Regeringskansliet

2026-05-28
Fi2026/01233

Finansdepartementet

En molnpolicy för Sverige – för ökad säkerhet, effektivitet och innovation i den offentliga förvaltningen

1. Inledning

Syftet med denna policy för användning av molntjänster är att bidra till ökad säkerhet, effektivitet och innovation i den offentliga förvaltningen.

Aktörer inom den offentliga förvaltningen (offentliga aktörer) har behov av olika it-lösningar, inklusive olika molntjänster, för att säkerställa kostnadseffektivitet, hög säkerhet och tillgänglighet för sina respektive verksamheter. Aktörerna behöver vidare kunna välja mellan olika leverantörer och verktyg utifrån sin respektive verksamhets krav och behov. Varje aktör måste göra en självständig bedömning och är själv ansvarig för sin användning av molntjänster.

Användning av molntjänster kan möjliggöra innovation, medföra ökad effektivitet i verksamheten och öka motståndskraften (resiliensen) i den offentliga förvaltningen, samtidigt som det även kan medföra nya sårbarheter. Policyn kan bidra till arbetet för en kostnadseffektiv och säker it-drift, och även till en effektiv verksamhet i övrigt. Syftet med policyn knyter därmed an till dels den statliga förvaltningspolitikens mål om en innovativ och samverkande statsförvaltning, dels det i grunden förändrade säkerhetsläget. Det osäkra geopolitiska läget påverkar många olika områden, så även det digitala, och är något som Sverige behöver förhålla sig till och navigera på bästa sätt. Sverige är ett i hög grad digitaliserat land och digital teknik berör numera närmast varje del av det svenska samhället. Detta aktualiserar sammantaget kraven på att staten i alla lägen har tillgång till och rådighet över samhällsviktiga system, tjänster och funktioner.

Policyn kan användas som stöd av de offentliga aktörerna vid deras användning av molntjänster. Med den offentliga förvaltningen avses statliga myndigheter under regeringen samt kommuner och regioner. Regleringen av kommunernas och regionernas skyldigheter ska enligt regeringsformen som utgångspunkt beslutas av riksdagen. Med detta som utgångspunkt är syftet att denna policy även ska kunna användas som stöd av och vara till nytta för kommuner, regioner och privata aktörer som bedriver offentligt finansierad verksamhet.

Molntjänster

Med molntjänster avses digitala tjänster och resurser med fjärråtkomst, vanligen via internet. Policyn omfattar molntjänster i en vid bemärkelse, exempelvis infrastrukturtjänster för bl.a. lagring och nätverk och plattformstjänster för exempelvis utveckling av program (applikationer).

Det är viktigt att den offentliga förvaltningen nyttjar de möjligheter som digitaliseringen för med sig i syfte att utveckla och nå ökad effektivitet i dess verksamhet samt säkerställa god service och tjänster till samhället, medborgare och företag.

Framväxten av molntjänster har varit en viktig del i den digitalisering av samhället som skett under de senaste åren. Molntjänster har exempelvis kommit att få stor betydelse för utvecklingen och användningen av artificiell intelligens (AI). AI har stor potential att höja kvaliteten i myndigheters tjänster, minska mängden administration, förbättra välfärden och stärka Sveriges konkurrenskraft.

Molntjänster kan även underlätta digital integration och interoperabilitet, dvs. förmågan hos olika system och applikationer att utbyta information på ett effektivt och korrekt sätt. Molntjänster möjliggör skalbarhet, dvs. att dataresurserna kan justeras efter belastning utan att prestandan påverkas negativt, vilket skapar möjlighet att snabbt anpassa och utöka kapaciteten i befintliga system samt att bygga nya lösningar för att utveckla verksamheten.

Efter bedömning av bl.a. vilken rådighet som krävs kan molntjänster även användas för att säkra funktionalitet och data som hanteras av den offentliga förvaltningen. Molntjänster kan även användas för att utföra verksamhet i annan lokal eller på annan ort än det ordinarie verksamhetsstället. Detta kan vara mycket värdefullt i händelse av kris, höjd beredskap och ytterst krig, i

synnerhet för samhällsviktig verksamhet. Samtidigt är det viktigt att myndigheterna kan fortsätta att bedriva sin verksamhet även vid avbrott i en molntjänst.

Samtidigt som behovet och nyttan av molntjänster är stort finns osäkerhet kring hur de bör användas. I AI-kommissionens Färdplan för Sverige lyfts utmaningar inom detta område, och det föreslås att de offentliga aktörernas möjligheter att använda sig av molntjänster som erbjuds av företag utanför EU ska förtydligas (SOU 2025:12).

2. Molntjänster i den offentliga förvaltningen

2.1 Utgångspunkter

I dagsläget är det vanligt förekommande att statliga myndigheter kombinerar olika driftsformer på it-området. De kan ha en blandning av it-drift i egen regi, utkontraktering till privata leverantörer och samordnad it-drift med andra myndigheter. Användningen av molntjänster från privata tjänsteleverantörer är utbredd inom den offentliga förvaltningen, även om andelen av myndigheterna som använder molntjänster i privat regi har minskat över tid (Stärkta förutsättningar för att följa den statliga it-driften, Statskontoret 2025:15).

Användningen av digitala tjänster i Europa präglas av ett beroende av leverantörer med hemvist utanför EU. Detta beroende har strategiska konsekvenser för Europas konkurrenskraft, innovation och suveränitet. Amerikanska företag är marknadsledande inom molntjänster i EU. Detta medför utmaningar, såsom beroenden, risk för inlåsningseffekter och höga priser vid bristande konkurrens, men även behov av datasäkerhet och rådighet över data.

Sveriges och Europas digitala suveränitet behöver öka och regeringen har därför undertecknat deklarationen om digital suveränitet (Fi2025/02129). Därtill behöver Europas digitala konkurrenskraft och tekniska självbestämmande stärkas, och det bör ske på ett öppet sätt. Sverige ska kunna agera självständigt och i linje med europeiska värderingar, samtidigt som fördelarna med samarbete med globala partners tillvaratas.

Inom EU pågår även initiativ som syftar till att stärka den digitala suveräniteten, t.ex. Cloud and AI Development Act, som Europeiska

kommissionen avser att presentera under 2026. Detta initiativ ska bl.a. bidra till att medlemsländerna har tillgång till digitalt suveräna molntjänster för verksamheter med höga skyddsvärden. Regeringen avser vara en aktiv part i förhandlingarna av rättsakten. Regeringen välkomnar en ökad konkurrens inom detta område, samt att svenska och europeiska molntjänstföretag utvecklar tjänster för den svenska och europeiska marknaden, vilket främjar vårt oberoende och vår rådighet över tjänsterna.

Sveriges geopolitiska situation är allvarlig och kännetecknas av stor osäkerhet. Den snabba utvecklingen i omvärlden påverkar vår säkerhet. Som framgår av regeringens utrikesdeklaration den 18 februari 2026 måste Europa stärkas. Regeringen ser ett ökat behov av internationella samarbeten i skärningspunkten mellan teknik, innovation, handel och säkerhet. Det är viktigt att minska sårbarheterna som följer med ensidiga ekonomiska beroenden.

Att öka vår digitala suveränitet innebär inte att Sverige ska isolera sig från omvärlden. Utifrån den offentliga förvaltningens varierande förutsättningar och behov av olika typer av it-drift, inklusive molntjänster, och med ett riskbaserat angreppsätt, kommer den offentliga förvaltningen även i fortsättningen kunna använda marknadsledande produkter och tjänster också om de kommer från företag med hemvist utanför EU. När en offentlig aktör väljer lösning, driftsform och leverantör bör valet styras av de krav som gäller för den aktuella verksamheten avseende bl.a. funktion, säkerhet, rådighet, suveränitet, robusthet och kostnadseffektivitet.

2.2 Principer för användning av molntjänster i den offentliga förvaltningen

Det är viktigt att den offentliga förvaltningen har tillgång till och förutsättningar för att använda moderna, effektiva och säkra molntjänster som uppfyller rättsliga och säkerhetsmässiga krav. Regeringen bedömer att följande principer kan fungera som stöd för den offentliga förvaltningens användning av molntjänster.

2.2.1 Arbeta riskbaserat inför molnanvändning

Hotbilden mot Sverige är i det rådande säkerhetsläget bred och allvarlig. I den nationella säkerhetsstrategin konstaterar regeringen att fientliga aktörer, såväl statliga som icke-statliga, ständigt försöker utnyttja det svenska samhällets sårbarheter för att uppnå sina mål (skr. 2023/24:163). Beroenden

inom t.ex. teknik och infrastruktur för informations- och kommunikationsteknik kan medföra risker för den nationella säkerheten. Detta ställer höga krav på myndigheters cybersäkerhetsarbete, oavsett vilken tjänst, lösning eller driftsform som används.

I samband med upphandlingar är det viktigt att offentliga aktörer beaktar att företag i vissa länder enligt respektive lands regelverk under vissa förutsättningar måste lämna ut data till sina berörda nationella myndigheter, även om dessa data hanteras och lagras utanför dessa länder.

Det är mot denna bakgrund viktigt att de offentliga aktörerna, i enlighet med gällande regelverk, bedriver ett systematiskt informations- och cybersäkerhetsarbete som också inkluderar planering för att säkerställa kontinuitet även under ogynnsamma förhållanden. I detta sammanhang är det viktigt att den information som avses hanteras i en molntjänst är bedömd utifrån dess skyddsvärde och relevanta informationssäkerhetsperspektiv. Det är även angeläget att de lösningar som används är robusta, dvs. motståndskraftiga mot fel, störningar och förändringar.

Behandling av personuppgifter i amerikanska molntjänster

År 2022 ingick EU ett avtal med USA om ett ramverk för dataskydd (EU-U.S. Data Privacy Framework). Med anledning av avtalet antog Europeiska kommissionen 2023 ett s.k. adekvansbeslut som baseras på ramverket och som innebär att det är tillåtet att överföra personuppgifter till amerikanska verksamheter som har anslutit sig till ramverket. Beslutet förenklar överföring av personuppgifter till USA genom att detta, under vissa förutsättningar, kan ske utan att ytterligare skyddsåtgärder behöver vidtas.

Offentliga aktörer har höga krav på säker hantering av personuppgifter samt på informations- och cybersäkerhet. Det är därför viktigt att den offentliga förvaltningen har tillgång till och förutsättningar att använda moderna, effektiva och säkra molntjänster eller andra tjänster som uppfyller rättsliga och säkerhetsmässiga krav. De offentliga aktörerna behöver bl.a. avgöra i vilken utsträckning som tjänsterna innebär överföring av personuppgifter till länder utanför EU och säkerställa att sådan överföring sker i enlighet med de krav som följer av Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende

på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Vägledning

- Myndigheten för civilt försvar (MCF) har tagit fram ett metodstöd för systematiskt informationssäkerhetsarbete. På myndighetens webbplats finns mer information om detta.
- MCF erbjuder även cybersäkerhetsrådgivning och har tagit fram stöd för bl.a. kommuners cybersäkerhetsarbete. Ytterligare information finns på myndighetens webbplats. MCF:s verksamhet inom cybersäkerhet kommer att flyttas till Nationellt cybersäkerhetscenter (NCSC), som är en del av Försvarets radioanstalt (FRA), den 1 juli 2026.
- Säkerhetspolisen har tagit fram ett stöd om informationssäkerhet som bl.a. ger vägledning om klassificering av säkerhetsskyddsklassificerade uppgifter och om skyldigheter vid exponering av säkerhetskänslig verksamhet. På myndighetens webbplats finns mer information om detta.
- Integritetsskyddsmyndigheten tillhandahåller information om vilka länder som kommissionen bedömer har en adekvat skyddsnivå, och som personuppgifter kan överföras till utan särskilt tillstånd. Mer information finns tillgänglig på myndighetens webbplats.

2.2.2 Välj effektiva molnlösningar

Det finns flera fördelar med att använda molntjänster framför lokala it-lösningar, bl.a. skalfördelar och möjlighet att nå högre effektivitet genom att snabbare kunna utveckla och lansera tjänster till medborgarna. Vidare kan molnbaserade lösningar ofta ha en högre nivå av säkerhet. Molnbaserade och standardiserade lösningar kan därför många gånger vara att föredra framför lokala it-lösningar. Nya applikationer och tjänster kan utvecklas och distribueras med hjälp av molntjänster och befintliga system migreras dit när detta bedöms vara lämpligt.

Vägledning

- Vid behov kan offentliga aktörer få stöd av nationella inköpscentraler vid upphandling av produkter och tjänster på it-området, inklusive upphandling av molntjänster. Statens inköpscentral är inköpscentral för statliga myndigheter, men även kommuner och regioner får avropa från dess ramavtal på it-området. Adda AB är inköpscentral för Sveriges Kommuner och Regioners medlemmar.

- Statliga myndigheter kan få stöd vid val av it-driftslösning. Regeringen har utsett Försäkringskassan till samordnande myndighet och leverantörsmyndighet enligt förordningen (2024:1005) om samordnad statlig it-drift. Försäkringskassan ska tillsammans med de övriga leverantörsmyndigheterna Lantmäteriet, Skatteverket och Trafikverket tillhandahålla it-driftstjänster, t.ex. molntjänster, inom ramen för det samordnade statliga tjänsteutbudet och stödja myndigheter vid valet av it-driftslösning.

2.2.3 Öka verksamhetsnyttan

En molntjänst kan tillhandahållas på flera olika sätt. Vissa verksamheter kan ha större behov att göra egna anpassningar, medan det för andra kan vara viktigare att snabbt börja använda tjänsterna. Inom den offentliga förvaltningen kan därför olika typer av molnlösningar behöva användas för att effektivt och säkert uppnå goda resultat och därmed öka verksamhetsnyttan.

Vägledning

- Myndigheten för digital förvaltning (Digg) har tagit fram ett metodstöd för arbete med dataskyddsfrågor som kan användas i arbetet med digitalisering och digital verksamhetsutveckling. Mer information finns på Diggs webbplats.
- Genom att delta i samarbeten, exempelvis Ena – Sveriges digitala infrastruktur, har offentliga aktörer möjlighet att utbyta erfarenheter i frågor om digital infrastruktur.

2.2.4 Främja portabilitet och en väl fungerande marknad

För regeringen är det viktigt att marknaden för molntjänster är dynamisk och välfungerande. Användning av molntjänster kan underlätta den offentliga förvaltningens hantering av data. Samtidigt kan det finnas risker som behöver hanteras om den offentliga aktören blir låst till en molntjänst och dess leverantör.

Det är mot denna bakgrund viktigt att offentliga aktörer säkerställer att det finns möjlighet att, vid behov, skyndsamt överföra data till och hantera system hos någon annan leverantör eller i egen regi. Regeringen välkomnar därför molntjänster med standarder och lösningar som främjar portabilitet, dvs. förmågan att t.ex. flytta data, funktioner eller tjänster från ett system till ett annat system, och minskar inlåsningseffekter.

I syfte att minska beroendet av en specifik molnlösning är det dessutom viktigt att de nya applikationerna inom den offentliga förvaltningen utvecklas på ett sådant sätt att både applikationer och data kan flyttas mellan t.ex. olika it-system. Det kan även finnas behov av att vid användning av s.k. proprietära tjänster, dvs. tjänster där användaren inte har fri tillgång till källkoden, ha en på förhand bestämd strategi för hur tjänsten kan bytas utom behov skulle uppstå. Det är även viktigt att avtal med molntjänstleverantörer innehåller villkor för utträde som möjliggör föraktören att vid behov t.ex. flytta applikationer och data till en annan leverantör eller att själv ta över hanteringen.

Det är viktigt att den offentliga förvaltningen har en god dialog med leverantörerna av molntjänster. Om myndigheter, kommuner och regioner tydligt kommunicerar sina behov till marknaden ökar förutsättningarna för marknaden att tillgodose dessa.

Vägledning

- Direktupphandling kan vara en möjlighet för små företag att kunna ingå större offentliga kontrakt. Den mest effektiva leverantören behöver inte vara den tidigare eller mest välkända leverantören. Det är därför värdefullt att försöka nå flera leverantörer och säkerställa att de är medvetna om den rådande konkurrensen. I färdplanen för de offentliga affärerna 2025–2030 (Fi2025/01827), som finns tillgänglig på regeringens webbplats, finns vägledning till upphandlande aktörer om hur de kan förbättra förutsättningarna för sina inköpsverksamheter.
- Det ska bli enklare för kunder att byta mellan olika molntjänstleverantörer, vilket stärker förutsättningarna för datadelning och interoperabilitet inom EU. Europaparlamentets och rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data och om ändring av förordning (EU) 2017/2394 och direktiv (EU) 2020/1828 (dataförordningen) är en del av EU:s strategi för att stärka dataekonomin i Europa genom gemensamma europeiska dataområden, och började tillämpas den 12 september 2025.

2.2.5 Upprätthåll relevant kontroll över data, drift och teknik

Det är viktigt att stärka Sveriges digitala suveränitet, minska strategiska beroenden och samtidigt stärka den offentliga förvaltningens möjlighet att välja olika typer av digitala lösningar.

Vid användning av molntjänster behöver både rådighet över bl.a. data och behovet av suveränitet beaktas, men i varierande grad beroende på t.ex. hur skyddsvärd datan är och vilken funktion som behövs. Offentliga aktörer behöver välja molnlösningar med lämplig nivå av kontroll över data, drift och teknik – samtidigt som aktören uppfyller krav på säkerhet och regelefterlevnad.

Den offentliga förvaltningens verksamheter är mångskiftande och aktörerna hanterar information med olika skyddsvärden. Det kan handla om uppgifter av känslig karaktär, t.ex. personuppgifter, sekretessbelagd information och säkerhetsskyddsklassificerade uppgifter. Att hantera sådan information i en molntjänst kräver bl.a. tillgång till dimensionerade säkerhetslösningar, dvs. säkerhetslösningar anpassade efter verksamhetens behov, risker och skyddsvärden. Vidare behöver de offentliga aktörerna enligt säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) i varje enskilt fall säkerställa att tillämpliga krav i fråga om säkerhetsskydd uppfylls.

I krissituationer – t.ex. vid allvarliga geopolitiska händelser eller cybersäkerhetsincidenter – är förmågan att upprätthålla samhällsviktig verksamhet och utöva effektiv kontroll genom att byta leverantör av avgörande betydelse.

Digital suveränitet handlar om att ha rådighet över data och system och tillse att någon utomstående part inte kan påverka, få tillgång till eller förneka tillgång till data eller nödvändig funktionalitet. Sådan suveränitet kan säkerställas med såväl tekniska som icke-tekniska åtgärder. De tekniska åtgärderna syftar ofta till att förhindra leverantören att få tillgång till informationen som lagras i molnlösningen genom t.ex. kryptering. Det kan även handla om åtgärder för att hindra att en användare kommer åt en annan användares data. Med icke-tekniska åtgärder avses ofta att molntjänsterna tillhandahålls från datacenter som är lokaliserade i EU, med personal som är EU-medborgare och uppfyller nödvändiga säkerhetskrav, samt faller under svensk eller EU:s jurisdiktion. Det förekommer även att leverantörer har huvudkontor i Sverige eller EU för att kunna vara digitalt suveräna i detta hänseende. Utkontraktering av it-drift till en europeisk leverantör kan dock också innebära avkall på nationell digital suveränitet, t.ex. om det i den aktuella staten finns regler som ger nationella myndigheter rätt till åtkomst till data.

I praktiken går det att betrakta digital suveränitet som en skala där högre krav på suveränitet bör gälla där riskerna är som störst, t.ex. för kritiska data och inom funktioner eller sektorer av stor betydelse, såsom samhällsviktig verksamhet.

Information med höga skyddsvärden och kritiska funktioner med höga krav på tillgänglighet, som behandlas i molntjänster, bör hanteras genom lösningar med hög rådighet.

Vägledning

- I 10 kap. 2 a § offentlighets- och sekretesslagen (2009:400) har en sekretessbrytande bestämmelse införts som möjliggör för myndigheter att lämna uppgifter som omfattas av sekretess till en enskild eller till en annan myndighet som har i uppdrag att tekniskt bearbeta eller tekniskt lagra uppgifterna för den uppgiftslämnande myndighetens räkning. Ändringen syftar till att skapa bättre förutsättningar för myndigheter att utkontraktera eller samordna sin it-drift, samt att stärka skyddet för de uppgifter som lämnas till en enskild vid utkontraktering av it-drift.
- Europeiska kommissionen har tagit fram ett ramverk för suveräna molnlösningar benämnt Cloud Sovereignty Framework. En upphandlande aktör kan genom ramverket få stöd att ställa relevanta frågor till leverantören av molntjänster, och därigenom säkerställa en relevant grad av digital suveränitet i den tjänst som väljs.

2.2.6 Säkerställ god kravställning på leverantörerna

Det är viktigt att offentliga aktörer fortsatt ställer tydliga krav på leverantörer av molntjänster, bl.a. för att få klarhet kring hur data hanteras, lagras, överförs och skyddas i hela leverantörskedjan.

Vägledning

- Regeringen har gett NCSC vid FRA i uppdrag (Fö2026/00737) att ta fram riktlinjer om bl.a. cybersäkerhetsrelaterade krav vid offentlig upphandling och cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster (informations- och kommunikationsteknik). Uppdraget ska redovisas senast den 11 december 2026.
- Regeringen gav 2025 MCF i uppdrag (Fö2025/00390) att ta fram en modell för uppföljning av digitala leveranskedjor, som ska komplettera den befintliga strukturen för uppföljning av det systematiska

informationssäkerhetsarbetet i den offentliga förvaltningen. Uppdraget har redovisats (Fö2026/00812).

3. Åtgärder för att främja användning av molntjänster

Regeringen har vidtagit flera åtgärder för att underlätta för den offentliga förvaltningen vid upphandling av molntjänster.

3.1 Forum för bättre genomförande av it-inköp

Det är viktigt att myndigheter och andra aktörer som tillhandahåller upphandlingsstöd har möjlighet att utbyta erfarenheter och genomföra samverkansinsatser i syfte att öka upphandlingsstödets genomslag och samstämmighet samt effektivisera resursutnyttjandet.

Vägledning

- Regeringen har gett Upphandlingsmyndigheten i uppdrag att genomföra insatser för att främja genomförandet av färdplanen för de offentliga affärerna 2025–2030. Inom ramen för uppdraget ska Upphandlingsmyndigheten inrätta ett forum som ska samordna upphandlingsstöd kopplat till inköpskategorin informationsteknik, och bidra till att främja måluppfyllelsen för de upphandlande myndigheterna och enheternas it-inköp.

3.2 Förstudie om inrättande av ett dynamiskt inköpssystem för innovativa digitala lösningar

Regeringen bedömer att den offentlig förvaltningens inköp av digitala tjänster behöver bli effektivare och mer tillgängliga för fler leverantörer. Det kan stärka konkurrensen, öka innovationen och minska beroendet av stora globala aktörer. För att stärka Sveriges digitala suveränitet behöver vidare fler tjänster köpas från svenska och europeiska leverantörer, samtidigt som trösklarna behöver sänkas så att små och medelstora företag lättare kan vinna offentliga kontrakt.

Vägledning

- Kammarkollegiet har getts i uppdrag (Fi2026/00311) att genomföra en förstudie om ett s.k. dynamiskt inköpssystem för innovativa digitala lösningar för den offentliga förvaltningen. Leverantörer kan ansluta sig till ett sådant system när som helst, så länge de uppfyller vissa krav. Leverantörerna kan sedan lämna anbud på alla förfrågningar inom de

produktkategorier som de är godkända för, utan att kvalificera sig på nytt. I förstudien ska Kammarkollegiet lämna förslag på åtgärder som gör det attraktivt för små och medelstora företag att delta i det aktuella systemet. Dessutom ska myndigheten analysera vilka typer av produkter som bör omfattas av ett sådant inköpssystem och vid urvalet prioritera produktkategorier där det finns många svenska och europeiska leverantörer.

3.3 Förslag om ändrade upphandlingsregler för att skydda Sverige från antagonistiska stater

Regeringen har tidigare bedömt att de svenska upphandlingslagarna bör ses över. Det nuvarande upphandlingsregelverket gör ingen uttrycklig skillnad mellan leverantörer från EU och leverantörer från tredjeländer som saknar frihandelsavtal med EU. Det innebär att alla leverantörer kan delta i upphandlingar och har rätt till likabehandling och domstolsprövning.

Den 25 november 2025 presenterades promemorian Tredjelands-leverantörers tillträde till upphandlingsförfaranden (Ds 2025:29). I promemorian föreslås att upphandlingslagarna ändras så att de inte gäller för tredjelandsleverantörer från stater som saknar frihandelsavtal med EU. Upphandlande myndigheter kommer därmed att få möjlighet att välja om dessa leverantörer ska tillåtas delta i upphandlingar och om deras anbud ska behandlas på samma sätt som anbud från leverantörer från Sverige eller EU. Den föreslagna regleringen innebär även att leverantörer från stater som saknar frihandelsavtal med EU inte längre kommer omfattas av de möjligheter till domstolsprövning som finns enligt upphandlingslagarna.

3.4 AI-verkstaden

Regeringen bedömer att AI har potential att förändra den offentliga förvaltningen i grunden och därigenom effektivisera processer, höja kvaliteten på tjänster till medborgarna, leda till effektivare användning av skattemedel och spara resurser. En AI-verkstad ska byggas upp över tid och erbjuda en förvaltningsgemensam infrastruktur med tillhörande stödfunktioner för att underlätta införandet av AI i den offentliga förvaltningen.

Vägledning

- Regeringen har gett Försäkringskassan och Skatteverket i uppdrag att i en första etapp etablera en AI-verkstad för den offentliga förvaltningen

(Fi2026/00018). Verkstaden bedöms kunna etableras i en s.k. hybridlösning, vilket innebär etablering av ett gemenskapsmoln med hög rådighet som kan interagera med privata aktörers infrastrukturer. Den ska utgöra en plattform som skapar förutsättningar för samverkan mellan den offentliga förvaltningen och den privata sektorn, stärker långsiktig styrning och kompetensutveckling samt främjar innovation och hållbar digital utveckling.