



Remissvar

Datum
2026-02-20

Ärendenummer
MSB 2025-15295-2

Ert datum
2025-11-11

Er referens
Fi2025/0169

Sektionen för tjänsteutveckling (CS-SK-TU)
Linnea Danielsson
010-240 4676
Linnea.Danielsson@mcf.se

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Betänkandet SOU 2025:101 Anpassningar till AI-förordningen – Säker användning, effektiv kontroll och stöd för innovation

Sammanfattning

Myndigheten för civilt försvar stödjer utredningens inriktning och betonar att AI-regleringen måste stärka både innovation och säkerhet genom tydliga regler, samordning och resurser. För att säkerställa detta belyser Myndigheten för civilt försvar följande:

- Bestämmelser kring sekretess och säkerhet är av vikt för att säkerställa att samarbete, informationsdelning och marknadskontroll kan ske säkert och effektivt.
- Myndigheten för civilt försvar förstår perspektivet att ansvaret för marknadskontroll av AI föreslås fördelas enligt det sakområde som berörs. Det är av stor vikt att respektive marknadskontrollmyndighet får tid och utrymme att bygga upp en AI-förmåga genom resurser, teknisk infrastruktur och specialiserad AI-kompetens, möjlighet att genomföra gemensamma samordning- och kompetensforum samt stärkt samverkan med näringsliv och högre utbildning.
- Säkra informationskanaler mellan marknadskontrollmyndigheterna och leverantörer av AI-system med hög risk är avgörande, där Swedish Government Secure Intranet (SGSI) kan utgöra en robust kanal för skyddsvärd kommunikation.
- En kompletterande AI-strategi, AI-verkstad och regulatorisk sandlåda för totalförsvaret kan säkerställa en robust digital försvarslinje, utan att begränsa den generella AI-utvecklingen inom offentlig förvaltning.

Datum
2026-02-20

Ärendenummer
MSB 2025-15295-2

Specifika synpunkter

Myndigheten för civilt försvar ställer sig positiv till utredningens förslag om behovet av kompletterande regelverk. Frågor om sekretess, säkerhet och transparens är särskilt viktiga för att säkerställa en säker, robust och innovativ nationell AI-utveckling. Dessa frågor påverkar möjligheterna till samarbete, informationsdelning och marknadskontroll, inte minst för AI-system med hög risk samt system som används inom totalförsvaret eller samhällsviktig verksamhet.

Myndigheten för civilt försvar förstår perspektivet att ansvaret för marknadskontroll av AI föreslås fördelas i enlighet med det sakområde som berörs. Respektive marknadskontrollmyndighet, däribland Myndigheten för civilt försvar, behöver dock ges utrymme och resurser för att kunna etablera förmåga och kompetens inom AI-området. Av detta skäl, och med anförda förutsättningar, har myndigheten inga synpunkter på förslaget om att vi tilldelas ansvar som marknadskontrollmyndighet för AI i gasanordningar, i den utsträckning som ansvaret inte tillfaller Elsäkerhetsmyndigheten.

För att säkerställa en enhetlig marknadskontroll finns ett stort behov av samordning och samverkan kopplat till AI-förordningen. Detta förutsätter nära samarbete med övriga marknadskontrollmyndigheter genom informationsutbyte och kompetenssamverkan. Här kan SGSI spela en viktig roll genom att en robust och säker kommunikationskanal för informationsutbyte mellan marknadskontrollmyndigheter, men även marknadskontroll av AI-system med hög risk samt användning av regulatoriska sandlådor.

Vidare betonar Myndigheten för civilt försvar att marknadskontrollmyndigheterna behöver tillräckliga resurser, teknisk infrastruktur och specialiserad AI-kompetens. Det kräver både kapacitet att bygga kompetens internt och resurser för samordning och kompetensutbyte med andra myndigheter.

Mot bakgrund av den stora efterfrågan på AI-kompetens nationellt och inom EU bör samarbeten mellan myndigheter, näringsliv och högre utbildning (universitet, högskolor och yrkeshögskolor) underlättas. Tydliga regelverk och strukturer för säker datadelning mellan både offentliga och privata aktörer kan stärka en bred och innovationskraftig AI-kompetens i Sverige. Genom statliga utbildningspremier per anställd som genomgår en AI-utbildning eller premier per student som utför praktik kan en nationell kompetensförsörjning inom AI säkerställas på sikt.

Regeringen beslutade den 20 november 2025 om uppdrag till Myndigheten för civilt försvar att förbereda cybersäkerhetsverksamheten vid myndigheten till

Datum
2026-02-20

Ärendenummer
MSB 2025-15295-2

Försvarets radioanstalt. Beslutet motsvarar de antaganden som låg till grund för myndighetens svar till utredningen. Dessa bedömningar är därför oförändrade.¹

Myndigheten för civilt försvar betonar även vikten av harmonisering av regelverk och hur de gemensamt påverkar samhällsviktig verksamhet och kritisk infrastruktur. Ett omfattande cyber- och informationssäkerhetsarbete är avgörande för att bygga ett robust och innovationsvänligt nationellt AI-ekosystem.

Vidare krävs tydliga strukturer för incidentrapportering och hantering av AI-relaterade händelser, inklusive kopplingar till befintliga rapporteringskrav enligt cybersäkerhetslagen. Säker kommunikation och gemensamma rutiner för hantering av skyddsvärd information är centrala för ett effektivt samarbete.

Myndigheten för civilt försvar anser att det system för rapportering bör harmoniseras mellan berörda parter.² Myndigheten bedömer dock att frågan om vem som bör ansvara för att ta fram och tillhandahålla ett sådant system inte är tillräckligt utrett.

Myndigheten för civilt försvar är mycket positiva till ett aktivt nationellt deltagande på EU-nivå. En tydlig och ändamålsenlig svensk representation i AI-styrelsen och dess under grupper är central för att säkerställa att svenska förhållanden beaktas i det fortlöpande tillämpningsarbetet.

Behov av fördjupad analys

Myndigheten för civilt försvar vill belysa totalförsvarets särskilda utmaningar gällande innovation och utveckling av AI-system för nationell säkerhet. Aktörer inom totalförsvaret har striktare krav på sekretess och informationssäkerhet, samtidigt som ett ökat behov av samarbete och informationsutbyte har växt fram inom totalförsvaret.

En gemensam AI-strategi för totalförsvaret inriktar och underlättar utvecklingen av gemensamma AI-förmågor mellan civila och militära aktörer på ett organiserat sätt. Då AI-förordningen inte tillämpas på AI-system för nationell säkerhet ger en separat AI-verkstad och regulatorisk sandlåda för totalförsvaret en robust och resilient digital försvarslinje, där aktörer inom totalförsvaret kan samarbeta och utveckla AI-system för att stärka Sveriges totalförsvar.

¹ Regeringen gav Försvarets radioanstalt samtidigt uppdrag att förbereda mottagandet av cybersäkerhetsverksamheten vid Myndigheten för civilt försvar.

² I ett motsvarande exempel relaterat till NIS2- och CER-direktiven tar Myndigheten för civilt försvar fram en gemensam incidentrapporteringsplattform med utgångspunkt i myndighetens samhällsviktiga kommunikationstjänst webbaserat informationssystem (WIS)

Datum
2026-02-20

Ärendenummer
MSB 2025-15295-2

Förslagen till gemensam AI-strategi, AI-verkstad och regulatorisk sandlåda för totalförsvaret ska ses som ett komplement till de AI-tjänster som kan gynna alla aktörer inom offentlig förvaltning. Att hantera detta särskilt bidrar till att understödja totalförsvaret behov utan att medföra en begränsning för den generella AI utvecklingen.³

Detta är nödvändigt då det i Försäkringskassans och Skatteverkets svar på regeringsuppdraget att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen framkommer att möjligheter för samskapande och delning av AI-lösningar inte kommer kunna tillgodoses initialt i AI-verkstaden för offentlig förvaltning.⁴

I detta ärende har överdirektör Anna Starbrink beslutat. Linnea Danielsson har varit föredragande. I den slutliga handläggningen har också avdelningschefen Åke Holmgren, enhetschefen Ronny Harpe och sektionschefen Per Deland deltagit.

Anna Starbrink

Linnea Danielsson

³ Se även myndighetens remissvar på SOU 2025:12 AI-kommissionens Färdplan för Sverige (MSB 2025-03664-3)

⁴ Försäkringskassan och Skatteverket (2026) Svar på regeringsuppdraget att utreda förutsättningarna för en AI-verkstad för den offentliga förvaltningen (Fi 2025/01523), FK 2025/016953, SKV 8-8583-2026.