uppdragsfinansierad myndighet är detta avgörande, då många av de uppdrag som myndigheten utför inte självklart skulle falla under undantagen för försvar och säkerhet (2009/81/EC) och inte heller undanta teknik med dubbla användningsområden eller civil innovation med tillämpningar inom försvar, säkerhet eller resiliens.

FOI konstaterar samtidigt att uppdrag till svenska myndigheter under regeringen från andra staters myndigheter, från kommuner och regioner samt från institutioner som EU och Nato däremot träffas av förslaget till förordning i den mån de inte omfattas av undantagen för försvarsrelaterad upphandling. Det kan påverka uppdrag till FOI.

Idag finns det undantag i upphandlingslagstiftningen som medger direktupphandling av tjänster avseende forskning och utveckling under förutsättning att; (1) resultaten tillfaller fler än den upphandlande myndigheten (2) tjänsten finansieras av fler än den upphandlande myndigheten. Dessa undantag försvinner i och med förslaget till förordning, vilket försvårar myndigheters upphandling av säkerhetskänslig forskning och utveckling som inte faller under LUFS. FOI avråder därför från förslaget.

Skydd av säkerhetskänslig FoU

Ur ett försvarsinnovations- och totalförsvarsperspektiv aktualiseras frågor om skydd av säkerhetskänslig FoU som inte undantas från förordningen. Målet att påskynda innovation, underlätta deltagande för startup- och scaleup-företag, främja gränsöverskridande samarbete och stödja kommersialisering av FoU-resultat behöver balanseras mot risker förknippade med strategiskt känslig teknik, såsom teknik med dubbla användningsområden. Riskerna omfattar bland annat teknik- och kunskapsläckage, utländskt ägande, förändring av ägarbilder, samt tillgång till strategiskt viktig teknik och produktionskapacitet under kris eller konflikt.

Säkerhet är därför ett viktigt ramvillkor för såväl FoU-upphandling som EUIPO:s ramverk för IP-värdering och kommersialisering. Nedan behandlas två områden där FOI identifierar behov av förbättringar.

Förtydliga ramvillkoren för identifiering och hantering av säkerhetsrisker vid FoU-upphandling

Förordningen innehåller redan flera säkerhetsbestämmelser som avser FoU-upphandling. Artikel 26 skyddar information som den ekonomiska aktören själv har klassat som konfidentiell, däribland tekniska hemligheter, företagshemligheter och konfidentiella delar av anbud. Artikel 28 reglerar skyddet av bland annat känsliga data, forskning och immateriella rättigheter mot obehörig åtkomst eller överföring genom hela upphandlingsprocessen, från planering av upphandlingen och marknadsdialog till fullgörandet av kontraktet. Artikel 29 ger möjlighet att säga upp avtal eller utesluta leverantörer vid bristande efterlevnad av säkerhetskrav eller vid risker för säkerhet och allmän säkerhet. Artikel 30 ger därutöver möjlighet att ställa särskilda cybersäkerhetskrav.

Bestämmelserna lägger det primära ansvaret på respektive upphandlande myndighet eller annan upphandlande aktör *att identifiera säkerhetskänslig FoU och* besluta om

lämpliga skyddsåtgärder. Artiklarna 26 och 28–30 anger flera riskfaktorer som upphandlande myndigheter får beakta som grund för skyddsåtgärder. Sådana bedömningar kan dock vara utmanande då de ofta kräver specialistkompetens och tillgång till information som inte är allmänt tillgänglig. Det gäller exempelvis bedömningar av tekniksäkerhetsrisker, utländskt ägande och inflytande, strategiska beroenden och långsiktiga konsekvenser av att kommersialisera teknik med dubbla användningsområden.

Man riskerar därmed att skapa sårbarheter, kvalitetsbrister liksom skillnader i tillämpningen. FOI bedömer därför att förordningen bör kompletteras med tydligare vägledning och institutionellt stöd för att möjliggöra en mer enhetlig tillämpning av säkerhetsbestämmelserna.

Följande åtgärder kan stärka förutsättningarna för att identifiera säkerhetskänslig FoU i ett tidigt skede och tillämpa proportionerliga skyddsåtgärder:

- *Institutionellt stöd och samverkan:* Rådets rekommendation om ökad forskningssäkerhet (C/2024/3510) kan utgöra en relevant utgångspunkt för hur upphandlande myndigheter kan stödjas vid tillämpningen av säkerhetsbestämmelserna. Den betonar behovet av stödfunktioner med sektorsövergripande kompetens, informationsutbyte mellan forskningsorganisationer och underrättelsemyndigheter samt stärkt samverkan mellan ansvariga myndigheter. Liknande stödstrukturer skulle kunna underlätta säkerhetsbedömningarna, om det kan etableras på effektiva sätt.

- *Tydligare vägledning för identifiering och riskbedömning:* Förordningen bör ge tydligare vägledning om när FoU-upphandling kan vara säkerhetskänslig, särskilt avseende kritisk teknik och teknik med dubbla användningsområden. Kommissionens rekommendation (EU) 2023/2113 kan utgöra en referenspunkt. Den identifierar tio kritiska teknikområden och prioriterar inledningsvis avancerade halvledare, artificiell intelligens, kvantteknik och bioteknik. Liknande metoder för riskbedömning skulle kunna stödja identifieringen av FoU-upphandlingar som kan kräva förstärkta skyddsåtgärder. Samtidigt bör säkerhetskänsligheten bedömas utifrån den specifika tekniken, dess tillämpning och de konkreta riskerna, snarare än enbart utifrån en fast lista över teknikområden.

- *Tydligare koppling mellan riskbedömning och skyddsåtgärder:* Förordningen bör tydligare ange vilka åtgärder som bör övervägas vid olika risknivåer när en upphandling har identifierats som säkerhetskänslig. Proportionerliga

minimikrav skulle exempelvis kunna avse granskning av ägande och kontroll, säkerhetsprövning av personal, cybersäkerhet, hantering av känslig information, säkerhet hos underleverantörer och i leveranskedjor. Det bör även framgå när upphandlande myndigheter bör samråda med eller hänskjuta ärenden till behöriga nationella myndigheter inom säkerhet och ekonomisk säkerhet.

- *Stärkt skydd av känslig teknisk information vid digital upphandling:* Artikel 26 innehåller särskilda bestämmelser om lokalisering, behandling och åtkomst av data, men dessa gäller endast personuppgifter. Även icke-personrelaterad teknisk information, såsom källkod, tekniska specifikationer, forskningsdata, testresultat och modeller, kan vara skyddsvärd. Förordningen bör därför förtydliga när särskilda krav på lagring, behandling, överföring och åtkomst är motiverade för teknisk information. Sådana krav kan vara särskilt relevanta när informationen rör prioriterade teknikområden eller medför förhöjd risk för teknik- eller kunskapsläckage.

Inför ett säkerhetsperspektiv i EUIPO:s ramverk för IP-värdering och kommersialisering

Ökad synlighet och överlåtbarhet för europeiska immateriella tillgångar förbättrar möjligheterna till värdering och finansiering. Samtidigt kan det medföra ökad exponering när tillgångarna avser strategiskt känslig teknik. Det gäller särskilt teknik som unionen identifierat som känslig eller prioriterad ur ett tekniksäkerhets- eller teknikläckageperspektiv, däribland viss teknik med dubbla användningsområden.

För sådana immateriella tillgångar bör proportionerliga skyddsåtgärder kunna övervägas inom EUIPO:s ramverk för värdering och kommersialisering. Beroende på risk kan åtgärderna exempelvis omfatta differentierad åtkomst till icke-offentlig information, kontroll av motparter och beaktande av relevanta exportkontrollkrav. För särskilt känslig information kan även krav på lämplig behörighet eller granskning av personer med tillgång till informationen vara motiverade. Sådana krav skulle exempelvis kunna övervägas inom ramen för certifieringen av IP-värderare enligt artikel 35, som i sin nuvarande utformning saknar uttryckliga säkerhetsrelaterade krav. Syftet bör inte vara att utesluta strategiskt viktiga immateriella tillgångar från EUIPO:s ramverk, utan att säkerställa att ökad synlighet förenas med proportionerliga skyddsåtgärder.

FOI
Totalförsvarets forskningsinstitut

Datum 2026-10-15

Beteckning FOI-2026-1811

Detta remissvar har beslutats av generaldirektör Jens Mattsson efter föredragning av innovationsdirektör Karin Nygren. I den slutliga handläggningen har även avdelningschef Malek Finn Khan, stabschef Niclas Karlsson, chefsjurist Eva Liljefors, forskningsdirektör Katarina Wilhelmsen, sektionschef Henrik Ekholm, forskare Eve-Michelle Basu och stabshandläggare Pär Eriksson deltagit.

Jens Mattsson *Karin Nygren*

Sändlista:
kn.registrator@regeringskansliet.se, kn.nim.remisser@regeringskansliet.se

För kännedom:
forsvarsdepartementet.registrator@regeringskansliet.se

Internt FOI:
Registrator
Överdirektör
ÖD-sekreterare
Stabschef
Chefsjurist
Avdelningschef Försvarsanalys