

Försvarsutskottets betänkande 2025/26:FöU15

Lagändringar för ett stärkt nationellt cybersäkerhetscenter

Sammanfattning

Utskottet ställer sig bakom regeringens förslag till en ny lag om uppgiftsskyldighet som ska gälla för de myndigheter som samverkar inom det nationella cybersäkerhetscentret (NCSC). Lagen syftar till att skapa förutsättningar för ett ändamålsenligt informationsutbyte inom ramen för centret. Genom att NCSC därigenom kan bedriva sin verksamhet effektivt stärks cybersäkerheten i samhället. Utskottet tillstyrker även regeringens förslag till en ny lag om Försvarets radioanstalts behandling av personuppgifter inom ramen för centrets verksamhet och en sekretessbestämmelse till skydd för enskilda för uppgifter som förekommer hos centret. Lagändringarna föreslås träda i kraft den 15 juli 2026. Utskottet anser att riksdagen bör avslå motionsyrkandet.

I betänkandet finns en reservation (C).

Behandlade förslag

Proposition 2025/26:214 Lagändringar för ett stärkt nationellt cybersäkerhetscenter.

Ett yrkande i en följdmotion.

Innehållsförteckning

| | |
|------------------------------------------------------------------------|----|
| Utskottets förslag till riksdagsbeslut | 3 |
| Redogörelse för ärendet | 4 |
| Ärendet och dess beredning..... | 4 |
| Propositionens huvudsakliga innehåll | 4 |
| Utskottets överväganden..... | 5 |
| Lagändringar för ett stärkt nationellt cybersäkerhetscenter | 5 |
| Reservation | 15 |
| Vissa frågor om lagstiftningens framtida utformning, punkt 2 (C) | 15 |
| <i>Bilaga 1</i> | |
| Förteckning över behandlade förslag..... | 17 |
| Propositionen | 17 |
| Följdmotionen | 17 |
| <i>Bilaga 2</i> | |
| Regeringens lagförslag | 18 |

Utskottets förslag till riksdagsbeslut

1. Lagändringar för ett stärkt nationellt cybersäkerhetscenter

Riksdagen antar regeringens förslag till

1. lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret,
2. lag om Försvarets radioanstalts behandling av personuppgifter inom det nationella cybersäkerhetscentret,
3. lag om ändring i offentlighets- och sekretesslagen (2009:400).

Därmed bifaller riksdagen proposition 2025/26:214 punkterna 1–3.

2. Vissa frågor om lagstiftningens framtida utformning

Riksdagen avslår motion

2025/26:4093 av Niels Paarup-Petersen och Mikael Larsson (båda C).

Reservation (C)

Stockholm den 26 maj 2026

På försvarsutskottets vägnar

Peter Hultqvist

Följande ledamöter har deltagit i beslutet: Peter Hultqvist (S), Matheus Enholm (SD), Jörgen Berglund (M), Helén Pettersson (S), Björn Söder (SD), Johan Andersson (S), Helena Bouveng (M), Hanna Westerén (S), Gulan Avci (L), Erik Ezelius (S), Alexandra Anstrell (M), Hanna Gunnarsson (V), Mikael Oscarsson (KD), Mikael Larsson (C), Lars Püss (M), Camilla Brunsberg (M) och Janine Alm Ericson (MP).

Redogörelse för ärendet

Ärendet och dess beredning

I betänkandet behandlar utskottet proposition 2025/26:214 Lagändringar för ett stärkt nationellt cybersäkerhetscenter. I propositionen finns en redogörelse för ärendets beredning fram till regeringens beslut om propositionen.

Regeringens förslag till riksdagsbeslut finns i bilaga 1. Regeringens lagförslag finns i bilaga 2. En motion har väckts med anledning av propositionen. Förslaget i motionen finns i bilaga 1.

Propositionens huvudsakliga innehåll

I propositionen anför regeringen att nuvarande sekretessreglering innebär att det saknas förutsättningar för ett ändamålsenligt informationsutbyte inom det nationella cybersäkerhetscentret (NCSC), som är placerat inom Försvarets radioanstalt (FRA), och att det utgör ett hinder för sådan samverkan som krävs för att stärka cybersäkerheten i vårt samhälle. Regeringen föreslår därför en ny lag om uppgiftsskyldighet som ska gälla för de myndigheter som samverkar inom NCSC. Regeringen föreslår också en ny lag om FRA:s behandling av personuppgifter inom ramen för centrets verksamhet och en sekretessbestämmelse till skydd för enskilda för uppgifter som förekommer hos centret. Därutöver föreslås ytterligare en ändring i offentlighets- och sekretesslagen.

Lagändringarna föreslås träda i kraft den 15 juli 2026.

Utskottets överväganden

Lagändringar för ett stärkt nationellt cybersäkerhetscenter

Utskottets förslag i korthet

Riksdagen antar regeringens förslag till lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret och lag om Försvarets radioanstalts behandling av personuppgifter inom det nationella cybersäkerhetscentret samt förslag till ändring i offentlighets- och sekretesslagen.

Jämför reservationen (C).

Bakgrund

Det nationella cybersäkerhetscentret (NCSC) bildades 2020 och centrets verksamhet bedrevs tidigare gemensamt av Försvarets radioanstalt (FRA), Försvarmakten, Myndigheten för civilt försvar (MCF) och Säkerhetspolisen i nära samverkan med Polismyndigheten, Försvarets materielverk (FMV) samt Post- och telestyrelsen (PTS). Regeringen inledde under 2023 ett arbete med att utveckla NCSC med målet att centret bl.a. ska utgöra navet i det nationella cybersäkerhetsarbetet. NCSC är sedan 2024 placerat inom FRA.

Av 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt (FRA:s instruktion) framgår att NCSC har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Centret bedrivs i dag organisatoriskt som en egen avdelning inom FRA.

Den 20 mars 2025 beslutade regeringen förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen) som innehåller kompletterande bestämmelser för centrets verksamhet. Av 2 § NCSC-förordningen framgår att det nationella cybersäkerhetscentret ska utgöra en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet. Centret ska också vara en kontaktpunkt för sådana frågor. Av 3 § samma förordning framgår att centret särskilt ska

1. bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet
2. lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet
3. lämna råd och stöd till privata och offentliga aktörer vid it-incidenter
4. genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet

5. till privata och offentliga aktörer ta fram samlade lägesbilder av antagonistiska cyberhot och andra it-incidenter
6. bistå Regeringskansliet (Försvarsdepartementet) med samlade lägesbilder som bland annat innehåller bedömningar av hotnivån
7. vara en kontaktpunkt gentemot motsvarande funktioner i internationella sammanhang och utveckla samarbetet och informationsutbytet med dessa
8. rapportera till regeringen om förhållanden på cybersäkerhetsområdet som kan leda till behov av åtgärder samt lämna förslag på sådana åtgärder
9. informera regeringen om relevanta förhållanden vid ett sådant hot eller en annan incident som avses i 5 § andra stycket i förordningen.

Enligt 4 § NCSC-förordningen ska FRA organisera, leda och planera den verksamhet som bedrivs inom ramen för NCSC. FRA ska enligt samma paragraf också samverka med FMV, Försvarsmakten, MCF, Polismyndigheten, PTS och Säkerhetspolisen (samverkansmyndigheterna) i den verksamhet som bedrivs inom centret.

Samverkansmyndigheterna ska, inom ramen för sina respektive befintliga ansvarsområden, löpande bistå centret med kunskap, kompetens och information och NCSC ska löpande bistå samverkansmyndigheterna med kunskap och information (5 § första stycket). Vid ett antagonistiskt cyberhot eller en annan it-incident som har vållat eller som kan antas ha potential att vålla betydande skada ska NCSC och samverkansmyndigheterna utbyta kunskap, kompetens och information för att förbättra samordningen mellan myndigheterna och bidra till att effektivisera myndigheternas arbete med att hantera cyberhotet eller incidenten (5 § andra stycket).

Regeringen beslutade den 14 november 2024 att ge en särskild utredare i uppdrag att åstadkomma en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete genom att utreda förutsättningarna för och konsekvenserna av en överföring av arbetsuppgifter från Myndigheten för samhällsskydd och beredskap, numera MCF, till FRA. I juli 2025 överlämnade utredningen betänkandet *Samlade förmågor för ökad cybersäkerhet (SOU 2025:79)* till regeringen. I betänkandet föreslogs bl.a. att flera uppgifter på cybersäkerhetsområdet ska föras över från MCF till FRA. Regeringen beslutade den 20 november 2025, i enlighet med förslagen i betänkandet, att ge MCF i uppdrag att förbereda för en överföring av dessa uppgifter till FRA genom NCSC och FRA gavs samtidigt det motsvarande uppdraget att förbereda för att inordna uppgifterna i NCSC till den 1 juli 2026.

Propositionen

I propositionen anför regeringen att det försämrade säkerhetspolitiska omvärldsläget med hot och krigföring kräver en avsevärt högre nivå av motståndskraft i Sverige och inom EU. I takt med att det säkerhetspolitiska läget har försämrats och cyberhoten och sårbarheterna ökat, både sett till antal och komplexitet, ställs allt högre krav på Sveriges förmåga att säkra, skydda och stärka samhällets funktioner även i cyberområdet. Regeringen anser att

det, med hänvisning till utvecklingen på cybersäkerhetsområdet, finns starka skäl för att NCSC ska kunna bedriva sin verksamhet på ett effektivt sätt, vilket i sin tur förutsätter ett välfungerande informationsutbyte. Regeringen konstaterar dock att nuvarande sekretessreglering innebär att det saknas förutsättningar för ett sådant ändamålsenligt informationsutbyte och att det utgör ett hinder för sådan samverkan som krävs för att stärka den nationella cybersäkerheten. Mot den bakgrunden lämnar regeringen i huvudsak följande förslag.

En ny lag om uppgiftsskyldighet vid samverkan inom NCSC

Regeringen föreslår att det ska införas en ny lag om uppgiftsskyldighet vid samverkan mellan myndigheter inom NCSC vid FRA. Inom ramen för samverkan ska en myndighet, enligt lagförslaget, lämna en uppgift till en annan myndighet om det behövs för den mottagande myndighetens deltagande i samverkan. En uppgift ska inte lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Endast myndigheter som regeringen bestämmer ska vara skyldiga att lämna eller få ta emot uppgifter enligt lagen.

Skälen för regeringens förslag är i huvudsak följande. Det behövs bättre förutsättningar för informationsdelning inom NCSC för att centret ska fungera effektivt. Av NCSC-förordningen framgår bl.a. att samverkansmyndigheterna och centret löpande och regelmässigt ska bistå varandra med kunskap och information. Men flera omständigheter kan utgöra eller upplevas utgöra hinder för informationsutbyte mellan myndigheterna, t.ex. att personal från de olika myndigheterna inte i tillräckligt stor omfattning har kunskap om regelverket kring sekretess, vilket medför att information inte delas med andra myndigheter i den utsträckning som är möjlig enligt gällande lagstiftning. En annan omständighet att beakta är att vissa myndigheter som samverkar inom NCSC är underrättelsemyndigheter medan andra inte är det. Lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott förbjuder att uppgifter från FRA:s underrättelseverksamhet används för att utreda brott. Även detta kan försvåra informationsutbytet eftersom såväl Polismyndigheten som, i viss utsträckning, Säkerhetspolisen utreder brott.

De uppgifter som behöver kunna delas inom ramen för NCSC:s verksamhet kan omfattas av sekretess till skydd för allmänna eller enskilda intressen. Det kan t.ex. handla om uppgifter som omfattas av utrikessekretess enligt 15 kap. 1 § offentlighets- och sekretesslagen (2009:400), förkortad OSL, eller försvarssekretess enligt 15 kap. 2 § samma lag. Det kan även handla om uppgifter som omfattas av tillämpningsområdet för 17 kap. 1 § OSL som rör sekretess för uppgift om planläggning eller andra förberedelser för sådan inspektion, revision eller annan granskning som en myndighet ska göra. Även uppgifter som omfattas av t.ex. underrättelsesekretess enligt 18 kap. 2 § OSL kan förekomma. Vidare kan det handla om uppgifter som omfattas av sekretess

enligt 35 kap. 1 § OSL som gäller för uppgifter som förekommer i exempelvis förundersökning, brottsförebyggande verksamhet eller vissa register.

Med anledning av synpunkter från ett par remissinstanser som ifrågasätter behovet av en ny reglering bedömer regeringen att de sekretessbrytande bestämmelser som finns i OSL inte är tillräckliga. Regeringen redovisar att den s.k. generalklausulen i 10 kap. 27 § OSL innebär att sekretess inte hindrar att uppgifter lämnas till en annan myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen ska skydda. Syftet med generalklausulen är att den ska utgöra en ventil för det fall ett utbyte av uppgifter uppenbart behöver ske och situationen inte har kunnat förutses i lagstiftningen. Ett rutinemässigt uppgiftsutbyte av sekretessreglerade uppgifter ska dock som utgångspunkt vara särskilt författningsreglerat (prop. 1979/80:2 del A s. 326 och 327). Enligt regeringen ska information inom ramen för NCSC kunna utbytas rutinemässigt och löpande. I NCSC-förordningen anges uttryckligen att NCSC och samverkansmyndigheterna löpande ska bistå varandra med kunskap och information. NCSC behöver kunna dra nytta av att myndigheterna har olika uppdrag och kompetenser och därmed innehar olika typer av information som kan vara användbar i samhällets cybersäkerhetsarbete. Mot bakgrund av den täta samverkan som behöver kunna ske inom ramen för NCSC:s verksamhet och i och med att tanken är att rutinemässigt informationsutbyte i regel ska vara författningsreglerat bedömer regeringen att generalklausulen inte är en lämplig reglering för informationsutbytet mellan FRA och samverkansmyndigheterna.

Enligt regeringen utgör inte heller 10 kap. 2 § OSL en ändamålsenlig reglering i sammanhanget. Bestämmelsen, som anger att sekretess inte hindrar att en myndighet lämnar ut uppgifter om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet, ska tillämpas restriktivt (prop. 1979/80:2 del A s. 465 och 494). Det är vidare den utlämnande myndighetens intresse av att lämna ut uppgiften, inte den mottagande myndighetens intresse att få del av densamma, som är avgörande för om en uppgift kan lämnas ut med stöd av bestämmelsen.

Regeringen instämmer i remissynpunkten att det visserligen är så att information som omfattas av sekretess till skydd för allmänna intressen många gånger torde kunna delas mellan FRA och samverkansmyndigheterna utan tillämpning av en sekretessbrytande bestämmelse. Det kan dock enligt regeringen inte uteslutas att en uppgift kan omfattas av sekretess i ett enskilt fall, och dessutom kan det vara så att uppgifterna också omfattas av sekretess till skydd för enskilda.

När det gäller sekretess till skydd för enskilda intressen gäller sedan den 1 december 2025 en generell sekretessbrytande bestämmelse (10 kap. 15 a § OSL). Bestämmelsen bryter sekretess till skydd för enskilda mellan myndigheter i vissa syften, bl.a. om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet eller utreda brott. Den informationsdelning

som är aktuell inom ramen för NCSC:s verksamhet kan dock, enligt regeringen, ske i andra syften än de som anges i den aktuella bestämmelsen.

Det finns enligt regeringens bedömning inte heller någon annan sekretessbrytande bestämmelse som möjliggör ett sådant löpande informationsutbyte som behöver kunna ske mellan FRA och samverkansmyndigheterna. Regeringen anför att 5 § NCSC-förordningen, enligt vilken NCSC och samverkansmyndigheterna löpande ska bistå varandra med information, inte har någon sekretessbrytande verkan i enlighet med 10 kap. 28 § OSL. Den aktuella bestämmelsen i OSL anger att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om det finns en uppgiftsskyldighet som följer av lag eller förordning.

Mot den bakgrunden anser regeringen att det finns behov av att införa en tydlig reglering som utökar möjligheterna till informationsutbyte mellan FRA och samverkansmyndigheterna. Regeringen bedömer att behovet av informationsdelning vid myndigheternas samverkan inom NCSC bäst tillgodoses genom en uppgiftsskyldighet som innebär att sekretess bryts enligt 10 kap. 28 § OSL.

I fråga om vilka myndigheter som bör omfattas av uppgiftsskyldigheten och hur skyldigheten bör avgränsas i övrigt bedömer regeringen att den bör gälla när samverkan sker mellan myndigheter inom NCSC. Det finns enligt regeringens mening inte skäl att peka ut vilka myndigheter som ska omfattas av uppgiftsskyldigheten i lag och det finns dessutom fördelar med en viss flexibilitet i detta avseende. Vilka myndigheter som är samverkansmyndigheter regleras i dag i NCSC-förordningen. Bedömningen av vilka myndigheter som bör delta i centrets verksamhet kan variera över tid utifrån bl.a. förändrade ansvarsområden, men även omvärldsutvecklingen. Regeringen anser därför att den föreslagna lagen endast ska ange att uppgiftsskyldigheten gäller för de myndigheter som regeringen bestämmer. Genom att det finns ett krav på att det ska röra sig om samverkan inom NCSC begränsas kretsen av personer som kan få del av uppgifterna till personer som arbetar vid FRA och samverkansmyndigheterna och därutöver till de personer som för berörda myndigheters räkning deltar i NCSC:s verksamhet.

Med anledning av en remissynpunkt bedömer regeringen att det inte finns något skäl att avstå från att ge Säkerhetspolisen en uppgiftsskyldighet i enlighet med den nya lagen. Regeringen konstaterar bl.a. att Säkerhetspolisen redan i dag har en liknande uppgiftsskyldighet enligt lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet. Dessutom föreslås (se nedan) att det ska finnas utrymme för myndigheten att avstå från uppgiftslämnande efter en intresseavvägning. Med hänvisning till det föreslagna utrymmet för att avstå från att lämna ut uppgifter finns det enligt regeringen inte heller anledning att undanta Försvarsmakten.

Regeringen anför vidare att skyldigheten att lämna en uppgift till en annan myndighet endast bör gälla om den mottagande myndigheten har ett behov av uppgiften för att delta i samverkan. Därigenom uppnås en balans mellan ett effektivt informationsutbyte och skyddet för den personliga integriteten.

Uppgifter bör kunna lämnas ut med stöd av uppgiftsskyldigheten dels efter begäran, dels på eget initiativ. Uppgiftsskyldigheten inträder alltså först när det kan konstateras att det finns ett visst behov av uppgiften och övriga förutsättningar för utlämnande av uppgifter är uppfyllda.

Eftersom uppgifter som är sekretessreglerade kan vara känsliga och av olika anledningar särskilt skyddsvärda anser regeringen att uppgiftsskyldigheten enligt den föreslagna lagen bör utformas så att det finns en möjlighet att i varje enskilt fall beakta intressen som talar för att en uppgift inte ska lämnas ut. Denna intresseavvägning bör uttryckas som att det ska krävas att det finns en sekretessbestämmelse som är tillämplig på uppgiften och att övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. På så sätt finns det enligt regeringen möjlighet att hemlighålla såväl skyddsvärda uppgifter om enskilda som skyddsvärda uppgifter om myndigheters verksamhet.

Regeringen anför vidare att det, med den föreslagna utformningen, är den myndighet som förfogar över den aktuella uppgiften som ska pröva om det finns förutsättningar för att lämna uppgiften till en annan myndighet. Kravet på övervägande skäl innebär att behovet av informationsutbyte vid samverkan inom NCSC normalt sett har företräde framför andra intressen. Det råder således en presumtion för att uppgiften ska lämnas ut.

Exempel på uppgifter som ofta skyddas av sekretess och som det kan finnas starka skäl att inte lämna ut kan enligt regeringen vara uppgifter om metoder, förmågor, namn på uppdragsgivare och liknande uppgifter som skyddas av utrikes- eller försvarssekretess. Även uppgifter som skyddas av underrättelsesekretess kan i vissa fall hänföras till denna kategori. Det kan också vara fråga om uppgifter om en myndighets egna säkerhets- och bevakningsåtgärder. Regeringen instämmer således med Säkerhetspolisens remissynpunkt om att informationsutbytet inom NCSC inte får inskränka en myndighets möjlighet att utföra sitt primära uppdrag.

Regeringen bemöter slutligen en remissynpunkt om att det vid intresseavvägningen bör beaktas vilken verksamhet som finns hos den mottagande myndigheten och hur myndigheten behandlar överlämnade uppgifter. För att utövare av säkerhetskänslig verksamhet ska vara benägna att lämna uppgifter om sårbarheter eller incidenter till NCSC kommer det, enligt remissynpunkten, att vara viktigt att det står klart att de därigenom inte riskerar att bli föremål för ett tillsynsärende enbart på grund av den information som sedan delas med Säkerhetspolisen i dess egenskap av samverkansmyndighet. Säkerhetspolisen är nämligen tillsynsmyndighet enligt säkerhetsskyddslagen (2018:585). Regeringen anför att som intresseavvägningen är formulerad finns inget utrymme för att ta hänsyn till att uppgiftslämnande till en myndighet i sig kan upphöra eller på annat sätt påverkas av om uppgifter lämnas ut. Regeringen bedömer inte heller att det bör finnas ett sådant utrymme. Hur uppgifter som lämnas till en myndighet används i slutändan av mottagaren får avgöras av den mottagande myndigheten med beaktande av bl.a. det data-skyddsrättsliga regelverket.

En ny sekretessbestämmelse för FRA

Regeringen föreslår att det ska föras in en ny sekretessbestämmelse i OSL om att sekretess ska gälla hos FRA i verksamhet vid NCSC för uppgifter om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgifterna kan röjas utan att den enskilde lider skada eller men.

Sekretessen ska enligt förslaget inte gälla i ärenden om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning. För uppgifter i en allmän handling ska sekretessen gälla i högst sjuttio år.

Rätten att meddela och offentliggöra uppgifter ska inte ha företräde framför den tystnadsplikt som följer av sekretessen.

Regeringen anför att den nya sekretessbestämmelsen behövs bl.a. med anledning av den överflyttning av uppgifter från MCF till FRA som regeringen beslutat om. FRA ska bl.a. ta över rollen som enhet för hantering av it-säkerhetsincidenter (CSIRT) och gemensam kontaktpunkt enligt NIS 2-direktivet¹. Direktivet har genomförts i Sverige i huvudsak genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507). Regeringen bedömer att även andra artiklar i direktivet som ställer krav på skydd av uppgifter (t.ex. vid anonym anmälan av sårbarheter och frivilliga underrättelser) motiverar en ny sekretessbestämmelse. Därutöver har NCSC ett brett uppdrag och ska vara kontaktpunkt för samverkan med bl.a. privata aktörer. En stor mängd uppgifter om enskilda av varierande slag kan således komma att behandlas i den verksamhet som FRA ska bedriva inom ramen för NCSC. Regeringen bedömer därför att det behövs en ny bestämmelse till skydd för uppgifter om enskilda.

En ny lag om FRA:s personuppgiftsbehandling inom ramen för NCSC:s verksamhet

Regeringen föreslår att det ska införas en ny lag om behandling av personuppgifter som ska gälla för behandling av personuppgifter inom NCSC vid FRA. Lagen ska gälla när FRA inom den del av myndigheten som utgör NCSC utför uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Syftet med den nya lagen är enligt förslaget dels att FRA ska få möjlighet att behandla personuppgifter på ett ändamålsenligt sätt, dels att skydda människor mot att deras personliga integritet kränks vid en sådan behandling.

Lagens tillämpningsområde i övrigt och förhållandet till annan reglering

Regeringen föreslår att lagen ska gälla endast om personuppgiftsbehandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller

¹ Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148.

kommer att ingå i ett register. Det ska vidare anges i lagen att den inte gäller vid behandling av personuppgifter som omfattas av lagen om behandling av personuppgifter vid FRA.

Det ska också anges i lagen att den kompletterar EU:s dataskyddsförordning. Hänvisningar till förordningen i den nya lagen ska vara dynamiska. Dataskyddslagen och föreskrifter som har meddelats i anslutning till den lagen ska gälla vid behandlingen av personuppgifter enligt den föreslagna lagen, om inte annat följer av den föreslagna lagen eller av föreskrifter som har meddelats i anslutning till den föreslagna lagen.

Det ska framgå av den nya lagen att FRA är personuppgiftsansvarigt för den behandling av personuppgifter som myndigheten utför enligt lagen.

Personuppgiftsbehandlingen rättsliga grund och ändamål

Enligt förslaget ska FRA få behandla personuppgifter med stöd av lagen om det är nödvändigt för att myndigheten inom NCSC ska kunna utföra uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Personuppgifter som behandlas för dessa ändamål ska också få behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Personuppgifter ska också få behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Tillgången till personuppgifter ska begränsas

Regeringen föreslår att tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Behandling av känsliga personuppgifter

Enligt lagförslaget ska FRA få behandla känsliga personuppgifter med stöd av den nya lagen, om det är nödvändigt med hänsyn till ändamålet med behandlingen.

Regeringen föreslår vidare att det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Personuppgifter ska få lämnas ut elektroniskt

Personuppgifter ska enligt lagförslaget få lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Personuppgifter ska få behandlas under en begränsad tid

Regeringen föreslår att personuppgifter inte ska få behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Det ska införas en bestämmelse i den nya lagen som upplyser om att detta inte hindrar att FRA arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Rätten att göra invändningar ska inte gälla

Rätten för registrerade att göra invändningar enligt artikel 21.1 i EU:s dataskyddsförordning ska inte gälla vid sådan behandling av personuppgifter som är tillåten enligt lagen eller föreskrifter som har meddelats i anslutning till lagen.

Ikraftträdande- och övergångsbestämmelser

De nya lagarna och övriga lagändringar föreslås träda i kraft den 15 juli 2026. Regeringen bedömer att det inte finns behov av några övergångsbestämmelser.

Motionen

I kommittémotion 2025/26:4093 begär Niels Paarup-Petersen och Mikael Larsson (båda C) att regeringen ska återkomma till riksdagen med en fördjupad analys av vilka faktiska hinder mot informationsdelning som föreligger och för att säkerställa att myndigheter som bedriver säkerhets-känslig verksamhet inte riskerar att bli föremål för tillsynsärenden enbart på grund av den information som delas.

Utskottets ställningstagande

Som regeringen konstaterar har det försämrade säkerhetspolitiska läget och den snabba tekniska utvecklingen medfört att cyberhoten och sårbarheterna har ökat, både i antal och komplexitet. Detta ställer allt högre krav på Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Att kunna säkra och skydda viktiga samhällsfunktioner även på cyberområdet är centralt för ett motståndskraftigt samhälle. Liksom regeringen anser därför utskottet att Sverige ska ha ett väl fungerande NCSC med målet att bl.a. utgöra navet i det nationella cybersäkerhetsarbetet. Utskottet delar regeringens bedömning att det kräver att NCSC också ges förutsättningar att kunna bedriva sin verksamhet på ett effektivt sätt, vilket i sin tur förutsätter ett fungerande informationsutbyte mellan berörda aktörer. Utskottet anser att regeringens förslag på hur det ska åstadkommas är ändamålsenligt utformat och väl avvägt.

Utskottet tillstyrker därmed regeringens lagförslag av de skäl som anförs i propositionen.

Av detta följer att utskottet ställer sig bakom regeringens bedömning att det i nuläget inte finns tillämpliga bestämmelser som möjliggör ett sådant löpande informationsutbyte mellan berörda aktörer som krävs för ett effektivt NCSC och att det därför finns behov av en ny, tydligare reglering. Utskottet har inte heller någon annan uppfattning än regeringen i fråga om hur en mottagande myndighet ska kunna använda uppgifter som lämnas enligt den nya lagen. Det får mottagande myndighet avgöra med beaktande av tillämpliga regler bl.a. det dataskyddsrättsliga regelverket. Utskottet anser således att det inte finns

anledning för riksdagen att göra något sådant tillkännagivande som motionärerna efterfrågar. Utskottet avstyrker därmed motion 2025/26:4093 (C).

Reservation

Vissa frågor om lagstiftningens framtida utformning, punkt 2 (C)

av Mikael Larsson (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion

2025/26:4093 av Niels Paarup-Petersen och Mikael Larsson (båda C).

Ställningstagande

En stark cybersäkerhetsförmåga är naturligtvis av största vikt. Arbetet med att stärka denna måste dock utföras på ett sätt som innebär en rimlig balans mellan effektiv informationsdelning och skyddet för verksamheter med särskilt känsliga uppdrag. Regeringen föreslår i propositionen lagstiftning som syftar till att stärka informationsutbytet inom NCSC. En väl fungerande samverkan mellan berörda myndigheter är central för att möta komplexa cyberhot. Samtidigt aktualiserar förslagen en del principiellt viktiga frågor. Flera remissinstanser har i sina yttranden framfört invändningar av grundläggande karaktär. Dessa invändningar bör enligt min mening tas på stort allvar, inte minst då de kommer från myndigheter med centrala roller i Sveriges säkerhets- och underrättelsearbete.

Viktiga remissinstanser har bl.a. framhållit att det inte är tillräckligt klarlagt att det föreligger ett behov av ytterligare lagstiftning för att möjliggöra informationsutbyte mellan berörda myndigheter. Nu gällande regelverk innehåller redan bestämmelser som medger informationsdelning i relevanta situationer. Det finns därför skäl att ifrågasätta om den föreslagna regleringen riskerar att innebära en överreglering snarare än en faktisk effektivisering. Vidare har det gjorts principiella invändningar mot att införa en generell uppgiftsskyldighet i ett sammanhang där vissa berörda myndigheter har särskilda uppdrag kopplade till nationell säkerhet. Sådana verksamheter bygger i stor utsträckning på förtroende, skyddsintressen och behovet av att kunna kontrollera informationsflöden. En ordning som innebär en långtgående skyldighet att dela information kan i vissa situationer vara svår att förena med myndigheternas uppdrag i övrigt. FRA påpekar särskilt att Säkerhetspolisens uppdrag är att vara tillsynsmyndighet enligt säkerhetsskyddslagen. För att utövare av säkerhetskänslig verksamhet ska vara benägna att lämna uppgifter om sårbarheter eller incidenter till NCSC, kommer det enligt FRA att vara viktigt att det står klart att de därigenom inte riskerar att bli föremål för ett

tillsynsärende enbart på grund av den information som sedan delas med Säkerhetspolisen i dess egenskap av samverkansmyndighet.

Jag instämmer således i remissinstansernas synpunkter och anser att regeringen bör återkomma till riksdagen med en fördjupad analys av vilka faktiska hinder mot informationsdelning som föreligger i dag och i vilken utsträckning dessa kan hanteras inom ramen för befintlig lagstiftning. En fördjupad analys bör även säkerställa att myndigheter som bedriver säkerhets-känslig verksamhet inte riskerar att bli föremål för tillsynsärenden enbart på grund av den information som delas.

BILAGA I

Förteckning över behandlade förslag

Propositionen

Proposition 2025/26:214 Lagändringar för ett stärkt nationellt cybersäkerhetscenter:

1. Riksdagen antar regeringens förslag till lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret.
2. Riksdagen antar regeringens förslag till lag om Försvarets radioanstalts behandling av personuppgifter inom det nationella cybersäkerhetscentret.
3. Riksdagen antar regeringens förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).

Följdmotionen

2025/26:4093 av Niels Paarup-Petersen och Mikael Larsson (båda C):

Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör återkomma till riksdagen med en fördjupad analys av vilka faktiska hinder mot informationsdelning som föreligger och för att säkerställa att myndigheter som bedriver säkerhetskänslig verksamhet inte riskerar att bli föremål för tillsynsärenden enbart på grund av den information som delas, och detta tillkännager riksdagen för regeringen.

BILAGA 2

Regeringens lagförslag

1 Förslag till lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret

Härigenom föreskrivs följande.

1 § Denna lag innehåller bestämmelser om skyldigheter att lämna uppgifter vid samverkan mellan Försvarets radioanstalt och andra myndigheter inom ramen för den verksamhet som bedrivs inom det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

Endast myndigheter som regeringen bestämmer ska vara skyldiga att lämna eller få ta emot uppgifter enligt denna lag.

2 § Inom ramen för samverkan enligt denna lag ska en myndighet lämna uppgift till en annan myndighet om det behövs för den mottagande myndighetens deltagande i samverkan.

En uppgift ska inte lämnas om det finns en sekretessbestämmelse som är tillämplig på uppgiften och övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Denna lag träder i kraft den 15 juli 2026.

2 Förslag till lag om Försvarets radioanstalts behandling av personuppgifter inom det nationella cybersäkerhetscentret

Härigenom föreskrivs följande.

Lagens syfte

1 § Syftet med denna lag är att ge Försvarets radioanstalt möjlighet att behandla personuppgifter på ett ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Lagens tillämpningsområde

2 § Denna lag gäller vid behandling av personuppgifter vid Försvarets radioanstalt när myndigheten inom den del av myndigheten som utgör det nationella cybersäkerhetscentret utför uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Lagen gäller endast om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Förhållandet till annan reglering

3 § Lagen gäller inte vid behandling av personuppgifter som omfattas av lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt.

4 § Denna lag kompletterar 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), här benämnd EU:s dataskyddsförordning.

5 § Vid behandling av personuppgifter enligt denna lag gäller lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och föreskrifter som har meddelats i anslutning till den lagen, om inte annat följer av denna lag eller föreskrifter som meddelats i anslutning till lagen.

Personuppgiftsansvar

6 § Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt denna lag.

Ändamål med personuppgiftsbehandlingen

7 § Personuppgifter får behandlas om det är nödvändigt för att Försvarets radioanstalt ska kunna utföra den uppgift som anges i 2 § första stycket.

8 § Personuppgifter som behandlas enligt 7 § får även behandlas för att fullgöra ett uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Personuppgifterna får även behandlas för andra ändamål, under förutsättning att uppgifterna inte behandlas på ett sätt som är oförenligt med det ändamål för vilket uppgifterna samlades in.

Tillgången till personuppgifter

9 § Tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Behandling av känsliga personuppgifter och sökbegränsning

10 § Personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) får behandlas med stöd av artikel 9.2 g i förordningen endast om uppgifterna är nödvändiga för fullgörandet av den uppgift som anges i 2 § första stycket.

11 § Det är förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Elektroniskt utlämnande av personuppgifter

12 § Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

Längsta tid som personuppgifter får behandlas

13 § Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Första stycket hindrar inte att Försvarets radioanstalt arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Rätten att göra invändningar

14 § Artikel 21.1 i EU:s dataskyddsförordning om rätten att göra invändningar gäller inte vid sådan behandling som är tillåten enligt denna lag eller föreskrifter som har meddelats i anslutning till lagen.

Denna lag träder i kraft den 15 juli 2026.

3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 40 kap. 8 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 40 kap. 7 i §, och närmast före 40 kap. 7 i § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

40 kap.

Verksamhet vid det nationella cybersäkerhetscentret

7 i §

Sekretess gäller hos Försvarets radioanstalt i verksamhet vid det nationella cybersäkerhetscentret för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Sekretessen gäller inte i ett ärende om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

8 §¹

Den tystnadsplikt som följer av 1, 2, 4, 5, 7 d och 7 g §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1, 2, 4, 5, 7 d, 7 g och 7 i §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Denna lag träder i kraft den 15 juli 2026.

¹ Senaste lydelse 2025:1495.