Regeringens proposition 2025/26:214

Lagändringar för ett stärkt nationellt cybersäkerhetscenter

Prop. 2025/26:214

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 1 april 2026

Elisabeth Svantesson

Carl-Oskar Bohlin
(Försvarsdepartementet)

Propositionens huvudsakliga innehåll

Det nationella cybersäkerhetscentret (NCSC), som är placerat inom Försvarets radioanstalt (FRA), har i uppdrag att utveckla och stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. FRA ska samverka med de så kallade samverkansmyndigheterna i den verksamhet som bedrivs inom ramen för centret.

En grundläggande förutsättning för att man inom NCSC ska kunna bedriva ett effektivt arbete är att FRA och samverkansmyndigheterna kan utbyta nödvändig information med varandra. Nuvarande sekretessreglering innebär att det saknas förutsättningar för ett ändamålsenligt informationsutbyte och detta är 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 myndigheterna 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.

Innehållsförteckning

1 Förslag till riksdagsbeslut

Regeringens förslag:

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).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 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.

2.2 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.

2.3 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.

3 Ärendet och dess beredning

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 Myndigheten för civilt försvar (MCF), till Försvarets radioanstalt (FRA) (dir. 2024:111). Därutöver fick utredaren i uppdrag att bland annat analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling.

Utredningen antog namnet Utredningen om ett stärkt nationellt cybersäkerhetscenter. I juli 2025 överlämnade utredningen sitt betänkande Samlade förmågor för ökad cybersäkerhet (SOU 2025:79). En sammanfattning av betänkandet finns i *bilaga 1* och betänkandets lagförslag i relevanta delar finns i *bilaga 2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissvaren finns tillgängliga på regeringens webbplats (regeringen.se) och i lagstiftningsärendet (Fö2025/01133).

I betänkandet lämnas förslag om 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 det nationella cybersäkerhetscentret (NCSC) och FRA gavs samtidigt det motsvarande uppdraget att förbereda för ett inordnande av uppgifterna i NCSC till den 1 juli 2026 (Fö2025/01703 och Fö2025/01704). Det krävs ingen lagreglering för att genomföra utredningens förslag om verksamhetsöverföring och förslagen behandlas därför inte i denna proposition. I betänkandet lämnas också förslag om ändringar i 15 kap. offentlighets- och sekretesslagen (2009:400). Dessa förslag behandlas i propositionen Explosiva varor – förbättrade möjligheter till kontroll som beslutades den 12 februari 2026 (se vidare prop. 2025/26:123).

Lagrådet

Regeringen beslutade den 26 februari 2026 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 4*. Lagrådets yttrande finns i *bilaga 5*. Regeringen följer delvis Lagrådets synpunkter och förslag, som behandlas i avsnitt 5.1, 6.3 och 6.5 samt i författningskommentaren (avsnitt 9). I förhållande till lagrådsremissen har ikraftträdandet av förslagen flyttats fram. Förslaget om senare ikraftträdande är författningstekniskt och även i övrigt av sådan beskaffenhet att Lagrådets hörande skulle sakna betydelse. Regeringen har därför inte inhämtat Lagrådets yttrande över det förslaget. I förhållande till lagrådsremissens förslag görs dessutom vissa språkliga och redaktionella ändringar.

4 Utvecklingen inom cybersäkerhet och FRA:s och NCSC:s uppgifter på cybersäkerhetsområdet

4.1 Utvecklingen på cybersäkerhetsområdet

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 cyberdomänen. Sveriges cybersäkerhet påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. Dessa sårbarheter kan samlat eller var för sig utgöra strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet.

Sverige står, likt andra länder, inför en dynamisk och föränderlig hotbild där cyberhotaktörer kontinuerligt utvecklar nya metoder och anammar ny teknik. Såväl att upptäcka sofistikerade cyberangrepp som att definitivt attribuera angrepp till en specifik hotaktör är komplext och bidrar till att cyberangrepp ofta innebär låg risk för påföljder, motåtgärder eller personliga konsekvenser för hotaktörer.

Regeringens nationella strategi för cybersäkerhet, Nationell strategi för cybersäkerhet 2025–2029 (skr. 2024/25:121), beslutades i mars 2025 och ersatte den tidigare strategin Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Strategin utgår från nationella behov och NIS 2-direktivet, det vill säga 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 (NIS 2-direktivet). Strategin utgår från NIS 2-direktivets allriskperspektiv för att hantera en bredd av utmaningar såsom kompetensbrist, komplex reglering, sårbara leveranskedjor och bristande systematiskt cybersäkerhetsarbete. Mot bakgrund av det säkerhetspolitiska läget fokuserar strategin därtill i vissa delar särskilt på antagonistiska hot i hela hotskalan. Uttrycket organisationer används i strategin som ett samlingsbegrepp och avser bland annat statliga myndigheter, statligt ägda bolag, kommuner, regioner samt privata och kommunala bolag.

I strategin beskrivs bland annat typiska hotaktörer, däribland cyberaktivister, cyberbrottslighet och kriminella grupperingar, och sårbarheter som påverkar Sveriges cybersäkerhet. Cyberangrepp utförda av statliga eller statsunderstödda aktörer mot svenska verksamheter har, som anges i strategin, ökat i omfattning och kan få allvarliga konsekvenser. Statliga aktörer har sofistikerade offensiva cyberförmågor som bland annat kan användas för teknikstöld, underrättelseinhämtning eller annan verksamhet som tillfälligt stör eller förstör hela eller delar av system, ofta inom kritisk infrastruktur och samhällsviktig verksamhet. Cyberangrepp kan frikopplat

från, eller inför eller under, en väpnad konflikt komplettera politiska, diplomatiska, ekonomiska, militära och andra medel som en hotaktör nyttjar. Statliga aktörer bedriver också informationspåverkan, till exempel med stöd av cyberangrepp, och nyttjar det fria informationsflödet på internet för antagonistiska syften. Metoderna som aktörerna använder för att påverka Sverige är en del av det som kallas hybridhot. Cyberangrepp i olika former är en ofta förekommande metod i dessa hybridaktiviteter. God cybersäkerhet försvårar för hotaktörer att utöva hybridaktiviteter mot Sverige och svenska intressen.

Brister i det förebyggande systematiska cybersäkerhetsarbete utgör, som också anges i strategin, en strategisk sårbarhet. Bristande incidenthantering utgör en allvarlig risk för förlust av känslig information, förlust av förmågan att tillhandahålla kritiska tjänster och finansiella förluster. Ett mörkertal i rapporteringen av it-incidenter har länge varit en realitet nationellt och internationellt. Detta påverkar, som anges i strategin, möjligheten att skapa en operativ lägesbild och varna andra organisationer, vilket riskerar att förvärra en pågående incident. Bristande incidentrapportering minskar också möjligheterna att dra lärdomar och inrikta det förebyggande arbetet. Mörkertalet i antalet rapporterade cyberbrott försvårar också brottsbekämpande myndigheters förebyggande arbete, operativa hantering och utredning vid cybersäkerhetsincidenter. I förlängningen påverkas möjligheten att lagföra den som har utfört en brottslig handling.

Som nämns i strategin har också privata och offentliga organisationer tillgång till olika informationsflöden. Expert- och tillsynsmyndigheter tar exempelvis emot incident- och sårbarhetsrapporter, medan privata organisationer innehar majoriteten av samhällets cyberresurser och är centrala för nationell cybersäkerhetsförmåga. Informationsdelning och samarbete mellan och inom privat och offentlig sektor kräver bland annat uppbyggda kommunikationsvägar och adekvata processer samt tillit aktörer emellan. Dessa processer behöver exempelvis utgå från och ta hänsyn till privata aktörers affärsintressen och sekretess för affärs- och driftförhållanden. Outvecklat och bristande samarbete mellan det privata och offentliga, såväl nationellt som internationellt, utgör i sig en sårbarhet.

4.2 FRA:s och NCSC:s uppgifter på cybersäkerhetsområdet

Försvarets radioanstalt (FRA) har till huvuduppgift att bedriva signalspaning och stödja andra myndigheter i frågor som rör signalspaning och kryptologi. Enligt 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt (FRA:s instruktion) ska myndigheten därtill ha en hög teknisk kompetens på informationssäkerhetsområdet. Myndigheten får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Myndigheten ska dessutom särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-

säkerhetsanalyser och ge annat tekniskt stöd. Myndigheten ska även samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet.

Det nationella cybersäkerhetscentret (NCSC) bildades 2020 och centrets verksamhet bedrevs tidigare gemensamt av FRA, Försvarsmakten, 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 bland annat ska utgöra navet i det nationella cybersäkerhetsarbetet. NCSC är sedan 2024 placerat inom FRA. Av 4 a § FRA:s instruktion framgår att centret 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, och
9. informera regeringen om relevanta förhållanden vid ett sådant hot eller annan incident som avses i 5 § andra stycket i förordningen.

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

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 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 i syfte att förbättra samordningen mellan myndigheterna och bidra till att effektivisera myndigheternas arbete med att hantera cyberhotet eller incidenten (5 § andra stycket).

Som nämns i avsnitt 3 har regeringen beslutat att FRA och MCF ska förbereda för överföringen av vissa uppgifter som i dag utförs av MCF. Bland de uppgifter som omfattas av regeringens beslut, och som är av relevans för förslagen i denna proposition, återfinns uppdragen att vara nationell funktion för it-incidenthantering (CSIRT-enhet) och gemensam kontaktpunkt enligt artiklarna 8–10 i NIS 2-direktivet (se vidare avsnitt 5.2). En annan uppgift som omfattas av regeringens beslut om överföring av uppgifter, och som är av viss relevans för förslagen i denna proposition, är uppdraget att pröva frågor om stöd samt meddela föreskrifter om verkställighet enligt 6 och 22 §§ förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

5 Ny reglering om sekretess

5.1 En ny lag om uppgiftsskyldighet vid samverkan inom NCSC

Regeringens förslag

Det ska införas en ny lag om uppgiftsskyldighet vid samverkan mellan myndigheter inom det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

Inom ramen för samverkan 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.

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

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Arbetsgivarverket* anser att den föreslagna lagen är välmotiverad och att dess tillämpningsområde är tydligt avgränsat. *Certezza AB*, som tillstyrker förslaget, instämmer med utredningen i fråga om att det finns ett behov av utökade utbildningsinsatser om nuvarande sekretessreglering

för berörda myndigheters personal men anför att det även finns skäl att förbättra regelverket. *Försvarets materielverk (FMV)* bedömer i likhet med utredningen att informationshanteringen inom det nationella cybersäkerhetscentret (NCSC) bör förenklas och understryker vikten av att uppgiftsskyldigheten, så som utredningen föreslår, endast omfattar samverkan mellan myndigheterna kopplat till de uppgifter som anges i NCSC-förordningen. *Försvarets radioanstalt (FRA)* framhåller den föreslagna regleringen som nödvändig för en ändamålsenlig samverkan inom NCSC. En ytterligare omständighet som enligt FRA bör beaktas vid intresseavvägningen är dock vilken verksamhet som finns hos den mottagande myndigheten och hur myndigheten behandlar överlämnade uppgifter. FRA nämner att ett av Säkerhetspolisens uppdrag är att vara tillsynsmyndighet enligt säkerhetsskyddslagen (2018:585). 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. *Integritetsskyddsmyndigheten* ställer sig särskilt bakom att uppgiftsskyldigheten förenas med en möjlighet att avstå från att lämna uppgifter efter en intresseavvägning och anser att det är positivt att utredningen för fram att uppgifter av särskilt integritetskänslig art kan utgöra sådana uppgifter. *Polismyndigheten* och *Statskontoret* bedömer att förslaget skapar förutsättningar för en mer utvecklad samverkan inom NCSC.

Försvarsmakten och *Säkerhetspolisen* motsätter sig att förslaget genomförs och anser att det saknas behov av att utöka de rättsliga möjligheterna till informationsdelning. Försvarsmakten pekar på att det redan framgår av NCSC-förordningen att samverkansmyndigheterna och NCSC ska bistå varandra med information och att därmed även andra sekretessbrytande bestämmelser än den så kallade generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen (2009:400) (OSL), såsom 10 kap. 2 § samma lag, kan bli tillämpliga. Försvarsmakten bedömer vidare att den information som kommer att delas mellan myndigheterna huvudsakligen är sådan som omfattas av sekretess till skydd för allmänna intressen. Försvarsmakten framhåller att sådan information många gånger bör kunna delas utan att en sekretessbrytande bestämmelse behöver tillämpas, eftersom skaderekvisitet i respektive bestämmelse inte är uppfyllt i förhållande till den mottagande myndigheten. Säkerhetspolisen framhåller att det är av principiell vikt att en säkerhetstjänst inte får någon uppgiftsskyldighet och att andra faktorer än sekretess kan vara ett hinder för myndighetens möjlighet att dela information inom centret. Viss information är exempelvis på grund av sin natur svår eller omöjlig att dela med vissa eller samtliga myndigheter som samverkar inom centret med hänsyn till Säkerhetspolisens konkreta skyddsintressen.

Vissa remissinstanser har synpunkter på valet av regleringsform. Certezza AB anför att uppgiftsskyldigheten har karaktären av en instruktion till deltagande myndigheter och därför bör regleras i förordning, exempelvis i NCSC-förordningen, samt att den sekretessbrytande bestämmelsen bör placeras i 10 kap. OSL för att underlätta för tillämpare av bestämmelsen. Försvarsmakten anser, om regeringen bedömer att det finns behov av en bestämmelse som bryter sekretess till

skydd för enskildas intressen, att en sådan bestämmelse bör placeras i förordning.

Några remissinstanser anför att det i vissa avseenden är oklart hur den föreslagna lagen ska tillämpas. FMV påpekar att det kan uppstå situationer där samverkansmyndigheter som innehar samma information gör olika bedömningar av om informationen ska lämnas ut. I en sådan situation är det enligt FMV oklart om informationen kommer att lämnas ut. Enligt *Sveriges advokatsamfund* är det inte tydligt vilken myndighet som ska bedöma rekvisitet behövs och hur denna bedömning ska ske. Advokatsamfundet efterfrågar vidare någon form av begränsning som säkerställer att personuppgifter inte utväxlas i onödan, eller att uppgifterna anonymiseras eller pseudonymiseras innan de lämnas ut. Advokatsamfundet framhåller att cybersäkerhetsåtgärder endast i undantagsfall torde förutsätta att det går att identifiera eller kartlägga individerna bakom uppgifterna.

Skälen för regeringens förslag

Myndighetssamverkan och sekretessbrytande bestämmelser

En myndighet ska enligt 8 § förvaltningslagen (2017:900) samverka med andra myndigheter inom sitt verksamhetsområde. I 6 kap. 5 § OSL anges vidare att en myndighet på begäran av en annan myndighet ska lämna en uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång.

För att underlätta samarbetet mellan myndigheter, och för att bland annat upprätthålla kravet på förvaltningens effektivitet och rättssäkerhet, är det ofta nödvändigt att myndigheter kan få tillgång till sekretessreglerade uppgifter. Av den anledningen finns det bestämmelser som i olika situationer bryter sekretess. I 10 kap. OSL finns en mängd sådana bestämmelser. Enligt 10 kap. 2 § OSL hindrar inte sekretess att en myndighet lämnar ut uppgifter om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Bestämmelsen ska tillämpas restriktivt (se prop. 1979/80:2 Del A s. 465 och 494).

I 10 kap. 27 § OSL finns den så kallade generalklausulen som 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. Bestämmelsen tillkom för att göra det möjligt för myndigheter att utväxla uppgifter i situationer där intresset av att uppgifterna lämnas ut bör ha företräde framför det intresse som sekretessen avser 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 rutinmässigt uppgiftsutbyte av sekretessreglerade uppgifter ska dock som utgångspunkt vara särskilt författningsreglerat. (Se prop. 1979/80:2 Del A s. 326 och 327).

Enligt 10 kap. 28 § OSL hindrar inte sekretess att en uppgift lämnas till en annan myndighet, om det finns en uppgiftsskyldighet som följer av lag eller förordning. Med uppgiftsskyldighet avses att det i annan lag eller av förordning följer att uppgift ska lämnas (se prop. 1979/80:2 Del A s. 322). Sekretessbrytande uppgiftsskyldigheter grundar sig på överväganden om vilket sekretesskydd uppgiften har hos den utlämnande myndigheten och

om den mottagande myndighetens behov generellt sett kan anses väga tyngre än det intresse som sekretessen skyddar. Bestämmelser om uppgiftsskyldighet mellan myndigheter är alltså ett sätt för lagstiftaren att särskilt reglera ett ofta förekommande informationsutbyte och att säkerställa att en viss myndighet får de uppgifter som den behöver. För utlämnandet är det inte nödvändigt att bestämmelsen om uppgiftsskyldighet har utformats utifrån att uppgifterna är sekretessbelagda. Såväl offentliga som sekretessbelagda uppgifter kan därför omfattas av en uppgiftsskyldighet.

Det finns flera exempel på uppgiftsskyldigheter som bryter sekretess mellan myndigheter med stöd av 10 kap. 28 § OSL. Ett exempel är lagen (2016:774) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet (LUS), som gäller vid särskilt beslutad samverkan för att förebygga, förhindra eller upptäcka brottslig verksamhet som är av allvarlig eller omfattande karaktär och bedrivs i organiserad form eller systematiskt av en grupp individer. Lagen innebär en skyldighet att inom ramen för sådan samverkan lämna uppgift till en annan myndighet om det behövs för den mottagande myndighetens deltagande i samverkan. Endast myndigheter som regeringen bestämmer ska vara skyldiga att lämna eller ska få ta emot uppgifter enligt lagen (3 §).

Det behövs bättre förutsättningar för informationsdelning inom NCSC

FRA ska enligt 4 § NCSC-förordningen organisera, leda och planera verksamheten som bedrivs inom ramen för NCSC (se även avsnitt 4.2). FRA ska enligt samma paragraf också samverka med samverkansmyndigheterna i den verksamhet som bedrivs inom centret. Enligt 5 § NCSC-förordningen ska samverkansmyndigheterna, inom ramen för sina respektive befintliga ansvarsområden, löpande bistå NCSC med kunskap, kompetens och information. NCSC ska vidare löpande bistå samverkansmyndigheterna med kunskap och information. Vid ett antagonistiskt cyberhot eller 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 i syfte att förbättra samordningen mellan myndigheterna och bidra till att effektivisera myndigheternas arbete med att hantera cyberhotet eller incidenten.

Den informationsdelning som sker vid samverkan inom NCSC kan, enligt vad utredningen anger, bland annat omfatta följande typer av uppgifter:

- Teknisk information. Uppgifter om tekniska detaljer när det gäller cyberhot eller incidenter (till exempel ip-adresser).
- Taktisk information. Uppgifter om taktiska detaljer när det gäller cyberhot och cyberfenomen (till exempel mål och motiv).
- Strategisk information. Uppgifter om strategiska detaljer när det gäller cyberhot (till exempel förslag på åtgärder).
- Operativ information. Uppgifter om detaljer när det gäller cyberhot (till exempel status för pågående attacker).
- Aktörsinformation. Uppgifter om aktörer (till exempel deras modus).
- Säkerhetsinformation. Uppgifter om säkerhetsåtgärder och rekommendationer.

- Kontextuell information. Uppgifter om kontexten kring cyberhot och cyberfenomen (till exempel uppgifter om pågående händelser och trender).

Informationsdelning kan också enligt utredningen behöva ske i mer strategiska frågor som exempelvis rör olika former av EU-arbete, drabbade målgrupper samt organisations- och samhällskonsekvenser. Även information om digital infrastruktur kan behöva delas mellan FRA och samverkansmyndigheterna. På samhällsnivå kan det även handla om att dela information om vilka aktörer som är samhällsviktiga, kontaktuppgifter till dessa och vilka lösningar de använder, i syfte att FRA inom ramen för centret ska kunna identifiera vilka aktörer som befinner sig i riskzonen för exempelvis cyberhot.

Det finns, som utredningen anför, flera omständigheter som kan utgöra eller upplevas utgöra hinder för informationsutbyte mellan myndigheter. Det kan handla om uppgifter som inte är sekretessreglerade, men där skillnader i myndighetskulturer och uppdrag medför att det är svårt att dela information. Det kan också röra sig om uppgifter som är sekretessreglerade och där tjänstepersoner är, eller upplever sig vara, förhindrade att lämna ut information.

Riksrevisionen har tidigare granskat hur regeringen arbetar för att stärka Sveriges informations- och cybersäkerhet. Riksdagen överlämnade rapporten Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig (RiR 2023:8) till regeringen i april 2023. Riksrevisionen har bland annat rekommenderat regeringen att identifiera hinder för informationsutbyte och se till att det finns strukturer som medger det informationsutbyte som är nödvändigt mellan myndigheter, såväl som mellan det offentliga och det privata, för att arbetet med samhällets informations- och cybersäkerhet ska fungera effektivt. När det gäller informationsdelningen inom NCSC lyfter utredningen bland annat 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. Denna omständighet har också lyfts fram i flera lagstiftningsärenden (se bland annat prop. 2024/25:65). Ofta påpekas att ett utökat uppgiftslämnande inte enbart uppnås genom att utöka de rättsliga förutsättningarna för att dela information.

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, som utredningen anger, 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. Som exempel kan nämnas uppgifter som omfattas av utrikessekretess enligt 15 kap. 1 § OSL eller försvarssekretess enligt 15 kap. 2 § samma lag. En annan typ av uppgifter är sådana som faller inom

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 sekretess enligt 18 kap. OSL kan förekomma, till exempel underrättelsesekretess enligt 18 kap. 2 § OSL eller sekretess avseende säkerhets- eller bevakningsåtgärd enligt 18 kap. 8 § OSL. Det kan även röra sig om uppgifter som omfattas av sekretess i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt (se 30 kap. 23 § OSL och 9 § offentlighets- och sekretessförordningen [2009:641] [OSF]). Det kan även 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. Ytterligare en typ av uppgifter är sådana som omfattas av tillämpningsområdet för den bestämmelse som föreslås införas i avsnitt 5.2 och som skulle innebära sekretess hos FRA i verksamhet vid NCSC för uppgift om enskildas personliga eller ekonomiska förhållanden.

Som *Försvarsmakten* för fram är det visserligen 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 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 (se 10 kap. 15 a § OSL). Bestämmelsen bryter sekretess till skydd för enskilda mellan myndigheter i vissa syften, bland annat 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 ske i andra syften än de som anges i 10 kap. 15 a § OSL.

Informationsutbyte inom ramen för NCSC ska kunna ske rutinmässigt 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 då tanken är att rutinmässigt informationsutbyte i regel ska vara författningsreglerat bedömer regeringen, i likhet med utredningen, att generalklausulen i 10 kap. 27 § OSL inte är en lämplig reglering för informationsutbytet mellan FRA och samverkansmyndigheterna.

Enligt regeringen utgör inte heller 10 kap. 2 § OSL, som Försvarsmakten pekar ut som en möjlig bestämmelse att tillämpa vid informationsutbytet inom NCSC, en ändamålsenlig reglering i sammanhanget. Som anges ovan är bestämmelsen avsedd att tillämpas restriktivt. 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. 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. Det bör i sammanhanget framhållas att 5 § NCSC-förordningen, enligt vilken NCSC och samverkansmyndigheterna löpande ska bistå varandra med information, inte har någon sekretessbrytande verkan (jfr 10 kap. 28 § OSL). Regeringen delar mot den bakgrunden utredningens uppfattning att det finns behov av att införa en tydlig reglering som utökar möjligheterna till informationsutbyte mellan FRA och samverkansmyndigheterna. Frågan om hur en sådan reglering bör utformas behandlas nedan.

Det bör införas en ny lag om uppgiftsskyldighet

En utökad möjlighet att dela information vid samverkan inom NCSC kan formuleras på olika sätt. Ett alternativ är att införa en sekretessbrytande bestämmelse som innebär att en uppgift får lämnas ut. Ett annat alternativ är att införa en uppgiftsskyldighet som innebär att sekretess bryts enligt 10 kap. 28 § OSL.

Regeringen bedömer, i likhet med utredningen, att behovet av informationsdelning vid myndigheternas samverkan inom NCSC bäst tillgodoses genom en uppgiftsskyldighet. En sådan reglering innebär en presumtion för att information ska delas och bör vara enklare att tillämpa för de enskilda tjänstemän som ska pröva om en uppgift ska lämnas ut eller inte. Till skillnad från en sekretessbrytande bestämmelse kan en uppgiftsskyldighet också omfatta uppgifter som inte är sekretessbelagda och därmed bidra till att undanröja sådana hinder för informationsdelning mellan myndigheterna som inte är hänförliga till sekretess. En uppgiftsskyldighet kan vidare få en mer handlingsdirigerande effekt än en sekretessbrytande bestämmelse. Sammantaget bedömer därför regeringen, i likhet med utredningen, att en uppgiftsskyldighet kan förväntas leda till en mer effektiv och utvecklad samverkan än en sekretessbrytande bestämmelse. Eftersom en uppgiftsskyldighet kan förenas med en så kallad ventil bör, som utredningen poängterar, skillnaden i förhållande till en sekretessbrytande bestämmelse inte heller överdrivas.

Ett införande av en uppgiftsskyldighet kan innebära risker för den personliga integriteten. Sekretess mellan myndigheter syftar i första hand till att värna om enskildas integritet och en utgångspunkt är att information som omfattas av sekretess inte ska vidarebefordras utanför den verksamhet i vilken den har hämtats in. Det finns dock ett stort värde i att NCSC kan utföra sitt uppdrag så effektivt som möjligt och vara en nationell plattform för samverkan och informationsutbyte rörande cybersäkerhet.

Det bör därtill noteras att syftet med en uppgiftsskyldighet inte är att myndigheterna ska samla in fler uppgifter om enskilda. De uppgifter som ska kunna delas är sådana som redan finns hos en myndighet. Den uppgiftsskyldighet som föreslås av utredningen är vidare tydligt avgränsad och ger, som framgår nedan, berörda myndigheter möjlighet att avstå från att lämna uppgifter efter en intresseavvägning. Härigenom skapas en reglering som kan upprätthålla balansen mellan behovet av informationsutbyte och skyddet för den personliga integriteten. En mer utförlig analys av förslagets konsekvenser för den personliga integriteten finns i avsnitt 8.3. Enligt regeringen är förslaget om införandet av en uppgiftsskyldighet

sammantaget proportionerligt och motiverat i förhållande till samhällsintresset av att NCSC kan bedriva ett så effektivt arbete som möjligt.

Sammantaget bör det införas en uppgiftsskyldighet kopplat till NCSC:s verksamhet. Regeringen bedömer, i likhet med utredningen men i motsats till bland annat *Försvarsmakten*, att uppgiftsskyldigheten av tydlighetsskäl och med hänsyn till rättssäkerhetsaspekter bör regleras i en särskild lag. En sådan reglering bör även underlätta för tillämpare av uppgiftsskyldigheten.

Vilka myndigheter bör omfattas av uppgiftsskyldigheten? Och i vilket sammanhang bör den gälla?

I fråga om vilka myndigheter som bör omfattas av uppgiftsskyldigheten och hur skyldigheten bör avgränsas i övrigt bedömer regeringen, i likhet med utredningen och *FMV*, att den bör gälla när samverkan sker mellan myndigheter inom NCSC. Som utredningen anför framstår det inte som lämpligt att i lagen hänvisa till NCSC-förordningen i någon del, varken i fråga om vilka myndigheter som omfattas av uppgiftsskyldigheten eller genom att till exempel knyta uppgiftsskyldigheten till vissa arbetsuppgifter som framgår av NCSC-förordningen.

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 bland annat förändrade ansvarsområden, men även omvärldsutvecklingen. Som utredningen föreslår bör det därför av den föreslagna lagen endast framgå att uppgiftsskyldigheten gäller för de myndigheter som regeringen bestämmer.

Att uttryckligen knyta uppgiftsskyldigheten till vissa av NCSC:s uppgifter enligt NCSC-förordningen skulle enligt regeringens bedömning medföra risk för osäkerhet vad gäller sekretessgenombrottets omfattning. En alltför snäv avgränsning av uppgiftsskyldighetens tillämpningsområde riskerar också att leda till att den föreslagna lagen inte innebär den effektivisering av informationsutbytet som behövs kopplat till NCSC:s verksamhet. Med ett krav på att det ska röra sig om samverkan inom NCSC begränsas samtidigt 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. Andra myndigheter som på olika sätt samarbetar med FRA och samverkansmyndigheterna träffas inte av uppgiftsskyldigheten. Uppgiftsskyldigheten gäller inte heller om FRA och samverkansmyndigheterna skulle samarbeta i andra sammanhang än inom ramen för centrets verksamhet.

Lagrådet anser att lagtexten och författningskommentaren ger intryck av att samverkansmyndigheterna är inordnade i NCSC och att lagen endast reglerar samverkan mellan dessa myndigheter sinsemellan. Enligt Lagrådet bör lagtexten förtydligas så att det framgår att samverkansmyndigheterna inte är en del av centret och alltså inte en del av FRA. Regeringen har förståelse för denna synpunkt och bedömer att vissa justeringar bör göras i den föreslagna lagen i förhållande till lagråds-

remissens förslag för att undvika att paragrafen tolkas på sådant sätt. Att samverkan enligt lagen avser såväl samverkan mellan FRA och en samverkansmyndighet, som samverkansmyndigheter sinsemellan kan, som Lagrådet anför, tydliggöras i författningskommentaren.

Enligt 3 § LUS ska endast myndigheter som regeringen bestämmer vara skyldiga att lämna eller få ta emot uppgifter enligt den lagen. Enligt 3 § förordningen (2016:775) om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet (LUS-förordningen) får, utöver de myndigheter som anges i 2 § samma förordning, en åklagarmyndighet ta emot uppgifter enligt LUS. Uppgiftsskyldigheten enligt den nya lagen bör enligt regeringen som utgångspunkt gälla för samtliga myndigheter som deltar i samverkan inom NCSC utan åtskillnad. Syftet med den nya lagen är att underlätta informationsdelningen vid samverkan inom NCSC och skapa förutsättningar för NCSC att bedriva en effektiv verksamhet. För att uppnå detta syfte behöver myndigheterna ha en enhetlig lagstiftning att tillämpa. Uppgiftsskyldigheten bör därför gälla oavsett vilken av myndigheterna som förfogar över uppgiften och oavsett vilken typ av sekretess som gäller för uppgiften (jfr dock nedan om exempelvis 15 kap. 1 a § OSL). En sådan enhetlig utformning kan förväntas skapa tydligare praxis kring vilka uppgifter som kan och bör delas vid samverkan inom NCSC. Det bör dock, av flexibilitetsskäl och på samma sätt som i LUS, vara möjligt för regeringen att bestämma att en enskild myndighet endast ska få ta emot uppgifter enligt den nya lagen. Detta bör framgå av lagen.

Det finns enligt regeringens bedömning inte något skäl att avstå från att ge *Säkerhetspolisen* en uppgiftsskyldighet så som myndigheten gör gällande. Det kan i sammanhanget konstateras att Säkerhetspolisen redan i dag har en uppgiftsskyldighet enligt LUS (se 2 § LUS-förordningen). Dessutom föreslås, som framgår 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 inte heller anledning att undanta Försvarsmakten.

Skyldigheten att lämna en uppgift till en annan myndighet bör endast gälla om den mottagande myndigheten har ett behov av uppgiften för att delta i samverkan. Som utredningen anför uppnås därigenom en balans mellan ett effektivt informationsutbyte och skyddet för den personliga integriteten. Uppgifter bör vidare kunna lämnas ut med stöd av uppgiftsskyldigheten dels efter begäran, dels på eget initiativ. Uppgiftsskyldigheten inträder, vid genomförandet av detta förslag, först när det kan konstateras att det finns ett visst behov av uppgiften och övriga förutsättningar för utlämnande av uppgifter är uppfyllda. På så sätt säkerställs, vilket *Sveriges advokatsamfund* efterfrågar, att personuppgifter inte utväxlas i onödan. Om det uppstår tveksamheter kring vilka uppgifter som behövs hos mottagaren får det förutsättas att FRA och samverkansmyndigheterna samverkar med varandra så att endast relevanta uppgifter lämnas över. Detta är också viktigt eftersom myndigheterna måste förhålla sig till principen om uppgiftsminimering som följer av artikel 5.1 c i 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) (EU:s dataskyddsförordning), eller i förekommande fall av de för-

fattningar som särskilt reglerar personuppgiftsbehandling för FRA och vissa av samverkansmyndigheterna. Enligt denna princip krävs det att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Frågor om personuppgiftsbehandling behandlas i övrigt i avsnitt 5.3 och 6.

Det bör ske en intresseavvägning

Det finns, med hänvisning till utvecklingen på cybersäkerhetsområdet som beskrivs i avsnitt 4.1, starka skäl för att NCSC ska kunna bedriva sin verksamhet på ett effektivt sätt. Detta förutsätter i sin tur ett välfungerande informationsutbyte. Samtidigt kan uppgifter som är sekretessreglerade vara känsliga och av olika anledningar särskilt skyddsvärda. Som utredningen föreslår bör uppgiftsskyldigheten därför utformas så att det finns en möjlighet att i varje enskilt fall beakta intressen som talar för att en uppgift inte ska lämnas ut. Intresseavvägningen bör uttryckas som att det ska krävas att 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. På så sätt finns det möjlighet att hemlighålla såväl skyddsvärda uppgifter om enskilda som skyddsvärda uppgifter om en myndighets verksamhet. En liknande ventil finns i exempelvis 7 § första stycket lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna.

Den föreslagna utformningen innebär att utgångspunkten för intresseavvägningen är det sekretessintresse som bestämmelsen avser att skydda och att intresseavvägningen blir fristående från tillämpningen av OSL. Den menbedömning som vanligtvis görs vid tillämpningen av en sekretessbestämmelse ersätts alltså av intresseavvägningen. En viss nackdel med en sådan reglering är visserligen att det krävs en intresseavvägning även i de fall då sekretess för uppgiften inte gäller i det enskilda fallet. Det innebär i sin tur att prövningen – när fråga är om utlämnande på eget initiativ – kan resultera i att en skyldighet att lämna ut en uppgift inte föreligger trots att uppgiften i det enskilda fallet inte omfattas av sekretess. Om intresseavvägningen förutsätter att man redan har konstaterat att sekretess gäller i det enskilda fallet riskerar regleringen emellertid att bli ytterligare ett steg i den prövning som ska göras vid ett utlämnande, i stället för att bidra till en enklare och mer enhetlig tillämpning. Regeringen delar utredningens uppfattning att risken i sådana fall är stor att lagstiftningen blir kontraproduktiv i förhållande till syftet, som är att underlätta informationsutbytet mellan myndigheterna. Som utredningen framhåller hindrar inte heller den föreslagna regleringen av uppgiftsskyldigheten att en uppgift, som inte omfattas av sekretess, lämnas ut med stöd av bestämmelserna i OSL. Om en myndighet har begärt ut uppgiften föreligger då i stället en skyldighet att lämna ut uppgiften enligt 6 kap. 5 § OSL.

Det är, med den föreslagna utformningen, 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. Bedömningen av om en uppgift

ska lämnas ut bör kunna göras utifrån det behov av sekretess som typiskt sett finns för en viss kategori av uppgifter (se till exempel prop. 2024/25:180 s. 44). Intresseavvägningen hindrar inte heller ett rutinmässigt utlämnande av en större mängd uppgifter. Det är dock viktigt att myndigheterna tar fram lämpliga former för att se till att endast relevanta uppgifter utbyts.

Exempel på uppgifter som ofta skyddas av sekretess och som det kan finnas starka skäl att inte lämna ut kan vara uppgifter om metoder, förmågor, namn på uppdragsgivare och liknande uppgifter som skyddas av utrikessekretess eller försvarssekretess. Även uppgifter som skyddas av underrättelsesekretess skulle, beroende på omständigheterna i det enskilda fallet, kunna hänföras till denna kategori. Det kan också vara fråga om uppgifter om en myndighets egna säkerhets- och bevakningsåtgärder. Samtidigt som det är viktigt att berörda myndigheter kan utbyta relevant information och samverka inom ramen för NCSC:s verksamhet får, i linje med vad *Säkerhetspolisen* anför, informationsutbytet inte inskränka en myndighets möjlighet att utföra sitt primära uppdrag. Ytterligare exempel på situationer där det är möjligt att avstå från ett utlämnande kan vara då ett utlämnande av en viss uppgift framstår som mycket olämpligt, exempelvis när det är fråga om känsliga personuppgifter. Sekretessens styrka – alltså skaderekvisitets utformning – kan ge ledning vid intresseavvägningen. Ett omvänt skaderekvisit kan tala för att uppgifterna är mer skyddsvärda än ett rakt skaderekvisit. Sekretessens föremål ska emellertid också beaktas. Med detta avses vilken typ av uppgift det är fråga om och hur skyddsvärd uppgiften är i den konkreta situationen. En uppgift som lagstiftaren tidigare har bedömt ska omfattas av sekretess med omvänt skaderekvisit kan i det enskilda fallet utgöra en relativt harmlös uppgift, om den exempelvis är offentlig i något annat sammanhang.

Vid intresseavvägningen bör också sekretesskyddet hos den mottagande myndigheten vägas in i bedömningen. Om uppgiften får ett svagare sekretesskydd hos den mottagande myndigheten kan intresseavvägningen utmynna i att en uppgift inte lämnas ut. En omständighet som i det sammanhanget kan få betydelse för intresseavvägningen är reglerna om partsinsyn. Dessa kan innebära att sekretessen hos mottagaren kan få ge vika för en parts rätt till insyn i handläggningen av ett mål eller ärende.

FRA anser att det bör beaktas vid intresseavvägningen 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 myndigheten 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. Som intresseavvägningen är formulerad enligt utredningens förslag finns dock inget utrymme för att ta hänsyn till att uppgiftslämnande till en myndighet i sig kan upphöra eller på annat sätt påverkas av om utlämnande sker. 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 bland annat det dataskyddsrättsliga regelverket.

Som *FMV* påpekar kan det uppstå situationer där flera samverkansmyndigheter innehar samma information och gör olika bedömningar av om informationen ska lämnas ut. Detta är ofrånkomligt, men det kan förutsättas att viss gemensam praxis utvecklas mellan de samverkande myndigheterna.

Vissa internationella avtal hindrar utlämnande

I OSL finns flera bestämmelser om sekretess enligt internationella avtal. Enligt exempelvis 15 kap. 1 a § OSL gäller sekretess för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, under vissa förutsättningar. Av paragrafen framgår att den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL inte får tillämpas i strid med ett sådant avtal eller en sådan rättsakt. Liknande bestämmelser om internationella avtal finns även i exempelvis 27 kap. 5 § och 34 kap. 4 § OSL. Den uppgiftsskyldighet som nu föreslås bryter således inte sekretess för sådana uppgifter.

Förslaget är förenligt med regeringsformens skydd mot betydande intrång i den personliga integriteten

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden, Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är enligt förarbetena inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp (se prop. 2009/10:80 s. 177).

Genom förslaget om uppgiftsskyldighet möjliggörs att berörda myndigheter får del av fler uppgifter, som kommer från flera olika myndigheter. Det finns en risk att flera olika uppgifter om enskilda kan ge en mer heltäckande bild av en persons livssituation och förehavanden än om uppgifterna hålls åtskilda. Myndigheterna kan också få en mer heltäckande bild av personers förehavanden som indikerar involvering i brottslig verksamhet. Mängden uppgiftskategorier som kan utbytas med stöd av uppgiftsskyldigheten medför en viss integritetsrisk. Det är dock inte fråga om övervakning eller kartläggning av enskildas personliga förhållanden. Den personuppgiftsbehandling som förslaget leder till omfattas därmed inte av 2 kap. 6 § andra stycket regeringsformen.

5.2 En ny sekretessbestämmelse för FRA

Regeringens förslag

Det ska föras in en ny sekretessbestämmelse i offentlighets- och sekretesslagen om att sekretess ska gälla 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 ska inte gälla i ärenden om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

För uppgift 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.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att sekretessen inte ska gälla i ärende om stöd enligt förordningen om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller har inga synpunkter på förslaget. *Försvarets radioanstalt (FRA)* framhåller förslaget som viktigt för att det nationella cybersäkerhetscentrets (NCSC) verksamhet ska kunna bedrivas på ett optimalt sätt. *Säkerhetspolisen*, som tillstyrker förslaget, ser ett behov av att sekretessbestämmelsen även blir tillämplig för samverkansmyndigheterna. *Säkerhets- och försvarsföretagen* och *Teknikföretagen* understryker betydelsen av att affärshemligheter och känslig teknisk information skyddas och framhåller att ett offentliggörande av information om cyberincidenter i vissa fall kan skada enskilda företag och orsaka negativa ekonomiska konsekvenser.

Försvarshögskolan anser att utredningen saknar perspektivet att cybersäkerhet i vissa fall bäst gagnas av att information offentliggörs och anför att regleringen av offentlighet och sekretess inom NCSC:s verksamhet bör möjliggöra offentlighet när det gagnar säkerheten bäst. *Svenska Journalistförbundet (Journalistförbundet)* och *Tidningsutgivarna (TU)* avstyrker förslaget med motiveringen att det finns ett stort insynsintresse i NCSC:s verksamhet och att förslaget risker att få en effekt motsvarande absolut sekretess. Enligt Journalistförbundet och TU är det inte heller motiverat med en sekretessperiod om sjuttio år. Vad avser förslaget kopplat till meddelarfriheten anser Journalistförbundet och TU att skälen för att inskränka denna inte är tillräckliga.

Sveriges advokatsamfund ifrågasätter varför ärenden om stöd enligt förordningen om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning undantas och föreslår att bestämmelsen justeras på ett sätt som innebär sekretess när övervägande skäl talar för att sekretessintresset ska ges företräde.

Skälen för regeringens förslag

Krav på konfidentialitet och anonymitet i NIS 2-direktivet

Syftet med NIS 2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen (se vidare prop. 2025/26:28 s. 34 f.).

Varje medlemsstat ska enligt artikel 8 i direktivet utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för vissa tillsynsuppgifter samt utse eller inrätta en gemensam kontaktpunkt. Varje medlemsstat ska vidare enligt artikel 10 i NIS 2-direktivet utse eller inrätta en eller flera enheter för hantering av it-säkerhetsincidenter, så kallade CSIRT-enheter.

Av artikel 12.1 i NIS 2-direktivet framgår bland annat att medlemsstaterna ska säkerställa att fysiska eller juridiska personer kan, anonymt om de så begär, rapportera en sårbarhet till den CSIRT-enhet som har utsetts till samordnare för den samordnade delgivningen av information om sårbarheter. Det rör sig om en möjlighet till frivillig och, om så begärs, anonym rapportering av sårbarheter. Den CSIRT-enhet som har utsetts till samordnare ska enligt samma artikel säkerställa att skyndsamma uppföljningsåtgärder vidtas med avseende på den rapporterade sårbarheten och säkerställa anonymiteten för den fysiska eller juridiska personen som rapporterar sårbarheten. Kravet på att CSIRT-enheten ska kunna säkerställa anonymiteten för den som rapporterar sårbarheter innebär att det behöver finnas ett adekvat skydd för uppgifter som lämnas.

Artikel 23 i NIS 2-direktivet reglerar rapporteringsskyldighet när det gäller betydande incidenter. Enligt artikel 23.6 ska, när så är lämpligt och särskilt om den betydande incidenten berör två eller flera medlemsstater, CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa (Europeiska unionens cybersäkerhetsbyrå) om den betydande incidenten. Sådan information ska åtminstone inbegripa viss typ av information som har mottagits. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

I artikel 30 i NIS 2-direktivet, som gäller frivillig underrättelse om relevant information, anges att medlemsstaterna ska säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23, kan lämnas in till CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna, på frivillig basis av väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud. Underrättelser ska även kunna lämnas av andra entiteter oberoende av om de omfattas av direktivet eller inte, vad gäller betydande incidenter, cyberhot och tillbud.

Vad som avses med cyberhot och betydande incident regleras i artiklarna 6.10 och 23.3 i NIS 2-direktivet. Med tillbud avses enligt artikel 6.5 en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod. Det anges vidare i artikel 30 att CSIRT-enheterna och i tillämpliga fall de behöriga myndigheterna vid behov ska informera de gemensamma kontaktpunkterna om underrättelser som har mottagits i enlighet med artikeln och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt.

NIS 2-direktivet har i huvudsak genomförts i Sverige genom cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507) som trädde i kraft den 15 januari 2026. I förarbetena till cybersäkerhetslagen lämnade regeringen flera förslag och gjorde flera överväganden gällande sekretess kopplat till genomförandet av direktivet (se prop. 2025/26:28 s. 194 f.). I cybersäkerhetslagen används uttrycket verksamhetsutövare i stället för uttrycket entitet som används i NIS 2-direktivet.

Det infördes genom förslagen i propositionen som gäller cybersäkerhetslagen bland annat en ny sekretessbestämmelse i OSL, 18 kap. 8 b §, så att sekretess gäller för uppgift i en incidentrapport som lämnas enligt cybersäkerhetslagen samt för uppgift om vilka åtgärder som verksamhetsutövaren har vidtagit till följd av en incident. Sekretessen kan även omfatta vem som har lämnat in en sådan rapport. Sekretessen tar sikte på incidentrapportering enligt artikel 23 i NIS 2-direktivet men gäller däremot inte för uppgifter som lämnas inom ramen för en frivillig underrättelse enligt artikel 30 (se prop. 2025/26:28 s. 203). Sekretess gäller enligt paragrafen om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas. Sekretessen gäller i högst fyrtio år. Rätten att meddela och offentliggöra uppgifter har, genom en ändring av 18 kap. 19 § OSL, inte företräde framför den tystnadsplikt som följer av sekretessen. Genom förslagen i propositionen fördes det även in en ny bestämmelse i OSL, 15 kap. 3 c §, som gäller sekretessen i det internationella samarbetet. Regeringen föreslår en viss ändring av paragrafen i propositionen Explosiva varor – förbättrade möjligheter till kontroll som beslutades den 12 februari 2026 (se vidare prop. 2025/26:123).

Incidentrapportering enligt 2 kap. 5–8 §§ cybersäkerhetslagen ska göras till CSIRT-enheten enligt 31 § cybersäkerhetsförordningen (6 § cybersäkerhetsförordningen). CSIRT-enhetens uppgifter framgår i övrigt av bland annat 32 och 33 §§ cybersäkerhetsförordningen. Den gemensamma kontaktpunktens uppgifter regleras i samma förordning (se bland annat 24 §). Myndigheten för civilt försvar (MCF) är i dag både CSIRT-enhet och gemensam kontaktpunkt enligt NIS 2-direktivet. Vilka myndigheter som är Sveriges behöriga myndigheter, det vill säga tillsynsmyndigheter, framgår också av cybersäkerhetsförordningen. Det rör sig om Statens energimyndighet, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket, Läkemedelsverket, Post- och telestyrelsen, Transportstyrelsen och ett antal länsstyrelser.

Vilka uppgifter lämnas och kommer att lämnas till FRA?

Som nämns i avsnitt 4.2 har regeringen gett FRA i uppdrag att förbereda för att ta över uppgiften att vara CSIRT-enhet och gemensam kontaktpunkt från MCF. FRA kommer i egenskap av CSIRT-enhet, utöver att ta emot incidentrapporter, även att få del av uppgifter om sårbarheter, betydande incidenter, cyberhot och tillbud i enlighet med artiklarna 12 och 30 i NIS 2-direktivet. Det kan röra sig om uppgifter om namn, kontaktuppgifter och ip-adresser, men även mer indirekta uppgifter som skulle kunna användas för att ta reda på vem rapportören är.

NCSC har, som anges i avsnitt 4.2, ett brett uppdrag. Centret ska vara en kontaktpunkt för samverkan med bland annat privata aktörer. NCSC ska också exempelvis lämna råd och stöd till privata aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet samt vid it-incidenter. Centret ska därutöver genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet.

En stor mängd uppgifter om enskilda av varierande slag kan komma att behandlas i den verksamhet som bedrivs av FRA inom ramen för NCSC. Det kan, som utredningen nämner, röra sig om uppgifter som avslöjar ekonomiska förhållanden, förhållanden av betydelse för konkurrenssituationen och säkerhetshöjande åtgärder eller andra uppgifter kopplat till den verksamhet som bedrivs av aktören. Utredningen nämner även att uppgifter som lämnas vid rapportering av sårbarheter kan avslöja en företrädares etniska ursprung, politiska åskådning eller religiösa tillhörighet. Som utredningen anger kan också uppgifter om användarnamn och e-postadresser innehålla känsliga personuppgifter.

Informationsdelningen med näringslivet behöver utvecklas

I Riksrevisionens rapport Regeringens styrning av samhällets informations och cybersäkerhet – både brådskande och viktig (RiR 2023:8) har Riksrevisionen rekommenderat att hinder för informationsutbyte identifieras och att regeringen ser till att det finns strukturer som medger nödvändigt informationsutbyte mellan myndigheter, såväl som mellan det offentliga och det privata, för att arbetet med samhällets informations- och cybersäkerhet ska fungera effektivt.

Företrädare för näringslivet har till utredningen framhållit bristen på återkoppling från myndigheter som problematisk. Enskilda företag kan lämna information om till exempel sårbarheter till myndigheter, men får inte veta hur informationen tas om hand. Det skapar också en oro kring hur informationen sprids.

Regeringen har tidigare uttryckt att privat-offentligt samarbete kring cybersäkerhetsincidenter behöver utvecklas och nyttja den incidenthanteringskompetens som finns i privat sektor. Outvecklat och bristande samarbete mellan det privata och offentliga, såväl nationellt som internationellt, utgör en sårbarhet. Det finns också en strävan mot att NCSC ska ha väletablerade metoder för internationellt och privat-offentligt samarbete (se skr. 2024/25:121 s. 24). För att nå fram till ett sådant läge är det av stor vikt att privata aktörer vågar dela med sig av information om exempelvis sårbarheter och säkerhetshöjande åtgärder till FRA och inte undanhåller viktig information av rädsla för att uppgifterna ska spridas vidare eller utnyttjas i konkurrenssyfte.

Relevanta sekretessbestämmelser utöver 18 kap. 8 b § OSL

Enligt 2 kap. 2 § tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, till exempel rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation, myndigheters verksamhet för inspektion, kontroll eller annan tillsyn, intresset av att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden. En sådan begränsning ska anges noga i en bestämmelse i en

särskild lag eller, om det i ett visst fall anses lämpligare, i en annan lag som den särskilda lagen hänvisar till. Efter bemyndigande i en sådan bestämmelse får regeringen genom förordning meddela närmare föreskrifter om bestämmelsens tillämplighet. Den särskilda lagen är OSL och regeringen har meddelat närmare föreskrifter i OSF. Av 3 kap. 1 § OSL framgår att sekretess i lagen avser ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

I 18 kap. 8 § OSL regleras sekretess för säkerhets- eller bevakningsåtgärd. Sekretessen gäller enligt paragrafens tredje punkt bland annat för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information.

Med ordet telekommunikation avses i paragrafen överföring av meddelande med tråd, radio eller en liknande metod. Med uttrycket system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka eller distribuera information. Sekretessen avser bland annat att skydda funktioner för användning av lösenord, loggning och kryptering, installation och konfigurering av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord eller bevakning av loggar och larm.

Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas. Vidare kan till exempel inte kostnader för införskaffande och installation av ett datorsystem hemlighållas med stöd av bestämmelsen, även om uppgifter i en faktura om vilken typ och/eller version av system som har införskaffats kan komma att hemlighållas (se prop. 2003/04:93 s. 88 och 89).

Enligt 30 kap. 23 § OSL och 9 § OSF gäller sekretess, i den utsträckning som anges i bilagan till förordningen, i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för bland annat uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. I bilagan till OSF anges dels vad aktuell verksamhet består i, dels vilka särskilda begränsningar i sekretessen som gäller. Med affärs- och driftförhållanden avses förvärv, överlåtelse, upplåtelser eller användning av egendom, tjänster eller annat, till exempel elektricitet, gas, vatten eller värme. Hit räknas också affärshemligheter av mera allmänt slag som marknadsundersökningar, marknadsplaneringar, prissättningskalkyler och planer rörande reklamkampanjer.

En ny sekretessbestämmelse till skydd för uppgifter om enskilda bör införas

De befintliga sekretessbestämmelser som är av störst intresse vid bedömningen av behovet av en ändrad sekretessreglering i detta sammanhang är 18 kap. 8 § 3 och 8 b § OSL. I förarbetena till cybersäkerhetslagen

gjorde regeringen bland annat bedömningen att det saknas ett ändamålsenligt sekretesskydd för uppgifter med koppling till en incidentrapport som har sin grund i artikel 23 i NIS 2-direktivet, både med beaktande av 18 kap. 8 § 3 OSL och övrig sekretessreglering (se prop. 2025/26:28 s. 194 f.). Skaderekvisitet i 18 kap. 8 § 3 OSL innebär att sekretess gäller om det kan antas att syftet med åtgärden motverkas om uppgiften röjs. Bestämmelsens syfte är inte att skydda enskilda intressen.

18 kap. 8 b § OSL omfattar inte uppgifter som lämnas inom ramen för en frivillig underrättelse enligt artikel 30 i NIS 2-direktivet (se prop. 2025/26:28 s. 203). Regeringen bedömer vidare, som utredningen, att varken 18 kap. 8 b § OSL eller övrig sekretessreglering ger ett tillräckligt skydd för uppgifter som lämnas inom ramen för en anonym sårbarhetsrapport enligt artikel 12 i NIS 2-direktivet. Vid en sådan rapportering är det visserligen inte möjligt att genom sekretessreglering skydda en anmälares identitet i förhållande till CSIRT-enheten. Denna fråga kan i stället hanteras på andra sätt och till exempel genom olika tekniska lösningar som finns tillgängliga i samband med en anmälan. Precis som vid en frivillig underrättelse behöver det dock finnas ett skydd för uppgifter som riskerar att avslöja vem som har rapporterat en sårbarhet i förhållande till utomstående. Det kan röra sig om uppgifter om namn, kontaktuppgifter och ip-adresser, men även mer indirekta uppgifter som skulle kunna användas för att ta reda på vem rapportören är.

Som utredningen nämner finns det alltså ett behov av att kunna skydda både sådana uppgifter som lämnas kopplat till artiklarna 12 och 30 i NIS 2-direktivet, men även andra uppgifter om enskilda som lämnas till FRA genom NCSC med anledning av centrets uppdrag. Det finns därför behov av att ta ställning till om det krävs en ny sekretessbestämmelse.

När en ny sekretessbestämmelse övervägs ska det alltid göras en avvägning mellan sekretessintresset och insynsintresset (se prop. 1979/80:2 Del A s. 75 f.). Utredningen anför att det kan finnas ett intresse av insyn i NCSC:s verksamhet bestående i att enskilda vill få reda på om det föreligger sårbarheter i olika it-system för att på så sätt själva kunna vidta säkerhetsåtgärder, men att allmänintresset av att få del av uppgifter om enskilda som förekommer hos NCSC torde vara lågt. Utredningen bedömer vidare att insynsintresset utifrån att allmänheten ska kunna granska centrets verksamhet är relativt begränsat avseende den stora del av verksamheten som inte omfattar myndighetsutövning och ärendehandläggning. Regeringen gör samma bedömning.

Regeringen har förståelse för *Försvarshögskolans* ståndpunkt att cybersäkerheten i vissa fall bäst gagnas av att information offentliggörs. Mot allmänintresset av insyn står dock, som utredningen nämner, bland annat intresset av att undvika situationer där olika typer av uppgifter om sårbarheter, konsekvenser av incidenter samt potentiella hot kan användas för att kartlägga samhällets sårbarheter kopplat till cybersäkerhetsområdet i ett antagonistiskt syfte. Det finns en risk för att enskilda aktörer avstår från att lämna underrättelser och rapportera sårbarheter av rädsla för att uppgifterna kommer att lämnas vidare och potentiellt skada den egna verksamheten. Vidare finns det ett behov av att på ett bättre sätt möta NIS 2-direktivets krav på konfidentialitet rörande frivillig rapportering till FRA genom NCSC. Om sekretess inte gäller för dessa uppgifter finns också risken för att informationsdelningen mellan FRA, i egenskap av CSIRT-

enhet, och CSIRT-enheter i andra EU-medlemsstater försvåras. NCSC har dessutom till uppgift att, utan koppling till NIS 2-direktivet, utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Det finns ett starkt intresse av att uppgifter om enskilda lämnas till FRA genom NCSC givet detta intresse och att uppgifterna skyddas. Ur enskilda aktörers perspektiv är det vidare viktigt även ur bland annat konkurrenshänseende att information om exempelvis arbetssätt som lämnas till FRA genom NCSC inte sprids på ett omotiverat sätt. Ett offentliggörande av information om exempelvis cyberincidenter kan, som *Säkerhets- och försvarsföretagen* och *Teknikföretagen* framhåller, skada enskilda företag och orsaka negativa ekonomiska konsekvenser.

Sammanfattningsvis bedömer regeringen att sekretessintresset väger tyngre än allmänhetens intresse av insyn i NCSC:s verksamhet. Det bör därför, till skillnad från vad *Journalistförbundet* och *TU* anser men i likhet med vad utredningen föreslår, införas en ny sekretessbestämmelse som ger skydd för uppgifter om enskilda som förekommer hos FRA i den verksamhet som bedrivs inom NCSC. Det finns inte utrymme för att inom ramen för denna proposition utöka tillämpningsområdet för regleringen som *Säkerhetspolisen* efterfrågar så att den även omfattar uppgifter som lämnas till samverkansmyndigheterna.

Sekretessbestämmelsens föremål och räckvidd

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, det vill säga förutsättningar för bestämmelsens tillämplighet. Dessa tre rekvisit anger sekretessens föremål, sekretessens räckvidd och sekretessens styrka. Sekretessens föremål är den information som kan hemlighållas och kommer till uttryck i sekretessregleringen genom att ordet uppgift används tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, till exempel uppgift om en enskilds personliga förhållanden. En sekretessbestämmelses räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna endast gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. En uppgift kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den förekommer. Som exempel på en sådan bestämmelse kan nämnas utrikessekretessen i 15 kap. 1 § OSL.

Utredningen föreslår att det ska införas en bestämmelse om att sekretess ska gälla hos FRA i verksamhet som bedrivs inom 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. När det gäller preciseringen av uppgifternas art anger utredningen att skydd för anmälarens identitet inte skulle täckas av en bestämmelse som skyddar uppgifter om enskildas affärs- och driftförhållanden.

Formuleringen uppgift om enskilds personliga respektive ekonomiska förhållanden förekommer i flera sekretessbestämmelser (se till exempel 35 kap. 1 § OSL). Uttrycket enskild avser såväl en fysisk som en juridisk person (se prop. 1979/80:2 Del A s. 329 och prop. 2008/09:150 s. 349).

Uppgifter om en fysisk persons ekonomi kan exempelvis falla in under uttrycket personliga förhållanden (jfr prop. 1979/80:2 Del A s. 84). I uttrycket ekonomiska förhållanden ingår uppgifter om affärs- och driftförhållanden.

Den sekretessbestämmelse som införs behöver bland annat skydda uppgifter som lämnas kopplat till artiklarna 12 och 30 i NIS 2-direktivet på ett liknande sätt som krävdes för genomförandet av artikel 23 i direktivet. Den brist som har uppmärksammats i den nuvarande sekretessregleringen är att uppgifter som kan förekomma i sådana rapporter och underrättelser som lämnas i enlighet med artiklarna och uppgifter om vilka åtgärder som har vidtagits till följd av till exempel tillbud inte alltid kommer att kunna skyddas. Sekretessens föremål bör dock enligt regeringens mening i detta fall inte begränsas till visst uppgiftslämnande på motsvarande sätt som i 18 kap. 8 b § OSL (jfr prop. 2025/26:28 s. 202 f.). Även andra uppgifter om enskilda som lämnas till FRA genom NCSC med anledning av centrets uppdrag, utöver sådana som lämnas kopplat till artiklarna 12 och 30 i NIS 2-direktivet, behöver som utredningen resonerar om skyddas av bestämmelsen. I sistnämnda fall kan det röra sig om uppgifter om enskilda av varierande slag givet centrets breda uppdrag, till exempel uppgifter som avslöjar ekonomiska förhållanden, förhållanden av betydelse för konkurrenssituationen och säkerhetshöjande åtgärder eller andra uppgifter kopplat till den verksamhet som bedrivs av aktören.

För att säkerställa ett ändamålsenligt skydd bedömer regeringen, i likhet med utredningen, att sekretessens föremål bör omfatta uppgifter om en enskilds personliga och ekonomiska förhållanden. När det gäller sekretessens räckvidd delar regeringen utredningens uppfattning att bestämmelsen bör avse verksamhet som bedrivs av FRA vid NCSC. NCSC har visserligen ett brett uppdrag men centrets verksamhet är tydligt avgränsad. Sekretessen kommer vidare endast att gälla hos en enskild myndighet. En mer preciserad räckvidd än den som utredningen föreslår skulle innebära en uppenbar risk för att enskilda undviker att rapportera incidenter och sårbarheter eller undviker att lämna andra slags uppgifter till FRA vid övrig kontakt med NCSC, eftersom det framstår som osäkert om uppgifterna skyddas av sekretess eller inte.

Som utredningen föreslår bör ärenden om stöd enligt förordningen om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning undantas från bestämmelsens tillämpningsområde. Uppgiften att pröva stöd enligt förordningen ingår i den verksamhetsöverföring från MCF till FRA genom NCSC som regeringen har gett myndigheterna i uppdrag att förbereda (se avsnitt 4.2). Någon sekretessbestämmelse särskilt avsedd för tillämpning vid handläggning av ärenden enligt förordningen finns inte i dag. Det har inte framkommit några tydliga skäl för att uppgifter i dessa ärenden ska hemlighållas generellt. Till skillnad från merparten av den verksamhet som FRA genom NCSC ska bedriva rör dessa ärenden prövning av om enskilda ska få ta del av stöd som finansieras av offentliga medel. Det innebär att allmänintresset av insyn är starkt. Regeringen bedömer därför att enskildas intresse av att uppgifter hemlighålls i denna ärendehandläggning inte överväger insynsintresset. Mot denna bakgrund bedömer regeringen att det inte heller är motiverat med en reglering som möjliggör sekretess i ärendehandläggningen när övervägande skäl talar för att sekretessintresset ska ges företräde, så som *Sveriges advokatsamfund*

föreslår. Att ärendehandläggningen undantas från den föreslagna bestämmelsens tillämpningsområde påverkar dock inte tillämpligheten av andra sekretessbestämmelser i OSL. En hänvisning till en förordning i en lagbestämmelse bör undvikas och den av utredningen föreslagna bestämmelsen bör därför omformuleras något. Det bör i stället anges att sekretessen inte ska gälla i ärenden om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

Sekretessens styrka

När det gäller utformningen av sekretessens styrka, är utgångspunkten att inte mer än endast det som är oundgängligen nödvändigt ska sekretessbeläggas för att skydda det intresse som har föranlett bestämmelsen. Detta görs genom skaderekvisit (se prop. 1979/80:2 Del A s. 78 och 79).

Ett rakt skaderekvisit innebär att utgångspunkten är att uppgifterna är offentliga och att sekretess gäller endast om det kan antas att viss skada uppstår. Skadebedömningen ska då kunna göras med utgångspunkt i själva uppgiften, alltså om uppgiften är av den arten att ett utlämnande typiskt sett kan vara ägnat att medföra skada (se prop. 1979/80:2 Del A s. 80).

Ett omvänt skaderekvisit innebär att utgångspunkten är att sekretess gäller, om det inte står klart att uppgiften kan röjas utan skada. Det innebär att varje begäran att få ut uppgifter som omfattas av bestämmelsen ska bedömas ingående. Den som begär ut uppgifter kommer att behöva redogöra för dels sin identitet, dels syftet med begäran. Många gånger kan inte en uppgift lämnas ut utan att tillämparen har kännedom om mottagarens identitet och avsikter med att få del av uppgiften (se prop. 1979/80:2 Del A s. 82). Ett omvänt skaderekvisit innebär dock inte att rätten att ta del av information i ärenden saknas, vilket *Journalistförbundet* och *TU* uttrycker oro för, utan uppgifter kan i det enskilda fallet komma att lämnas ut efter en sekretessprövning.

Intresseavvägningen mellan insynsintresset och skyddsintresset bör spegla det skaderekvisit som ska gälla för de aktuella uppgifterna. Om allmänhetens intresse av insyn väger tyngst bör ett rakt skaderekvisit införas. Om i stället sekretessintresset väger tyngst bör ett omvänt skaderekvisit införas. Sekretessbestämmelsen i 18 kap. 8 b § OSL, som bland annat omfattar uppgifter i incidentrapporter som ska lämnas enligt cybersäkerhetslagen, har ett omvänt skaderekvisit. Som skäl för detta angavs bland annat betydelsen av verksamhetsutövares tilltro till regelverket, den skada som känsliga uppgifter i en incidentrapport kan orsaka om de röjs och svårigheten i att i ett tidigt skede bedöma om uppgifter i incidentrapporter är känsliga, vilket innebär att känsliga uppgifter inledningsvis riskerar att uppfattas som harmlösa (se prop. 2025/26:28 s. 204). Den nu föreslagna regleringens tillämpningsområde är visserligen bredare än tillämpningsområdet för 18 kap. 8 b § OSL. När det gäller anonym sårbarhetsrapportering enligt artikel 12 i NIS 2-direktivet finns det vidare endast krav på möjlighet till anonym rapportering om anmälaren så begär vilket, som utredningen anför, i viss mån talar för att den typen av uppgifter bör omfattas av ett rakt skaderekvisit.

De omständigheter som anges som skäl för det omvända skaderekvisitet i 18 kap. 8 b § OSL gör sig dock även gällande när det handlar om den frivilliga rapportering som ska kunna ske enligt NIS 2-direktivet. Om upp-

gifter om enskilda, särskilt enskildas affärs- och driftförhållanden, sprids kan det göra det möjligt för antagonister att rikta cyberattacker. En risk för spridning av sådana uppgifter kan dessutom ha en hämmande effekt på enskilda aktörers villighet till frivillig rapportering och därmed inverka negativt på cybersäkerheten i stort. Precis som vid incidentrapportering enligt cybersäkerhetslagen kan det dessutom i ett tidigt skede vara svårt att bedöma känsligheten i de uppgifter som lämnas, vilket medför en risk för att känsliga uppgifter inledningsvis riskerar att uppfattas som harmlösa.

Journalistförbundet och TU bedömer att det finns det ett stort intresse av insyn i NCSC:s verksamhet eftersom verksamheten rör frågor kopplade till nationell säkerhet. Regeringen bedömer att det i vissa fall visserligen kan finnas ett journalistiskt intresse av att få ut uppgifter om enskilda kopplade till exempelvis organiserade cyberattacker, men att insynsintresset främst bör röra frågor på en mer allmän nivå om exempelvis förekomsten av cyberhot och cyberattacker. Som utredningen anför torde allmänintresset av att få del av uppgifter om enskilda som förekommer hos NCSC vara lågt. Bestämmelsen bör därmed, som utredningen föreslår, innehålla ett omvänt skaderekvisit.

Sekretesstid och bestämmelsens placering

När det gäller sekretess till skydd för enskildas personliga förhållanden är sekretesstiden i regel bestämd till högst sjuttio år med utgångspunkt i att sekretessen bör gälla under större delen av den enskildes livstid (se prop. 1979/80:2 Del A s. 459, 460, 493 och 494). Sekretessbestämmelser som skyddar uppgifter om affärs- eller driftförhållanden innehåller vanligen en sekretesstid om högst tjugo år (se exempelvis 30 kap. 4, 10 och 11 §§ samt 31 kap. 5 a § och 38 kap. 6 § OSL). Sekretesstiden i 18 kap. 8 b § OSL är bestämd till fyrtio år, vilket är samma sekretesstid som gäller för incidentrapporter i bland annat domstolar enligt 18 kap. 8 a § OSL.

Regeringen delar utredningens uppfattning att uppgifter om enskildas personliga förhållanden inte bör förekomma i stor omfattning hos NCSC. Mot bakgrund av att utgångspunkten är att enskildas personliga förhållanden ska skyddas under sjuttio år bedömer regeringen vidare, i motsats till *Journalistförbundet* och *TU*, att sekretessen bör gälla under så lång tid som utredningen föreslår.

Den nu föreslagna paragrafen syftar till att skydda enskildas personliga och ekonomiska förhållanden i verksamhet vid NCSC. Bestämmelsen är inte lämplig att placera under någon av de befintliga samlade rubrikerna i femte avdelningen i OSL. Det är därför mest lämpligt att placera den, i likhet med vad utredningen föreslår, i 40 kap. som gäller sekretess hos övriga myndigheter och i övriga verksamheter. Bestämmelsen passar dock inte in under någon av de befintliga rubrikerna i kapitlet. Den nya sekretessbestämmelsen bör därför placeras under den nya rubriken ”Verksamhet vid det nationella cybersäkerhetscentret”.

Uppgifter som omfattas av den nya sekretessbestämmelsen kan även falla in under tillämpningsområdet för andra sekretessbestämmelser, såsom 18 kap. 8 § OSL. I förekommande fall får konkurrensfrågor hanteras enligt bestämmelsen i 7 kap. 3 § OSL.

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av allmän handling eller på något annat sätt. Bestämmelserna om sekretess innefattar alltså såväl handlingssekretess som tystnadsplikt. Den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen har som huvudregel företräde framför tystnadsplikten. Utredningen bedömer dock att rätten att meddela och offentliggöra uppgifter inte bör ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen.

Stor återhållsamhet bör iakttas vid prövningen av om det bör göras undantag från rätten att meddela och offentliggöra uppgifter. Redan den omständigheten att en sekretessbestämmelse är försedd med ett omvänt skaderekvisit talar dock i viss utsträckning för att den tystnadsplikt som följer av bestämmelsen bör ha företräde framför rätten att meddela och offentliggöra uppgifter. Sekretessbestämmelsen föreslås vidare inte omfatta den myndighetsutövning som FRA kommer att utföra i ärenden om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning, något som annars hade talat för att meddelarfriheten borde ges företräde (jfr prop. 1979/80:2 Del A s. 111 och 112). I likhet med utredningen, men till skillnad från *Journalistförbundet* och *TU*, anser regeringen därför att rätten att meddela och offentliggöra uppgifter inte bör ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen. Det kan noteras att samma sak gäller i förhållande till såväl 18 kap. 8 § som 18 kap. 8 b § OSL enligt 18 kap. 19 § samma lag.

Av 40 kap. 8 § OSL framgår i vilka fall den tystnadsplikt som följer av en bestämmelse om sekretess i 40 kap. samma lag inskränker rätten att meddela och offentliggöra uppgifter. Den föreslagna bestämmelsen bör läggas till i uppräkningen i enlighet med utredningens förslag.

5.3 Personuppgiftsbehandling och övriga frågor om sekretess

Regeringens bedömning

Det behöver inte införas någon ny sekretessbestämmelse som skyddar uppgifter hos de mottagande myndigheterna med anledning av förslaget om en ny lag om uppgiftsskyldighet.

Det behöver inte införas någon ytterligare reglering av personuppgiftsbehandlingen med anledning av förslagen som rör sekretessregleringen.

Utredningens bedömning

Utredningen gör samma bedömning i fråga om att det inte krävs något ytterligare sekretesskydd för överlämnade uppgifter. Utredningen gör ingen särskild bedömning av om personuppgiftsbehandlingen behöver regleras ytterligare.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt över frågorna.

Skälen för regeringens bedömning

Vilka förslag kan kräva ytterligare reglering?

I avsnitt 6 behandlas frågan om införandet av en ny registerlag för Försvarets radioanstalt (FRA). Förslaget i avsnitt 5.2 om införandet av en ny sekretessbestämmelse innebär inte att det krävs några ytterligare bestämmelser om personuppgiftsbehandling. Frågan är om förslaget i avsnitt 5.1 om införandet av en ny lag om uppgiftsskyldighet innebär att det finns behov av ytterligare personuppgifts- och sekretessreglering.

Uppgiftsskyldigheten föreslås i praktiken gälla för FRA och samverkansmyndigheterna. Samverkansmyndigheterna är i dag Försvarets materielverk, Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen. Vilka myndigheter som ska omfattas av lagen föreslås dock inte regleras i den nya lagen och frågan är därmed inte föremål för behandling i denna proposition. En bedömning måste samtidigt göras i frågan om det finns stöd för den personuppgiftsbehandling som kan aktualiseras för dessa myndigheter med anledning av förslaget.

Kravet på rättslig grund

En grundläggande förutsättning för att behandling av personuppgifter ska vara tillåten enligt EU:s dataskyddsförordning är att behandlingen ryms inom någon av de rättsliga grunder som finns i artikel 6.1.

Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och förordningen (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning kompletterar EU:s dataskyddsförordning. Enligt 2 kap. 1 § dataskyddslagen får personuppgifter behandlas med stöd av artikel 6.1 c i EU:s dataskyddsförordning, om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse som följer av bland annat lag. I 2 kap. 2 § dataskyddslagen anges att personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av till exempel lag eller som ett led i den personuppgiftsansvariges myndighetsutövning enligt lag eller annan författning. Alla uppgifter som riksdagen eller regeringen har gett statliga myndigheter i uppdrag att utföra är av allmänt intresse. Enligt artikel 6.3 i EU:s dataskyddsförordning måste en rättslig förpliktelse vara fastställd i enlighet med unionsrätten eller den nationella rätten för att kunna läggas till grund för behandling av personuppgifter.

EU:s dataskyddsförordning ska inte tillämpas på behandling av personuppgifter som behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2.2 d). På det området gäller i stället det så kallade dataskyddsdirektivet, det vill säga Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer

med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF. Direktivet har genomförts i Sverige genom brottsdatadatalagen (2018:1177) (BDL).

De tillåtna rättsliga grunderna för personuppgiftsbehandling enligt BDL framgår av 2 kap. 1 och 2 §§. BDL kompletteras av de brottsbekämpande myndigheternas registerförfattningar, det vill säga författningar som innehåller särskild reglering om myndigheternas personuppgiftsbehandling. BDL gäller, enligt 1 kap. 4 §, inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen (se vidare lagen [2019:1182] om Säkerhetspolisens behandling av personuppgifter och lagen [2018:1693] om polisens behandling av personuppgifter inom brottsdatalagens område).

Vid Försvarsmaktens behandling av personuppgifter i verksamhet som rör Sveriges försvar och säkerhet samt internationellt försvars- och säkerhetssamarbete gäller lagen (2021:1171) om behandling av personuppgifter vid Försvarsmakten. Vid behandling av personuppgifter enligt den lagen gäller inte EU:s dataskyddsförordning och inte heller dataskyddslagen.

Kravet på ändamål

Utöver krav på rättslig grund måste myndigheter vid personuppgiftsbehandling som omfattas av EU:s dataskyddsförordnings tillämpningsområde även uppfylla de grundläggande principer som framgår av bland annat artikel 5 i EU:s dataskyddsförordning. Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och de får enligt den så kallade finalitetsprincipen inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (jfr även artikel 4.1 b i dataskyddsdirektivet).

Om det i lag eller förordning finns en sekretessbrytande bestämmelse som reglerar att en myndighet ska lämna ut personuppgifter, innebär det att någon särskild prövning enligt finalitetsprincipen inte behöver ske (se till exempel 2 kap. 22 § andra stycket BDL och 2 kap. 4 § andra stycket lagen om Säkerhetspolisens behandling av personuppgifter). I registerförfattningar finns ofta en reglering av tillåtna ändamål för behandling av personuppgifter.

Regleringen om känsliga personuppgifter

Personuppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening eller som på visst sätt rör hälsa, sexualliv eller sexuell läggning utgör känsliga personuppgifter och får som huvudregel inte behandlas (se till exempel artikel 9.1 i EU:s dataskyddsförordning). Det finns en rad undantag från denna huvudregel. Av artikel 9.2 g i EU:s dataskyddsförordning framgår till exempel att förbudet inte gäller om behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till

dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (jfr artikel 10 i dataskyddsdirektivet).

Av 2 kap. 11 § andra stycket BDL framgår att uppgifter om en person som behandlas på annan grund får kompletteras med känsliga personuppgifter, om det är absolut nödvändigt för ändamålet med behandlingen (jfr 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter). Det innebär att om andra uppgifter om en person samlas in i samband med till exempel en förundersökning får de kompletteras med uppgifter om religiös övertygelse eller etniskt ursprung, om det är av betydelse för utredningen. Det kan exempelvis inträffa i en utredning om hets mot folkgrupp. Behovet måste dock prövas noga mot kravet på absolut nödvändighet. Känsliga personuppgifter får även behandlas om det är nödvändigt för diarieföring eller om uppgifterna har lämnats till en behörig myndighet i en anmälan, ansökan eller liknande och behandlingen är nödvändig för myndighetens handläggning (se 2 kap. 2 och 13 §§ BDL).

Förslaget om en ny lag om uppgiftsskyldighet innebär ökad personuppgiftsbehandling

Förslaget i avsnitt 5.1 syftar till att öka informationsflödet mellan FRA och samverkansmyndigheterna. Informationsflödet syftar i sin tur till att förbättra myndigheternas förmåga att bidra till det nationella cybersäkerhetscentrets (NCSC) verksamhet och uppdrag. Informationen som lämnas kan många gånger innehålla personuppgifter. Det ökade informationsflödet kommer därmed att medföra en ökad personuppgiftsbehandling såväl hos den som lämnar information som hos de myndigheter som tar emot den. I de flesta fall är det dock inte fråga om en ny form av personuppgiftsbehandling. Det handlar snarast om att fler uppgifter av samma karaktär kan lämnas ut. Som utredningen framhåller är det förenat med svårigheter att uppskatta den närmare omfattningen av den utökade personuppgiftsbehandling som följer av förslaget.

Det finns rättsligt stöd för den personuppgiftsbehandling som myndigheterna kommer att behöva utföra med anledning av förslaget. Förslaget rör bland annat myndigheter vars personuppgiftsbehandling omfattas av EU:s dataskyddsförordning, till exempel PTS, men även exempelvis Polismyndigheten vars personuppgiftsbehandling omfattas av dataskyddsdirektivet. Syftet med uppgiftsskyldigheten beskrivs i avsnitt 5.1. Det övergripande syftet med den nya lagen är att förbättra myndigheternas möjligheter att utbyta information som de behöver för att fullgöra sina respektive uppdrag kopplat till NCSC. Bestämmelsen möjliggör ett informationsutbyte som krävs för att stärka cybersäkerheten och i förlängningen stärka den brottsbekämpande verksamheten. Det rör sig om uppgifter som är av allmänt intresse.

Den behandling av personuppgifter som är nödvändig för att till exempel PTS ska kunna uppfylla uppgiftsskyldigheten ryms inom den rättsliga grunden i artikel 6.1 e i EU:s dataskyddsförordning och 2 kap. 2 § dataskyddslagen. Eftersom myndigheten skulle omfattas av en uppgiftsskyldighet, kommer personuppgiftsbehandlingen som sker för att fullfölja den även vara nödvändig för att fullgöra en rättslig förpliktelse enligt artikel 6.1 c i EU:s dataskyddsförordning och 2 kap. 1 § dataskyddslagen.

Grunden för behandlingen är vidare fastställd i den nationella rätten på det sätt som krävs enligt artikel 6.3 i EU:s dataskyddsförordning. Medlemsstaternas nationella rätt ska därtill enligt artikel 6.3 b i EU:s dataskyddsförordning uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Myndigheter som tar emot informationen har ett tydligt och stort behov av att få fler uppgifter för att på ett effektivt sätt kunna fullgöra sina uppdrag. De förväntade effekterna av den nya lagen om uppgiftsskyldighet bedöms vara av betydande vikt. Andra mindre ingripande alternativ har övervägts, vilket framgår av avsnitt 5.1. Den reglering av rättsliga grunder som gäller för personuppgiftsbehandlingen för myndigheterna vars personuppgiftsbehandling omfattas av EU:s dataskyddsförordning är tillräcklig och behöver därmed inte kompletteras.

Eftersom personuppgiftsbehandlingen hos Polismyndigheten ska ske för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott, omfattas behandlingen av tillämpningsområdet för BDL. Det finns rättslig grund för den personuppgiftsbehandling som aktualiseras hos Polismyndigheten genom 2 kap. 1 och 2 §§ lagen om polisens behandling av personuppgifter inom brottsdatalagens område. Den utökade personuppgiftsbehandling som kommer att ske som en konsekvens av förslaget syftar till att effektivisera samverkan inom NCSC och i förlängningen Polismyndighetens arbete med att förebygga och bekämpa brott. Ändamålet med behandlingen är alltså brottsbekämpning. Den behandling som skulle aktualiseras för Säkerhetspolisen har stöd i 2 kap. 1 § lagen om Säkerhetspolisens behandling av personuppgifter.

När det i lag eller förordning är reglerat att en myndighet ska lämna ut personuppgifter, behöver myndigheten som anges ovan inte pröva om utlämnandet är förenligt med det ursprungliga ändamålet. De myndigheter som kommer att lämna uppgifter med stöd av den nya lagen behöver alltså inte göra någon bedömning av om ändamålet med utlämnandet är förenligt med det ändamål för vilka uppgifterna har samlats in. Sammantaget finns stöd för den personuppgiftsbehandling som utlämnande myndigheter kommer att behöva utföra med anledning av förslaget.

Det behövs ingen ytterligare reglering av myndigheternas behandling av känsliga personuppgifter

Förslaget kan innebära en utökad behandling även av känsliga personuppgifter. Stöd för behandlingen av känsliga personuppgifter finns i artikel 9.2 g i EU:s dataskyddsförordning som kompletteras av 3 kap. 3 § dataskyddslagen. Genom dels de villkor som gäller för uppgiftslämnande, dels det sekretesskydd och den reglering för behandling av personuppgifter som gäller hos myndigheterna får kraven på proportionalitet och lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen anses vara uppfyllda (artikel 9.2 g i EU:s dataskyddsförordning).

Den behandling av känsliga uppgifter som kan komma att ske hos brottsbekämpande myndigheter måste i regel anses vara absolut nödvändig och ske enligt de förutsättningar som anges i 2 kap. 11 § andra stycket BDL och 2 kap. 9 § lagen om Säkerhetspolisens behandling av personuppgifter.

Inte heller i detta avseende behövs någon ändring av den reglering som gäller för personuppgiftsbehandlingen.

Uppgiftsminimering, behörighetsbegränsning och behörighetskontroll

En annan grundläggande princip för personuppgiftsbehandling är principen om uppgiftsminimering, det vill säga att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (artikel 5.1 c i EU:s dataskyddsförordning och 2 kap. 8 § BDL). Det ankommer på de berörda myndigheterna att se till att inte fler uppgifter än vad som är nödvändigt behandlas. Det får förutsättas att de berörda myndigheterna i samråd med varandra, gemensamt tar fram lämpliga former för att verka för att de uppgifter som lämnas är relevanta.

Av artiklarna 24.1 och 32 i EU:s dataskyddsförordning följer exempelvis att den personuppgiftsansvarige är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas i verksamheten och säkerställa att behandlingen utförs i enlighet med förordningen. De utlämnande myndigheterna måste alltså, med utgångspunkt i den egna myndighetens organisation och dess behov, se till att tillgången till personuppgifter begränsas och även i övrigt vidta åtgärder för att säkerställa en lämplig säkerhetsnivå. Motsvarande krav finns för de brottsbekämpande myndigheterna (se bland annat 3 kap. 2–6 §§ BDL). Det nu aktuella förslaget förändrar inte de personuppgiftsansvarigas skyldigheter i dessa avseenden.

Sekretesskyddet hos de mottagande myndigheterna är tillräckligt

Vid ett ökat uppgiftsutbyte mellan myndigheter är det viktigt att bedöma om det sekretesskydd som finns för de uppgifter som utbyts mellan myndigheterna är tillräckligt eller om det behövs någon ytterligare sekretessreglering till skydd för sådana uppgifter.

När en myndighet lämnar över sekretessbelagd information till en annan myndighet följer som huvudregel sekretessen inte med till den mottagande myndigheten. I förarbetena till den numera upphävda sekretesslagen (1980:100) har detta främst motiverats med att behovet av sekretess inte enbart kan bestämmas med hänsyn till sekretessintresset. I stället måste behovet också vägas mot intresset av insyn i myndigheternas arbete, vilket kan skilja sig åt från myndighet till myndighet (se prop. 1979/80:2 Del A s. 75 f.). Samma uppgift kan därför ha ett mer eller mindre starkt skydd beroende på vilken myndighet som förvarar uppgiften, både när det gäller sekretessens omfattning och dess styrka.

Sekretess gäller endast hos den mottagande myndigheten om sekretess följer av en så kallad primär sekretessbestämmelse hos den mottagande myndigheten eller om det finns en bestämmelse om överföring av sekretess (7 kap. 2 § OSL). En primär sekretessbestämmelse är en bestämmelse som en myndighet ska tillämpa på grund av att bestämmelsen riktar sig direkt till myndigheten eller omfattar en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller omfattar vissa uppgifter som finns hos myndigheten (3 kap. 1 § OSL).

När den utlämnande myndigheten vid en sådan intresseavvägning som behandlas i avsnitt 5.1 prövar om sekretessintresset talar mot att lämna ut en uppgift kan det få betydelse om uppgiften i fråga skyddas av sekretess

hos den mottagande myndigheten. Hos de olika myndigheter som samverkar inom NCSC kan, som utredningen redogör för, ett antal olika sekretessbestämmelser aktualiseras. Det är bland annat fråga om sekretessbestämmelser till skydd för enskilda intressen, som exempelvis 30 kap. 23 §, 35 kap. 1 § och 38 kap. 4 § OSL. Det är även fråga om sekretessbestämmelser som skyddar allmänna intressen, som exempelvis 15 kap. 1 och 2 §§, 17 kap. 1 och 2 §§ samt 18 kap. 1, 8 och 13 §§ OSL.

Även underrättelsesekretessen enligt 18 kap. 2 § OSL kan aktualiseras i sammanhanget. Underrättelsesekretessen omfattar uppgifter som hänför sig till verksamhet hos vissa myndigheter för att förebygga, förhindra eller upptäcka brottslig verksamhet. Sekretessen gäller med ett omvänt skaderekvisit. När det gäller informationsutbytet inom ramen för NCSC:s verksamhet kan underrättelsesekretessen aktualiseras om det exempelvis handlar om uppgifter om cyberattacker eller andra uppgifter med koppling till brottslig verksamhet. Underrättelsesekretessen i 18 kap. 2 § OSL är konstruerad så att sekretessen följer med uppgifterna. Uppgifter som skyddas av sekretess på grund av att de hänför sig till underrättelseverksamhet hos en brottsbekämpande myndighet skyddas av samma sekretess efter utlämnande, oavsett om de har lämnats till en annan brottsbekämpande myndighet eller till en icke brottsbekämpande myndighet.

Det är inte möjligt att fastslå att samtliga uppgifter som kommer att lämnas ut med stöd av förslaget i avsnitt 5.1 kommer att omfattas av ett lika starkt sekretesskydd som före utlämnandet, men de regler som finns är enligt regeringen tillräckliga och ändamålsenliga. Det finns därför, som utredningen också resonerar om, inget behov av eller anledning att föreslå nya sekretessbestämmelser till skydd för allmänna intressen eller för enskilds personliga eller ekonomiska förhållanden med anledning av förslaget (jfr avsnitt 5.2).

6 Personuppgiftsbehandling av FRA inom ramen för NCSC:s verksamhet

6.1 Det ska införas en ny lag

Regeringens förslag

Det ska införas en ny lag om behandling av personuppgifter som ska gälla för behandling av personuppgifter vid Försvarets radioanstalt (FRA) inom det nationella cybersäkerhetscentret (NCSC).

Lagen ska gälla vid behandling av personuppgifter vid FRA när myndigheten 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 ska vara dels att FRA ska få möjlighet att behandla personuppgifter på ett ändamålsenligt sätt, dels att skydda

människor mot att deras personliga integritet kränks vid sådan behandling.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Majoriteten av remissinstanserna yttrar sig inte över förslaget. Vissa remissinstanser, däribland *Försvarshögskolan, Integritetsskyddsmyndigheten* och *Myndigheten för digital förvaltning*, tillstyrker förslaget. *Sveriges advokatsamfund* befarar att det kan uppstå gränsdragningsproblem mellan den föreslagna lagen och lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt och efterfrågar närmare vägledning avseende i vilka situationer respektive lag ska tillämpas. *Säkerhetspolisen* anför att det, utifrån vissa skrivningar i betänkandet, är oklart om utredningen med uttrycket det nationella cybersäkerhetscentret avser en del av FRA eller de i centret samverkande myndigheterna. Säkerhetspolisen framhåller bland annat att den personuppgiftsbehandling som sker av myndigheten inom ramen för samverkan inom NCSC sker med stöd av lagen om Säkerhetspolisens behandling av personuppgifter.

Skälen för regeringens förslag

Olika regelverk styr FRA:s personuppgiftsbehandling i dag

Som utredningen anger är det i huvudsak två olika regelverk som är tillämpliga när FRA behandlar personuppgifter. Det första regelverket är EU:s dataskyddsförordning som kompletteras av bland annat dataskyddslagen. Utredningen bedömer att den personuppgiftsbehandling som FRA genom NCSC ska utföra omfattas av EU:s dataskyddsförordning och regelverket kring den förordningen.

EU:s dataskyddsförordning är direkt tillämplig i varje medlemsstat, men förutsätter att det i vissa fall finns nationella bestämmelser som kompletterar eller utgör undantag från förordningens regler. EU:s dataskyddsförordning ställer krav på att all behandling av personuppgifter ska ha en rättslig grund och genomföras i enlighet med vissa grundläggande principer (se artiklarna 5.1 och 6.1 i EU:s dataskyddsförordning). De grundläggande principerna genomsyrar hela dataskyddsregleringen och kan medföra krav på rättslig reglering av personuppgiftsbehandling i form av bland annat ändamålsbegränsningar och särskilda skyddsåtgärder (se artikel 6.2 och 6.3 i EU:s dataskyddsförordning).

I vilken omfattning det krävs särskild rättslig reglering till skydd för personuppgifter beror på en rad olika faktorer, bland annat vem som är personuppgiftsansvarig, behandlingens omfattning och om behandlingen omfattar känsliga personuppgifter. I artikel 4 i EU:s dataskyddsförordning definieras personuppgifter som varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en

lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

FRA har också en egen registerlag, lagen om behandling av personuppgifter vid Försvarets radioanstalt (FRAPuL), med tillhörande förordning (se förordningen [2021:1208] om behandling av personuppgifter vid Försvarets radioanstalt). I 1 kap. 4 § FRAPuL anges att vid personuppgiftsbehandling enligt den lagen gäller inte EU:s dataskyddsförordning och inte heller dataskyddslagen.

Enligt 1 kap. 2 § FRAPuL tillämpas lagen vid behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten samt informationssäkerhetsverksamheten vid FRA (jfr prop. 2025/26:179). Myndighetens försvarsunderrättelse- och utvecklingsverksamhet regleras i lagen (2000:130) om försvarsunderrättelseverksamhet och lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, samt i anslutande förordningar. Enligt 4 § FRA:s instruktion ska myndigheten ha hög teknisk kompetens inom informationssäkerhetsområdet. FRA får efter begäran stödja sådana statliga myndigheter och enskilda verksamhetsutövare som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifieringen av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. FRA ska även samverka med andra organisationer inom informationssäkerhetsområdet såväl inom som utom landet. FRA har vidare till uppgift enligt förordningen (2015:1053) om totalförsvar och höjd beredskap att tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer.

BDL är som, utredningen resonerar om, inte tillämplig vid FRA:s personuppgiftsbehandling.

Vilken slags personuppgifter behöver behandlas av FRA inom NCSC?

NCSC utgör en nationell plattform för samverkan och informationsutbyte mellan såväl privata som offentliga aktörer i cybersäkerhetsfrågor. NCSC har, som beskrivs i avsnitt 4.2, ett brett uppdrag. FRA behöver, som utredningen anger, inom ramen för NCSC behandla olika slags personuppgifter och bland annat personuppgifter som avser utomstående personer som berörs av centrets verksamhet eller som kommer i kontakt med myndigheten. Personuppgiftsbehandling kan behöva ske inom ramen för samverkansforum med näringslivet eller deltagande vid konferenser och andra event som FRA genom NCSC arrangerar. Personuppgifter kan också behöva behandlas av FRA i samband med förmedling av information om NCSC:s verksamhet som en del av centrets uppdrag att förmedla råd och stöd avseende hot, sårbarheter och risker. Exempel på vilka typer av personuppgifter som FRA behöver kunna behandla är namn, befattning, adressuppgifter, telefonnummer, e-postadresser, användarnamn, organisationstillhörighet, foton, ip-adresser samt kakor (cookies). Behandling av uppgifter om hälsa kan också, som utredningen anger, aktualiseras i exempelvis utbildnings- och övningssituationer.

FRA kommer, i egenskap av CSIRT-enhet, att övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå, vilket kan aktualisera behandling av bland annat ip-adresser. Incidentrapportering enligt 2 kap. 5–8 §§ cybersäkerhetslagen ska göras till CSIRT-enheten enligt 31 § cybersäkerhetsförordningen (se vidare avsnitt 5.2). Det kan bli fråga om relativt omfattande personuppgiftsbehandling från FRA:s sida när det exempelvis är fråga om att hantera större it-incidenter som berör många enskilda individer. I många fall kommer personuppgifter samlas in direkt från de enskilda själva, men FRA kommer också att ta del av personuppgifter som har samlats in av andra aktörer. Som exempel kan nämnas uppgifter som ska lämnas enligt den föreslagna uppgiftsskyldigheten i avsnitt 5.1. Även realtidsövervakning av nätverks- och informationssystem kan aktualisera behandling av ip-adresser som kan utgöra sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning, det vill säga uppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott, samt uppgifter om misstankar om brott (se artikel 11.3 i NIS 2-direktivet och 33 § cybersäkerhetsförordningen). Enligt utredningens förordningsförslag, som inte är föremål för denna proposition, ska FRA vidare, om det kan antas att en incident som rapporterats har sin grund i en brottslig gärning, skyndsamt uppmana den rapporterande myndigheten att anmäla incidenten till Polismyndigheten. Misstankar om brott omfattas vanligen av artikel 10 i EU:s dataskyddsförordning (se IMYRS 2021:1).

FRA kan även, som utvecklas i avsnitt 6.5, behöva behandla känsliga personuppgifter.

Det finns behov av en ny reglering

Vid bedömningen av om befintlig reglering om personuppgiftsbehandling är tillräcklig är utgångspunkten EU:s dataskyddsförordnings krav på proportionalitet (artikel 6.3) samt tydlighet, precision och förutsebarhet för de registrerade (skäl 41). Vid bedömningen är integritetsriskerna av avgörande betydelse. Ett mer kännbart intrång kräver en mer preciserad rättslig grund som gör intrånget förutsebart, medan personuppgiftsbehandling med lägre integritetsrisker kan ske med stöd av en mer allmänt hållen rättslig grund enligt artikel 6.3. För att kravet på proportionalitet ska vara uppfyllt kan bestämmelser med kompletterande skyddsåtgärder behöva införas.

Utredningen anser att det utifrån EU:s dataskyddsförordnings krav på bland annat tydlighet och förutsebarhet för de registrerade, är lämpligt att FRA:s behandling av personuppgifter inom NCSC regleras i en ny lag. För detta talar också effektivitetsskäl enligt utredningen. Utredningen bedömer att det finns en risk för att arbetet i NCSC inte kan bedrivas på önskvärt sätt om FRA behöver förlita sig på att andra aktörer ska avsätta resurser för att sammanställa och avidentifiera personuppgifter så att de inte längre utgör personuppgifter, om det framstår som tveksamt om myndigheten får behandla vissa typer av personuppgifter. Utredningen bedömer vidare att det behövs en särskild reglering som föreskriver anpassade skyddsåtgärder för att FRA ska kunna behandla känsliga personuppgifter som kan förekomma i verksamheten som myndigheten bedriver inom ramen för NCSC (se vidare avsnitt 6.5).

Regeringen bedömer, i likhet med utredningen, att det är lämpligt att den reglering som gäller för FRA:s personuppgiftsbehandling kompletteras genom en ny lag som tar sikte på verksamheten som bedrivs inom NCSC. NCSC:s övergripande uppgifter framgår av 4 a § FRA:s instruktion. Centrets uppgifter beskrivs närmare i NCSC-förordningen. Det framstår inte som ändamålsenligt att avgränsa tillämpningsområdet för den nya lagen till vissa arbetsuppgifter som FRA utför inom ramen för NCSC. För att säkerställa att FRA kan utföra en ändamålsenlig personuppgiftsbehandling bör den nya lagen alltså gälla inom ramen för all verksamhet som bedrivs av myndigheten inom ramen för NCSC (se vidare avsnitt 6.2). Som framgår av utredningens förslag, och som *Säkerhetspolisen* resonerar om, är det dock fråga om kompletterande reglering som blir tillämplig endast för FRA och inte för samverkansmyndigheterna.

När det gäller förutsättningarna för personuppgiftsbehandling anger utredningen att FRA måste hålla isär den verksamhet som bedrivs på informationssäkerhetsområdet och omfattas av FRAPuL respektive den bredare verksamhet på informations- och cybersäkerhetsområdet som bedrivs inom ramen för NCSC. FRA:s uppdrag att tilldela säkra kryptografiska funktioner till ett antal myndigheter och organisationer hör till den förstnämnda verksamheten, medan exempelvis skyldigheten att tillhandahålla utbildningar och övningar på informations- och cybersäkerhetsområdet hör till den senare verksamheten. *Sveriges advokatsamfund* befarar att det kan uppstå gränsdragningsproblem mellan den föreslagna lagen och FRAPuL och efterfrågar närmare vägledning avseende i vilka situationer respektive lag ska tillämpas.

Enligt 1 kap. 2 § FRAPuL tillämpas den lagen vid behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten samt informationssäkerhetsverksamheten vid FRA (jfr prop. 2025/26:179). Verksamheten inom NCSC bedrivs i dag av en enskild avdelning inom myndigheten. Regeringen kan redan av den anledningen inte se att det finns en risk för gränsdragningsproblem. Därutöver har de olika delarna av myndigheten olika uppdrag. I avsnitt 6.2 föreslås vidare att det ska införas reglering i den nya lagen om förhållandet till FRAPuL. Regeringen bedömer, mot denna bakgrund, att det inte kommer att uppstå sådana gränsdragningsproblem som Advokatsamfundet befarar.

Den nya lagstiftningen bör ha dubbla syften. Dels bör den möjliggöra en ändamålsenlig personuppgiftsbehandling när FRA utför sitt författningsreglerade uppdrag kopplat till NCSC. Dels bör den skydda enskilda mot integritetsintrång. En bestämmelse om syftet och en bestämmelse som tydliggör den rättsliga grunden för behandling av personuppgifter, det vill säga arbetsuppgifter som FRA utför inom ramen för NCSC, bör införas i den nya lagen.

6.2 Lagens tillämpningsområde i övrigt och förhållandet till annan reglering

Regeringens förslag

Lagen ska gälla endast om personuppgiftsbehandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register.

Det ska anges i lagen att den inte gäller vid behandling av personuppgifter som omfattas av lagen om behandling av personuppgifter vid Försvarets radioanstalt.

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 Försvarets radioanstalt är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt lagen.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

I artikel 2.1 i EU:s dataskyddsförordning anges att förordningen ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår eller kommer att ingå i ett register. Enligt artikel 4.6 i förordningen definieras register som en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella och geografiska förhållanden. Som utredningen bedömer bör den föreslagna lagen ha samma tillämpningsområde som EU:s dataskyddsförordning i detta avseende. Detta bör komma till uttryck i lagen.

I 1 kap. 4 § FRAPuL anges att vid personuppgiftsbehandling enligt lagen så gäller inte EU:s dataskyddsförordning och inte heller dataskyddslagen. För att tydliggöra hur den föreslagna registerlagen förhåller sig till FRAPuL bör det framgå av lagen att den inte ska tillämpas när FRAPuL är tillämplig.

EU:s dataskyddsförordning är direkt tillämplig i varje medlemsstat. Förordningen gäller därmed oavsett om det i den föreslagna lagen införs en bestämmelse som hänvisar till den eller inte. Det finns dock skäl att införa

en upplysningsbestämmelse för att tydliggöra att lagen innehåller kompletterande bestämmelser till EU:s dataskyddsförordning. En sådan bestämmelse tydliggör den nya lagens förhållande till förordningen och klargör att lagen inte kan tillämpas fristående, utan att den ska tillämpas tillsammans med förordningen. Hänvisningar till EU:s dataskyddsförordning i lagen bör som utredningen föreslår vara dynamiska för att säkerställa att ändringar i EU-regleringen får omedelbart genomslag (jfr prop. 2017/18:105 s. 25 och 26).

Av 1 kap. 6 § dataskyddslagen följer att dataskyddslagens bestämmelser är subsidiära i förhållande till annan lag eller förordning. Dataskyddslagen kommer alltså att gälla i den mån en viss fråga inte regleras i den föreslagna lagen. För att tydliggöra detta bör det införas en bestämmelse om att dataskyddslagen och föreskrifter som har meddelats i anslutning till den lagen ska gälla vid personuppgiftsbehandling enligt den föreslagna lagen, om inte annat följer av den föreslagna lagen eller föreskrifter som har meddelats i anslutning till den föreslagna lagen.

Av definitionen i artikel 4.7 i EU:s dataskyddsförordning framgår att en personuppgiftsansvarig är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter. Försvarets radioanstalt är personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför inom ramen för det nationella cybersäkerhetscentrets verksamhet. Av tydlighetsskäl bör detta framgå direkt av lagen.

6.3 Rättslig grund för och ändamål med personuppgiftsbehandlingen

Regeringens förslag

Försvarets radioanstalt ska få behandla personuppgifter med stöd av lagen om det är nödvändigt för att myndigheten inom det nationella cybersäkerhetscentret 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.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Det finns rättslig grund för personuppgiftsbehandlingen

Av 2 kap. 2 § dataskyddslagen följer att personuppgifter får behandlas med stöd av artikel 6.1 e i EU:s dataskyddsförordning, om behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av lag eller annan författning. Sådana uppgifter som riksdag eller regering har gett i uppdrag åt statliga myndigheter att utföra anses vara uppgifter av allmänt intresse (se prop. 2017/18:105 s. 56 och 57). Försvarets radioanstalts (FRA) uppgift inom ramen för det nationella cybersäkerhetscentret (NCSC) utgör en uppgift av allmänt intresse som följer av författning. Den personuppgiftsbehandling som bör ske enligt den föreslagna lagen är vidare nödvändig för att FRA genom NCSC ska kunna utföra denna uppgift.

Medlemsstaternas nationella rätt ska därtill enligt artikel 6.3 i EU:s dataskyddsförordning uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Det är, med hänsyn till utvecklingen på cybersäkerhetsområdet som beskrivs i avsnitt 4.1, angeläget att FRA kan utföra sitt författningsreglerade uppdrag kopplat till NCSC på ett effektivt sätt. Detta förutsätter att FRA kan behandla personuppgifter på ett tillfredställande sätt inom ramen för NCSC:s verksamhet. Som framgår i det följande innehåller den föreslagna lagen vidare flera säkerhetsåtgärder som avser att ge enskildas personliga integritet ett tillfredsställande skydd, som sökbegränsningar och begränsad tillgång till personuppgifterna (se till exempel avsnitt 6.4 och 6.6). Den personuppgiftsbehandling som ska ske enligt den föreslagna lagen är mot denna bakgrund proportionerlig. Det finns följaktligen rättslig grund för behandlingen enligt artikel 6.1 e i EU:s dataskyddsförordning.

Två ändamålsbestämmelser bör finnas i lagen

Det krävs också att personuppgiftsbehandlingen uppfyller de grundläggande principerna i artikel 5 i EU:s dataskyddsförordning. Dessa innebär exempelvis att personuppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (artikel 5.1 b). Artikeln ger bland annat uttryck för den så kallade finalitetsprincipen. Bestämmelser som anger ett visst ändamål för behandling av personuppgifter tydliggör vilken behandling som är tillåten inom en viss verksamhet och begränsar vilken behandling som en personuppgiftsansvarig får utföra. Ändamålsbestämmelser kan därmed utgöra en form av åtgärd till skydd för personuppgifter som bidrar till att säkerställa en laglig och rättvis behandling (jfr artikel 6.2 och 6.3 i EU:s dataskyddsförordning).

I vissa författningar delas ändamålen in i primära och sekundära ändamål. Bestämmelser om primära ändamål reglerar behandling som behövs i den berörda myndighetens egen verksamhet medan sekundära ändamål bland annat reglerar i vilken utsträckning uppgifter som behandlas för något av de primära ändamålen får vidarebehandlas för att lämnas ut till enskilda eller till andra myndigheter. Ett syfte med denna uppdelning är att göra det tydligt för den registrerade hur personuppgifter får behandlas inom myndigheten respektive hur de får behandlas för att lämnas ut till andra.

Av tydlighetsskäl bör två ändamålsbestämmelser föras in i den nya lagen. Den första bestämmelsen bör behandla primära ändamål, medan den andra bestämmelsen bör behandla sekundära ändamål. De primära ändamålen för personuppgiftsbehandling bör avgränsas till sådan behandling som är nödvändig för utförandet av det uppdrag som följer av 4 a § FRA:s instruktion (se avsnitt 6.1). Genom att uttryckligen knyta ändamålet med behandlingen till vad som är nödvändigt för utförandet av uppdraget, inskränks möjligheterna att behandla personuppgifter som saknar koppling till NCSC:s verksamhet.

Lagrådet förordar att hänvisningen från 7 § i lagrådsremissens lagförslag görs till hela 2 § och därmed också omfattar 2 § andra stycket, som anger att lagen endast gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register. Som skäl för detta anför Lagrådet att en förutsättning för att lagen ska vara tillämplig är att det är fråga om sådan behandling som anges i 2 § andra stycket och att en hänvisning till hela den paragraf som anger lagens tillämpningsområde även blir konsekvent med många andra så kallade registerlagar. Regeringen konstaterar att det även finns exempel på registerlagar där motsvarande reglering endast avser den eller de uppgifter som omfattas av lagens tillämpningsområde (se exempelvis 1 kap. 2 § och 6 § lagen [2023:457] om behandling av personuppgifter vid Utbetalningsmyndigheten). Utifrån att hänvisningen i 7 § görs till en uppgift, och då 2 § andra stycket endast beskriver lagens tillämpningsområde, bör Lagrådets förslag inte genomföras.

Som utredningen anger är den föreslagna formuleringen av de primära ändamålen bred och FRA måste därför normalt precisera ändamålet när uppgifterna samlas in, för att uppfylla kravet på särskilda, uttryckligt angivna och berättigade ändamål enligt artikel 5.1 b i EU:s dataskyddsförordning. Att behandlingen ska vara nödvändig innebär dock inte ett krav på att behandlingsåtgärden ska vara oundgänglig. Om behandlingen leder till effektivitetsvinster kan den anses nödvändig (se prop. 2017/18:105 s. 189). Om syftet med behandlingen kan uppnås med andra medel, till exempel genom att anonymisera uppgifterna, innebär kravet på nödvändighet att personuppgifterna inte får behandlas (se prop. 2017/18:232 s. 117).

Det kan argumenteras för att en ändamålsbestämmelse, som inte tillför något i sak utöver vad som redan följer av 2 kap. 2 § dataskyddslagen, inte fyller någon egentlig funktion. Det kan dock, som utredningen resonerar om, i vissa fall finnas ett värde i att ändamålen anges uttryckligen. En ändamålsbestämmelse kan fungera som ett förtydligande för de registrerade. Vidare framstår det inte som önskvärt att avgränsa ändamålen i större utsträckning och ange mer konkreta och uttryckliga ändamål än vad utredningen har gjort. Anledningen till detta är att NCSC:s arbete spänner över ett brett område och måste kunna utföras så situationsstyrt och varierat som möjligt. En bred formulering innebär också att nya arbetsuppgifter som kan komma att aktualiseras för FRA inom ramen för NCSC, inom det materiella tillämpningsområdet, som utgångspunkt kommer att rymmas inom ändamålsbestämmelsen.

När det gäller de sekundära ändamålen, och närmare bestämt utlämnande till andra, bör en allmän förutsättning vara att utlämnande får ske om uppgiftslämnandet sker i överensstämmelse med lag eller förordning.

Detta innebär att personuppgifter får lämnas ut med stöd av bestämmelser som påbjuder eller tillåter utlämnande. I samband med att bestämmelser införs som innebär att uppgifter ska eller får lämnas ut görs regelmässigt en avvägning mellan intresset av att uppgiften lämnas ut och intresset av att skydda enskilda personers integritet. Denna avvägning har lett till att vissa typer av uppgifter ska eller får lämnas ut. En reglering med innebörden att personuppgifter får behandlas i överensstämmelse med lag eller förordning har också förlagor i ett flertal registerförfattningar, som till exempel 6 § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten och 1 kap. 7 § lagen om behandling av personuppgifter vid Utbetalningsmyndigheten. Ett utlämnande av uppgifter kan aktualiseras av skyldigheten för en myndighet att på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång enligt 6 kap. 5 § OSL. Bestämmelsen avser dock inte endast uppgiftslämnande till andra myndigheter, utan omfattar även situationen då lag eller förordning föreskriver uppgiftslämnande till andra aktörer.

Begränsningen i bestämmelsen till personuppgifter som behandlas enligt de primära ändamålen innebär att det inte kan bli aktuellt för FRA att samla in uppgifter i det enda syftet att senare lämna ut dessa. Uppgifter som får lämnas ut med stöd av bestämmelsen måste alltså redan vara föremål för behandling enligt ett särskilt, uttryckligt angivet och berättigat ändamål som ryms inom den ram som den primära ändamålsbestämmelsen ställer upp.

Förhållandet till finalitetsprincipen

Utredningen bedömer att det bör tydliggöras att personuppgifter som behandlas för de primära ändamålen även får behandlas för andra ändamål, under förutsättning att dessa inte är oförenliga med de ändamål för vilka uppgifterna samlades in. Bestämmelsen ger därmed uttryck för finalitetsprincipen (artikel 5.1 b i EU:s dataskyddsförordning). Det följer av artikel 5.1 b i EU:s dataskyddsförordning att bland annat behandling av arkivändamål av allmänt intresse, vetenskapliga forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i förordningen inte ska anses vara oförenlig med de ursprungliga ändamålen. Finalitetsprincipen bör utgöra den yttersta ramen inom vilken personuppgifter får behandlas på EU:s dataskyddsförordnings område enligt den föreslagna lagen (jfr prop. 2019/20:106 s. 40 och prop. 2022/23:34 s. 127 och 128).

Även om EU:s dataskyddsförordnings bestämmelser om finalitetsprincipen är direkt tillämpliga i FRA:s verksamhet kopplat till NCSC talar tydlighetsskäl, som utredningen anger, för att införa en bestämmelse som ger uttryck för principen (jfr prop. 2022/23:34 s. 128). Bestämmelsen bör ha samma innebörd som EU:s dataskyddsförordnings bestämmelse i artikel 5.1 b och tolkas på samma sätt. Det innebär att behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål inte ska anses vara oförenliga med insamlingsändamålen. Det innebär vidare att de omständigheter som anges i förordningen ska beaktas vid bedömningen av om behandlingen är förenlig med insamlingsändamålen. Ändamålsbestämmelserna och finalitetsprincipen kan innebära att det är tillåtet att behandla insamlade

personuppgifter för andra ändamål än det ursprungliga ändamålet. Det bör dock framhållas att det ytterst är FRA som personuppgiftsansvarig som måste bedöma om en behandling av personuppgifter är förenlig med finalitetsprincipen.

6.4 Tillgången till personuppgifter ska begränsas

Regeringens förslag

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

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

I artikel 5.1 c i EU:s dataskyddsförordning uttrycks den grundläggande principen att personuppgifter som behandlas ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (principen om uppgiftsminimering). Enligt artikel 25.2 i förordningen ska den personuppgiftsansvarige också genomföra lämpliga tekniska och organisatoriska åtgärder för att, som utgångspunkt, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

Vilken spridning av personuppgifter som en viss behandling innebär har stor inverkan på integritetsriskerna. Om personuppgifter sprids ökar risken för att uppgifterna kommer att användas på ett sätt som innebär ett intrång i de registrerades personliga integritet. Risken ökar även för personuppgiftsbehandling som det inte finns behov av. Utgångspunkten bör därför vara att personuppgifter inte ska spridas till fler än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det är viktigt för skyddet av den personliga integriteten att det vid Försvarets radioanstalt (FRA) säkerställs att personuppgifter i det nationella cybersäkerhetscentrets (NCSC) verksamhet endast görs tillgängliga för de medarbetare som behöver uppgifterna i sitt arbete. En bestämmelse med den innebörden bör därför införas i den nya lagen.

Bestämmelsen bör omfatta såväl tillsvidareanställd personal som exempelvis personer med tidsbegränsad anställning eller uppdragstagare. Samverkansmyndigheternas personal kan också delta i NCSC:s verksamhet. Alla dessa kategorier omfattas av uttrycket var och en. FRA bör aktivt ta ställning till vilket informationsbehov ett tjänsteåliggande eller uppdrag medför och tilldela den behörighet som behövs utifrån det. Som exempel

på åtgärder som kan behöva vidtas kan nämnas begränsning av behörigheter i it- eller handläggningssystem eller motsvarande åtgärder. Ytterst är det FRA som i egenskap av personuppgiftsansvarig har ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgifter inte sprids i större omfattning än vad som är nödvändigt.

6.5 Behandling av känsliga personuppgifter

Regeringens förslag

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

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

EU:s dataskyddsförordning förbjuder behandling av känsliga personuppgifter, vilket omfattar personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (artikel 9.1).

Ett antal undantag finns dock från förbudet. Som exempel kan nämnas att behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen (artikel 9.2 g). Artikel 9.2 g är direkt tillämplig, men det är möjligt för medlemsstaterna att i nationell rätt införa mer specifika bestämmelser avseende känsliga personuppgifter (se artikel 6.2 och skäl 10 till EU:s dataskyddsförordning).

I 3 kap. 3 § första stycket dataskyddslagen anges att känsliga personuppgifter får behandlas av en myndighet med stöd av artikel 9.2 g i EU:s dataskyddsförordning om uppgifterna har lämnats till myndigheten och behandlingen krävs enligt lag, om behandlingen är nödvändig för handläggningen av ett ärende, eller i annat fall, om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och inte innebär ett otillbörligt intrång i den registrerades personliga integritet. Enligt 3 kap. 3 § andra stycket är det vid behandling som sker enbart med stöd av första stycket

förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter (se vidare avsnitt 6.6).

Utredningen bedömer att Försvarets radioanstalt (FRA) inom ramen för det nationella cybersäkerhetscentret (NCSC) kan komma att behöva behandla känsliga personuppgifter, i en inte ringa omfattning. Utredningen nämner att FRA genom NCSC kommer att ha i uppdrag att erbjuda utbildningar inom informations- och cybersäkerhetsområdet. I samband med sådana utbildningar, konferenser eller liknande event kan det vara aktuellt att behandla personuppgifter om hälsa. När det gäller rapportering av sårbarheter och incidentrapporter så kan uppgifter om namnet på anmälaren enligt utredningen indirekt avslöja en företrädares etniska ursprung. Anmälaren kan också vara en politisk eller religiös organisation. Även i en sådan situation kan FRA inom ramen för NCSC:s verksamhet behöva behandla känsliga personuppgifter, exempelvis när det går att koppla enskilda individer till organisationen i fråga. Det är då fråga om känsliga personuppgifter avseende religiös eller filosofisk övertygelse. Det kan också vara så att uppgifter om användarnamn och e-postadresser kan innehålla känsliga personuppgifter.

Eftersom behandling av känsliga personuppgifter som huvudregel är förbjuden, måste något av undantagen från förbudet i artikel 9.2 i EU:s dataskyddsförordning vara tillämpligt för att behandlingen ska vara tillåten. I detta sammanhang är det centralt om behandlingen kan anses vara nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av unionsrätten eller medlemsstaternas nationella rätt (artikel 9.2 g).

Vad som avses med uttrycket ett allmänt intresse som används i artikel 6.1 e i förordningen respektive uttrycket ett viktigt allmänt intresse som används i artikel 9.2 g i förordningen är inte definierat i EU:s dataskydds-förordning. I förarbetena till dataskyddslagen konstateras att det är svårt att på ett generellt plan definiera vad som skiljer ett allmänt intresse från ett viktigt allmänt intresse. Det måste enligt regeringen utgöra ett viktigt allmänt intresse att svenska myndigheter, även utanför området myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (se prop. 2017/18:105 s. 83). NCSC:s uppgifter framgår av dels FRA:s instruktion, dels NCSC-förordningen. Syftet med FRA:s behandling av personuppgifter, i vilken känsliga personuppgifter kan ingå, är att utföra de författningsreglerade arbetsuppgifterna. När FRA genom NCSC behandlar känsliga personuppgifter som är nödvändiga för att utföra de uppgifter som framgår av författning rör det sig därmed om en sådan behandling som avses i artikel 9.2 g i EU:s dataskyddsförordning, det vill säga en behandling som är av viktigt allmänintresse på grundval av nationell rätt.

EU:s dataskyddsförordning ställer också krav på att det rättsliga stödet, som måste stå i proportion till det eftersträvade syftet, ska vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.

Regeringen bedömer att den personuppgiftsbehandling som FRA kommer att utföra enligt den nya registerlagen är proportionerlig (se vidare avsnitt 6.3). Bedömningen gäller även i relation till att det kan vara känsliga personuppgifter som behandlas. I fråga om förenlighet med det

väsentliga innehållet i rätten till dataskydd har regeringen tidigare uttalat att det är svårt att föreställa sig en rättslig grund för behandling av personuppgifter som uppfyller kraven i artikel 6, men som ändå inte är förenlig med det väsentliga innehållet i rätten till dataskydd (se prop. 2017/18:105 s. 84). Om grunden för behandlingen inte är förenlig med det väsentliga innehållet i rätten till dataskydd, torde den enligt regeringen inte utgöra en godtagbar rättslig grund för behandling av personuppgifter över huvud taget. Det kan enligt regeringen därför ifrågasättas om tillägget i artikel 9.2 g utgör ett krav som går utöver de krav som gäller enligt artikel 6 och som måste vara uppfyllda vid all behandling av personuppgifter i allmänt intresse. Detta innebär att så länge FRA, vid behandling av personuppgifter för ett allmänt intresse, har rättslig grund för den behandling som är nödvändig att utföra, bör alltså kravet på förenlighet med det väsentliga innehållet i rätten till dataskydd kunna ses som uppfyllt.

Artikel 9.2 g ställer också krav på bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande intressen. Den föreslagna regleringen innehåller skyddsåtgärder som upprätthåller skyddet för den personliga integriteten vid behandling av känsliga personuppgifter. Bestämmelserna om personuppgiftsansvar, tillgång till personuppgifter, sökbegränsningar och längsta tid för behandling är sådana bestämmelser. Även den sekretessbestämmelse som behandlas i avsnitt 5.2 utgör en sådan skyddsåtgärd. Sammantaget innebär det att den behandling som FRA behöver utföra av känsliga personuppgifter inom ramen för NCSC uppfyller kraven i artikel 9.2 g i EU:s dataskyddsförordning. Att FRA får behandla känsliga personuppgifter bör framgå av den föreslagna lagen.

Lagrådet förordar att hänvisningen från 10 § i lagrådsremissens lagförslag görs till hela 2 § och därmed också omfattar 2 § andra stycket, som anger att lagen endast gäller om behandlingen är helt eller delvis automatiserad eller om personuppgifterna ingår i eller kommer att ingå i ett register. Regeringen bedömer dock, av de skäl som framgår av avsnitt 6.3, att Lagrådets förslag inte bör genomföras.

6.6 Det ska vara förbjudet att utföra vissa sökningar kopplat till känsliga personuppgifter

Regeringens förslag

Det ska vara förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Sökningar som tar sikte på känsliga personuppgifter är typiskt sett förknippade med särskilda risker i integritetshänseende (jfr prop. 2018/19:33 s. 132). I 3 kap. 3 § andra stycket dataskyddslagen finns ett generellt förbud mot att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Bestämmelsen i 3 kap. 3 § dataskyddslagen om möjligheten att behandla känsliga personuppgifter är avsedd att gälla för offentlig verksamhet där sektorsspecifik reglering avseende känsliga personuppgifter saknas (se prop. 2017/18:105 s. 85).

Det har inte framkommit något behov för Försvarets radioanstalt att kopplat till det nationella cybersäkerhetscentret få använda sökbegrepp som avser känsliga personuppgifter. Det bör framgå av lagen att det är förbjudet att utföra sökningar i syfte att få fram ett personurval grundat på sådana uppgifter. Sökbegränsningen bör omfatta alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett sådant urval av personer. Det bör noteras att bestämmelsen inte hindrar sökningar som görs i ett annat syfte än att få fram ett personurval. Som exempel kan nämnas att sökningar görs med syftet att ta fram verksamhetsstatistik eller för registervård.

6.7 Personuppgifter ska få lämnas ut elektroniskt

Regeringens förslag

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

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Sveriges advokatsamfund bedömer att utredningens förslag förefaller innebära att direktåtkomst till uppgifterna ska vara tillåten. Detta borde i sådana fall, enligt Advokatsamfundets uppfattning, uttryckligen anges. Övriga remissinstanser tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Försvarets radioanstalt (FRA) behöver ha effektiva och tidsenliga former för utlämnande av information, inklusive personuppgifter, inom ramen för det nationella cybersäkerhetscentrets (NCSC) verksamhet. Behovet kan kopplas dels till NCSC:s uppdrag att vara en nationell plattform för samverkan och informationsutbyte, dels till möjligheten att få ut koordinerad information vid incidenter, till både offentliga och privata aktörer, på ett skyndsamt sätt. Behovet gör sig alltså gällande både vid kommunikation med andra myndigheter och internationella aktörer samt vid kommunikation med näringslivet. Det finns stora effektivitetsvinster med att låta FRA, inom ramen för verksamheten inom NCSC, ha möjlighet

att lämna ut personuppgifter elektroniskt. När personuppgifter lämnas ut elektroniskt kan det dock innebära risker för den personliga integriteten. Ett sådant utlämnande innebär nämligen att mottagaren kan bearbeta informationen, till exempel genom samkörning med information som har hämtats från andra källor.

EU:s dataskyddsförordning innehåller inte några bestämmelser som uttryckligen tar sikte på sättet att lämna ut personuppgifter. Av artikel 6.3 i förordningen framgår dock att den rättsliga grunden, som ska fastställas i enlighet med unionsrätten eller medlemsstaternas nationella rätt, kan innehålla särskilda bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen, bland annat vad gäller typer av behandling och förfaranden för behandling. Det är alltså möjligt att i nationell rätt införa regler som preciserar formerna för behandlingen av personuppgifter. I svensk rätt skiljer lagstiftningen ofta mellan två former av elektroniskt utlämnande: direktåtkomst och annat elektroniskt utlämnande.

Det finns inte någon legaldefinition av uttrycket direktåtkomst. Den grundläggande innebörden anses vara att någon har tillgång till information hos någon annan, och på egen hand kan söka i den, dock utan att själv kunna påverka innehållet. Direktåtkomst kan ge användaren möjlighet att även hämta in information till sitt eget system och bearbeta den där (se till exempel prop. 2016/17:58 s. 112). Direktåtkomst innebär typiskt sett att uppgifterna blir tillgängliga för fler personer och kan, beroende på hur åtkomsten utformas, minska möjligheterna för den utlämnande myndigheten att kontrollera utlämnandet och därmed öka risken för intrång i den personliga integriteten. Det bör samtidigt framhållas att en väl analyserad och förberedd direktåtkomst inte behöver innebära större risker för den enskildes integritet än andra former av elektroniskt utlämnande (se prop. 2025/26:88 s. 156 f.). Uttrycken elektroniskt utlämnande och utlämnande på medium för automatiserad behandling har samma innebörd. Det förstnämnda uttrycket förekommer i nyare registerförfattningar. Vad som avses med uttrycken har förändrats i takt med teknikutvecklingen, men de förhåller sig alltid på något sätt till utlämnande genom direktåtkomst. Med dagens teknik kan utlämnande av information ske genom annat elektroniskt utlämnande, exempelvis genom e-post, på ett usb-minne eller genom direkt överföring från ett datorsystem till ett annat. Vid ett mer omfattande informationsutbyte mellan myndigheter är det oftast den senare metoden som används (se prop. 2022/23:34 s. 140).

Utredningen bedömer att det behov av att lämna ut uppgifter som finns kan tillgodoses med en bestämmelse om elektroniskt utlämnande på annat sätt än genom direktåtkomst. *Sveriges advokatsamfund* bedömer att utredningens förslag förefaller innebära att direktåtkomst till uppgifterna ska vara tillåten. Som utredningen anger har det dock inte framkommit något tydligt behov av att möjliggöra utlämnande genom direktåtkomst. Däremot är det nödvändigt att FRA ska kunna lämna ut personuppgifter elektroniskt, för att kunna bedriva en effektiv verksamhet.

För att uppnå en ändamålsenlig avvägning mellan FRA:s intresse av att på ett effektivt sätt lämna ut personuppgifter i elektronisk form och riskerna med att överföra uppgifter elektroniskt bör utlämnande få ske om det inte är olämpligt. Som exempel på omständigheter att beakta vid bedömningen av om ett elektroniskt utlämnande är olämpligt kan nämnas

typen av personuppgifter, vilket också följer direkt av EU:s dataskyddsförordning. Vem som är mottagare av uppgifterna bör också ha betydelse för om ett utlämnande ska anses vara olämpligt. Vid prövningen av om personuppgifter ska lämnas ut elektroniskt bör även informationssäkerheten hos mottagaren vägas in. Det bör noteras att FRA som personuppgiftsansvarig är skyldig att säkerställa att bland annat adekvata tekniska och organisatoriska åtgärder har vidtagits. Detta följer direkt av artiklarna 24, 25 och 32 i EU:s dataskyddsförordning.

Den föreslagna bestämmelsen ska inte tolkas som att den medför en rätt för vare sig mottagande myndighet eller enskilda att få ut uppgifter elektroniskt. Bestämmelsen innebär inte heller någon skyldighet för FRA att lämna ut uppgifter på ett visst sätt.

6.8 Tiden som personuppgifter får behandlas ska begränsas

Regeringens förslag

Personuppgifter ska inte 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 Försvarets radioanstalt arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Vid all personuppgiftsbehandling är det ett grundläggande krav, enligt principen om lagringsminimiering, att uppgifterna inte behandlas under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas (artikel 5.1 e i EU:s dataskyddsförordning). Bestämmelser som tydliggör hur länge personuppgifter får behandlas inom en verksamhet innebär en form av skyddsåtgärd. Regeringen bedömer att det bör införas sådana bestämmelser i den nya lagen.

Det är, som utredningen anger, svårt att på ett generellt plan uttala sig om hur länge det kan vara nödvändigt att lagra uppgifter i den verksamhet som Försvarets radioanstalt bedriver inom ramen för det nationella cybersäkerhetscentrets verksamhet. När det gäller exempelvis ip-adresser kopplade till incidenter, kan det finnas behov av att lagra uppgifterna under en längre tid. Det bör anges att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet. Det som då avses är ändamålet i det enskilda fallet. Behovet av att fortsätta behandla uppgifterna måste därför prövas kontinuerligt. Om en personuppgift

behandlas för flera olika ändamål, kan behovet av behandling för ett ändamål ha upphört, medan behov kvarstår av behandling för något annat ändamål. Då får behandling ske enligt det senare ändamålet, så länge det behovet kvarstår.

EU:s dataskyddsförordning innehåller ett undantag från principen om lagringsminimering, som innebär att personuppgifter får lagras under längre perioder i den mån personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål (artikel 5.1 e i förordningen). För att tydliggöra att personuppgifter som utgör en del av en allmän handling får arkiveras bör det uttryckligen framgå att det som anges när det gäller längsta tid för behandling av personuppgifter inte hindrar att sådana uppgifter arkiveras i enlighet med gällande arkivlagstiftning. I vilken utsträckning personuppgifter ska gallras i samband med arkivering regleras i det arkivrättsliga regelverket.

6.9 Rätten att göra invändningar ska inte gälla

Regeringens förslag

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.

Utredningens förslag

Förslaget i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna tillstyrker eller har inga synpunkter på förslaget.

Skälen för regeringens förslag

Vid behandling av personuppgifter för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning har den registrerade rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne (artikel 21.1 i EU:s dataskyddsförordning). Den personuppgiftsansvarige får då inte längre behandla personuppgifterna om inte denne kan visa tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter eller om det sker för fastställande, utövande eller försvar av rättsliga anspråk. Rätten att göra invändningar innebär att den registrerade har möjlighet att få till stånd en prövning av om viss behandling är tillåten. Under tiden som en sådan prövning pågår har den registrerade rätt att kräva att behandlingen av personuppgifterna begränsas (artikel 18.1 d i EU:s dataskyddsförordning). Om det bedöms saknas berättigade skäl för behandlingen har den registrerade rätt att få personuppgifterna raderade (artikel 17.1 c i EU:s dataskyddsförordning).

Medlemsstaterna har möjlighet att begränsa rätten att göra invändningar under de förutsättningar som framgår av artikel 23.1 i EU:s dataskyddsförordning. En sådan begränsning får göras om den sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna. Begränsningen måste utgöra en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa olika uppräknade intressen, bland annat den allmänna säkerheten, förebyggande eller förhindrande av brott eller andra viktiga mål av generellt allmänt intresse. Sådana lagstiftningsåtgärder ska enligt artikeln innehålla specifika bestämmelser när så är relevant, avseende bland annat ändamålen med behandlingen, lagringstiden samt tillgängliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål (artikel 23.2).

Rätten att göra invändningar har begränsats i ett flertal myndigheters registerförfattningar (se prop. 2022/23:34 s. 122 och 123 med hänvisningar). Det har i dessa fall ansetts vara av stor betydelse att personuppgifter får behandlas i myndigheternas verksamheter, oberoende av den registrerades inställning, samtidigt som regeringen bedömt att den personuppgiftsansvarige närmast undantagslöst skulle kunna påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet (se till exempel prop. 2017/18:254 s. 45).

Den personuppgiftsbehandling som Försvarets radioanstalt (FRA) utför för att fullgöra uppgiften enligt 4 a § FRA:s instruktion genomförs för att utföra en uppgift av allmänt intresse. Regleringen i EU:s dataskyddsförordning om rätten att göra invändningar gäller således vid behandlingen av personuppgifter. Det finns ett klart behov av att FRA ska kunna behandla personuppgifter på ett ändamålsenligt sätt för att kunna utföra det författningsreglerade uppdrag som ålagts myndigheten inom ramen för det nationella cybersäkerhetscentret (NCSC). FRA kan behöva hantera personuppgifter oavsett den registrerades inställning. Så länge personuppgiftsbehandlingen sker för de ändamål som stadgas i den föreslagna lagen så står det klart att FRA regelmässigt skulle kunna påvisa skäl för fortsatt behandling som väger tyngre än den registrerades intressen i det enskilda fallet. En rätt för den registrerade att invända mot behandling av personuppgifter kan dock ändå tänkas påverka effektiviteten i NCSC:s verksamhet.

För att säkerställa förutsättningarna för FRA att behandla relevanta personuppgifter bör därför den registrerade inte ha någon rätt att motsätta sig sådan personuppgiftsbehandling som är tillåten enligt lagen. Det bör därför införas en bestämmelse som innebär att rätten att göra invändningar enligt artikel 21.1 i EU:s dataskyddsförordning inte ska gälla vid sådan behandling av personuppgifter som är tillåten enligt den föreslagna lagen, eller föreskrifter som har meddelats i anslutning till den. En sådan begränsning utgör en nödvändig och proportionerlig åtgärd i syfte att säkerställa sådana viktiga mål av generellt allmänt intresse som krävs enligt artikel 23.1 i EU:s dataskyddsförordning. Förslagen om bestämmelser om ändamålen med behandlingen, sökbegränsningar och längsta tid för behandling minimerar också risken för kränkning av den registrerades rättigheter och friheter. Den föreslagna lagen uppfyller även, som utredningen anger, de övriga krav som uppställs i artikel 23.1 i EU:s dataskyddsförordning.

6.10 Det behövs ingen bestämmelse om begränsning av skyldigheten att informera den registrerade

Regeringens bedömning

Personuppgiftsbehandlingen inom lagens tillämpningsområde omfattas av undantaget i artikel 14.5 c i EU:s dataskyddsförordning från skyldigheten att lämna information när personuppgifter har getts in av någon annan än den registrerade själv. Det saknas behov av ytterligare bestämmelser som begränsar rätten för den registrerade att ta del av sådan information.

Utredningens bedömning

Bedömningen i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna ställer sig bakom eller har inga synpunkter på bedömningen.

Skälen för regeringens bedömning

Enligt EU:s dataskyddsförordning finns en skyldighet att lämna information till den registrerade om den personuppgiftsbehandling som sker med avseende på denne när personuppgifterna inte har erhållits från den registrerade (artikel 14.1–4). I artikel 13.1–3 regleras skyldigheten att lämna information till den registrerade när personuppgifterna har samlats in från den registrerade. Förordningen skiljer alltså på situationen då den personuppgiftsansvarige samlar in personuppgifter direkt från den registrerade och situationer då personuppgifterna samlas in från andra än den registrerade. Den senare situationen kan exempelvis vara aktuell när Försvarets radioanstalt (FRA) får in uppgifter om incidenter eller sårbarheter där uppgifter om ip-adresser framgår. I artikel 14.5 c i EU:s dataskyddsförordning finns ett undantag som säger att artikel 14.1–4 inte ska tillämpas om erhållande eller utlämnande av uppgifter uttryckligen föreskrivs genom unionsrätten eller genom en medlemsstats nationella rätt som den registrerade omfattas av och som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen.

Regeringen har tidigare bedömt att kravet i artikel 14.5 på uttryckliga föreskrifter om erhållande eller utlämnande av uppgifter i nationell rätt inte kan tolkas på annat sätt än som ett krav på föreskrifter om en rätt att få uppgifter eller föreskrifter om en uppgiftsskyldighet (se prop. 2017/18:298 s. 110).

Den informationsdelning som kommer att ske från myndigheter till FRA inom ramen för det nationella cybersäkerhetscentrets (NCSC) verksamhet kommer att grunda sig på den uppgiftsskyldighet som föreslås i avsnitt 5.1, när det handlar om annars sekretessbelagda uppgifter som lämnas av myndigheterna som samverkar. Den informationsdelning som kommer att ske i övrigt grundar sig ytterst på bestämmelserna om myndigheters samverkansskyldighet i 8 § förvaltningslagen samt 6 kap. 5 § OSL. Den

senare bestämmelsen har av regeringen bedömts uppfylla kravet i artikel 14.5 c i EU:s dataskyddsförordning på en uttrycklig föreskrift om utlämnande av uppgifter som fastställer lämpliga åtgärder för att skydda den registrerades berättigade intressen. Ett utlämnande enligt dessa föreskrifter innebär därmed att informationsskyldigheten enligt artikel 14.1–4 inte blir aktuell. Detta gäller oavsett för vilket ändamål som uppgifterna lämnas ut (se prop. 2017/18:298 s. 111 och 112).

Bestämmelser om behandling av personuppgifter i registerförfattningar är en sådan typ av reglering som avses i artikel 14.5 c i EU:s dataskyddsförordning (se exempelvis prop. 2017/18:113 s. 32 f. och prop. 2017/18:115 s. 25–27). Den personuppgiftsbehandling som sker inom den föreslagna lagens tillämpningsområde omfattas av undantaget i artikel 14.5 c. Av lagen framgår för vilka ändamål som personuppgifterna får behandlas. Ett antal bestämmelser som skyddar den registrerades personliga integritet när FRA behandlar personuppgifter föreslås också, till exempel bestämmelser om sök- och behörighetsbegränsningar (se avsnitt 6.6 och 6.7). Uppgifterna kan också komma att vara sekretessbelagda enligt den sekretessbestämmelse som föreslås i avsnitt 5.2. Det finns därmed i nationell rätt ett tillräckligt skydd för den registrerades intressen för att undantaget i artikel 14.5 c i EU:s dataskyddsförordning ska kunna tillämpas. Det behövs därför inte någon ytterligare reglering för att FRA ska kunna tillämpa undantaget.

I vissa fall kan personuppgifter som lämnas till FRA inom ramen för NCSC:s verksamhet av en annan aktör, exempelvis en myndighet, härröra från den enskilde själv. Av artikel 13.3 i EU:s dataskyddsförordning följer att om en personuppgiftsansvarig avser att ytterligare behandla personuppgifter för ett annat syfte än det för vilket de insamlades, ska den personuppgiftsansvarige före denna ytterligare behandling ge den registrerade information om syftet. I den mån utlämnandet av personuppgifter till FRA genom NCSC kan anses göras för ett nytt syfte, är den aktör som lämnar ut personuppgifterna alltså skyldig att informera den registrerade om detta. Det finns undantag från denna skyldighet i 5 kap. 1 § dataskyddslagen, när uppgifterna inte får lämnas ut till den registrerade enligt lag eller annan författning eller enligt beslut som har meddelats med stöd av författning. Är den personuppgiftsansvarige inte en myndighet, gäller undantaget även för uppgifter som hos en myndighet skulle ha varit sekretessbelagda. I de fall som personuppgifterna är sekretessbelagda hos den utlämnande aktören kan det vara så att sekretessen inte gäller i förhållande till den enskilde själv. I sådana situationer kan en aktör som lämnar uppgifter till FRA genom NCSC ha en skyldighet att upplysa den person som uppgifterna avser om detta. Det har inte framkommit behov, inom ramen för detta lagstiftningsärende, att föreslå en reglering med undantag från informationsskyldigheten i artikel 13.3 i EU:s dataskyddsförordning. Det kan noteras att om ett tydligt behov framkommer av detta kan frågan regleras på förordningsnivå, med stöd av 5 kap. 1 § dataskyddslagen.

7 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag

De nya lagarna och övriga lagändringar ska träda i kraft den 15 juli 2026.

Regeringens bedömning

Det behövs inte några övergångsbestämmelser.

Utredningens förslag och bedömning

Förslaget från utredningen stämmer inte överens med regeringens. Utredningen föreslår att de nya lagarna och övriga lagändringar ska träda i kraft den 1 juli 2026. Utredningen gör samma bedömning som regeringen i fråga om behovet av övergångsbestämmelser.

Remissinstanserna

Remissinstanserna uttalar sig inte särskilt om tidpunkten för ikraftträdande eller behovet av övergångsbestämmelser. Några remissinstanser, däribland *RISE Research Institutes of Sweden*, framför dock synpunkter på utredningens förslag om att verksamhetsöverföringen från Myndigheten för civilt försvar till Försvarets radioanstalt ska ske den 1 juli 2026.

Skälen för regeringens förslag och bedömning

Frågan om när och hur en verksamhetsöverföring ska ske är inte en fråga som behandlas i denna proposition. De föreslagna lagändringarna är angelägna och bör, som utredningen anger, träda i kraft så snart som möjligt. Ett tidigare ikraftträdande än den 15 juli 2026 är dock inte möjligt för något av förslagen. Det behövs inte några övergångsbestämmelser.

8 Konsekvenser av förslagen

8.1 Konsekvenser för cybersäkerheten

Regeringens bedömning

Förslagen bidrar till en mer effektiv samverkan mellan Försvarets radioanstalt och samverkansmyndigheterna. Därigenom stärks cybersäkerheten i samhället.

Utredningens bedömning

Bedömningen som görs i betänkandet stämmer överens med regeringens.

Remissinstanserna
Remissinstanserna ställer sig bakom eller har inga synpunkter på bedömningen.

Skälen för regeringens bedömning

Utredningen redogör noggrant för konsekvenserna av verksamhetsöverföringen i betänkandet. Flertalet remissinstanser framför synpunkter om huruvida utredningens förslag bör genomföras och kommer att få avsedd effekt. Genom förslagen i denna proposition, som inte behandlar själva verksamhetsöverföringen utan endast informationsutbyte och personuppgiftsbehandling som krävs med anledning av verksamhetsöverföringen, får Försvarets radioanstalt (FRA) och samverkansmyndigheterna inom det nationella cybersäkerhetscentret (NCSC) bättre förutsättningar att utbyta information och samverka. Förslagen är förenliga med visionen som kommer till uttryck i regeringens nationella strategi för cybersäkerhet, Nationell strategi för cybersäkerhet 2025–2029, där ett välfungerande NCSC bidrar till att samordna samhällets arbete med att stärka den nationella cybersäkerhetsförmågan (se skr. 2024/25:121 s. 4). Förslagen innebär också att enskilda får bättre förutsättningar att lämna uppgifter till FRA utan risk för att uppgifterna sprids på ett sätt som i sig skulle kunna innebära risker genom att sårbarheter offentliggörs. Förslagen bidrar till en mer effektiv samverkan mellan FRA och samverkansmyndigheterna men förbättrar även förutsättningarna för informationsutbyte med enskilda. Förslagen stärker därmed cybersäkerheten i samhället.

8.2 Ekonomiska konsekvenser för den offentliga sektorn

Regeringens bedömning

De kostnader som kan uppstå till följd av förslagen kan hanteras inom berörda statliga myndigheters befintliga ekonomiska ramar.

Utredningens bedömning

Bedömningen som görs i betänkandet stämmer överens med regeringens.

Remissinstanserna
Remissinstanserna ställer sig bakom eller har inga synpunkter på bedömningen. *Certezza AB* delar utredningens uppfattning att det finns ett behov av ökade utbildningsinsatser kring sekretessregelverket.

Skälen för regeringens bedömning

Förslaget i avsnitt 5.1 som rör informationsutbyte berör Försvarets radioanstalt (FRA) men även Försvarets materielverk, Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen i egenskap av samverkansmyndigheter. Vilka

myndigheter som ska omfattas av lagen föreslås dock inte regleras i den nya lagen och frågan är därmed inte föremål för behandling i denna proposition. Ett visst behov av utbildning kan, som utredningen och *Certezza AB* nämner, antas uppkomma kopplat till tillämpningen av den föreslagna lagen för de som omfattas av densamma. Framför allt kan behovet förväntas röra befintlig sekretesslagstiftning och hur intresseavvägningen enligt förslaget kan göras. Den tillkommande kostnaden för utbildning avseende den föreslagna uppgiftsskyldigheten bedöms vara av marginell karaktär och rymmas inom befintliga ekonomiska ramar.

Förslaget om en ny registerlag för FRA i avsnitt 6 kan också innebära behov av utbildning, vilket kan innebära kostnader för myndigheten. Den föreslagna lagen ska dock komplettera den allmänna dataskyddsregleringen. Den eventuella tillkommande kostnaden för utbildning med anledning av förslaget bedöms vara så låg jämfört med kostnaden i dag att den bör rymmas inom FRA:s befintliga ekonomiska ramar.

Förslaget till en ny sekretessbestämmelse i avsnitt 5.2 kan komma att medföra att FRA behöver ta ställning till och fatta fler beslut om utlämnande av allmänna handlingar. Fler beslut kan i sin tur leda till fler avslagsbeslut som kan överklagas till domstol. I vilken omfattning detta kommer att öka beror till viss del på i vilken utsträckning FRA behandlar aktuella uppgifter om enskilda. Den eventuella tillkommande kostnaden för denna hantering bedöms dock, för såväl FRA som domstolarna, vara så begränsad att den ryms inom befintliga ekonomiska ramar.

8.3 Konsekvenser för enskilda

Regeringens bedömning

Förslagen om en ny lag om uppgiftsskyldighet och registerlag innebär godtagbara inskränkningar av den personliga integriteteten.

Förslagen innebär ingen ökad administrativ börda eller kostnader för enskilda. Förslagen bedöms därmed inte ha någon ekonomisk påverkan på enskilda.

Utredningens bedömning

Bedömningen i betänkandet stämmer överens med regeringens.

Remissinstanserna

Remissinstanserna ställer sig bakom eller har inga synpunkter på bedömningen.

Skälen för regeringens bedömning

Uttrycket personlig integritet och konsekvenser för densamma

Någon enhetlig definition av uttrycket personlig integritet finns inte. En kränkning av den personliga integriteten har bland annat beskrivits som ett intrång i en fredad sfär som den enskilde bör vara tillförsäkrad och där ett

oönskat intrång, såväl psykiskt som fysiskt, bör kunna avvisas (se prop. 2005/06:173 s. 15).

Det finns ingen definition av vad uttrycket integritetsrisk rent konkret innebär i EU:s dataskyddsförordning. Däremot anges exempel på när risker typiskt sett kan uppkomma i skäl 75 till förordningen. Där nämns personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till bland annat skadat anseende eller förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt. Känsliga personuppgifter och uppgifter om lagöverträdelser anges också särskilt. Det anges också kunna föreligga integritetsrisker om behandling sker rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade. En särskild risk kan också föreligga om de registrerade hindras från att utöva kontroll över sina personuppgifter. Hur sannolik och allvarlig risken för den registrerades rättigheter och friheter är bör enligt skäl 76 fastställas utifrån behandlingens art, omfattning, sammanhang och ändamål. Risken bör utvärderas på grundval av en objektiv bedömning, genom vilken det fastställs huruvida uppgiftsbehandlingen inbegriper en risk eller en hög risk.

Uttrycket skyddsåtgärder förekommer i olika sammanhang i EU:s dataskyddsförordning. Uttrycket definieras inte i förordningen men olika exempel anges. I artikel 6.4 e anges att lämpliga skyddsåtgärder kan inbegripa kryptering eller pseudonymisering. I svensk kontext har uttalats att skyddsåtgärder som avses i artikel 9.2 g i EU:s dataskyddsförordning exempelvis kan bestå i bestämmelser som reglerar sekretess, rätt till partsinsyn och föreskrifter om informationssäkerhet och gallring samt bestämmelser om sökbegränsningar (se prop. 2017/18:105 s. 88). Vid införandet av sekretessbrytande bestämmelser har de villkor som gäller för uppgiftslämnandet ansetts utgöra skyddsåtgärder i denna mening (se exempelvis prop. 2019/ 20:123 s. 41). Skyddsåtgärder torde därmed kunna förstås som åtgärder som begränsar det integritetsintrång som följer av en bestämmelse.

Risken för integritetsintrång kopplat till lagen om uppgiftsskyldighet

Förslaget om en ny lag om uppgiftsskyldighet i avsnitt 5.1 bör innebära att myndigheterna som omfattas av regleringen kommer att utbyta fler sekretessreglerade uppgifter med varandra, vilket också är syftet med regleringen. Vilka enskilda myndigheter som ska omfattas av sekretessgenombrottet föreslås inte regleras i lag. Det kan ändå konstateras att det i större utsträckning bör bli fråga om att utbyta uppgifter som omfattas av sekretess till skydd för allmänna intressen, än till skydd för enskilda intressen. Förslaget innebär inte i sig att myndigheter kommer att vara skyldiga att utföra någon ny slags personuppgiftsbehandling. Uppgifter kan också lämnas ut anonymiserat eller utan att personuppgifter förekommer. Det är samtidigt rimligt att anta att uppgiftsskyldigheten kommer att innebära att fler personuppgifter utbyts mellan berörda myndigheter. Att avgöra omfattningen av den personuppgiftsbehandling som aktualiseras av förslaget om uppgiftsskyldighet är dock svårt. Som konstateras i avsnitt 5.1 möjliggörs genom förslaget att myndigheterna får del av fler

uppgifter från fler uppgiftskategorier, som kommer från flera olika myndigheter. Detta kan i sig utgöra en viss integritetsrisk.

Förutom själva utlämnandet av uppgifter kan till exempel strukturering, kontroll, bearbetning och justering av uppgifter behöva göras, vilket alltsammans innebär personuppgiftsbehandling. I sammanhanget kan även det arkivrättsliga regelverket nämnas, vilket bland annat medför att mottagande myndigheter som utgångspunkt måste behandla inkomna uppgifter i sina arkiv. Myndigheterna som omfattas av lagen kan alltså komma att behandla personuppgifter i flera led när uppgifter utbyts med stöd av uppgiftsskyldigheten. Det bör i begränsad omfattning röra sig om integritetskänslig information. Behandling av känsliga personuppgifter och uppgifter om lagöverträdelser kommer dock kunna aktualiseras. Den nya lagen innehåller inte någon avgränsning till en eller flera särskilda uppgiftskategorier. Det är därför inte möjligt att bedöma integritetsriskerna med informationsutbytet för varje specifik uppgiftstyp. Riskerna i det enskilda fallet beror på ett antal faktorer, som till exempel vilken eller vilka myndigheter som tar del av vilka uppgifter, syftet med informationsutbytet samt eventuella skyldigheter för mottagaren att i sin tur lämna uppgifter vidare till andra aktörer. Uppgiftsskyldigheten är dock begränsad till när det finns ett konkret behov hos den mottagande myndigheten för att den ska kunna delta i centrets verksamhet. Informationsdelning får inte ske i syfte att information ska användas i den ordinarie verksamheten hos mottagande myndighet, om det saknas koppling till den reglerade samverkan som ska ske inom ramen för det nationella cybersäkerhetscentrets (NCSC) verksamhet.

Spridningen av personuppgifter kommer ske inom den offentliga sektorn. Myndigheterna är genom dataskyddsregleringen och legalitetsprincipen förhindrade att behandla andra eller fler uppgifter än de som krävs för att de ska kunna utföra sina författningsreglerade uppgifter. Hur personuppgifterna behandlas inom den mottagande myndighetens verksamhet regleras av den lagstiftning som gäller för respektive myndighet.

Den intresseavvägning som ska göras enligt den nya lagen inför ett utlämnande av uppgifter innebär ytterligare begränsning till skydd för enskildas personliga integritet. Som utgångspunkt bör de uppgifter som lämnas mellan myndigheterna omfattas av sekretess – antingen sekretess som är tillämplig oavsett var uppgiften förekommer, eller annan sekretess och till exempel till följd av den bestämmelse som föreslås i avsnitt 5.2. Detta utgör också en skyddsåtgärd som begränsar integritetsintrånget.

Genom förslaget om uppgiftsskyldighet möjliggörs att myndigheterna får del av fler uppgifter, som kommer från flera olika myndigheter. Det finns en risk att flera olika uppgifter om enskilda kan ge en mer heltäckande bild av personens livssituation och förehavanden än om uppgifterna hålls åtskilda. Myndigheterna kan också få en mer heltäckande bild av personers förehavanden som indikerar involvering i brottslig verksamhet. Mängden uppgiftskategorier som kan utbytas med stöd av bestämmelserna kan alltså i sig anses utgöra en viss integritetsrisk. Det är dock inte fråga om övervakning eller kartläggning av enskildas personliga förhållanden (se vidare avsnitt 5.1).

Uppgiftslämnande som kan ske enligt den nya lagen om uppgiftsskyldighet är sammanfattningsvis förenat med viss integritetsrisk men

också ett antal skyddsåtgärder. Det är, som utvecklas i avsnitt 5.1, mycket angeläget att det myndighetsgemensamma arbetet inom NCSC fungerar effektivt och ändamålsenligt. För att det arbetet ska kunna bedrivas på bästa sätt krävs att kontaktvägarna är korta mellan myndigheterna och att det finns tydliga förutsättningar för informationsutbyte mellan dessa. Även om informationsdelning inte är ensamt avgörande för att NCSC:s arbete ska kunna bedrivas framgångsrikt så är förslaget nödvändigt för att NCSC ska kunna präglas av en effektiv samverkan. Som beskrivs i avsnitt 5.1 är det inte heller möjligt att åstadkomma samma resultat med någon mindre långtgående reglering, till exempel en sekretessbrytande bestämmelse. Förslaget är därmed nödvändigt och proportionerligt för att nå syftet med regleringen och vidare förenligt med det dataskyddsrättsliga regelverket. Konsekvenserna för den personliga integriteten är därmed godtagbara.

Registerlagen

Förslaget om införandet av en ny registerlag för Försvarets radioanstalt (FRA) i avsnitt 6 innebär att myndigheten får utökade möjligheter att behandla personuppgifter, jämfört med vad som gäller i dag. Det kan också förutsättas att personuppgiftsbehandlingen kommer att öka med anledning av förslaget. FRA ges vidare enligt förslaget ett uttryckligt stöd för behandlingen av känsliga personuppgifter. En stor del av informationsutbytet inom ramen för NCSC:s verksamhet kommer att kunna ske i anonymiserad form. Även om förslaget inte utesluter att uppgifter som rör särskilt skyddsvärda grupper, som personer med skyddade personuppgifter och barn, kan komma att behandlas så har inte utredningen identifierat några särskilda situationer där förslagen skulle kunna leda till sådan behandling. Sådan personuppgiftsbehandling torde därmed, som utredningen anger, ske i begränsad omfattning till följd av förslaget. Även om behandling av känsliga personuppgifter och uppgifter om lagöverträdelser kan förväntas ske i begränsad omfattning så innebär förslagen ändå en viss särskild risk i detta avseende som utredningen nämner.

Förslaget är samtidigt nödvändig för att uppnå det eftersträvade målet, vilket bland annat är att FRA ska kunna behandla personuppgifter på ett tillfredsställande sätt inom ramen för den verksamhet som NCSC bedriver. Samhällsintresset av ett effektivt cybersäkerhetsarbete är, som utvecklas i avsnitt 4.1, angeläget. Syftet med den nya lagen är dessutom även att skydda människor mot att deras personliga integritet kränks. Förslaget innehåller vidare begränsningar på så sätt att FRA, med stöd av den nya lagen, endast får behandla personuppgifter i den utsträckning som är nödvändig för att utföra sina arbetsuppgifter inom NCSC. Dessutom föreslås en rad säkerhetsåtgärder, som sökbegränsningar och begränsad tillgång till personuppgifterna samt en ny sekretessbestämmelse till skydd för enskilda inom ramen för NCSC:s verksamhet (se vidare avsnitt 5.2). Sammantaget bedömer regeringen, i likhet med utredningen, att de bestämmelser som föreslås uppfyller kraven på nödvändighet och proportionalitet. Förslaget är vidare förenligt med det dataskyddsrättsliga regelverket. Konsekvenserna för den personliga integriteten är därmed godtagbara.

NCSC 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. Centret ska också bland annat lämna råd och stöd till privata aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet och vid it-incidenter (3 § NCSC-förordningen). Förslaget i avsnitt 5.1 ger bättre förutsättningar för FRA och samverkansmyndigheterna att utföra sitt gemensamma uppdrag, vilket i sig kan få positiva effekter för enskilda som behöver stöd i sitt cybersäkerhetsarbete. Förslaget i avsnitt 5.2 innebär också att känsliga uppgifter om enskilda kommer att omfattas av sekretess. Förslagen innebär inte någon ökad administrativ börda eller kostnader för enskilda. Förslagen bedöms därmed inte ha någon ekonomisk påverkan på enskilda eller innebära några övriga konsekvenser.

8.4 Övriga konsekvenser

Regeringens bedömning

Förslagen kan få positiv inverkan på det brottsförebyggande arbetet. Förslagen kommer inte att medföra några andra konsekvenser.

Utredningens bedömning

Bedömningen från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen gör ingen särskild bedömning i fråga om inverkan på det brottsförebyggande arbetet.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning

Det nationella cybersäkerhetscentret (NCSC) har till uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter (4 a § FRA:s instruktion). NCSC ska bland annat lämna råd och stöd till privata och offentliga aktörer i frågor om hot, sårbarheter och risker med koppling till cybersäkerhet och lämna råd och stöd till aktörer vid it-incidenter. Genom förslagen får Försvarets radioanstalt och samverkansmyndigheterna inom NCSC bättre förutsättningar att utbyta information och samverka och kan därmed samverka på ett mer effektivt sätt. En effektivisering av NCSC:s verksamhet innebär att det skapas förutsättningar för en ökad cybersäkerhet i samhället. Förslagen kan i förlängningen leda till att brott på cybersäkerhetsområdet förebyggs, upptäcks, förhindras och beivras. Förslagen bedöms därför få viss betydelse för det brottsförebyggande arbetet.

Förslagen bedöms inte ha betydelse för sysselsättning och offentlig service i olika delar av landet. Förslagen bedöms inte heller ha betydelse

för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen eller få några andra konsekvenser.

9 Författningskommentar

9.1 Förslaget till lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret

En ny lag om uppgiftsskyldighet införs. Lagen gäller när Försvarets radioanstalt (FRA) och andra myndigheter samverkar inom det nationella cybersäkerhetscentret (NCSC). NCSC är placerat inom FRA. Allmänna överväganden om behovet av en ny lag finns i avsnitt 5.1. I följande avsnitt kommenteras förslagen till den nya lagen.

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.

I paragrafen regleras bland annat lagens innehåll och tillämpningsområde. Paragrafen utformas efter synpunkter från *Lagrådet*. Övervägandena finns i avsnitt 5.1.

En förutsättning för att lagen ska vara tillämplig är att det är fråga om samverkan mellan FRA och andra myndigheter inom ramen för den verksamhet som bedrivs inom NCSC. Myndigheternas samverkan regleras i förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen).

Av paragrafen framgår också att regeringen bestämmer vilka myndigheter som ska omfattas av skyldigheten att lämna uppgifter och vilka myndigheter som ska få ta emot uppgifter med stöd av lagen. Som utgångspunkt kommer detta att framgå av NCSC-förordningen.

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.

Paragrafen innebär en sekretessbrytande uppgiftsskyldighet för de myndigheter som omfattas av lagen enligt 1 §. Övervägandena finns i avsnitt 5.1.

Av *första stycket* följer att skyldigheten att lämna ut en uppgift gäller vid samverkan inom NCSC:s verksamhet. Uppgiftsskyldigheten gäller mellan såväl FRA och en samverkansmyndighet som samverkansmyndigheter

sinsemellan, under förutsättning att myndigheterna omfattas av lagen enligt 1 §. Utbyte av uppgifter mellan myndigheterna i andra sammanhang får ske med stöd av andra bestämmelser, till exempel generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen (2009:400) (OSL). Uppgiftsskyldigheten gäller vidare endast då en myndighet har behov av att få en viss uppgift från en annan myndighet för att kunna delta i samverkan. Behovet av uppgifter kan variera eftersom myndigheternas deltagande i NCSC:s verksamhet kan se ut på olika sätt. Som exempel på när en myndighet kan anses ha behov av uppgifter kan nämnas att FRA behöver information om status för en pågående it-attack och vilka tekniska lösningar en drabbad aktör använder för att FRA ska kunna bidra med rekommendationer om motåtgärder. Det är den utlämnande myndigheten som prövar om förutsättningarna för utlämnande är uppfyllda. Eftersom lagen innebär en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL, ger den inte stöd för utlämnande av uppgifter som härrör från tillämpning av sådana internationella avtal och rättsakter som nämns i exempelvis 15 kap. 1 a § OSL.

Av *andra stycket* följer att en uppgift inte ska lämnas ut 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. Detta innebär att den utlämnande myndigheten ska göra en intresseavvägning innan en uppgift lämnas ut. För att en intresseavvägning ska bli aktuell krävs det inte att uppgiften omfattas av sekretess i den konkreta situationen. Det är i stället tillräckligt att uppgiften omfattas av en sekretessbestämmelses räckvidd. Bedömningen av om en uppgift ska lämnas ut bör kunna göras utifrån det behov av sekretess som typiskt sett finns för en viss kategori av uppgifter (se till exempel prop. 2024/25:180 s. 44).

Kravet på övervägande skäl innebär att behovet av en viss uppgift hos den mottagande myndigheten normalt ska ha företräde framför andra intressen. Det råder därmed en presumtion för uppgiftslämnande. Det kan dock exempelvis finnas utrymme för att avstå från att lämna ut uppgifter om metoder, förmågor, namn på uppdragsgivare och liknande uppgifter som skyddas av utrikessekretess enligt 15 kap. 1 § OSL eller försvarssekretess enligt 15 kap. 2 § samma lag. Även uppgifter som skyddas av underrättelsesekretess enligt 18 kap. 2 § OSL skulle, beroende på omständigheterna i det enskilda fallet, kunna hänföras till denna kategori. Det kan också finnas skäl att avstå från uppgiftslämnande om det rör sig om uppgifter av särskilt integritetskänslig art, till exempel känsliga personuppgifter enligt artikel 9.1 i 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).

Vid intresseavvägningen ska, som utgångspunkt, också sekretesskyddet hos mottagaren vägas in. En omständighet som i det sammanhanget kan få betydelse för intresseavvägningen är reglerna om partsinsyn, som kan innebära att sekretessen hos mottagaren kan få ge vika för en parts rätt till insyn i handläggningen av ett mål eller ärende. Det faktum att styrkan i sekretessen skiljer sig åt hos den utlämnande och den mottagande myndigheten är dock inte av avgörande betydelse.

9.2 Förslaget till lag om Försvarets radioanstalts behandling av personuppgifter inom det nationella cybersäkerhetscentret

En ny lag om personuppgiftsbehandling införs. Lagen gäller när Försvarets radioanstalt (FRA) behandlar personuppgifter inom det nationella cybersäkerhetscentret (NCSC). Allmänna överväganden om behovet av en ny lag finns i avsnitt 6.1. I följande avsnitt kommenteras förslagen till den nya lagen.

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.

Paragrafen anger syftet med lagen. Övervägandena finns i avsnitt 6.1.

Enligt paragrafen är syftet med lagen dubbelt. Lagen ska dels göra det möjligt för FRA att behandla personuppgifter på ett ändamålsenligt sätt inom NCSC, dels 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.

Paragrafen anger tillämpningsområdet för lagen. Paragrafen kompletteras genom 3–5 §§ som anger lagens förhållande till annan dataskyddsreglering. Övervägandena finns i avsnitt 6.1 och 6.2.

Av *första stycket* framgår att lagen gäller FRA:s behandling av personuppgifter när myndigheten 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. I 4 § anges att lagen innehåller kompletterande bestämmelser till 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) (EU:s dataskyddsförordning). Definitioner av uttrycken behandling och personuppgifter finns i artikel 4.1 och 4.2 i EU:s dataskyddsförordning.

Andra stycket innebär att lagens tillämpningsområde är begränsat till att avse en viss typ av personuppgiftsbehandling, nämligen då behandlingen är helt eller delvis automatiserad eller då det rör sig om personuppgifter som ingår i eller kommer att ingå i ett register. Med register avses en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller

spridd på grundval av funktionella eller geografiska förhållanden (se artikel 4.6 i EU:s dataskyddsförordning). Manuell behandling av personuppgifter som inte ingår eller kommer att ingå i ett register faller utanför lagens tillämpningsområde.

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.

I paragrafen anges att lagen inte gäller vid behandling av personuppgifter som omfattas av lagen om behandling av personuppgifter vid Försvarets radioanstalt (FRAPuL). FRAPuL gäller vid behandling av personuppgifter i myndighetens försvarsunderrättelse- och utvecklingsverksamhet samt informationssäkerhetsverksamhet (se 1 kap. 2 § samma lag). Övervägandena finns i avsnitt 6.2.

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.

I paragrafen anges att lagen innehåller kompletterande bestämmelser till EU:s dataskyddsförordning. Detta innebär att lagen inte kan tillämpas fristående, utan endast tillsammans med den förordningen (se till exempel prop. 2017/18:105 s. 183). Hänvisningen till EU:s dataskyddsförordning är dynamisk och avser förordningen i dess vid varje tidpunkt gällande lydelse. Övervägandena finns i avsnitt 6.2.

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.

Paragrafen anger lagens förhållande till lagen med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och föreskrifter som har meddelats i anslutning till den lagen. Dataskyddslagen, som kompletterar EU:s dataskyddsförordning, är subsidiär i förhållande till den nya lagen. Om inte annat följer av den nya lagen eller föreskrifter som har meddelats i anslutning till lagen, gäller dataskyddslagen (se till exempel prop. 2023/24:146 s. 90). Övervägandena finns i avsnitt 6.2.

Personuppgiftsansvar

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

Paragrafen reglerar personuppgiftsansvaret vid behandling av personuppgifter enligt lagen. Övervägandena finns i avsnitt 6.2.

En definition av uttrycket personuppgiftsansvarig finns i artikel 4.7 i EU:s dataskyddsförordning. Av EU:s dataskyddsförordning följer vissa skyldigheter för den som är personuppgiftsansvarig. Den personuppgifts-

ansvarige ansvarar bland annat för att kunna visa att behandlingen av personuppgifter sker på ett korrekt sätt (artikel 5.1 och 5.2), att se till att lämpliga tekniska och organisatoriska åtgärder genomförs (artikel 24.1) och att den registrerade ersätts för skada som en rättsstridig behandling av personuppgifter har medfört (artikel 82). FRA är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt lagen.

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.

I paragrafen anges för vilka primära ändamål personuppgifter får behandlas. Övervägandena finns i avsnitt 6.3.

Personuppgifter får behandlas om det är nödvändigt för att FRA inom NCSC ska kunna utföra uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Det primära ändamålet är brett formulerat och FRA måste normalt precisera ändamålet när uppgifter samlas in, för att leva upp till kravet på särskilda, uttryckligt angivna och berättigade ändamål i artikel 5.1 b i EU:s dataskyddsförordning (se till exempel prop. 2023/24:146 s. 91). Att behandlingen ska vara nödvändig innebär inte ett krav på att den ska vara oundgänglig. Behandlingen kan anses nödvändig om den leder till effektivitetsvinster (se till exempel prop. 2017/18:105 s. 189). Kravet på nödvändighet innebär dock att personuppgifter inte får behandlas om syftet med behandlingen kan uppnås med andra medel, till exempel genom att anonymisera uppgifterna.

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.

Paragrafen anger för vilka sekundära ändamål personuppgifter får behandlas. Övervägandena finns i avsnitt 6.3.

Av *första stycket* framgår att personuppgifter som får behandlas enligt 7 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandling får då ske både för uppgiftslämnande som sker på grund av en skyldighet att lämna ut uppgifter och för uppgiftslämnande som sker med stöd av bestämmelser som innebär att uppgifter får lämnas ut, till exempel den så kallade generalklausulen i 10 kap. 27 § offentlighets- och sekretesslagen (2009:400) (OSL).

Andra stycket uttrycker att den så kallade finalitetsprincipen i artikel 5.1 b i EU:s dataskyddsförordning gäller vid behandling av personuppgifter enligt lagen och bestämmelsen har samma innebörd som den artikeln. Detta innebär att bland annat behandling för arkivändamål av allmänt intresse, vetenskapliga forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 i EU:s dataskyddsförordning inte ska anses vara oförenlig med de ursprungliga ändamålen. Det innebär också att de

omständigheter som anges i artikel 6.4 i EU:s dataskyddsförordning ska beaktas vid bedömningen av om behandlingen är förenlig med finalitetsprincipen.

Tillgången till personuppgifter

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

Paragrafen reglerar den interna tillgången till personuppgifter. Övervägandena finns i avsnitt 6.4.

Av paragrafen följer att FRA är skyldig att se till att tillgången till personuppgifter begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter. Uttrycket var och en inkluderar tillsvidareanställd personal men även till exempel personer med en tidsbegränsad anställning eller uppdragstagare. FRA ska ta ställning till vilket informationsbehov ett tjänsteåliggande eller uppdrag medför och ge den behörighet som behövs utifrån det. Tillgången kan begränsas genom tekniska och organisatoriska åtgärder (jfr artikel 32 i EU:s dataskyddsförordning).

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.

Paragrafen anger när känsliga personuppgifter får behandlas. Övervägandena finns i avsnitt 6.5.

Känsliga personuppgifter är sådana särskilda kategorier av uppgifter som räknas upp i artikel 9.1 i EU:s dataskyddsförordning, det vill säga personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Av paragrafen framgår att FRA får behandla sådana uppgifter, med stöd av artikel 9.2 g i EU:s dataskyddsförordning, endast om uppgifterna är nödvändiga för fullgörandet av uppgiften som anges i 2 § första stycket. Nödvändighetsrekvisitet har samma innebörd som i 7 § (jfr prop. 2017/18:105 s. 75 och 76). Hänvisningen till EU:s dataskyddsförordning är dynamisk.

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

Paragrafen innebär en sökbegränsning. Övervägandena finns i avsnitt 6.6.

Det är enligt paragrafen förbjudet att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter. Sökbegränsningen omfattar alla tekniska åtgärder som innebär att uppgifter används för att strukturera eller systematisera information i syfte att få fram ett urval av personer grundat på sådana uppgifter. Därmed förbjuds

sökningar som görs för att få fram ett urval av personer som exempelvis har en viss politisk åsikt eller religiös åskådning. Däremot hindrar paragrafen inte sökningar som görs i ett annat syfte än att identifiera ett urval av individer, till exempel för att ta fram verksamhetsstatistik eller för registervård (se till exempel prop. 2025/26:88 s. 213).

Elektroniskt utlämnande av personuppgifter

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

Paragrafen reglerar förutsättningarna för elektroniskt utlämnande. Övervägandena finns i avsnitt 6.7.

Paragrafen innebär att elektroniskt utlämnande på annat sätt än genom direktåtkomst är tillåtet om det inte är olämpligt. Det kan vara fråga om att utlämnande sker genom att personuppgifter lämnas ut på usb-minne, genom e-post eller genom direkt överföring från ett datasystem till ett annat via elektroniska kommunikationsnät (se till exempel prop. 2022/23:34 s. 140). Vid bedömningen av om ett elektroniskt utlämnande är olämpligt bör bland annat beaktas vilken slags personuppgifter det är fråga om. Vem som är mottagare av uppgifterna har också betydelse för bedömningen av om ett utlämnande är olämpligt. Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informationssäkerheten hos mottagaren vägas in.

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.

Paragrafen reglerar hur länge personuppgifter får behandlas. Övervägandena finns i avsnitt 6.8.

I *första stycket* föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen i det enskilda fallet. Paragrafen innebär en skyldighet för FRA att upphöra med behandlingen av personuppgifter så snart personuppgifterna inte längre behövs med hänsyn till det ändamål för vilket de behandlas.

Av *andra stycket* framgår att regleringen om längsta tid för behandling inte hindrar att personuppgifterna arkiveras och bevaras av FRA 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.

Paragrafen innebär ett undantag från den registrerades rätt att göra invändningar enligt EU:s dataskyddsförordning. Övervägandena finns i avsnitt 6.9.

Av artikel 21.1 i EU:s dataskyddsförordning följer att den registrerade har rätt att när som helst invända mot myndigheters behandling av personuppgifter avseende honom eller henne som grundar sig på sådan behandling som är nödvändig för att utföra en uppgift av allmänt intresse. Enligt artikel 23 i förordningen kan dock rätten att göra invändningar begränsas under vissa förutsättningar. Undantaget utgör en sådan begränsning i den nationella rätten som är tillåten enligt artikel 23 i EU:s dataskyddsförordning. Hänvisningen till förordningen är dynamisk.

9.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

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.

Paragrafen, som är ny, reglerar sekretess hos Försvarets radioanstalt (FRA) i verksamhet vid det nationella cybersäkerhetscentret (NCSC). Övervägandena finns i avsnitt 5.2.

Av *första stycket* framgår att sekretess gäller hos FRA i verksamhet vid NCSC 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. Med enskild avses såväl en fysisk som en juridisk person. Paragrafen tar bland annat sikte på uppgifter om enskildas affärs- och driftförhållanden och uppgifter om identiteten på den som har rapporterat en sårbarhet. Skaderekvisitet är omvänt, vilket innebär att sekretess gäller om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Av *andra stycket* följer att uppgifter som förekommer vid handläggning av ett ärende om statligt stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning inte omfattas av bestämmelsens tillämpningsområde. Sekretessen gäller därmed inte i ett ärende om stöd enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

Enligt *tredje stycket* gäller för uppgift i en allmän handling sekretessen i högst sjuttio år.

8 § 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.

I paragrafen regleras rätten att meddela och offentliggöra uppgifter. Paragrafen ändras så att den nya 7 i § omfattas av den uppräkning av paragrafer som görs. Rätten att meddela och offentliggöra uppgifter får därmed inte företräde framför den tystnadsplikt som följer av 7 i §. Övervägandena finns i avsnitt 5.2.

Sammanfattning av betänkandet Samlade förmågor för ökad cybersäkerhet (SOU 2025:79)

Uppdraget

Utredningens uppdrag har varit 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 (MSB) till Försvarets radioanstalt (FRA). Därutöver har utredningen haft i uppdrag att analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling. Det har ingått i uppdraget att lämna nödvändiga författningsförslag.

Verksamhetsöverföring

Utgångspunkter

Enligt kommittédirektivet ska en organisatorisk åtskillnad mellan stödjande verksamhet och tillsynsverksamhet inom cybersäkerhetsområdet upprätthållas när arbetsuppgifter flyttas till FRA. En annan utgångspunkt för verksamhetsöverföringen är att skapa en tydlig ansvarsfördelning, utan överlapp eller dubblering av uppgifter och ansvar, och att verksamheten ska kunna bedrivas effektivt utifrån de behov som finns att samla informations- och cybersäkerhetsfrågorna. Överföringen av arbetsuppgifter från MSB till FRA får vidare inte påverka Sveriges möjligheter att uppfylla sina EU-rättsliga förpliktelser eller få del av EU-rättsligt stöd. Förslagen får inte heller medföra krav på insyn från EU i FRA:s verksamhet som rör nationell säkerhet och försvar eller i övrigt inverka negativt på denna verksamhet.

Med hänsyn till utgångspunkterna för uppdraget har utredningen haft som målsättning att samla FRA:s och MSB:s uppgifter inom informations- och cybersäkerhet i det nationella cybersäkerhetscentret (NCSC). Centret är placerat inom FRA. Utredningens bedömning är att en sådan kraftsamling på området kommer att leda till synergier som i sin tur kommer att öka Sveriges strategiska och operativa förmåga på informations- och cybersäkerhetsområdet. En sådan förmågehöjning i NCSC ligger även i linje med regeringens vision för centret som framgår av den nationella cybersäkerhetsstrategin. Eftersom NCSC inte är en fristående myndighet är det dock FRA som anges i de författningsändringar som föreslås.

Centrala delar av MSB:s verksamhet på informations- och cybersäkerhetsområdet ska föras över till FRA

Då utredningen har funnit att FRA och MSB har överlappande ansvarsområden på informations- och cybersäkerhetsområdet föreslår utredningen att centrala delar av MSB:s verksamhet på informations- och cybersäkerhetsområdet ska föras över till FRA. Förslagen innebär bland

annat att följande uppgifter som regleras i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap ska föras över till FRA.

- Ansvaret för att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt analysera och bedöma omvärldsutvecklingen som nu återfinns i 11 a § första stycket.
- Rapporteringsskyldigheten till regeringen på informations- och cybersäkerhetsområdet som regleras i 11 a § andra och tredje stycket.
- Uppdraget att ha en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter som i dag regleras i 11 b §.
- MSB:s uppdrag enligt 11 c § att utgöra nationellt samordningscenter (NCC-SE) enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (CCCN-förordningen)
- Uppgiften i 18 j § att utgöra teknisk kontaktpunkt för Organisationen för säkerhet och samarbete i Europa.

MSB har ansvaret för informations- och cybersäkerhetsarbetet i det nationella beredskapssystemet. För statliga myndigheter regleras detta i förordning (2022:524) om statliga myndigheters beredskap. Förslagen innebär att ansvaret för incidentrapporteringsfunktionen enligt regleringen överförs till FRA. Därtill får FRA i uppdrag att ansvara för föreskrifter för beredskapsmyndigheternas arbete med informationssäkerhet.

Europaparlamentets och rådet 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 (NIS 2-direktivet) gäller sedan 2024 och medför ytterligare krav på cybersäkerhetsområdet för både offentliga och privata aktörer. Arbetet pågår med att genomföra direktivet i svensk rätt. I betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) ges förslag på en ny lag om cybersäkerhet och förordning om cybersäkerhet. I förslaget till förordning om cybersäkerhet ges MSB rollen som CSIRT-enhet, gemensam kontaktpunkt samt cyberkrishanteringsmyndighet. MSB ges även ansvaret för att meddela vissa föreskrifter och stå värd för ett samarbetsforum för de myndigheter som tilldelas tillsynsuppgifter i förordningen. Utredningens bedömning är att FRA uppfyller samtliga krav för att utföra motsvarande uppgifter. Utredningen föreslår därför att FRA ska utses till CSIRT-enhet, gemensam kontaktpunkt och cyberkrishanterings-myndighet. FRA ska även få ansvar för tillsynssamordning och ett visst föreskriftsansvar.

MSB behåller ansvaret för säkra kommunikationstjänster

Förslagen innehåller inte en överföring av uppgifter avseende säkra kommunikationstjänster, beslut om tilldelning av signalskyddssystem, ledningsmetoder och stödsystem samt uppdrag inom unionens

rymdprogram och GPRS. Dessa uppdrag är intimt sammankopplade med myndighetens övriga arbete med krisberedskap och civilt försvar. MSB har vidare en särskild upparbetad kompetens på dessa områden. Uppgifterna är även sådana att MSB ensam är ansvarig för dem och uppgifterna överlappar inte på något betydande sätt med de övriga uppgifter som omfattas av verksamhetsöverföringen.

Informationshanteringen hos NCSC ska förenklas

En ny lag om uppgiftsskyldighet vid samverkan i verksamhet inom NCSC

Utredningen föreslår en ny lag med en skyldighet för NCSC och samverkansmyndigheterna att lämna information till varandra. Uppgiftsskyldigheten bryter sekretess med stöd av 10 kap. 28 § offentlighets- och sekretesslagen (2009:400), förkortad OSL. Lagen gäller vid samverkan i verksamhet inom NCSC. Inom ramen för denna samverkan ska en myndighet lämna en uppgift till en annan myndighet om det behövs för den mottagande myndighetens deltagande i samverkan.

Skyldigheten att lämna uppgifter skulle både underlätta informationsdelningen inom NCSC och skapa ett tydligt incitament för NCSC och samverkansmyndigheterna att lämna den information som behövs. I vissa situationer kan det finnas skäl att avstå från att lämna ut en uppgift och utredningen föreslår därför att en intresseavvägning ska göras. 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.

En ny sekretessbestämmelse till skydd för enskilda

Utredningen bedömer att uppgifter om enskildas personliga och ekonomiska förhållanden och som förekommer hos NCSC bör skyddas av sekretess. Det finns utmaningar gällande informationsdelning med näringslivet. Utmaningarna handlar om att privata aktörer befarar att exempelvis affärshemligheter sprids. Detta kan innebära att man undviker att lämna uppgifter till NCSC. Även NIS 2-direktivets krav på anonymitet aktualiserar ett sekretessbehov för vissa typer av uppgifter. Bedömningen görs att befintlig lagstiftning inte omfattar alla uppgifter som behöver skyddas av sekretess. Med anledning av detta föreslås en bestämmelse om sekretess som ska gälla uppgifter som förekommer hos NCSC. Sekretessen ska gälla för enskildas personliga eller ekonomiska förhållanden med ett omvänt skaderekvisit. Utredningen föreslår också att den tystnadsplikt som följer av sekretessbestämmelsen ska ha företräde framför den så kallade meddelarfriheten enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Handläggningen av ärenden enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning ska inte omfattas av sekretessbestämmelsens tillämpningsområde.

Ytterligare förslag till ändringar av offentlighets- och sekretesslagstiftningen har lagts fram i slutbetänkandet *Motståndskraft i*

samhällsviktiga tjänster (SOU 2024:64). Vid en överföring av arbetsuppgifter från MSB till FRA så behöver dessa förslag omfatta FRA i stället för MSB. Utredningen har därför lämnat förslag om ändringar även avseende dessa delar.

En ny lag om personuppgiftsbehandling hos NCSC

Utredningen bedömer att behandlingen av personuppgifter inom den verksamhet som bedrivs av NCSC omfattas 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) med kompletterande lagstiftning. Utredningen föreslår en ny lag om personuppgiftsbehandling. Syftet med lagen är att ge FRA, inom ramen för NCSC:s verksamhet, möjlighet att behandla personuppgifter på ett ändamålsenligt sätt och att skydda människor mot att deras personliga integritet kränks vid sådan behandling.

Personuppgifter ska få behandlas om det är nödvändigt för att FRA ska kunna utföra de uppgifter som ankommer på NCSC att utföra. Personuppgifter ska också få behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning.

Den föreslagna lagen innehåller flera olika skyddsåtgärder som avser att ge enskildas personliga integritet ett tillfredsställande skydd. Som exempel kan nämnas att tillgången till personuppgifter ska begränsas till det som var och en behöver för att kunna fullgöra sina arbetsuppgifter. Lagen innehåller också en bestämmelse om sökbegränsningar avseende känsliga personuppgifter.

Förslagens konsekvenser

Konsekvenser för MSB och FRA

För FRA innebär förslagen att myndigheten får ett utökat uppdrag inom arbetet med samhällets informations- och cybersäkerhet. De nya uppgifterna kommer verksamhetsmässigt utföras i NCSC.

För att arbetet i centret ska kunna fungera krävs att denna del av myndighetens verksamhet bedrivs på ett öppet sätt. Detta är väsentligt för att åstadkomma ett nära samarbete med såväl offentliga som privata aktörer i arbetet med samhällets samlade informations- och cybersäkerhet. Det är även en förutsättning för att Sverige ska kunna dra nytta av de stora ekonomiska satsningar som EU aviserat på området samt för att centret ska kunna verka i unionssamarbetet och ta till vara Sveriges intressen på ett ändamålsenligt sätt.

För MSB innebär förslagen organisatoriskt att verksamheterna för strategisk och operativ cybersäkerhet överförs till FRA. Däremot kommer myndigheten även fortsättningsvis bedriva verksamhet inom samhällsviktiga kommunikationstjänster. Myndigheten får därmed ett mer koncentrerat uppdrag vad gäller samordningen av frågor om skydd mot olyckor, krisberedskap och civilt försvar.

EU-rättsliga konsekvenser

Utredningens bedömning är att förslagen inte medför något hinder för Sverige att uppfylla sina förpliktelser i förhållande till EU. FRA har förutsättningar för att fullgöra de uppgifter som uppdragen som CSIRT-enhet, gemensam kontaktpunkt och cyberkrishanteringsmyndighet medför.

NIS 2-direktivet innehåller möjligheter att undanta information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. Det är därför möjligt för NCSC att uppfylla kraven på informationsdelning som NIS 2-direktivet medför utan att den sekretess som gäller för FRA:s verksamhet inom nationell säkerhet och försvar påverkas. FRA bedöms även ha förmågan att driva NCC-SE i enlighet med kraven i CCCN-förordningen. Förslagen bör inte heller minska Sveriges förmåga att ta emot EU-rättsligt stöd. MSB har tagit emot EU-stöd i sitt arbete med att implementera NIS 2-direktivet. Genom stödavtalen med EU är även FRA förpliktigad att tillgodose EU:s krav på insyn efter att uppgifterna enligt NIS 2-direktivet och tillhörande stödavtal förs över. Möjligheten för FRA att exkludera information med koppling till nationell säkerhet från att omfattas av EU:s revisionsrätt är begränsad, och kräver förhandlingar med kommissionen när frågan aktualiseras. För att tillmötesgå unionens krav på insyn behöver FRA därför organisera sin verksamhet på ett sådant sätt att verksamheten i NCSC särredovisas från myndighetens övriga verksamhet. På detta vis är det möjligt för EU att bedöma om EU-stödet har hanterats på ett korrekt sätt samtidigt som myndighetens övriga verksamhet inte omfattas av granskningen. Samma förutsättningar gäller för hanteringen av EU-stöd inom ramen för NCC-SE.

Parallellt med NIS 2-direktivet införs Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet) som syftar till att öka motståndskraften hos kritiska verksamhetsutövare. Enligt förslagen i slutbetänkandet *Motståndskraft i samhällskritiska verksamhetsutövare* (SOU 2024:64) ska MSB ges ansvaret för att ta emot incidentrapporter, utgöra kontaktpunkt samt utfärda föreskrifter. NIS 2- och CER-direktiven ställer krav på att regelverken ska implementeras på ett samordnat sätt. Utredningen bedömer att detta är möjligt även om rollerna enligt NIS 2-regelverket förs över till FRA. En nära samordning i frågorna mellan FRA och MSB, i synnerhet avseende rollen som cyberkrishanteringsmyndighet, kommer dock vara nödvändig.

NIS 2-regelverket utgör en bas för ytterligare EU-rättsakter på informationssäkerhetsområdet, där flera initiativ redan är i olika genomförandestadier. Utredningen identifierar flera sådana rättsakter som direkt påverkar arbetet i NCSC. Det är av vikt att hänsyn tas till de ytterligare uppgifter som dessa rättsakter kan komma att medföra för NCSC i det fortsatta arbetet med att utveckla centret.

Ekonomiska konsekvenser

Ekonomiska konsekvenser av verksamhetsöverföringen till FRA

Den verksamhet som omfattas av förslagen om verksamhetsöverföring uppgår i nuläget till cirka 85 medarbetare, med en uppskattad lönekostnad om 85 000 000 kronor. Lönekostnaderna kan dock antas komma att öka till följd av kommande rekryteringar. Därutöver tillkommer andra kostnader för driften av den verksamhet som förs över. Utredningen bedömer att verksamhetsöverföringen i huvudsak kan finansieras genom en omfördelning av anslag från MSB.

På kort sikt kommer förslagen leda till vissa merkostnader för verksamheterna. Storleken på dessa merkostnader är bland annat beroende av de arbetsrättsliga förhandlingar som kommer att ske inför verksamhetsöverföringen. Erfarenhetsmässigt leder också verksamhetsövergångar till andra merkostnader på grund av de inblandade organisationernas varierande förmåga att förena olika arbetskulturer, ta fram nya ledningsstrukturer med mera. Det är således svårt att i dagsläget uppskatta hur höga merkostnaderna kommer bli.

På lång sikt gör utredningen bedömningen att förslagen kan leda till minskade kostnader genom att kompetens samlas i en verksamhet, dubbelarbete minskas och synergieffekter uppnås.

Ekonomiska konsekvenser av förslagen rörande informationshantering

Förslagen om en ny lag om uppgiftsskyldighet, ändring i OSL och en ny registerlag bedöms inte medföra ett ökat resursbehov för de statliga myndigheter som berörs. Förslagen berör i första hand FRA men även samverkansmyndigheterna i NCSC. Det är framför allt förslaget om uppgiftsskyldighet som samverkansmyndigheterna berörs av.

Förslagen om uppgiftsskyldighet samt en särskild registerlag för NCSC kommer att medföra behov av utbildning av personal. Kostnaderna för dessa insatser bedöms dock vara sådana att de ryms inom befintliga ekonomiska ramar. Förslagen om ändringar i OSL befaras medföra en marginell ökning av antalet ärenden om utlämnande av allmän handling. Kostnaderna för denna ökning bedöms kunna hanteras inom befintliga ekonomiska ramar.

Personella konsekvenser och lokaler

Förslagen innebär enligt utredningens bedömning att bestämmelserna om verksamhetsövergång i 6 b § lagen (1982:80) om anställningsskydd och i 28 § lagen (1976:580) om medbestämmande i arbetslivet bör beaktas avseende den personal som arbetar på de enheter hos MSB som ansvarar för verksamheten i dag. Utredningen bedömer att centret vid en verksamhetsövergång kommer att ha tillgång till adekvat personal för att bedriva verksamheten. Ytterligare rekryteringar kan dock komma att behövas för att möta centrets växande uppdrag.

NCSC:s verksamhet bedrivs i MSB:s lokaler. Detta kommer fortsätta vara fallet under en övergångsperiod efter verksamhetsöverföringen. Utredningen bedömer att dessa lokaler uppfyller de tekniska kraven för att

verksamheten ska kunna bedrivas där. Men detta gäller under förutsättning att MSB fortsätter tillhandahålla vissa tekniska lösningar för verksamheten under en övergångsperiod. Utredningen anser samtidigt att det är av vikt att en flytt till de nya lokaler som nu planeras kommer till stånd så snart som möjligt.

Säkerhetsskydd

Verksamhetsöverföringen till centret innebär att FRA blir ansvarig för informationssäkerheten och den fysiska säkerheten för den utökade verksamheten vid centret. Genom förslagen blir FRA även personalsäkerhetsansvarig myndighet. FRA blir därmed ansvarig för att genomföra en säkerhetsprövning av all personal som omfattas av en eventuell verksamhetsövergång. Myndigheten blir även ansvarig för att personalen har tillräcklig kunskap om säkerhetsskydd.

Utredningen utesluter dock inte att situationer kan förekomma då det inte är självklart att FRA är ansvarig för säkerhetsskyddet, särskilt eftersom NCSC:s arbetsformer inte ännu är fastslagna. I en sådan situation kan det uppkomma behov av att träffa någon form av säkerhetsskyddsöverenskommelse mellan berörda aktörer.

Konsekvenser för skyddet för den personliga integriteten

Utredningen har gjort en analys av om förslagen är förenliga med bestämmelserna om skyddet för den personliga integriteten vid behandling av personuppgifter, en så kallad integritetsanalys. Förslagen om en lag om uppgiftsskyldighet och en registerlag innebär konsekvenser för enskildas personliga integritet. Utredningen bedömer att förslagen trots det är proportionerliga i förhållande till behovet av förbättrade möjligheter till informationsutbyte mellan de aktuella myndigheterna och behovet av att åstadkomma en ändamålsenlig kompletterande dataskyddsreglering. Förslagen är därför nödvändiga och proportionerliga. De avvägningar som gjorts vid utformningen av den föreslagna uppgiftsskyldigheten samt registerlagen är en viktig del i att säkerställa att den behandling av personuppgifter som förslagen innebär är proportionerlig.

Ikraftträdande

Förslagen föreslås träda i kraft den 1 juli 2026. Utredningen har då beaktat att förslagen bör träda i kraft så snart som möjligt. Hänsyn har tagits till sedvanlig tid för remissbehandling och beredning inom Regeringskansliet. Tidsplanen är dock avhängig att beslut i frågor som rör verksamhetsöverföringen och som regleras i förordning fattas så snart det är möjligt. Detta bland annat för att nödvändiga förhandlingar med kommissionen vid en överföring av stödavtal och utnämnandet av ett nytt samordningscenter ska kunna initieras i tid av FRA och MSB.

Betänkandets lagförslag i relevanta delar

Förslag till lag (2025:000) om uppgiftsskyldighet vid samverkan i verksamhet inom det nationella cybersäkerhetscentret

Härigenom föreskrivs följande.

1 § Denna lag gäller vid samverkan som sker mellan myndigheter i verksamhet inom det nationella cybersäkerhetscentret vid Försvarets radioanstalt.

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.

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

Denna lag träder i kraft den 1 juli 2026.

Förslag till lag (2025:000) om behandling av personuppgifter i viss verksamhet vid Försvarets radioanstalt

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 utför uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter inom det nationella cybersäkerhetscentret.

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

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

Förhållandet till annan reglering

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 någon av de uppgifter som anges i 2 §.

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

Personuppgifterna får behandlas även 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

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

Sökbegränsningar

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 1 juli 2026.

Förslag till lag om ändring av 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 g §, och närmast före 40 kap. 7 g § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	40 kap.
	Viss verksamhet vid Försvarets radioanstalt
	7 g § *Sekretess gäller hos Försvarets radioanstalt i verksamhet som bedrivs inom 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.* *För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.* *Sekretessen gäller inte i ärende om stöd enligt förordning (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.*
8 §[1]	
Den tystnadsplikt som följer av 1, 2, 4, 5 *och* 7 d §§ 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 *och g* §§ 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 1 juli 2026.

[1] Senaste lydelse 2023:460.

Förteckning över remissinstanserna

Efter remiss har yttranden inkommit från Arbetsgivarverket, Certezza AB, Ekonomistyrningsverket, Finansinspektionen, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Försäkringskassan, Förvaltningsrätten i Stockholm, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Kammarrätten i Stockholm, Livsmedelsverket, Luftfartsverket, Lunds universitet, Läkemedelsverket, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Västerbottens län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Örebro län, Länsstyrelsen i Östergötlands län, Myndigheten för civilt försvar (tidigare Myndigheten för samhällsskydd och beredskap), Myndigheten för digital förvaltning, Myndigheten för psykologiskt försvar, Netnod AB, Polismyndigheten, Post- och telestyrelsen, RISE Research Institutes of Sweden, Skatteverket, Socialstyrelsen, Statens energimyndighet, Statens inspektion för försvarsunderrättelseverksamheten, Statskontoret, Svenska Journalistförbundet, Sveriges advokatsamfund, Sveriges riksbank, Säkerhets- och försvarsföretagen, Säkerhets- och integritetsskyddsnämnden, Säkerhetspolisen, Tech Sverige, Teknikföretagen, Tidningsutgivarna, Tillväxtverket, Totalförsvarets forskningsinstitut, Trafikverket, Transportstyrelsen, Tullverket, Verket för innovationssystem (Vinnova) och Vetenskapsrådet.

Därutöver har yttranden inkommit från Svensk Försäkring och Fia Ewald Consulting AB.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: Kungl. Tekniska Högskolan, Linköpings universitet, Myndigheten för totalförsvarsanalys, Regelrådet, Riksdagens ombudsmän (JO), Svenskt Näringsliv, Sveriges akademikers centralorganisation (Saco) och Tjänstemännens centralorganisation (TCO).

Lagrådsremissens lagförslag

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 myndigheter 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 1 juli 2026.

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 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 1 juli 2026.

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 1 juli 2026.

[1] Senaste lydelse 2025:1495.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2026-03-18

Närvarande: F.d. justitieråden Mahmut Baran och Mari Andersson samt justitierådet Christine Lager

Lagändringar för ett stärkt nationellt cybersäkerhetscenter

Enligt en lagrådsremiss den 26 februari 2026 har regeringen (Försvarsdepartementet) beslutat inhämta Lagrådets yttrande över 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).

Förslagen har inför Lagrådet föredragits av rättssakkunnige Rasmus Neu Kjulin.

Förslagen föranleder följande yttrande.

Förslaget till lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret

I remissen föreslås att det ska införas en ny lag om uppgiftsskyldighet som ska gälla för myndigheter som ska samverka inom ramen för den verksamhet som bedrivs i det nationella cybersäkerhetscentret, som är placerat som en avdelning inom Försvarets radioanstalt. Avsikten är att ge bättre förutsättningar för ett ändamålsenligt informationsutbyte mellan Försvarets radioanstalt och de s.k. samverkansmyndigheterna inom ramen för den samverkan som redan sker enligt förordningen om det nationella cybersäkerhetscentret vid Försvarets radioanstalt. Enligt 4 § andra stycket i förordningen ska Försvarets radioanstalt i den verksamhet som bedrivs inom ramen för centret samverka med Försvarets materielverk, Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen.

1 §

I paragrafens första stycke regleras lagens innehåll och tillämpningsområde. Där anges att lagen innehåller bestämmelser om skyldigheter att lämna uppgifter vid samverkan mellan myndigheter inom det nationella cybersäkerhetscentret vid Försvarets radioanstalt. I författningskommentaren anges att en förutsättning för att lagen ska vara tillämplig är att det är fråga om samverkan mellan myndigheter inom det nationella cybersäkerhetscentret.

Både lagtexten och författningskommentaren ger intryck av att de myndigheter som ska samverka är inordnade i cybersäkerhetscentret vid Försvarets radioanstalt och att lagen endast reglerar samverkan mellan dessa myndigheter sinsemellan. På andra ställen i lagrådsremissen framgår dock att det nationella cybersäkerhetscentret är en avdelning inom Försvarets radioanstalt. Vid föredragningen har upplysts att avsikten med lagen dels är att reglera uppgiftsskyldighet mellan centret vid Försvarets radioanstalt och andra myndigheter, dels mellan dessa andra myndigheter sinsemellan inom ramen för den verksamhet som bedrivs vid centret.

Enligt Lagrådet bör lagtexten förtydligas så att det framgår att de myndigheter som ska samverka med Försvarets radioanstalt inte är en del av centret, och alltså inte en del av Försvarets radioanstalt. Vidare bör det förtydligas – i vart fall på lämpligt ställe i författningskommentaren – att samverkan såväl avser samverkan mellan Försvarets radioanstalt och de andra myndigheterna, som mellan dessa myndigheter sinsemellan, allt inom ramen för den verksamhet som bedrivs vid centret.

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

I remissen föreslås även att det ska införas en ny lag om Försvarets radioanstalts behandling av personuppgifter inom ramen för det nationella cybersäkerhetscentret. Det är en s.k. registerlag som innehåller vissa specialbestämmelser i förhållande till dataskyddslagen (2018:218) och som kompletterar EU:s dataskyddsförordning.

7 och 10 §§

I 7 § regleras för vilka ändamål personuppgifter får behandlas och i 10 § regleras när känsliga personuppgifter får behandlas.

Enligt förslagen i de båda paragraferna får en sådan behandling av personuppgifter ske endast om det är nödvändigt för att Försvarets radioanstalt ska kunna utföra den uppgift som anges i 2 § första stycket.

I 2 § föreskrivs:

> Denna lag gäller vid behandling av personuppgifter vid Försvarets radioanstalt när myndigheten inom 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.

Lagrådet har noterat att i många andra registerlagar har en motsvarande hänvisning gjorts till hela den paragraf som anger lagens tillämpningsområde. Se t.ex. 6 och 9 §§ lagen (2025:31) om viss personuppgiftsbehandling vid Brottsförebyggande rådet som hänvisar till 2 § i den lagen liksom 6 § tulldatalagen (2026:127) som hänvisar till 2 § i den lagen.

Lagrådet förordar att hänvisningarna i de båda paragraferna, 7 och 10 §§, görs till hela 2 §, dvs att orden ”första stycket” tas bort. Lagen – och därmed också 2 § första stycket – gäller ju endast i den utsträckning det är fråga om sådan behandling som anges i andra stycket. En sådan reglering blir också konsekvent med många andra registerlagar.

Övrigt lagförslag

Lagrådet lämnar förslaget utan erinran.

Försvarsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 1 april 2026

Närvarande: statsrådet Svantesson, ordförande, och statsråden Edholm, Waltersson Grönvall, Jonson, Strömmer, Forssmed, Tenje, Forssell, Wykman, Kullgren, Liljestrand, Bohlin, Carlson, Rosencrantz, Dousa, Larsson, Britz, Lann

Föredragande: statsrådet Bohlin

Regeringen beslutar proposition Lagändringar för ett stärkt nationellt cybersäkerhetscenter