Enheten för systematisk informationssäkerhet (CS-SI)
Callisto Utriainen
010-240 4153
callisto.utriainen@msb.se

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Remissvar SOU 2023:96 En reform för datadelning

Sammanfattning

Myndigheten för samhällsskydd och beredskap (MSB) lämnar följande synpunkter på betänkandet En reform för datadelning (SOU 2023:96):

MSB är positiva till förslaget att det ska föreskrivas om interoperabilitetslösningar.

Samtliga lösningar behöver uppfylla adekvata krav inom informationssäkerhet samt uppnå totalförsvarets krav.

Samma krav på informationssäkerhet bör gälla för samtliga nationella interoperabilitetslösningar, oaktat om de rekommenderas eller föreskrivs om.

MSB bedömer att NIS2-reglering och tillsyn enligt NIS2 kommer att påverka informationssäkerhetskraven på de flesta nationella interoperabilitetslösningar, men vill påtala vikten av att samtliga verksamhetsutövare som utvecklar, tillhandahåller eller använder nationella interoperabilitetslösningar omfattas av reglering och tillsyn.

MSB anser att kraven på samtliga nationella interoperabilitetslösningar bör utgå från erkända standarder och utvecklas med ”säkerhet som standard”.

MSB delar inte utredningens syn på att det idag skulle saknas interoperabilitetslösningar att nyttja vid kris och höjd beredskap då MSB tillhandahåller kommunikationstjänsterna WIS, SGSI och Rakel.

MSB anser att frågan om kontinuitet för samhällskritiska verksamheter som producerar eller konsumerar delad data bör analyseras vidare utifrån ett läge där tillgången till data stängs av.

Lagen (1992:1402) om undanförsel och förstöring samt Förordningen (2022:524) om statliga myndigheters beredskap bör beaktas i utvecklingen av informationssystem för offentlig förvaltning.

MSB är positiva till att medverka som expertmyndighet i arbetet med nationella interoperabilitetslösningar.

MSB:s roll och mandat som expertmyndighet i arbetet med nationella interoperabilitetslösningar behöver förtydligas och regleras.

För de verksamhetsutövare som utvecklar, tillhandahåller eller använder nationella interoperabilitetslösningar och som inte omfattas av annan reglering inom informationssäkerhet bedömer MSB att det är lämpligt att MSB ges föreskriftsrätt.

MSB delar utredningens syn på behovet av och är positiva till MSB ska utreda frågan om koordinerade skyddsnivåer och andra adekvata säkerhetsåtgärder som bör ligga till grund för kravställningen för nationella interoperabilitetslösningar.

MSB vill påtala vikten av att utredningen av adekvata säkerhetsåtgärder ska genomföras innan Digg börjar rekommendera eller föreskriva om nationella interoperabilitetslösningar.

MSB avstyrker förslaget om att andra myndigheter ska kunna rådfråga MSB om enskilda nationella interoperabilitetslösningars lämplighet utifrån informationssäkerhets- och säkerhetsskyddsperspektiv.

MSB föreslår istället för responsuppdrag att MSB ges en stark och tydlig roll i kravställnings- och utvecklingsfaserna för nationella interoperabilitetslösningar.

MSB delar inte utredningens bedömning om att uppdraget som expertmyndighet inom arbetet med nationella interoperabilitetslösningar skulle kunna utföras inom befintligt anslag på ett ändamålsenligt vis, utan föreslår särskilda anslag för arbetet.

Generella synpunkter

Med anledning av det säkerhetspolitiska läget är det angeläget att i alla lägen ta totalförsvarets krav i beaktande och säkerställa att det finns god redundans och kontinuitet inom samhällsviktiga verksamheter. Kommunikation och tillgång till information är avgörande för att säkerställa samhällets funktionalitet även i händelse av kris eller vid höjd beredskap. Samtliga nationella interoperabilitetslösningar måste leva upp till god informationssäkerhet och motsvara totalförsvarets krav.

Utredningen nämner att det finns risk att nödvändiga investeringar och förvaltning för att stödja den digitala effektiviseringen inte prioriteras av aktörerna, eftersom nyttan inte alltid realiseras hos den enskilde aktören. MSB håller med i det resonemanget och önskar att ansvarsfördelningen görs ännu tydligare, eftersom tydliga roller och mandat är en förutsättning för att kunna genomföra en effektiv och ansvarsfull digitalisering. Ansvaret behöver också kopplas till resurser för att utföra arbetet på ett ändamålsenligt och hållbart vis.

Om författningsförslagen

MSB är positiva till att det ska föreskrivas om nationella interoperabilitetslösningar. I *Förslag till förordning (202X:000) om den offentliga förvaltningens interoperabilitet* framgår att Myndigheten för digital förvaltning (Digg) ska höra berörda aktörer inför föreskrivning av en nationell interoperabilitetslösning. MSB anser att berörda parter bör höras inför kravställningen även för lösningar man avser att rekommendera, även om detta skulle innebära en längre handläggning. En myndighets rekommendation ses av många aktörer som en garanti för att lösningen håller god kvalitet och lever upp till relevanta lagar och

krav på säkerhetsåtgärder. Dessutom kan en rekommenderad lösning komma att föreskivas om i ett senare skede.

Vidare anser MSB att vår roll och vårt mandat som expertmyndighet i arbetet med nationella interoperabilitetslösningar bör förtydligas och regleras.

Om säkerhetsaspekter

Nationella interoperabilitetslösningar kommer att påverka många aktörer, såväl offentliga som privata, men också medborgare. Lösningar som påverkar stora delar av den offentliga förvaltningen utgör en attraktiv attackyta för antagonister. Dataanalys av innehåll i en omfattande infrastruktur ger många möjligheter att analysera individer eller organisationer. Genom att stora datamängder aggregeras och samlas kan en antagonist orsaka stor skada, både genom att få åtkomst till stora mängder information och genom att ett intrång eller avbrott kan leda till att stora delar av den offentliga sektorn påverkas samtidigt. Dessa lösningar måste därför vara robusta, redundanta och säkra samt leva upp till totalförsvarets krav. Infrastrukturen behöver utöver detta vara responsiv och skalbar för att möta upp mot både teknisk utveckling och en rörlig hotbild.

En förutsättning för säker datadelning är att det finns en samsyn kring skyddsnivåer och säkerhetsåtgärder för den data som ska delas i infrastrukturen. Att varje aktör enskilt ska komma överens om skyddsnivåer med alla andra i infrastrukturen och göra en egen analys är inte hållbart utan det krävs gemensamma lösningar.

En del av kravbilden samt tillsyn av efterlevnaden kommer sannolikt att regleras via NIS2-direktivet ((EU) 2022/2555). Förordningen ställer krav på riskarbete samt ändamålsenliga säkerhetsåtgärder för de verksamheter som omfattas. Till skillnad från MSB:s föreskrifter om informationssäkerhet och säkerhetsåtgärder för statliga myndigheter (MSBFS 2020:6 och MSBFS 2020:7) kommer NIS2-direktivet även att gälla kommuner, regioner och samhällsviktiga verksamheter. NIS2 kommer också att påverka kravställningen mot leverantörer och underleverantörer för dessa aktörer.

Informationssäkerhetskraven för utveckling, urval och förvaltning av nationella interoperabilitetslösningar bör utgå från erkända standarder. Cybersäkerhetsakten ((EU) 2019/881) pekar ut säkerhet som standard som inriktning för IKT-produkter. Det är inte minst av förtroendeskäl viktigt att lösningar som rekommenderas, utvecklas eller föreskrivs om av statliga myndigheter visar vägen med produkter som är säkra i sitt grundutförande.

Om krishanterings- och totalförsvarsperspektivet

På flera ställen i betänkandet anges att det saknas nationella interoperabilitetslösningar. MSB vill dock framhålla att det finns flera nationella lösningar som står offentlig sektor tillbuds, men att det saknas styrning av vilka lösningar som bör eller ska användas. MSB levererar och utvecklar idag de samhällsviktiga kommunikationstjänsterna Rakel, SGSI och WIS till aktörer inom totalförsvaret. I MSB:s uppdrag ingår det att förvalta, utveckla och tillhandahålla dessa system. Tjänsterna är anpassade utifrån totalförsvarets krav och vänder sig till samhällsviktiga aktörer. Rakel används idag av 752 aktörer, SGSI av 61 aktörer och WIS av 862 aktörer. Utöver förvaltningen av befintliga system arbetar MSB med att ta

fram nya robusta och säkra system som svarar upp mot framtidens behov och krav på samhällsviktiga kommunikationstjänster.

Utredningen föreslår att nationella interoperabilitetslösningar ska användas vid datadelning mellan myndigheter. Man nämner möjligheten att göra undantag med hänsyn till informationssäkerhet eller krav på skydd av Sveriges säkerhet. MSB önskar att frågan runt kontinuitet för samhällskritiska verksamheter som producerar eller konsumerar delad data bör analyseras på likande sätt – ur perspektivet att den producerande eller konsumerande aktören behöver (eller väljer att) stänga tillgången till öppet internet vid överbelastning eller annan störning för att fortsatt kunna fungera ostört. Enligt 13 § Förordningen (2022:524) om statliga myndigheters beredskap åläggs alla statliga myndigheter ansvaret för att säkerställa att informationssystemen uppfyller adekvata krav på informationssäkerhet.

Eftersom Digg antingen ska utveckla eller välja ut nationella interoperabilitetslösningar, som ska rekommenderas eller föreskrivas om, behöver säkerhetsåtgärder för sådana system vara konsekventa, transparenta och väl dokumenterade. Dokumentationen är en förutsättning för att verksamhetsutövare som ska använda de nationella interoperabilitetslösningarna ska kunna göra en bedömning av säkerhetsåtgärderna och deras lämplighet för den egna verksamheten. MSB kan då på ett resurseffektivt sätt ta fram stöd- och utbildningsmaterial för att underlätta för verksamhetsutövare för deras egna bedömningar om vidtagna säkerhetsåtgärder för respektive nationell interoperabilitetslösning.

Enligt 10 § Förordningen (2022:524) om statliga myndigheters beredskap ska varje myndighet i sin verksamhet beakta totalförsvarets krav. Rapportering och informationsdelning mellan olika aktörer under samhällsstörningar vid fred och krig är en förutsättning för välgrundade överenskommelser och beslut. Om informationsdelningen dessutom är effektiv och genomtänkt blir det lättare att få ett bra grepp om vad som har hänt, och om vad som måste göras. Därför är det angeläget att få tjänster att samverka så att resultatet blir sammanhängande. Förutsatt att interoperabilitetslösningar är robusta och säkra kan de alltså stärka totalförsvaret. Samtidigt kan data vara en strategisk resurs som inte ska falla i en angripares händer och underlätta dennes krigsansträngningar. Därför är det rimligt att också beakta lagen (1992:1402) om undanförsel och förstöring i utvecklingen av informationssystem för offentlig förvaltning.

Om MSB:s roll

MSB är positiva till att medverka som expertmyndighet i arbetet med interoperabilitetslösningar utifrån ett informationssäkerhets- och totalförsvarsperspektiv. Dock behöver rollens omfattning och mandat förtydligas och sannolikt också regleras.

MSB anser också att man ska delta i framtagandet av säkerhetskrav för de nationella interoperabilitetslösningar som utvecklas av andra än Digg för att motverka en fragmenterad kravbild. MSB ser vidare att man behöver förtydliga hur en konsekvent kravbild för skyddsnivåer och säkerhetsåtgärder ska säkerställas för samtliga nationella interoperabilitetslösningar, oavsett om de rekommenderas eller föreskrivs om.

För de fall där någon verksamhetsutövare som utvecklar, tillhandahåller eller använder nationella interoperabilitetslösningar inte träffas av gällande EU- eller nationell reglering föreslår MSB att MSB ges föreskriftsrätt för informationssäkerhetskrav.

MSB ställer sig positiva till att myndigheten ges i uppdrag att utreda behovet av koordinerade skyddsnivåer och andra relevanta säkerhetsåtgärder för de nationella interoperabilitetslösningarna. MSB delar utredningens syn på att ett regeringsuppdrag med särskilda anslag är en lämplig form för utredningen. Detta arbete behöver föregå framtagande, rekommendation och föreskrivande av nationella interoperabilitetslösningar för att säkerställa att samtliga lösningar motsvarar de informationssäkerhetskrav som utredningen tar fram.

För att säkerställa implementeringen av koordinerade skyddsnivåer bedömer MSB att man bör föreskriva om dessa samt eventuellt andra säkerhetsåtgärder som identifieras i det utredningsuppdrag till MSB som utredningen föreslår. Detta förutsatt att inte reglering som omfattar alla verksamhetsutövare som utvecklar, tillhandahåller eller använder nationella interoperabilitetslösningar faller ut av implementeringen av NIS2 eller annan rättsakt. MSB bedömer att den föreskriftsrätten då bör ges till MSB.

Rollen och mandatet för MSB föreslås vara desamma, oberoende av om Digg rekommenderar eller föreskriver om en lösning. Rollen behöver vara tydlig och stark i krav- och utvecklingsfaserna.

MSB avstyrker förslaget om att andra myndigheter ska kunna vända sig till MSB för bedömningar av lämpligheten i att nyttja enskilda interoperabilitetslösningar ur ett säkerhetsperspektiv. Det är mer resurseffektivt att arbeta med konsekvent och väl dokumenterad kravställning än att granska lösningar i efterhand. MSB föreslår att man istället för stöd till enskilda myndigheter tar fram råd och stödmaterial så att dessa myndigheter kan göra egna bedömningar av säkerhetshetsåtgärderna i nationella interoperabilitetslösningar.

Arbetet med interoperabilitetslösningar kommer att ta stora resurser i anspråk. MSB bedömer att detta arbete inte kan rymmas inom befintligt anslag, utan måste finansieras och resurssättas på ett ändamålsenligt och hållbart vis.

Om Diggs roll

MSB förutsätter att Digg tilldelas de resurser och ges de förutsättningar som krävs för det breddade uppdraget att utveckla, förvalta, koordinera och föreskriva om nationella interoperabilitetslösningar.

Inför det kommande arbetet med nationella interoperabilitetslösningar är det viktigt att Digg beskriver hur alla nationella interoperabilitetslösningar, även de som inte utvecklas av Digg, ska kravställas, kontrolleras och tillsynas. Kravställningen på de nationella interoperabilitetslösningarna, både de rekommenderade och de som man avser föreskriva om, behöver vara transparent och konsekvent, oavsett vilken verksamhetsutövare som utvecklar, tillhandahåller, förvaltar eller använder av en specifik nationell interoperabilitetslösning.

I detta ärende har överdirektör Camilla Asp beslutat. Handläggare Callisto Utriainen har varit föredragande. I den slutliga handläggningen har också avdelningschefen Åke Holmgren och enhetschefen Margareta Palmqvist deltagit.

Camilla Asp Skriv föredragande.