

Samlade förmågor för ökad cybersäkerhet

*Betänkande av Utredningen om
ett stärkt nationellt cybersäkerhetscenter*

Stockholm 2025



STATENS OFFENTLIGA
UTREDNINGAR

SOU 2025:79

SOU och Ds finns på [regeringen.se](https://www.regeringen.se) under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2021:1.

Information för dem som ska svara på remiss finns tillgänglig på [regeringen.se/remisser](https://www.regeringen.se/remisser).

Layout: Kommittéservice, Regeringskansliet

Omslag: Elanders Sverige AB

Tryck och remisshantering: Elanders Sverige AB, Stockholm 2025

ISBN 978-91-525-1315-6 (tryck)

ISBN 978-91-525-1316-3 (pdf)

ISSN 0375-250X

Till statsrådet Carl-Oskar Bohlin

Regeringen beslutade den 14 november 2024 att uppdra åt en särskild utredare att utreda hur en överföring av arbetsuppgifter inom informations- och cybersäkerhet från Myndigheten för samhällsskydd och beredskap till Försvarets radioanstalt kan genomföras (dir. 2024:111). Per Bergling, generaldirektören och chefen för Myndigheten för familjerätt och föräldraskapsstöd förordnades den 1 december 2024 som särskild utredare. Utredningen har antagit namnet Utredningen om ett stärkt nationellt cybersäkerhetscenter.

Till sakkunniga att biträda utredningen förordnades från och med den 17 december 2024 departementssekreteraren Rebecca Idestrom och rättssakkunnige Alfred Pucek samt från och med den 16 januari 2025 ämnessakkunnige Arvid Kjell. Rättssakkunnige Alfred Pucek entledigades från och med den 1 april 2025 som sakkunnig i utredningen och ersattes av rättssakkunniga Edina Cronholm.

Som experter att biträda utredningen förordnades från och med den 17 december 2024 enhetschefen Katarina Hellner, verksamhetsstrategen Helena Andersson, juristen Maria Uddenfeldt, kontorschefen Johan Bergström Ring, seniora rådgivaren Peter Wallström, seniora rådgivaren Dag Ströman, inspektören Anton Ayyad, verksamhetsutvecklaren Nina Gustafsson Åberg och försvarsjuristen Sara Westerlund.

Kammarrättsassessorn Karl Lindén anställdes från och med den 2 december 2024 som sekreterare i utredningen. Hovrättsassessorn Emilia Anders anställdes från och med den 21 december 2024 som huvudsekreterare i utredningen.

Härmed överlämnas betänkandet *Samlade förmågor för ökad cybersäkerhet* (SOU 2025:79).

Uppdraget är i och med detta slutfört.

Umeå i juli 2025

Per Bergling

Emilia Anders
Karl Lindén

Innehåll

Sammanfattning	11
1 Författningsförslag.....	21
1.1 Förslag till lag (2025:000) om uppgiftsskyldighet vid samverkan i verksamhet inom det nationella cybersäkerhetscentret	21
1.2 Förslag till lag (2025:000) om behandling av personuppgifter i viss verksamhet vid Försvarets radioanstalt	22
1.3 Förslag till lag om ändring av lagen (2025:000) om ändring av offentlighets- och sekretesslagen (2009:400).....	25
1.4 Förslag till lag om ändring av offentlighets- och sekretesslagen (2009:400).....	26
1.5 Förslag till förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt	28
1.6 Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap	31
1.7 Förslag till förordning om ändring i förordningen (2022:524) om statliga myndigheters beredskap	32
1.8 Förslag till förordning om ändring i förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.....	35

1.9	Förslag till förordning om ändring i förordningen om cybersäkerhet.....	38
2	Utredningens uppdrag och arbete	41
2.1	Utredningens uppdrag	41
2.2	Utredningens arbete.....	42
3	Verksamhetsöverföring.....	43
3.1	Uppdraget och utredningens utgångspunkter.....	43
3.1.1	Uppdraget.....	43
3.1.2	Utredningens utgångspunkter	43
3.2	Nuvarande ansvarsfördelning mellan MSB och FRA.....	46
3.2.1	MSB.....	46
3.2.2	FRA.....	48
3.3	Ett antal uppgifter ska föras över till FRA	49
3.3.1	FRA ska ha det övergripande ansvaret för samhällets informations- och cybersäkerhet	49
3.3.2	FRA ska utses till CSIRT-enhet, gemensam kontaktpunkt samt cyberkrishanteringsmyndighet.....	52
3.3.3	FRA ska ges viss föreskriftsrätt enligt förordningen om cybersäkerhet	61
3.3.4	FRA ska ansvara för tillsynssamordning	65
3.3.5	FRA ska ta emot incidentrapporter enligt fler regelverk.....	67
3.3.6	FRA ska ges föreskriftsrätt enligt beredskapsförordningen	69
3.3.7	FRA ska utses till nationellt samordningscenter för forskning och innovation inom cybersäkerhet.....	70
3.3.8	FRA ska vara teknisk kontaktpunkt för OSSE.....	73
3.4	Verksamhet som inte ska föras över till FRA.....	74
3.5	Verksamhet som inte omfattas av utredningens uppdrag....	75

4	Informationshantering	77
4.1	Uppdraget.....	77
4.2	En ny lag om uppgiftsskyldighet vid samverkan i verksamhet inom NCSC	78
4.2.1	Det finns behov av större rättsliga förutsättningar att dela information vid samverkan inom NCSC:s verksamhet	79
4.2.2	Den utökade möjligheten att dela information ska formuleras som en ny lag om uppgiftsskyldighet	83
4.2.3	Den nya lagen ska utgöra en balans mellan effektivitet och integritet	86
4.2.4	Utformningen av uppgiftsskyldigheten	88
4.2.5	Lagen omfattar endast myndigheter som regeringen bestämmer	95
4.2.6	Det behövs inget ytterligare sekretesskydd för överlämnade uppgifter.....	95
4.2.7	Förhållandet mellan den nya lagen och annan lagstiftning	97
4.3	En ny sekretessbestämmelse hos NCSC.....	99
4.3.1	Det finns utmaningar med informationsdelning med näringslivet.....	99
4.3.2	NIS 2-direktivet ställer krav på anonymitet	100
4.3.3	Vissa uppgifter om enskilda bör omfattas av sekretess hos NCSC	101
4.3.4	Befintliga sekretessbestämmelser är inte tillräckliga för enskildas personliga och ekonomiska förhållanden.....	102
4.3.5	Sekretessintresset väger tyngre än insynsintresset	109
4.3.6	Det behövs en ny sekretessbestämmelse	110
4.3.7	Utformningen av sekretessbestämmelsen.....	111
4.3.8	En bestämmelse om tystnadsplikt för enskilda kan övervägas.....	123
4.3.9	Konkurrens med andra sekretessbestämmelser...	124
4.3.10	Befintliga sekretessbestämmelser är tillräckliga för det allmännas affärs- och driftförhållanden ...	126

4.4	Det finns behov att ändra vissa tidigare föreslagna bestämmelser	127
4.4.1	En sekretessbrytande bestämmelse	127
4.4.2	Ytterligare ett förslag behöver ses över	128
4.5	Personuppgiftsbehandlingen hos NCSC	129
4.5.1	Olika regelverk styr personuppgiftsbehandlingen hos FRA	129
4.5.2	FRA behöver behandla personuppgifter inom ramen för NCSC:s verksamhet	133
4.5.3	En ny lag om personuppgiftsbehandling inom ramen för NCSC:s verksamhet	135
4.6	Integritetsrisker	160
4.6.1	En integritetsanalys ska göras i lagstiftningsarbetet	160
4.6.2	Förslagen medför en utökad behandling av personuppgifter	161
4.6.3	Integritetsrisker aktualiseras som en följd av förslagen	162
4.6.4	Omfattningen av personuppgiftsbehandlingen ...	165
4.6.5	Det finns skyddsåtgärder	166
4.6.6	Ny rättslig grund för personuppgiftsbehandling	167
4.6.7	Förslaget innebär att vidarebehandling av personuppgifter kommer att ske	169
4.6.8	Förslagen innebär inte övervakning eller kartläggning	172
4.6.9	Slutlig proportionalitets- och nödvändighetsbedömning	174
5	Konsekvenser	177
5.1	Krav på konsekvensanalysen	177
5.2	Utgångspunkter för konsekvensanalysen	178
5.3	Regleringsalternativ	179
5.3.1	Förslagen uppfyller syftena med uppdraget men skapar nya utmaningar	179
5.3.2	Andra modeller har övervägts	180

5.4	Verksamhetsmässiga konsekvenser	181
5.4.1	FRA får ett bredare samhällsuppdrag.....	181
5.4.2	MSB får ett mer koncentrerat uppdrag	183
5.5	EU-rättsliga konsekvenser	183
5.5.1	Förslagen hindrar inte Sverige från att uppfylla sina förpliktelser mot EU.....	183
5.5.2	Förslagen påverkar inte Sveriges möjligheter att ta emot EU-rättsligt stöd	184
5.5.3	Konsekvenser i förhållande till genomförandet av andra EU-rättsakter	189
5.6	Personella konsekvenser och lokaler	194
5.6.1	Personella konsekvenser	194
5.6.2	Lokaler.....	195
5.7	Ekonomiska konsekvenser	196
5.7.1	Ekonomiska konsekvenser av förslagen om överföring av uppgifter från MSB till FRA ...	196
5.7.2	Ekonomiska konsekvenser av förslagen om informationshantering	199
5.8	Säkerhetsskydd.....	201
5.9	Övriga konsekvenser	202
5.10	Tidpunkt för utvärdering av förslagen.....	202
6	Ikraftträdande och övergångsbestämmelser	205
7	Författningskommentar	207
7.1	Förslaget till lag om uppgiftsskyldighet vid samverkan i verksamhet inom det nationella cybersäkerhetscentret ...	207
7.2	Förslaget till lag om behandling av personuppgifter i viss verksamhet vid Försvarets radioanstalt	210
7.3	Förslaget till lag om ändring av lagen om ändring av offentlighets- och sekretesslagen (2009:400)	218
7.4	Förslaget till lag om ändring av offentlighets- och sekretesslagen (2009:400).....	218

Referenser	221
-------------------------	------------

Bilaga

Bilaga 1	Kommittédirektiv 2024:111	225
----------	---------------------------------	-----

Sammanfattning

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 cyberkrishanteringsmyndighet. 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 sök-
begränsningar avseende känsliga personuppgifter.

Förslagets 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. Där-
emot 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 stöдавtalet med EU är även FRA förpliktad 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. Kost-

naderna 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 stöдавtal och utnämmandet av ett nytt samordningscenter ska kunna initieras i tid av FRA och MSB.

1 Författningsförslag

1.1 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.

1.2 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.

1.3 Förslag till lag om ändring av lagen (2025:000) om ändring av offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om lagen (2025:000) om ändring av offentlighets- och sekretesslagen (2009:400) i dess lydelse enligt SOU 2024:64 *Motståndskraft i samhällsviktiga tjänster* att 15 kap. 3 c § ska ha följande lydelse.

Lydelse enligt SOU 2024:64

Föreslagen lydelse

15 kap.

3 c §

Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap lämnar en uppgift som avses där till tillsynsmyndigheten enligt *lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare* om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Myndigheten för samhällsskydd och beredskap.

En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Denna lag träder i kraft den 1 juli 2026.

1.4 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, 15 kap. 3 d §, av följande lydelse och

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

15 kap.

3 d §

Sekretessen enligt 1 a § hindrar inte att Försvarets radioanstalt lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om cybersäkerhet om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Försvarets radioanstalt.

En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

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.

1.5 Förslag till förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt

Härigenom föreskrivs i fråga om förordningen (2007:937) med instruktion för Försvarets radioanstalt att det ska införas fyra nya paragrafer, 4 b–4 e §§, av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

4 b §

Försvarets radioanstalt ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.

Myndigheten ska årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten av statliga myndigheter enligt 14 § förordningen (2022:524) om statliga myndigheters beredskap och 3 kap. 5–7 §§ lag (2025:000) om cybersäkerhet. Inför arbetet med att sammanställa rapporten ska myndigheten inhämta upplysningar från Säkerhetspolisen och Försvarmakten om de incidenter som rapporterats in till de myndigheterna enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen (2021:955).

4 c §

Försvarets radioanstalt ska ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska

1. agera skyndsamt vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,

2. återrapportera till berörda aktörer i samband med att en it-incident har rapporterats,

3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, och

4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

4 d §

Myndigheten ska vara svensk teknisk kontaktpunkt för Organisationen för säkerhet och samarbete i Europas (OSSE) verksamhet på cyberområdet. Innan svar på informationsförfrågningar lämnas ska myndigheten informera Regeringskansliet (Utrikesdepartementet).

4 e §

Myndigheten ska vara nationellt samordningscenter 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.

Denna förordning träder i kraft den 1 juli 2026.

1.6 Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Härigenom föreskrivs i fråga om förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap¹

dels att 11 a–11 c §§ samt 18 j § ska upphöra att gälla,

dels att rubriken närmast före 11 a § ska utgå.

Denna förordning träder i kraft den 1 juli 2026.

¹ Senaste lydelse av

11 a § 2022:1004

11 b § 2015:1065

11 c § 2022:123

18 j § 2022:1703.

1.7 Förslag till förordning om ändring i förordningen (2022:524) om statliga myndigheters beredskap

Härigenom föreskrivs i fråga om förordningen (2022:524) om statliga myndigheters beredskap att 14, 26 och 27 §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

14 §

Till stöd för arbetet med samhällets informationssäkerhet ska en myndighet till *Myndigheten för samhällsskydd och beredskap* skyndsamt rapportera it-incidenter som inträffat i den rapporterade myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation.

En myndighet som tillhandahåller tjänster åt en annan organisation ska i samband med rapporteringen informera och vid behov samråda med den eller de uppdragsgivare som berörs av incidenten.

Rapporteringsskyldigheten omfattar inte sådana incidenter som ska anmälas enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen (2021:955).

Om det kan antas att en incident som rapporterats till *Myndigheten för samhällsskydd och beredskap* har sin grund i en brottslig gärning, ska *Myndigheten för samhällsskydd och beredskap* skyndsamt uppmana den rapporterade myndigheten att anmäla incidenten till Polismyndigheten.

Till stöd för arbetet med samhällets informationssäkerhet ska en myndighet till *Försvarets radioanstalt* skyndsamt rapportera it-incidenter som inträffat i den rapporterade myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation.

Om det kan antas att en incident som rapporterats till *Försvarets radioanstalt* har sin grund i en brottslig gärning, ska *Försvarets radioanstalt* skyndsamt uppmana den rapporterade myndigheten att anmäla incidenten till Polismyndigheten.

26 §

Myndigheten för samhällsskydd och beredskap får meddela ytterligare föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i 13 § utom i fråga om Regeringskansliet, kommittéväsendet och Försvarsmakten. Myndigheten ska därvid beakta nationell och internationell standard för informationssäkerhet.

Försvarets radioanstalt får meddela ytterligare föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i 13 § utom i fråga om Regeringskansliet, kommittéväsendet och Försvarsmakten. Myndigheten ska därvid beakta nationell och internationell standard för informationssäkerhet.

Försvarets radioanstalt får meddela närmare föreskrifter om it-incidentrapportering enligt 14 § efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig.

27 §

Myndigheten för samhällsskydd och beredskap får meddela närmare föreskrifter om

1. risk- och sårbarhetsanalyser enligt 7 § och risk- och sårbarhetsbedömningar enligt 17 och 19 §§,

2. it-incidentrapportering enligt 14 § efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig,

3. beredskapsmyndigheternas informationsskyldighet enligt 22 § andra stycket,

4. uppgifter inför höjd beredskap enligt 10 och 11 §§ utom i fråga om Kustbevakningen, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Fortifikationsverket och Försvarshögskolan, och

2. beredskapsmyndigheternas informationsskyldighet enligt 22 § andra stycket,

3. uppgifter inför höjd beredskap enligt 10 och 11 §§ utom i fråga om Kustbevakningen, Försvarets materielverk, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Fortifikationsverket och Försvarshögskolan, och

5. uppgifter inför och vid höjd beredskap enligt 20 § 10 och 11 samt 21 § utom i fråga om Kustbevakningen.

4. uppgifter inför och vid höjd beredskap enligt 20 § 10 och 11 samt 21 § utom i fråga om Kustbevakningen.

Denna förordning träder i kraft den 1 juli 2026.

1.8 Förslag till förordning om ändring i förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning

Härigenom föreskrivs i fråga om förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning att 6–8, 10, 14, 16–17, 19, 20 och 22 §§ ska ha följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

6 §

Myndigheten för samhällsskydd och beredskap prövar frågor om stöd enligt denna förordning.

Försvarets radioanstalt prövar frågor om stöd enligt denna förordning.

7 §

En ansökan om stöd ska vara skriftlig och ges in till *Myndigheten för samhällsskydd och beredskap* på det sätt som myndigheten anvisar.

En ansökan om stöd ska vara skriftlig och ges in till *Försvarets radioanstalt* på det sätt som myndigheten anvisar.

Ansökan ska undertecknas av den sökande. Om ansökan ges in elektroniskt ska den ha en sådan avancerad elektronisk underskrift som avses i artikel 3 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG, i den ursprungliga lydelsen.

8 §

Den som ansöker om stöd ska lämna de handlingar och uppgifter som *Myndigheten för samhällsskydd och beredskap* behöver för att kunna pröva ansökan.

Den som ansöker om stöd ska lämna de handlingar och uppgifter som *Försvarets radioanstalt* behöver för att kunna pröva ansökan.

10 §

Innan ett stöd beviljas enligt kommissionens förordning (EU) 2023/2831 ska *Myndigheten för samhällsskydd och beredskap* lämna de upplysningar till stödmottagaren och göra den kontroll som framgår av artiklarna 6.4 och 7.4 i förordningen.

Innan ett stöd beviljas enligt kommissionens förordning (EU) 2023/2831 ska *Försvarets radioanstalt* lämna de upplysningar till stödmottagaren och göra den kontroll som framgår av artiklarna 6.4 och 7.4 i förordningen.

14 §

Den som ansöker om eller har beviljats bidrag enligt denna förordning ska snarast möjligt till *Myndigheten för samhällsskydd och beredskap* anmäla sådana ändrade förhållanden som kan påverka rätten till eller storleken på bidraget.

Den som ansöker om eller har beviljats bidrag enligt denna förordning ska snarast möjligt till *Försvarets radioanstalt* anmäla sådana ändrade förhållanden som kan påverka rätten till eller storleken på bidraget.

16 §

Myndigheten för samhällsskydd och beredskap ska besluta att stöd helt eller delvis inte ska betalas ut om

Försvarets radioanstalt ska besluta att stöd helt eller delvis inte ska betalas ut om

1. den som har ansökt om och beviljats stöd genom att lämna oriktiga uppgifter har orsakat att stödet beviljats felaktigt eller med för högt belopp,
2. stödet av något annat skäl har beviljats felaktigt eller med för högt belopp och mottagaren borde ha insett detta,
3. stödet inte har utnyttjats eller använts för det ändamål som det har beviljats för, eller
4. villkoren för stödet inte har följts.

17 §

Ett beslut om stöd ska innehålla villkor om att stödmottagaren på *Myndigheten för samhällsskydd och beredskap*s begäran ska lämna de uppgifter och hand-

Ett beslut om stöd ska innehålla villkor om att stödmottagaren på *Försvarets radioanstalts* begäran ska lämna de uppgifter

lingar som krävs för uppföljning och handlingar som krävs för uppföljning och kontroll av stödet.

Beslutet får även innehålla de övriga villkor som behövs för att tillgodose syftet med stödet.

19 §

Om en stödmottagare är återbetalningsskyldig enligt 18 § ska *Myndigheten för samhällsskydd och beredskap* besluta att helt eller delvis kräva tillbaka stödet.

Om en stödmottagare är återbetalningsskyldig enligt 18 § ska *Försvarets radioanstalt* besluta att helt eller delvis kräva tillbaka stödet.

Om ett belopp som har återkrävts inte betalas i rätt tid, ska dröjsmålsränta enligt räntelagen (1975:635) tas ut på beloppet.

Återbetalningskravet eller räntan får helt eller delvis sättas ned om det finns särskilda skäl.

20 §

Om *Myndigheten för samhällsskydd och beredskap* beslutat om återkrav eller ränta, får det belopp som ska betalas enligt beslutet räknas av mot annan utbetalning av stöd till samma stödmottagare som har beslutats enligt denna förordning.

Om *Försvarets radioanstalt* beslutat om återkrav eller ränta, får det belopp som ska betalas enligt beslutet räknas av mot annan utbetalning av stöd till samma stödmottagare som har beslutats enligt denna förordning.

Avräkning får inte ske i det fall som avses i 15 §.

22 §

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om verkställigheten av denna förordning.

Försvarets radioanstalt får meddela föreskrifter om verkställigheten av denna förordning.

Denna förordning träder i kraft den 1 juli 2026.

1.9 Förslag till förordning om ändring i förordningen om cybersäkerhet

Härigenom föreskrivs i fråga om förordning om cybersäkerhet i dess lydelse enligt SOU 2024:18 *Nya regler om cybersäkerhet* att 20, 27 och 31–37 §§ ska ha följande lydelse.

Lydelse enligt SOU 2024:18

Föreslagen lydelse

20 §

Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt. *Försvarets radioanstalt* ska vara gemensam kontaktpunkt.

27 §

Myndigheten för samhällsskydd och beredskap ska vara CSIRT-enhet. *Försvarets radioanstalt* ska vara CSIRT-enhet.

31 §

Myndigheten för samhällsskydd och beredskap ska vara cyberkris- hanteringsmyndighet. *Försvarets radioanstalt* ska vara cyberkris- hanteringsmyndighet.

32 §

Myndigheten för samhällsskydd och beredskap ska delta i det europeiska kontaktnätverket för cyber- kriser (EU-CyCLONe). *Försvarets radioanstalt* ska delta i det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

33 §

Myndigheten för samhällsskydd och beredskap får i föreskrifter ange vilka verksamhetsutövare som omfattas av 1 kap. 8 § lagen om cybersäkerhet och om verksamhetsutövaren är väsentlig. Tillsynsmyndigheten ska ges tillfälle att yttra sig. *Försvarets radioanstalt* får i föreskrifter ange vilka verksamhetsutövare som omfattas av 1 kap. 8 § lagen om cybersäkerhet och om verksamhetsutövaren är väsentlig. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

34 §

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om anmälningsskyldigheten i 2 kap. 2 § lagen om cybersäkerhet.

Försvarets radioanstalt får meddela föreskrifter om anmälningsskyldigheten i 2 kap. 2 § lagen om cybersäkerhet.

35 §

Tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet. *Myndigheten för samhällsskydd och beredskap* ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning och lärosäten med examens-tillstånd får *Myndigheten för samhällsskydd och beredskap* i stället för länsstyrelserna i 8 § meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet.

Tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet. *Försvarets radioanstalt* ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning och lärosäten med examens-tillstånd får *Försvarets radioanstalt* i stället för länsstyrelserna i 8 § meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet.

36 §

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande incident enligt 3 kap. 4 § och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

Försvarets radioanstalt får meddela föreskrifter om vad som utgör en betydande incident enligt 3 kap. 4 § och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

37 §

Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Försvarets radioanstalt ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Denna förordning träder i kraft den 1 juli 2026.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

I Försvarsberedningens rapport *Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret* (Ds 2023:34) ifrågasätts om dagens myndighetsstruktur är ändamålsenlig för att uppnå en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete. I november 2024 beslutade därför regeringen att tillsätta en särskild utredare med uppdrag att utreda hur en överföring av arbetsuppgifter inom informations- och cybersäkerhet från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt (FRA) kan genomföras (dir. 2024:111).

Utredningens uppdrag är att

- analysera och föreslå vilka uppgifter på informations- och cybersäkerhetsområdet hos MSB som bör föras över till FRA eller det nationella cybersäkerhetscentret (NCSC) vid FRA, och när en sådan överföring kan och bör genomföras,
- analysera och föreslå hur överföringen från MSB till FRA av aktuella uppgifter kan genomföras,
- analysera och lämna förslag på hur FRA efter en överföring av uppgifter kan tillgodose regeringens och samhällets behov av snabb och säker information om cyberincidenter,
- analysera och föreslå hur rapportering och uppföljning av informations- och cybersäkerhetsverksamheten vid en överföring av uppgifter kan struktureras så att verksamheten blir möjlig för regeringen att följa upp över tid,

- analysera och lämna förslag på hur en överföring av uppgifter kan ske utan att Sveriges möjligheter att uppfylla sina EU-rättsliga förpliktelser eller få del av EU-rättsligt stöd påverkas,
- analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling,
- analysera vilka följder en överföring av uppgifter får när det gäller FRA:s behov av personalresurser och lokaler,
- vid behov föreslå åtgärder för en fördjupad samverkan inom ramen för NCSC, och
- lämna nödvändiga författningsförslag.

2.2 Utredningens arbete

Utredningens arbete har bedrivits på sedvanligt sätt med regelbundna möten med sakkunniga och experter. Utredningen har haft tre protokollförda sammanträden med sakkunniga och experter. Utredningen har därutöver haft kontakt med enskilda sakkunniga och experter i vissa frågor.

Utredningen har haft en nära dialog med MSB och FRA. Utredningen har träffat generaldirektörerna för respektive myndighet och den mellan MSB och FRA myndighetsgemensamma projektgruppen rörande verksamhetsöverföringen. En dialog har också förekommit med Arbetsgivarverket, Post- och telestyrelsen, Myndigheten för psykologiskt försvar samt Ekonomistyrningsverket. Utredningen har träffat företaget Cparta Cyber Defence AB och branschorganisationen Säkerhets- och försvarsföretagen.

Utredningen har träffat Cyberresiliensutredningen (Fi 2024:07). I enlighet med direktiven har utredningen även i övrigt hållit sig informerad om och beaktat relevant arbete som pågår inom Regeringskansliet och kommittéväsendet. Utredningen har i arbetet kunnat beakta lagstiftning och andra förhållanden fram till början av juni 2025. Det innebär bland annat att lagrådsremissen *Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag*, som överlämnades till Lagrådet den 12 juni 2025 inte kunnat beaktas inom ramen för utredningen.

3 Verksamhetsöverföring

3.1 Uppdraget och utredningens utgångspunkter

3.1.1 Uppdraget

Utredningen har fått i uppdrag att undersöka och lämna förslag på en verksamhetsöverföring avseende arbetet med samhällets informations- och cybersäkerhet från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt (FRA). En utgångspunkt för utredaren ska vara att en organisatorisk åtskillnad mellan stödjande verksamhet och tillsynsverksamhet inom cybersäkerhetsområdet ska upprätthållas. Genom förslagen ska utredningen säkerställa en tydlig ansvarsfördelning, utan överlapp eller dubblering av uppgifter och ansvar, och att verksamheten kan bedrivas effektivt utifrån de behov som finns att samla informations- och cybersäkerhetsfrågorna.

I kommittédirektivet anges även att utredaren ska analysera och föreslå hur rapportering och uppföljning av informations- och cybersäkerhetsverksamheten vid en överföring av uppgifter kan struktureras så att verksamheten blir möjlig för regeringen att följa upp över tid.

3.1.2 Utredningens utgångspunkter

Av kommittédirektivet framgår att bakgrunden till utredningen är att försvarsberedningen i promemorian *Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret* (Ds 2023:34) konstaterat ett behov av att uppnå en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete. Även Totalförsvarets forskningsinstitut har identifierat att det delade ansvaret medför en risk för ett ineffektivt arbete med informations-

och cybersäkerhetsfrågor (FOI-R--5546--SE). Utredningen har därför bland annat till uppgift att analysera och bedöma hur en överföring av uppgifter och ansvar för dessa påverkar samhällets motståndskraft på informations- och cybersäkerhetsområdet.

I del 1 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) lämnades förslag om att det nationella cybersäkerhetscentret (NCSC), vars verksamhet tidigare bedrivits gemensamt av de samverkande myndigheterna, skulle bli en del av FRA. I promemorian identifierades stora överlapp mellan uppgifter som utförs av MSB och NCSC inom informations- och cybersäkerhet. Inom ramen för den dialog som fördes under framtagandet av den promemorian framfördes det från både offentliga och privata aktörer att de överlappande bemyndigandena mellan NCSC och MSB upplevdes som förvirrande och ineffektiva med en osäkerhet kring vart en aktör ska vända sig vid behov av stöd. Promemorian inriktade sig särskilt på frågan om CERT-SE, som är Sveriges nationella funktion för att stödja samhället i arbetet med att förebygga och hantera it-incidenter, vars uppgifter överlappar med NCSC. Bedömningen gjordes att CERT-SE skulle överföras till FRA och NCSC, men att frågan behövde utredas ytterligare.

I linje med förslagen i promemorian beslutade regeringen att NCSC skulle bli en del av FRA. Regeringen har vidare uttalat att CERT-SE behöver stärkas och utveckla förmågan att erbjuda kvalificerat stöd till drabbade aktörer, samt fortsätta att bygga förmåga att hantera cyberangrepp. Regeringen har även gjort bedömningen att MSB:s verksamhet med informations- och cybersäkerhet, där CERT-SE ingår, får större operativ effekt på FRA under det nya cybersäkerhetscentret och att en utredning ska tillsättas för att verkställa en överflytt (prop. 2024/25:1, utgiftsområde 6 s. 91).

Den 20 mars 2025 beslutade regeringen om en ny nationell strategi för cybersäkerhet (*Nationell strategi för cybersäkerhet 2025–2029*, skr. 2024/25:121). I strategin framhålls bland annat ambitionen att NCSC ska utgöra navet i det nationella cybersäkerhetsarbetet.

Med beaktande av ovan nämnda omständigheter är det en grundläggande utgångspunkt för utredningen att en överföring av uppgifter från MSB till FRA ska omfatta centrala delar av MSB:s uppgifter inom informations- och cybersäkerhet och att uppgifterna ska utföras inom ramen för NCSC. Utredningen bedömer att en sådan överföring ger förutsättningar för synergieffekter i förhållande

till FRA:s befintliga kompetenser. Detta kan i sin tur leda till en ökad operativ och strategisk förmåga på informations- och cybersäkerhetsområdet. Det åtgärdar även överlappningen i bemyndiganden mellan NCSC och MSB som har skapat osäkerhet hos såväl offentliga som privata aktörer. En sådan verksamhetsöverföring bidrar även till en mer samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete, vilket underlättar ett effektivt ansvarsutkrävande. Det ligger även i linje med ambitionen om att NCSC ska bli ett nav för det nationella informations- och cybersäkerhetsarbetet.

Utredningens utgångspunkt är att en verksamhetsöverföring till FRA ska ske genom att uppgifter författningsmässigt överförs till FRA som myndighet. Men uppgifterna kommer att utföras inom ramen för NCSC:s verksamhet.

En omständighet som utredningen behöver ta hänsyn till är att verksamheten i NCSC i stor utsträckning skiljer sig från FRA:s befintliga uppdrag inom nationell säkerhet och försvar. Utredningen återkommer i kapitel 5 med vissa överväganden om varför en sådan uppdelning mellan myndighetens arbete inom NCSC och dess uppdrag inom nationell säkerhet och försvar också fortsatt är nödvändig för att båda verksamheterna ska kunna bedrivas på ett ändamålsenligt sätt.

I Europaparlamentets och rådets direktiv 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) ges i artikel 6 definitioner som gäller för direktivet. Regeringen har därefter i sin nationella strategi för cybersäkerhet använt direktivets definition av cybersäkerhet. Utredningen konstaterar att begreppsdefinitionerna i direktivet inte till fullo överensstämmer med tidigare etablerade begrepp i svensk rätt på området. Utredningen kommer i den fortsatta framställningen att använda de begrepp som framgår av respektive regelverk. Utredningens begreppsanvändning kan därför framstå som något inkonsekvent. Ett exempel som lyfts till utredningen är att EU-rättens definition av begreppet cyberhot innebär att det inte är att likställa med en it-incident. Men det förekommer i svensk kontext att begreppen används likställda. Utredningen bedömer dock att alternativet att anpassa begreppsanvändningen i framställningen av den

nationella rätten för att åstadkomma samstämmighet med NIS 2-direktivets definitioner riskerar att leda till förvirring.

I avsnitt 3.2 ges en kort bakgrund till MSB:s och FRA:s respektive ansvarsområden på informations- och cybersäkerhetsområdet i dag. Där ges även en kort bakgrund till NCSC. Därefter ges i avsnitt 3.3 förslag på en verksamhetsöverföring från MSB till FRA och vilka överväganden som legat till grund för förslagen. I avsnitt 3.4 och 3.5 behandlas de uppgifter med anknytning till informations- och cybersäkerhetsområdet som inte omfattas av förslagen om verksamhetsöverföring till FRA.

3.2 Nuvarande ansvarsfördelning mellan MSB och FRA

3.2.1 MSB

Av 11 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap (MSB:s instruktion) framgår att myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer. Myndigheten har även i uppdrag att årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten från statliga myndigheter enligt förordningen (2022:524) om statliga myndigheters beredskap (beredskapsförordningen) samt att inhämta upplysningar om de incidenter som rapporterats in enligt säkerhetsskyddsförordningen (2021:955). Därutöver ska MSB även rapportera till regeringen om förhållanden på informations-säkerhetsområdet som kan leda till behov av åtgärder på olika nivåer och områden i samhället.

Enligt 11 b § MSB:s instruktion ska MSB ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter.

Myndigheten är enligt 11 c § MSB:s instruktion nationellt samordningscenter enligt artikel 6 i Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom närings-

liv, teknik och forskning och av nätverket av nationella samordningscentrum (CCCN-förordningen). Sedan 2024 handlägger även myndigheten ansökningar om bidrag enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

MSB är enligt 18 j § i instruktionen även svensk teknisk kontaktpunkt för Organisationen för säkerhet och samarbete i Europas (OSSE) verksamhet på cyberområdet.

Enligt 14 § beredskapsförordningen har MSB ansvaret för att ta emot incidentrapporter från de myndigheter som omfattas av förordningen. Myndigheten har enligt 26–27 §§ beredskapsförordningen därtill ett föreskriftsansvar avseende kompletterande säkerhetskrav för informationshanteringssystem samt närmare föreskrifter om it-incidentrapporteringen enligt förordningen.

Enligt förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster är MSB nationell kontaktpunkt (22 §) och CSIRT-enhet (12 §) och deltar i samarbetsgruppen som har inrättats enligt artikel 11 i NIS-direktivet (23 §). MSB har enligt förordningen även ansvaret att leda ett samarbetsforum för tillsynsmyndigheterna och Socialstyrelsen samt mandat att meddela föreskrifter. I betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) föreslås att myndigheten ska behålla dessa uppgifter samt även utgöra cyberkrishanteringsmyndighet. Betänkandet innehåller förslag för genomförandet av NIS 2-direktivet. Regeringen har i linje med förslagen i betänkandet gett MSB i uppdrag att vara behörig myndighet enligt NIS 2-direktivet gällande rollerna som gemensam kontaktpunkt, cyberkrishanteringsmyndighet, CSIRT-enhet samt som Sveriges representant i samarbetsgruppen (Fö2025/00387). Regeringsbeslutet fattades den 27 februari 2025 och gäller under året i avvaktan på att förslagen i betänkandet bereds.

MSB:s uppgifter på informations- och cybersäkerhetsområdet utförs i dag i huvudsak inom avdelningen för cybersäkerhet och samhällsviktiga kommunikationer.

3.2.2 FRA

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 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.

Som utredningen konstaterat tidigare finns NCSC numera 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. Utöver FRA deltar även Försvarmakten, MSB, Polismyndigheten, Säkerhetspolisen, Försvarets materielverk samt Post- och telestyrelsen som samverkansmyndigheter i centrets arbete. Centret bedrivs organisatoriskt som en egen avdelning inom FRA.

Den 20 mars 2025 utfärdade regeringen en förordning med kompletterande bestämmelser för centrets verksamhet (förordning [2025:237] om det nationella cybersäkerhetscentret vid Försvarets radioanstalt, förkortad NCSC-förordningen). 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 § 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.

3.3 Ett antal uppgifter ska föras över till FRA

3.3.1 FRA ska ha det övergripande ansvaret för samhällets informations- och cybersäkerhet

Utredningens förslag: FRA ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och regioner samt företag och organisationer.

Myndigheten ska årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten av statliga myndigheter enligt 14 § förordningen (2022:524) om statliga myndigheters beredskap och 3 kap. 5–7 §§ förslaget till lag om cybersäkerhet i dess lydelse enligt SOU 2024:18. Inför arbetet med att sammanställa rapporten ska myndigheten inhämta upplysningar från Säkerhetspolisen och Försvarmakten om de incidenter som rapporterats in till de

myndigheterna enligt 2 kap. 4 § första stycket 2 säkerhetsskydds-förordningen (2021:955).

Ett av syftena med utredningen är att skapa en ansvarsfördelning där förekomsten av dubbla ansvarsområden minimeras. Utredningen anser att det finns ett betydande överlapp av uppgifter och ansvar mellan MSB och NCSC. Detta med anledning av hur MSB:s instruktion och NCSC-förordningen är utformade. MSB har enligt 11 a § MSB:s instruktion i uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet samtidigt som NCSC ska vara samlad kontaktpunkt för frågor som rör cybersäkerhet. Både MSB och NCSC har vidare ansvar för att lämna råd till en bred krets rörande informationssäkerhet respektive cybersäkerhet. De har båda även ett rapporteringsuppdrag gentemot regeringen avseende behov av åtgärder på informations- respektive cybersäkerhetsområdet.

För att åtgärda dessa överlappande uppgifter anser utredningen att det är ändamålsenligt att samla ansvaret för dessa uppgifter hos en myndighet. I enlighet med utgångspunkterna för utredningen bör uppgifterna samlas hos FRA. Inom ramen för NCSC kommer myndigheten ha goda förutsättningar att stödja och samordna arbetet med samhällets informations- och cybersäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. Därigenom blir det även tydligt vilken myndighet som har det övergripande ansvaret för samhällets arbete med dessa frågor. Det ökar även tydligheten för såväl offentliga som privata aktörer kring vilken myndighet de ska vända sig till för råd och stöd.

MSB har i sin nuvarande verksamhet bedrivit utbildningar på informations- och cybersäkerhetsområdet med stöd av 11 a § och 5 § MSB:s instruktion. Även NCSC har ett uppdrag att genomföra övningar och utbildningar på cybersäkerhetsområdet genom 3 § 4 NCSC-förordningen. Detta behov kommer således fortsatt tillgodoses även efter att MSB:s samordnande uppdrag på informations- och cybersäkerhetsområdet förs över till FRA.

Utifrån förordnandet i 11 a § MSB:s instruktion har MSB till utredningen uppgett att myndigheten bland annat arbetar med att öka medvetenheten om informations- och cybersäkerhet i samhället, särskilt hos allmänheten och små och medelstora företag. Myndigheten utvecklar och tillhandahåller även forum och nätverk för informationsutbyte och samverkan inom informations- och cyber-

säkerhetsområdet. Den är ansvarig för att leda det gemensamma arbetet med informations- och cybersäkerhet i Ena, som är ett myndighetsgemensamt projekt under Myndigheten för digital förvaltning (DIGG) med syftet att utveckla Sveriges digitala infrastruktur. MSB tillhandahåller även en publik databas med svensk terminologi inom området informations- och cybersäkerhet, medverkar i standardiseringsarbetet på området och tillhandahåller utbildningar inom informations- och cybersäkerhet för specifika målgrupper. Myndigheten samlar även in data för och publicerar årliga mätningar på samhällets arbete med informations- och cybersäkerhet. För detta ändamål har MSB utvecklat tjänsten cybersäkerhetskollen där organisationer genom att svara på frågor själva kan utvärdera sitt arbete med informations- och cybersäkerhet. Myndigheten ger även ut ett metodstöd som syftar till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas utifrån standarderna om ledningssystem för informationssäkerhet. Metodstödet innehåller vägledningar, verktyg, tips, mallar och annat stöd och råd.

Enligt 11 a § andra stycket MSB:s instruktion ska myndigheten årligen lämna en rapport till regeringen med en sammanställning av de incidenter som rapporterats in till myndigheten enligt 14 § beredskapsförordningen. Inför arbetet med att sammanställa rapporten ska MSB inhämta upplysningar från Säkerhetspolisen och Försvarsmakten om de incidenter som rapporterats in till de myndigheterna enligt 2 kap. 4 § första stycket 2 säkerhetsskyddsförordningen. Utredningen föreslår i avsnitt 3.3.5 att incidentrapporteringen enligt beredskapsförordningen ska överföras till FRA. Det är därför naturligt att även ansvaret för att rapportera en sammanställning av inkomna incidentrapporter enligt förordningen till regeringen flyttas över.

Enligt förslaget till lag om cybersäkerhet i SOU 2024:18 kommer de flesta statliga myndigheter anmäla betydande incidenter till MSB som CSIRT-enhet enligt NIS 2-regleringen när denna har införlivats i svensk rätt. Utredningen föreslår i avsnitt 3.3.2 att FRA ska utses till CSIRT-enhet. För att bibehålla funktionen med den årliga redovisningen av statliga myndigheters incidenter till regeringen anser utredningen att det är ändamålsenligt att även rapporter enligt denna reglering ska inkluderas i rapporten till regeringen. Detta eftersom incidentrapporter som tidigare lämnats in genom beredskapsförordningen sannolikt kommer lämnas in enligt NIS 2-regelverket i stället. Utredningen föreslår därför att redovisningsuppdraget till reger-

ingen ska utvidgas så att det även innefattar statliga myndigheters rapporter om betydande incidenter enligt NIS 2-regleringen.

MSB har i dag i uppdrag att rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till ett behov av åtgärder på olika nivåer och områden i samhället. Även NCSC har ett sådant uppdrag på cybersäkerhetsområdet enligt 3 § 8 NCSC-förordningen. Genom att ansvaret för omvärldsanalys och stödjande insatser på informations- och cybersäkerhetsområdet samlas hos FRA kommer centret få förutsättningar för att uppnå en god förmåga att utföra denna uppgift. Utredningen föreslår därför att uppdraget ska samlas hos NCSC.

3.3.2 FRA ska utses till CSIRT-enhet, gemensam kontaktpunkt samt cyberkrishanteringsmyndighet

Utredningens förslag: Uppdragen att utgöra CSIRT-enhet, gemensam kontaktpunkt samt cyberkrishanteringsmyndighet enligt NIS 2-direktivet ska utföras av FRA. 20, 27, 31 och 32 §§ i förslaget till förordning om cybersäkerhet i dess lydelse enligt SOU 2024:18 ska ändras så att det framgår att FRA ska utföra uppdragen.

I NIS 2-direktivet fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen, i syfte att förbättra den inre marknadens funktion. Direktivet ålägger medlemsstaterna att anta nationella strategier för cybersäkerhet och att utse eller inrätta behöriga myndigheter, myndigheter för hantering av cyberkriser (cyberkrishanteringsmyndighet), gemensamma kontaktpunkter för cybersäkerhet (gemensamma kontaktpunkter) och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter). Direktivet innehåller även krav på riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter som omfattas av direktivet. Det innehåller även regler och skyldigheter när det gäller informationsutbyte om cybersäkerhet. Direktivet ålägger också medlemsstaterna att vidta åtgärder när det gäller tillsyn och efterlevnadskontroll.

Uppdraget som CSIRT-enhet

Enligt artikel 10 i NIS 2-direktivet ska varje medlemsstat utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheternas uppgifter regleras främst i artikel 11 i NIS 2-direktivet. I artikel 11.3 anges att CSIRT-enhetens uppgifter är följande.

- a) Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.
- b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.
- c) Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga entiteterna.
- d) Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.
- e) Tillhandahållande, på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.
- f) Deltagande i CSIRT-nätverket och ömsesidigt bistånd i enlighet med deras kapacitet och befogenheter till andra medlemmar i CSIRT-nätverket på deras begäran.
- g) I tillämpliga fall, fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.
- h) Bidrag till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3.

CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar.

När CSIRT-enheten utför dessa uppgifter får den prioritera särskilda uppgifter på grundval av en riskbaserad metod.

Av artikel 11.4 framgår därutöver att CSIRT-enheterna ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen för detta direktiv. För att främja ett sådant samarbete ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller förfaranden för incidenthantering samt samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Av artikel 12 i direktivet framgår vidare att varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av information om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som en betrodd mellanhand och vid behov underlätta interaktionen mellan den som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller tjänsterna. Uppgiften som samordnare innefattar att ha förmågan att ta emot anonyma sårbarhetsrapporter och agera på dessa samt säkerställa anonymiteten för den som rapporterat sårbarheten.

Det CSIRT-nätverk som CSIRT-enheterna ska medverka i enligt artikel 11.3 f beskrivs i artikel 15 i NIS 2-direktivet. Där framgår att nätverket ska ha ett omfattande uppdrag att möjliggöra delning av relevant information mellan de nationella CSIRT-enheterna samt utgöra ett forum för samarbete mellan de nationella enheterna vid incidenter.

CSIRT-enheten har ytterligare åtaganden, bland annat enligt artikel 23 i NIS 2-direktivet. I förslaget till förordning om cybersäkerhet enligt dess lydelse i SOU 2024:18 återfinns i 27–30 §§ bestämmelser om vilken myndighet som ska vara CSIRT-enhet och CSIRT-enhetens uppgifter.

Uppdraget som gemensam kontaktpunkt

Den gemensamma kontaktpunkten har enligt artikel 8.4 i NIS 2-direktivet i uppdrag att utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa. Kontaktpunkten ska även ha ett sektorsövergripande samarbete med andra behöriga myndigheter

i medlemsstaten. Den gemensamma kontaktpunktens ansvar för att vidarebefordra information framgår även av artiklarna 23, 27 och 37.

Enligt artikel 14 i direktivet inrättas en samarbetsgrupp. NIS 2-direktivet anger att bland annat företrädare för medlemsstaterna ska ingå, men inget närmare om att företrädaren ska inneha andra uppdrag enligt direktivet. Med hänsyn till samarbetsgruppens uppgifter har det varit MSB som nationell kontaktpunkt som har varit Sveriges representant i motsvarande grupp enligt NIS-direktivet. I förslaget till förordning om cybersäkerhet i SOU 2024:18 anges i 22 § att det tillhör den gemensamma kontaktpunktens uppgifter att delta i samarbetsgruppens arbete. Enligt artikel 14.4 i NIS 2-direktivet ska samarbetsgruppen ha följande uppgifter.

- a) Tillhandahålla vägledning till behöriga myndigheter angående införlivande och genomförande av detta direktiv.
- b) Tillhandahålla vägledning till behöriga myndigheter angående utarbetande och genomförande av strategier för den samordnade delgivningen av information om sårbarheter som avses i artikel 7.2 c.
- c) Utbyte av bästa praxis och information i fråga om genomförandet av detta direktiv, bland annat när det gäller cyberhot, incidenter, sårbarheter, tillbud, initiativ för att öka medvetenheten, utbildning, övningar och kompetens, kapacitetsuppbyggnad, standarder och tekniska specifikationer, samt identifiering av väsentliga och viktiga entiteter i enlighet med artikel 2.2 b–e.
- d) Utbyta råd och samarbeta med kommissionen om framväxande politiska initiativ för cybersäkerhet samt om den övergripande förenligheten mellan sektorsspecifika cybersäkerhetskrav.
- e) Utbyta råd och samarbeta med kommissionen om utkast till delegerade akter eller genomförandeakter som antas i enlighet med detta direktiv.
- f) Utbyta bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.
- g) Diskutera genomförandet av sektorsspecifika unionsrättsakter som innehåller bestämmelser om cybersäkerhet.
- h) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9 samt utarbeta slutsatser och rekommendationer.
- i) Genomföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor i enlighet med artikel 22.1.

- j) Diskutera fall av ömsesidigt bistånd, inbegripet erfarenheter och resultat av sådan gränsöverskridande gemensam tillsynsverksamhet som avses i artikel 37.
- k) På begäran av en eller flera berörda medlemsstater, diskutera särskilda begäranden om ömsesidigt bistånd som avses i artikel 37.
- l) Tillhandahålla strategisk vägledning till CSIRT-nätverket och EU-CyCLONe om specifika framväxande frågor.
- m) Utbyta åsikter om politiken för uppföljningsåtgärder efter storskaliga cybersäkerhetsincidenter och kriser på grundval av lärdomarna från CSIRT-nätverket och EU-CyCLONe.
- n) Bidra till cybersäkerhetskapaciteten i hela unionen genom att underlätta utbytet av nationella tjänstemän i form av ett kapacitetsuppbyggnadsprogram som inbegriper personal från behöriga myndigheter eller CSIRT-enheter.
- o) Anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.
- p) Diskutera det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.
- q) Fastställa metoder och organisatoriska aspekter för de sakkunnigbedömningar som avses i artikel 19.1 samt fastställa en självbedömningsmetod för medlemsstaterna i enlighet med artikel 19.5, med bistånd av kommissionen och Enisa, och, i samarbete med kommissionen och Enisa, utarbeta uppförandekoder som ligger till grund för de utsedda cybersäkerhetsexperternas arbetsmetoder i enlighet med artikel 19.6.
- r) Utarbeta rapporter för den översyn som avses i artikel 40 om de erfarenheter som förvärvats på strategisk nivå och från sakkunnigbedömningar.
- s) Regelbundet diskutera och genomföra en bedömning av läget när det gäller cyberhot.

I förslaget till förordning om cybersäkerhet enligt dess lydelse i SOU 2024:18 återfinns i 20–26 §§ bestämmelser om vilken myndighet som ska vara gemensam kontaktpunkt och den gemensamma kontaktpunktens uppgifter.

Uppdraget som cyberkrishanteringsmyndighet

Av artikel 9 i NIS 2-direktivet framgår att varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Enligt artikel 16.2 i direktivet ska det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) bland annat bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter. EU-CyCLONe ska bland annat ha i uppgift att öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser samt samordna hanteringen av storskaliga cybersäkerhetsincidenter. I förslaget till förordning om cybersäkerhet enligt dess lydelse i SOU 2024:18 återfinns motsvarande reglering i 31 och 32 §§.

Cyberkrishanteringsmyndighetens uppgifter och ansvarsområden på nationell nivå anges inte i direktivet. I stället ska medlemsstaterna enligt artikel 9.4 i direktivet anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av sådana situationer fastställs. Enligt artikel 9.4 b ska denna plan särskilt innehålla en beskrivning av cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Regeringen har den 27 februari 2025 gett FRA i uppdrag att ta fram en nationell operativ plan som bland annat ska innehålla en analys av detta (Fö2025/00388). Uppdraget ska redovisas den 1 december 2025.

FRA uppfyller kraven för att utses till CSIRT-enhet, gemensam kontaktpunkt samt cyberkrishanteringsmyndighet

I artikel 11.1 i NIS 2-direktivet framgår tekniska och andra krav på den myndighet som utses till CSIRT-enhet. I del 1 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) bedömdes FRA ha den tekniska förmåga som krävs för att vara CSIRT-enhet. Utredningen delar denna bedömning och konstaterar att det följer av FRA:s befintliga uppdrag att ha en hög teknisk kompetens på området. Utredningen återkommer i kapitel 5 till frågan om att ett visst behov av tekniskt stöd från MSB kan uppkomma under en övergångsperiod efter att verksamheten har flyttats över till FRA.

Enligt artikel 11.1 b och d i NIS 2-direktivet ska CSIRT-enheten även ha tillräckligt med personal för att säkerställa att enhetens

tjänster är ständigt tillgängliga och att personalen har fått lämplig utbildning. Den ska även ha lokaler som är belägna på säkra platser. Även rollerna som gemensam kontaktpunkt och cyberkrishanteringsmyndighet har krav på tilldelning av adekvata resurser i artikel 8.5 respektive 9.1. Utredningen återkommer till dessa frågor i konsekvensanalysen i kapitel 5.

Därutöver kräver samtliga uppgifter en förmåga att delta i internationella samarbetsnätverk med delning av information till motsvarande funktioner i andra medlemsländer samt andra EU-organ. Vad gäller CSIRT-enheten är detta även ett uttalat krav. FRA bedriver i dag främst verksamhet inom nationell säkerhet. Myndigheten tillhör därför som utgångspunkt den grupp myndigheter som NIS 2-direktivet inte är tillämpligt på i enlighet med artikel 2.7. Sverige har samtidigt en skyldighet att leva upp till kraven i direktivet, vilket innebär att FRA vid en överföring av uppdragen som CSIRT-enhet, cyberkrishanteringsmyndighet och gemensam kontaktpunkt till myndigheten ändå måste kunna verka i en EU-kontext.

Den informationsdelning som CSIRT-enheten, den gemensamma kontaktpunkten och cyberkrishanteringsmyndigheten har att delta i med utländska myndigheter och EU-organ behandlades i slutbetänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64). Där gjordes även en bedömning av de författningsmässiga förutsättningarna för ett sådant samarbete. Den utredningen gjorde bedömningen att sådana förutsättningar finns genom undantaget från sekretess i 8 kap. 3 § offentlighets- och sekretesslagen (2009:400), OSL. Av bestämmelsen framgår att en uppgift för vilken sekretess gäller enligt OSL inte får röjas för en utländsk myndighet eller en mellanfolklig organisation. Från denna huvudregel ges sedan två undantag. Det ena undantaget omfattar utlämnande som sker i enlighet med särskild föreskrift i lag eller förordning. Det andra undantaget gäller om uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen. I betänkandet SOU 2024:64 konstaterades att CSIRT-enheternas, den gemensamma kontaktpunktens samt cyberkrishanteringsmyndighetens uppgifter framgår i förslaget till förordning om cybersäkerhet. Eftersom informationsdelningen således kommer ske med stöd av särskild föreskrift i förordning

gjordes bedömningen att ytterligare författningsstöd inte krävdes för att uppgifter ska kunna delas med EU-organ och utländska myndigheter inom ramen för NIS 2-samarbetet. Utredningen instämmer i denna bedömning och konstaterar att en överföring av uppdragen till FRA inte förändrar dessa förutsättningar. FRA kommer således ha författningsstöd för att verka i en EU-kontext och uppfylla de krav på informationsdelning som ställs upp i NIS 2-direktivet. Utredningen återkommer i kapitel 4 till överväganden och förslag när det gäller vissa andra frågor om informationsdelning och -hantering.

Till följd av FRA:s arbete inom nationell säkerhet behöver även en analys göras av om nödvändig informationsdelning kan ske utan att myndigheten underkastas krav på delning av information rörande nationell säkerhet. Av artikel 2.11 i NIS 2-direktivet framgår att de skyldigheter som fastställs i direktivet inte ska medföra tillhållande av information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. Av artikel 2.13 framgår i övrigt att information som är konfidentiell enligt unionsbestämmelser eller nationella bestämmelser, såsom bestämmelser om affärshemligheter, ska utbytas med kommissionen och andra berörda myndigheter i enlighet med direktivet endast när ett sådant utbyte är nödvändigt för att tillämpa direktivet. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och berörda entiteters säkerhets- och affärsintressen skyddas. Motsvarande begränsningar i skyldigheten att dela sådan information anges även i skäl 9 till direktivet. I SOU 2024:18 har man mot denna bakgrund i förslaget till lag om cybersäkerhet, som dock avser verksamhetsutövarna, infört ett undantag genom 1 kap. 14 § som innebär att uppgiftsskyldighet enligt lagen inte gäller för uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Med hänsyn till ovanstående anser utredningen att FRA kommer kunna efterleva de krav på informationsdelning som medföljer uppdragen som gemensam kontaktpunkt, CSIRT-enhet och cyberkris-hanteringsmyndighet. Direktivet innehåller samtidigt sådana undantag att myndigheten inte kommer vara skyldig att dela information som rör nationell säkerhet. Det är FRA:s ansvar som informations-

ansvarig inom centret att tillse att adekvata rutiner finns för hanteringen och delningen av information med varierande känslighet.

Sammantaget bedömer utredningen att FRA kommer ha förutsättningar att uppfylla de krav som följer av NIS 2-direktivet i uppdragen som CSIRT-enhet, gemensam kontaktpunkt och cyberkris-hanteringsmyndighet inom ramen för NCSC. FRA besitter vidare hög teknisk förmåga och har förmågan att utföra de uppgifter som dessa uppdrag medför.

Uppdragen bör samlas hos FRA

NIS 2-direktivet ställer genom artikel 13 direkta krav på att CSIRT-enheterna, den gemensamma kontaktpunkten och cyberkris-hanteringsmyndigheten ska samverka med varandra. En samverkan mellan de olika uppdragen underlättas avsevärt av att de samlas på en myndighet. Att uppdragen samlas på en myndighet underlättar även i övrigt ett effektivt arbete och en konsekvent nationell hållning i förhållande till EU. I den samarbetsgrupp som den gemensamma kontaktpunkten deltar i hanteras till exempel frågor som får stor påverkan för CSIRT-enhetens arbete. Samtliga uppgifter ställer dessutom höga krav på teknisk kunskap och en uppdelning av dem på flera myndigheter skulle därför innebära en icke önskvärd uppdelning av värdefulla personalresurser.

FRA ska få det samlade ansvaret för stödjande och förebyggande insatser för samhällets informations- och cybersäkerhet samt för att analysera och bedöma omvärldsutvecklingen på området. NIS 2-direktivet ger medlemsstaterna stor frihet i hur myndighetsuppgifterna enligt direktivet ska organiseras. För att samla arbetet med informations- och cybersäkerhet under en huvudman och möjliggöra för NCSC att utföra sitt uppdrag på ett ändamålsenligt sätt anser utredningen att det finns skäl att överföra uppdragen att utgöra CSIRT-enhet, gemensam kontaktpunkt samt cyberkris-hanteringsmyndighet till FRA. Detta innebär även att FRA kommer delta i CSIRT-nätverket, NIS 2-samarbetsgruppen samt EU-CyCLONe.

3.3.3 FRA ska ges viss föreskriftsrätt enligt förordningen om cybersäkerhet

Utredningens förslag: FRA ska ges föreskriftsrätt genom ändring i 33–36 §§ i förslaget till förordning om cybersäkerhet i dess lydelse enligt SOU 2024:18.

Föreskriftsrätten ska avse incidentrapportering, verksamhetsutövare som inte uppfyller storlekskravet samt om anmälningsskyldighet. FRA får även meddela föreskrifter för sektorerna offentlig förvaltning och lärosäten med examenstillstånd om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. FRA ges även rätt att yttra sig över sektorsspecifika föreskrifter.

MSB har enligt den svenska implementeringen av NIS-direktivet haft föreskriftsrätt enligt förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. I förslaget till förordning om cybersäkerhet i SOU 2024:18 ges MSB genom 33–36 §§ rätten att meddela föreskrifter för genomförandet av NIS 2-direktivet. MSB får i föreskrifter ange vilka verksamhetsutövare som omfattas av 1 kap. 8 § i förslaget till lag om cybersäkerhet. Myndigheten får även meddela föreskrifter om anmälningsskyldigheten i 2 kap. 2 § i samma förslag. Vidare föreslås MSB få bemyndigandet att meddela föreskrifter om vad som utgör en betydande incident och om incidentrapportering. För sektorn offentlig förvaltning och lärosäten med examenstillstånd är förslaget att MSB ska få meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning. För övriga sektorer föreslås att MSB ska ges tillfälle att yttra sig över tillsynsmyndigheternas föreskrifter.

Förslagen i SOU 2024:18 bygger på en modell där övergripande föreskrifter utfärdas av en central myndighet, medan närmare föreskrifter om det konkreta arbetet med riskhanteringsåtgärder och det riskbaserade informationssäkerhetsarbetet i huvudsak utfärdas av tillsynsmyndigheterna för varje sektor. Modellen har kritiserats under remissförfarandet och ett flertal remissinstanser har där anförts att ansvaret bör ges till en myndighet att utfärda sektorsövergripande föreskrifter även gällande riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning.

I förslaget till förordning om cybersäkerhet i SOU 2024:18 ges MSB i stället rätten att yttra sig över de sektorsvisa föreskrifterna. Även andra förslag på hur föreskriftsrätten bör delas upp har framkommit. Denna utrednings förslag om verksamhetsöverflytt i dessa delar kan således komma att behöva omvärderas framöver med anledning av det fortsatta beredningsarbetet av den nya lagen och förordningen om cybersäkerhet.

Enligt kommittédirektivet ska en åtskillnad göras mellan stödjande verksamhet och tillsynsverksamhet. Verksamheten ska även kunna bedrivas effektivt utifrån de behov som finns att samla informations- och cybersäkerhetsfrågorna. Det har framförts till utredningen att dessa utgångspunkter i kommittédirektivet medför att FRA inte bör tilldelas föreskriftsrätt. Detta eftersom myndighetsföreskrifterna blir en del av det regelverk som tillsynsmyndigheterna har i uppdrag att kontrollera efterlevnaden av. Föreskriftsrätt kan därmed anses utgöra en del av det allmännas kontroll över verksamhetsutövare. Rådgivning som ges av centret kan därför komma att uppfattas som ett förhandsavgörande angående regelefterlevnad. Det kan även finnas en farhåga hos privata aktörer att uppgifter som lämnas till centret i förtroende sedan används för att skärpa kraven i föreskrifter. Dessa omständigheter skulle kunna påverka enskilda aktörers förtroende för centret och därmed deras villighet att dela information. Ett alternativ vore därför att FRA endast ska ägna sig åt mjuk normering genom rådgivning samt att centret kan bistå myndigheter med kunskap i myndigheternas arbete med att utfärda föreskrifter.

Utredningens utgångspunkt är dock att utfärdande av föreskrifter inte isolerat utgör tillsyn när dessa uppgifter inte kombineras med möjligheten att kontrollera efterlevnaden av föreskrifterna eller utfärda sanktioner. Utan dessa verktyg får verksamheten i stället anses som stödjande. Arbetet med tolkning av direktivet sker vidare till stor del inom ramen för den samarbetsgrupp där de gemensamma kontaktpunkterna deltar (jfr artikel 14.4 a–14.4 c i NIS 2-direktivet). Det är med hänsyn till detta av vikt att föreskriftsrätten enligt NIS 2-direktivet och uppdraget som gemensam kontaktpunkt hålls samman i så hög grad som möjligt. På det viset tillses att den kunskapsutveckling som sker inom ramen för EU-samarbetet också får genomslag i de föreskrifter som reglerar svenska förhållanden. Genom att föreskriftsrätten enligt NIS 2-direktivet till viss del för-

läggs inom ramen för NCSC:s arbete ges också en tydligare möjlighet till ansvarsutkrävande när privata aktörer upplever brister med den svenska implementeringen av direktivet. Utredningen anser därför att fördelarna med att samlokalisera uppgiften som gemensam kontaktpunkt med föreskriftsrätten är utslagsgivande och att ett sådant förslag inte går utanför ramarna för kommittédirektivet.

När det gäller föreskriftsrätten om incidentrapportering innefattar detta rätten att komplettera kommissionens genomförandeförordning (EU 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv [EU] 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster). I genomförandeförordningen ges i artiklarna 3–14 både allmänna och sektorsspecifika kriterier för vad som ska anses utgöra en betydande incident. Eftersom incidentrapporteringen enligt NIS 2-direktivet enligt förslaget till lag om cybersäkerhet i SOU 2024:18 ska lämnas till CSIRT-enheten har dessa frågor en tydlig koppling till uppgiften att utgöra en sådan enhet. Det är även en fråga som gäller samtliga sektorer. Ett alternativt förfarande där en eller flera andra myndigheter har föreskriftsansvaret på området skulle riskera att leda till dubbel normering om CSIRT-enheten och föreskrivande myndigheter inte är överens om underlaget för rapporteringen. För att skapa en effektiv ordning med så få överlappande ansvarsområden som möjligt är det därför viktigt att den normerande rollen hör ihop med CSIRT-enheten.

Vad gäller föreskrifter om verksamhetsutövare som inte uppfyller storlekskravet anges i SOU 2024:18 att frågan hör ihop med MSB:s allmänna uppdrag att stödja och samordna arbetet med samhällets informationssäkerhet samt uppdraget att analysera och bedöma omvärldsutvecklingen inom området. Genom dessa uppdrag får myndigheten antas ha den kunskap som behövs för att bedöma vilka verksamheter som ska omfattas av regleringen oavsett storlek.

Utredningen anser att motsvarande skäl kan göras gällande när FRA enligt förslaget i avsnitt 3.3.1 får det övergripande ansvaret för samhällets arbete med informations- och cybersäkerhet. Även dessa frågor är gemensamma för samtliga sektorer och bör således inte överlämnas till varje sektor att utforma.

När det kommer till föreskrifter om anmälningsskyldighet är det system som föreslås i SOU 2024:18 uppbyggt kring att de sektorsvisa tillsynsmyndigheterna upprättar register över väsentliga och viktiga verksamhetsutövare. Registren vidarebefordras sedan till den gemensamma kontaktpunkten som i sin tur vidareförmedlar informationen till kommissionen och samarbetsgruppen. Utredningen föreslår i avsnitt 3.3.2 att FRA ska utses till gemensam kontaktpunkt, varför slutmottagare för registren i Sverige kommer vara FRA. Eftersom uppgifterna som ska lämnas i en anmälan är de samma oberoende av sektor är det motiverat av effektivitetsskäl att det är den centrala myndigheten i Sverige som också utfärdar föreskrifterna.

Föreskriftsansvaret för varje sektors arbete med riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning ska enligt tidigare förslag till förordning om cybersäkerhet i SOU 2024:18 förläggas på respektive tillsynsmyndighet, med undantag för sektorerna offentlig förvaltning och lärosäten med examenstillstånd. Skälet för denna ordning är att tillsynsansvaret för dessa sektorer är uppdelat geografiskt på flera länsstyrelser. För att undvika att flera länsstyrelser ska meddela föreskrifter för samma sektor har föreskriftsrätten enligt förslaget samlats på en myndighet. Det saknas skäl att göra någon annan bedömning med anledning av att uppgifterna överförs till FRA. Denna fördelning av föreskriftsansvaret medför således att FRA, utöver de sektorsgemensamma föreskrifterna, även bör meddela föreskrifter om konkreta åtgärder kring statliga myndigheters arbete med informations- och cybersäkerhet. FRA bör även ta över möjligheten yttra sig över de föreskrifter som tillsynsmyndigheterna tar fram. Myndigheten får därigenom en möjlighet att bidra till ökad harmonisering av de sektorsspecifika föreskrifterna.

3.3.4 FRA ska ansvara för tillsynssamordning

Utredningens förslag: FRA ska ges ansvaret för att leda ett samarbetsforum för tillsynsmyndigheterna genom ändring i 37 § i förslaget till förordning om cybersäkerhet i dess lydelse enligt SOU 2024:18.

För att underlätta genomförandet av NIS-direktivet har MSB lett ett samarbetsforum för en effektiv och likvärdig tillsyn där tillsynsmyndigheterna samt Socialstyrelsen ingått, se 21 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster. I förslaget till förordning om cybersäkerhet i SOU 2024:18 anges i 37 § att MSB ska ha motsvarande uppgift för tillsynsmyndigheterna enligt NIS 2-direktivet. Syftet med forumet är att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn mellan de olika sektorerna. Av en utvärdering av tillsynssamordningen enligt NIS-direktivet som redovisas i SOU 2024:18 framgår att tillsynsmyndigheterna anser att samarbetsforumet bidragit till värdefullt erfarenhetsutbyte mellan myndigheterna. Det har också bidragit till viss harmonisering av tillsynen. Bland annat har gruppen tagit fram kriterier för hur myndigheterna ska göra urvalet av vilka verksamhetsutövare som ska kontrolleras via tillsyn. Samarbetsforumet har också bidragit till att nya tillsynsmyndigheter har kunnat dra nytta av metodstöd för att utforma sin tillsynsprocess. Flera myndigheter framförde till den utredningen att MSB i samband med implementeringen av NIS 2-direktivet borde få utökade möjligheter att styra tillsynsmyndigheterna. Jämförelser gjordes då bland annat med systemet för tillsynssamordning i säkerhetsskyddslagen. Utredaren ansåg dock att systemet skiljer sig åt på ett sådant sätt att ett motsvarande mandat för MSB inte är nödvändigt.

Av kommittédirektivet framgår att en åtskillnad ska göras mellan stödjande verksamhet och tillsyn. Det har framförts från flera håll till utredningen att denna rågång bör upprätthållas och att FRA inte bör tilldelas uppdraget som tillsynssamordnare. Skälet för detta är att en sammanblandning av uppgifter som rör stöd och uppgifter som rör tillsyn riskerar att påverka privata aktörers incitament att frivilligt anmäla sårbarheter. Även om CSIRT-enheten har i uppdrag att ta emot frivilliga rapporter om sårbarheter utan att röja anmälarens identitet kan ett organ som både tar emot anonyma

rapporter om sårbarheter och har ett nära förhållande till tillsynssystemet med utfärdande av tillhörande sanktionsavgifter utgöra ett hinder mot en hög tillit till centret. Eftersom kunskapen om sårbarheter i samhället på cybersäkerhetsområdet främst finns hos de privata aktörerna är detta ett viktigt perspektiv att beakta. Om privata aktörer har en låg tillit till CSIRT-enheten och därför inte delar all information som de hade kunnat dela försvagas hela samhällets möjlighet att agera i tid mot potentiella hot eller olyckor. I skäl 41 till NIS 2-direktivet anges också att medlemsstaterna bör kunna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet när en CSIRT-enhet är en del av en behörig myndighet.

Med ovanstående omständigheter i åtanke vore en alternativ lösning att tillsynssamordningen sköttes av tillsynsmyndigheterna internt, med en av de utpekade myndigheterna som sammankallande. Denna lösning hade inneburit att tillsynen helt separerats organisatoriskt från centret, vilket skulle kunna öka privata aktörers villighet att samarbeta med centret.

Det finns samtidigt starka skäl som talar för att rollen som tillsynssamordnare bör förläggas hos FRA i NCSC:s verksamhet. Den gemensamma kontaktpunkten har genom sitt deltagande i samarbetsgruppen på EU-nivå insyn i och möjlighet att påverka hur NIS 2-direktivet ska tillämpas. För att skapa förutsättningar för ett effektivt och likvärdigt tillsynsarbete krävs tillgång till experter med kunskap om de föreskrifter som tillsynen utgår ifrån. Behovet av sådan expertis ökar i samband med implementeringen av NIS 2-direktivet eftersom verksamhetsutövare som bedriver verksamhet i flera sektorer kommer att omfattas av överlappande tillsynsansvar från olika myndigheter. Genom utredningens förslag om överföring av uppgifter till FRA är det FRA som kommer ha den nödvändiga kompetensen för att kunna samordna tillsynsmyndigheterna. Det har även framförts till utredningen att ett återkommande önskemål från målgrupperna tidigare har varit att föreskrifter, stöd och samordning av tillsyn ska vara koherenta och samordnade och att en utpekad aktör kan ta ansvar för helheten om problem i någon del skulle uppstå och ändringar behöver göras. Utredningen anser att

det är en förutsättning att samordningen placeras i NCSC för att en sådan ordning ska vara möjlig att åstadkomma.

Sammantaget finns det flera legitima intressen hos verksamhetsutövarna som svårigen kan förverkligas fullt ut samtidigt. Å ena sidan finns behovet av en central aktör som kan ta ansvar för brister i implementeringen av regelverket och som besitter nödvändig kunskap för att kunna åtgärda problemen. Å andra sidan finns det legitima farhågor med ett för nära samröre mellan tillsynsmyndigheterna och CSIRT-enheten där ömsesidigt utbyte av information med verksamhetsutövare som står under tillsyn är en förutsättning för centrets arbete. Förslaget innebär dock inte att FRA får något tillsynsansvar. Det finns således alltjämt en skiljelinje mellan CSIRT-enhetens stödjande verksamhet och tillsynsmyndigheternas faktiska arbete med kontroll av de aktörer som omfattas av direktivet. Samordningsfunktionens syfte är inte heller att utgöra ett forum för informationsutbyte kring enskilda verksamhetsutövare, utan att arbeta fram gemensamma arbetssätt mellan tillsynsmyndigheterna och stärka kompetensen hos de myndigheter som tidigare inte arbetat med tillsynsfrågor på informations- och cybersäkerhetsområdet. Samordningen bör på detta sätt bidra till ett förutsebart och rätts-säkert tillsynsförfarande. Det åligger vidare FRA att tillförsäkra fysiska eller juridiska personer enligt artikel 12 i NIS 2-direktivet rätten att lämna anonyma underrättelser om sårbarheter. Utredningen återkommer i kapitel 4 med förslag till en ny sekretessbestämmelse för att möjliggöra detta. Det är utredningens bedömning att en god privat-offentlig samverkan med NCSC kan uppnås genom att rätten att lämna anonyma rapporter om sårbarheter och samarbetsforumets funktion tydligt kommuniceras till de privata aktörerna.

3.3.5 FRA ska ta emot incidentrapporter enligt fler regelverk

Utredningens förslag: FRA ska ta emot it-incidentrapporter enligt beredskapsförordningen.

FRA ska ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter. Myndigheten ska

1. agera skyndsamt vid it-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och

medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade,

2. återrapportera till berörda aktörer i samband med att en it-incident har rapporterats,
3. samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet, samt
4. vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.

Utöver NIS-regleringen finns bestämmelser om samhällets arbete med informations- och cybersäkerhet även i den nationella regleringen om samhällets krisberedskap. För statliga myndigheter ger beredskapsförordningen övergripande regler och krav på myndigheterna i hur de ska förbereda sig och agera under kris (Krisjuridik, Rättsliga befogenheter från olycka till höjd beredskap, Juno version 1). Statliga myndigheter är enligt förordningen bland annat skyldiga att genomföra risk- och sårbarhetsanalyser. Därutöver ska myndigheterna enligt 14 § beredskapsförordningen under vissa omständigheter lämna rapporter till MSB om it-incidenter i verksamheten. I det nuvarande systemet ansvarar MSB för incidentrapporteringsfunktionen enligt både NIS-regleringen och beredskapsförordningen. Myndigheten har därutöver till uppgift enligt 11 b § MSB:s instruktion att ansvara för att Sverige har en nationell funktion med uppgift att stödja samhället i arbetet med att förebygga och hantera it-incidenter, vilket möjliggör för myndigheten att motta både formell och informell frivillig incidentrapportering enligt. Dessa uppgifter bör även fortsatt hållas samman inom Sveriges nationella funktion för att stödja samhället i arbetet med att förebygga och hantera it-incidenter, CERT-SE. En ordning med flera CSIRT-enheter på olika myndigheter som mottar incidentrapporter enligt olika regelverk skulle gå emot ambitionen att samla ansvaret för arbetet med informations- och cybersäkerhetsfrågor och dessutom komplicera förfarandet för verksamhetsutövare som kan omfattas av flera regelverk samtidigt. Eftersom förslaget i avsnitt 3.3.2 innebär att FRA blir CSIRT-enhet enligt NIS 2-direktivet bör

även ansvaret för övriga delar av CERT-SE föras över för att hålla samman rapporteringsfunktionen.

Eftersom flera nya sektorer tillkommer genom NIS 2-direktivet kommer ett betydande överlapp uppstå mellan NIS 2-direktivet och beredskapsförordningen. Många statliga myndigheter kommer enligt förslaget till förordning om cybersäkerhet i SOU 2024:18 omfattas av båda regleringarna. Det finns även aktörer som inte kommer att omfattas av något av regelverken. För statliga myndigheters del kan det således uppstå situationer när incidentrapportering ska göras enligt flera regelverk. En analys av hur de överlappande systemen ska hanteras framöver kan dock inte göras inom ramen för denna utredning.

3.3.6 FRA ska ges föreskriftsrätt enligt beredskapsförordningen

Utredningens förslag: FRA ska få meddela ytterligare föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i 13 § beredskapsförordningen utom i fråga om Regeringskansliet, kommittéväsendet och Försvarsmakten. Myndigheten ska därvid beakta nationell och internationell standard för informationssäkerhet.

FRA ska få meddela närmare föreskrifter om it-incidentrapportering enligt 14 § beredskapsförordningen efter att ha gett Polismyndigheten, Säkerhetspolisen och Försvarsmakten tillfälle att yttra sig.

MSB får meddela föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i 13 § beredskapsförordningen samt närmare föreskrifter om it-incidentrapportering enligt 14 § beredskapsförordningen. En uppenbar nackdel med att överföra föreskriftsrätten enligt bestämmelserna till FRA är att det komplicerar systematiken i beredskapsförordningen. I dagsläget har MSB ett brett bemyndigande enligt förordningen som möjliggör för myndigheten att utgöra så kallad top-nod i beredskapssystemet. Vid en överföring av ansvaret för vissa föreskrifter till en annan myndighet delas ansvaret för regleringen upp på fler myndigheter.

Utredningen föreslår i avsnitt 3.3.5 att ansvaret för incidentrapporteringsfunktionen enligt beredskapsförordningen ska föras

över till FRA för att hålla samman CERT-SE. Samma skäl för att överföra föreskriftsrätt med koppling till incidentrapporteringen enligt NIS 2-regleringen gör sig även gällande här. Genom att motsvarande föreskriftsrätt som MSB nu har avseende it-incidentrapporteringen flyttas över till FRA hålls detta samband ihop vid överföringen av incidentrapporteringsuppdraget. Enligt förslagen i SOU 2024:18 kommer de flesta av de myndigheter som omfattas av beredskapsförordningen även att omfattas av NIS 2-regleringen och ingå i sektorn offentlig förvaltning. För att undvika situationen att motstridiga föreskrifter meddelas avseende samma myndigheter behöver därför föreskriftsansvaret för informationssäkerhet enligt beredskapsförordningen och föreskriftsansvaret för sektorn offentlig förvaltning enligt NIS 2-regleringen placeras på samma myndighet. Utredningen anser att dessa aspekter väger tyngre än nackdelarna med en överföring och föreslår därför att rätten att meddela föreskrifter om sådana säkerhetskrav för informationshanteringssystem som avses i 13 § beredskapsförordningen samt närmare föreskrifter om it-incidentrapportering enligt 14 § beredskapsförordningen ska föras över till FRA.

3.3.7 FRA ska utses till nationellt samordningscenter för forskning och innovation inom cybersäkerhet

Utredningens förslag: FRA ska vara nationellt samordningscenter enligt artikel 6 i CCCN-förordningen.

FRA ska även utses till handläggande myndighet enligt förordning (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning. FRA får även meddela föreskrifter om verkställigheten av förordningen.

MSB är i dag enligt 11 c § i sin myndighetsinstruktion nationellt samordningscenter enligt artikel 6 i CCCN-förordningen. Verksamheten bedrivs under namnet NCC-SE och har till uppgift att främja samarbete mellan svenska forskningsinstitut, företag och myndigheter för utveckling av cybersäkerhetslösningar. Verksamheten ska även främja kontakt mellan svenska och europeiska forskare och företag, underlätta för svenska aktörer att svara på europeiska forsknings- och innovationsutlysningar samt stödja EU:s

kompetenscentrum för cybersäkerhet (ECCC) i uppdraget för ökad cybersäkerhet inom EU. NCC-SE tillhandahåller i dag bland annat vägledningar för aktörer som vill söka EU-stöd, anordnar informationsträffar samt samordnar verksamheten i Cybernoden, som är en plattform för samverkan på cybersäkerhetsområdet som drivs av RISE Research Institutes of Sweden. Sedan 2024 har MSB rätt att pröva ansökningar om stöd till verksamhetsutövare enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning. Beslut enligt förordningen kan överklagas till allmän förvaltningsdomstol. MSB får meddela föreskrifter om verkställigheten av förordningen.

Utredningen har i första hand utrett om NCC-SE bör överföras till FRA. Vad som talar för en sådan ordning är inledningsvis att det leder till ett mer samlat företrädarskap på myndighetsnivå vid internationella kontakter i frågor som rör informations- och cybersäkerhet. För att samordningscentret ska fungera måste det även finnas ett kontinuerligt samarbete med uppdragen enligt NIS 2-direktivet. Därigenom tillförsäkras bland annat att arbetet i NCC-SE utgår ifrån de behov som uppmärksammas i CSIRT-enhetens arbete med sårbarheter. Eftersom uppdragen enligt NIS 2-direktivet ska samlas hos FRA enligt utredningens förslag talar detta för att FRA även ska utses till samordningscenter. Därutöver framgår av NCSC-förordningen att NCSC ska vara en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet. Utredningen bedömer att detta arbete skulle underlättas avsevärt av att FRA utses till nationellt samordningscenter för forskning och innovation inom cybersäkerhet.

Det som talar emot ett förslag om att utse FRA till värd för NCC-SE är att forskning och förmedling av EU-stöd ligger långt ifrån myndighetens övriga kärnverksamhet. Utredningen har därför även övervägt andra myndigheter för detta uppdrag, så som Post- och telestyrelsen, DIGG, Vinnova och Totalförsvarets forskningsinstitut. Genom den överföring av personal som kommer att ske i samband med verksamhetsöverföringen till FRA bör dock myndigheten tillförsäkras personal med erfarenhet av sådan verksamhet. Utredningen bedömer vidare att de skäl som redovisats ovan om den nära koppling som behöver finnas mellan NIS 2-uppdragen och NCC-SE samt NCC-SE:s potential att stärka NCSC i sitt

uppdrag är utslagsgivande. Frågan är därefter om FRA uppfyller kraven för att kunna utses till samordningscenter.

En medlemsstat får enligt artikel 6.4 i CCCN-förordningen när som helst utnämna en ny enhet till nationellt samordningscenter. Medlemsstaten får vid ett sådant beslut lämna in en begäran till kommissionen om ett erkännande av att den nya enheten har kapacitet att förvalta medel för att fullgöra uppdraget och uppnå de mål som fastställs i CCCN-förordningen.

Kriterierna för att utnämnas till samordningscenter framgår av artikel 6.5 i CCCN-förordningen. Där anges att samordningscentrumet ska vara en enhet inom den offentliga sektorn eller en enhet som huvudsakligen ägs av medlemsstaten, som utför offentliga förvaltningsuppgifter i enlighet med nationell rätt. Enheten ska kunna ge stöd åt ECCC och nätverket i fullgörandet av deras uppdrag och ska vidare antingen besitta eller ha tillgång till sakkunskap avseende forskning och teknik inom cybersäkerhet. Enheten ska även ha kapacitet att effektivt föra en dialog med och samordna arbetet med näringslivet, den offentliga sektorn, den akademiska världen, forskarsamhället och medborgarna.

FRA utgör en enhet inom den offentliga sektorn som utför offentliga förvaltningsuppgifter i enlighet med nationell rätt. Det krävs inga författningsändringar för att FRA ska kunna ge stöd åt ECCC och nätverket i fullgörandet av deras respektive uppdrag. Myndigheten bedöms även besitta god sakkunskap avseende teknik inom cybersäkerhet. Genom NCSC:s övriga uppdrag kommer det också finnas goda förutsättningar att samordna arbetet med näringslivet, den offentliga sektorn, den akademiska världen, forskarsamhället och medborgarna.

Utredningen bedömer sammantaget att FRA uppfyller förutsättningarna för att utses till nationellt samordningscenter enligt CCCN-förordningen. Av artikel 1 framgår vidare att förordningen inte påverkar medlemsstaternas befogenheter i fråga om allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på straffrättens område. Utredningen gör därför samma bedömning som i avsnitt 3.3.2 avseende FRA:s möjligheter och skyldigheter att dela information med utländska aktörer.

Genom att FRA utses till samordningscenter blir myndigheten även ansvarig för att handlägga ärenden enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv,

teknik och forskning. Myndigheten tar även över bemyndigandet att meddela föreskrifter som kompletterar förordningen.

Uppdraget att utgöra nationellt samordningscenter medför hantering av EU-medel. MSB har även ingått avtal om medfinansiering genom EU-stöd för utvecklingen av uppdragen enligt NIS 2-direktivet. Utredningen återkommer till dessa frågor samlat i kapitel 5.

3.3.8 FRA ska vara teknisk kontaktpunkt för OSSE

Utredningens förslag: FRA ska vara teknisk kontaktpunkt för OSSE.

MSB är i dag svensk teknisk kontaktpunkt för OSSE:s verksamhet på cyberområdet (18 j § MSB:s instruktion). Myndigheten har i kontakt med utredningen beskrivit uppdraget på följande sätt.

I rollen som teknisk kontaktpunkt ingår det att vid behov stödja den politiska kontaktpunkten på Utrikesdepartementet samt samverka gentemot den svenska representationen i Wien. I detta ingår att delta på möten, föra anteckningar och lyfta fram myndigheten som såväl som det nationella cybersäkerhetsarbetet där så är lämpligt. Rollen har även inneburit att besvara så kallade "Communication checks". Dessa comchecks övar på och syftar till att säkerställa informationsutbyte mellan OSSE:s medlemsstater vid händelse av en särskilt allvarlig incident eller kris. Dessa comchecks innehåller ett antal frågor som den tekniska kontaktpersonen stämmer av med CERT-SE innan den politiska kontaktpersonen besvarar ärendet. Kommunikation mellan medlemsstaterna sker i OSSE:s kommunikationsnät och integrerade meddelande-applikation.

Av kommittédirektivet framgår att utredaren bör beakta hur en överföring av arbetsuppgifter kan bidra till ett mer samlat internationellt företräderskap i cyberfrågor på myndighetsnivå. En överföring av rollen som teknisk kontaktpunkt bidrar till ett sådant samlat företräderskap. Även de nödvändiga kontakterna med CERT-SE som har beskrivits ovan underlättas av att uppgiften förläggs på samma huvudman som ansvarar för CERT-SE. Rollen som teknisk kontaktpunkt för OSSE bör därför föras över till FRA.

3.4 Verksamhet som inte ska föras över till FRA

Utredningens bedömning: MSB ska även fortsatt ansvara för uppgifterna enligt 5 § andra stycket, 16–16 a §§, 18 b §, 18 g–18 i §§ i MSB:s instruktion. Den ska även utgöra behörig myndighet enligt 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).

MSB har flera uppgifter i sin myndighetsinstruktion på informations- och cybersäkerhetsområdet som har ett nära samband med samhällets krisberedskap och civilförsvar. Bland annat ansvarar myndigheten enligt 16 § för driften, förvaltningen och utvecklingen av det säkra radiokommunikationssystemet Rakel. Myndigheten har enligt 16 a § i instruktionen ett motsvarande ansvar för kommunikationstjänsten SGSI som möjliggör delning av databaser och annan kommunikation mellan myndigheter i Sverige och i Europa. Systemen har gemensamt att de är utformade för att möjliggöra bibehållen kommunikation även vid störningar eller attacker mot andra system, så som telefoni och it-system. Myndigheten är därutöver enligt 5 § andra stycket i instruktionen ansvarig för ledningsmetoder och stödsystem för räddningstjänst, krishantering och civilt försvar samt att materiel för räddningstjänst och krishantering utvecklas och tillhandahålls. I linje med dessa uppdrag har MSB även behörighet att besluta om tilldelning av signalskyddssystem enligt förordning (2015:1053) om totalförsvar och höjd beredskap. MSB har även flera uppdrag inom unionens program för rymden och satellitkommunikationstjänster enligt 18 b § och 18 g–18 i §§ i instruktionen, såsom att utgöra behörig myndighet för EU:s program för säkra satellitkommunikationstjänster Govsatcom samt Galileo PRS, som är ett europeiskt satellitnavigeringssystem. MSB har även fortsatt förordnanden i beredskapsförordningen. Dessa uppdrag är intimt sammankopplade med myndighetens övriga arbete med krisberedskap och civilt försvar. MSB har vidare en särskild upparbetad kompetens i att fullgöra dessa uppgifter. Uppgifterna är dessutom sådana att MSB är ensamt ansvarig för dem och de överlappar inte på något betydande sätt de övriga ansvarsområden som omfattas av verksam-

hetsöverföringen. Det vore därför inte ändamålsenligt att överföra dessa uppgifter till annan myndighet.

3.5 Verksamhet som inte omfattas av utredningens uppdrag

Utredningens bedömning: Utredningens förslag eliminerar förekomsten av överlappande uppgifter som finns mellan NCSC och MSB. Det finns dock situationer när informations- och cybersäkerhetsperspektiv hanteras som en integrerad del i MSB:s allmänna uppdrag inom forskning och utbildning. Detta förhållande är viktigt att uppmärksamma i det fortsatta arbetet med verksamhetsöverföringen för att det inte ska uppstå otydliga gränsdragningar mellan myndigheternas uppdrag.

MSB:s verksamhet på informations- och cybersäkerhetsområdet är inte begränsad till de uppgifter som är särskilt angivna i författningar. Myndigheten bedriver även verksamhet med sådana inslag utifrån andra bemyndiganden i sin myndighetsinstruktion och genom regeringsbeslut. Denna verksamhet utförs också på andra avdelningar inom MSB än avdelningen för cybersäkerhet och samhällsviktiga kommunikationer. Bland annat har MSB ett forskningsuppdrag enligt 12 § i sin myndighetsinstruktion som innebär att myndigheten ska beställa, kvalitetssäkra och förmedla forskning och utvecklingsarbete för skydd mot olyckor, krisberedskap och civilt försvar. Med stöd av detta bemyndigande förmedlar MSB forskningsmedel för att utveckla Sveriges krisberedskap, där informations- och cybersäkerhet kan vara en integrerad del i större projekt. Detsamma gäller när myndigheten arrangerar övningar med stöd av 5 § i instruktionen. Någon fullständig bild av denna verksamhet, som i nuläget utgör en del av MSB:s större uppdrag inom krisberedskap och civilt försvar, kan inte ges inom ramen för utredningen. Utredningens uppfattning är vidare att MSB:s forsknings- och utbildningsuppdrag torde falla utanför utredningens uppdrag.

Utredningens förslag syftar till att kraftsamla på informations- och cybersäkerhetsområdet med NCSC som ett nationellt nav. Det är centralt att FRA inom ramen för NCSC ska ha möjlighet att utforma verksamheten på det vis som myndigheten anser bäst tillgodo-

ser samhällets behov. Det är dock av vikt att en samsyn uppnås mellan MSB och FRA om exempelvis hur det eventuella behovet av samkoordinerade forskningsprojekt och utbildningsinsatser ska tillgodoses framöver. Annars finns det en risk att otydlighet uppstår kring respektive myndighets ansvar på dessa områden, med ett ineffektivt utnyttjande av statens resurser som en konsekvens.

MSB föreslås i SOU 2024:64 att utses till gemensam kontaktpunkt enligt artikel 9.2 i CER-direktivet. CER-direktivet innehåller inget utpekad uppdrag som CSIRT-enhet, men enligt förslaget ska MSB ta emot incidentrapporteringen. En fråga som lyfts till utredningen är om det skulle vara ändamålsenligt att samla incidentrapporteringen enligt både NIS 2-direktivet och CER-direktivet hos FRA. Incidentrapporter enligt CER-direktivet innefattar störningar som inte rör cybersäkerhet. I MSB:s uppdrag ingår vidare enligt 7 § MSB:s instruktion att samordna samhällets gemensamma krishanteringsarbete. Utredningen ifrågasätter därför lämpligheten i att föra över uppdraget att ta emot incidentrapporter enligt CER-direktivet till FRA när CERT-SE förs över till myndigheten. Implementeringen av CER-direktivet ligger också utanför ramen för denna utredning. Utredningen återkommer dock kort till frågan om förslagens konsekvenser för genomförandet av NIS 2-direktivet och CER-direktivet i kapitel 5.

4 Informationshantering

4.1 Uppdraget

Utredningen har i uppdrag att analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling. Av direktiven framgår att det behövs en analys av om den informationshantering som krävs med anledning av överföringen av arbetsuppgifter till Försvarets radioanstalt (FRA) och det nationella cybersäkerhetscentret (NCSC) medför något behov av ändringar i offentlighets- och sekretesslagstiftningen eller av regelverket som gäller för personuppgiftsbehandling. Utredningen behöver bland annat ta ställning till om det finns förutsättningar för nödvändigt utbyte av information mellan Myndigheten för samhällsskydd och beredskap (MSB) och FRA i samband med och efter överföringen av arbetsuppgifter. Det behövs även en analys av om det finns förutsättningar för att genomföra nödvändigt informationsutbyte mellan FRA och privata aktörer. I uppdraget ingår därmed bland annat att ta ställning till om nu gällande regelverk innebär ett tillräckligt skydd för uppgifter som kommer att utbytas. Utredningens uppdrag innefattar också att vid behov föreslå åtgärder för en fördjupad samverkan inom ramen för NCSC.

Det kan konstateras att NCSC sedan den 1 november 2024 är en del av FRA och därmed inte utgör ett myndighetsgemensamt samverkanscenter som tidigare. Regeringen har också beslutat om förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen). I del 2 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) finns beskrivningar av vissa dataskyddsrättsliga regelverk med koppling till NCSC. Med tanke på att NCSC numera är en del av FRA måste det dataskyddsrättsliga regelverket för FRA beskrivas och analyseras i detta betänkande, vilket också görs nedan.

Utredningen har valt att angripa frågan om informationsdelning på två sätt. För det första handlar det om informationsdelning inom NCSC, och alltså mellan de samverkande myndigheterna. För det andra handlar det om informationsdelning mellan NCSC och andra aktörer, särskilt privata sådana.

Utredningen analyserar även om befintlig reglering erbjuder ett tillräckligt skydd för de uppgifter som kommer att hanteras av FRA inom NCSC.

I avsnitt 4.2 analyserar utredningen behovet av utökade möjligheter att dela information inom NCSC. Utredningen lämnar i samma avsnitt förslag om en ny lag om uppgiftsskyldighet vid samverkan i verksamhet inom NCSC. Behovet av sekretess för uppgifter som förekommer hos NCSC analyseras i avsnitt 4.3 och utredningen föreslår där en ny bestämmelse om sekretess. Avsnitt 4.4 handlar om behovet av ändringar i sekretessbestämmelser som föreslagits i betänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64) till följd av att FRA ska ta över vissa arbetsuppgifter från MSB. Avsnitt 4.5 ägnas åt förutsättningarna för NCSC att behandla personuppgifter i sin verksamhet. Utredningen lämnar där förslag om en ny registerlag för NCSC. Avslutningsvis görs en integritetsanalys avseende integritetsriskerna med utredningens förslag i avsnitt 4.6.

4.2 En ny lag om uppgiftsskyldighet vid samverkan i verksamhet inom NCSC

Utredningens bedömning: Befintliga rättsliga möjligheter att dela information mellan NCSC och samverkansmyndigheterna är inte tillräckliga för att fullt ut tillgodose behovet av att dela information som behövs och är befogad i den verksamhet som bedrivs av NCSC. En sekretessbrytande uppgiftsskyldighet bör införas för utlämnande av information.

Utredningens förslag: En ny lag om uppgiftsskyldighet inom ramen för NCSC:s verksamhet ska införas. Vid samverkan inom ramen för NCSC:s verksamhet 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 ska få ta emot uppgifter enligt lagen.

4.2.1 Det finns behov av större rättsliga förutsättningar att dela information vid samverkan inom NCSC:s verksamhet

För att utreda om det finns ett behov av utökade rättsliga möjligheter att lämna information är det viktigt att konkretisera vilken typ av uppgifter det rör sig om.

Det har sagts till utredningen att informationsdelning vid samverkan inom NCSC:s verksamhet bland annat kan behöva omfatta följande typer av uppgifter.

- Teknisk information. Uppgifter om tekniska detaljer om cyberhot eller incidenter (till exempel IP-adresser).
- Taktisk information. Uppgifter om taktiska detaljer om cyberhot/cyberfenomen (till exempel mål och motiv bakom).
- Strategisk information. Uppgifter om strategiska detaljer om cyberhot (till exempel förslag på åtgärder).
- Operativ information. Uppgifter rörande detaljer om cyberhot (till exempel status för pågående attacker).
- Aktörsinformation. Uppgifter om aktörer (till exempel uppgifter om aktörer och deras modus).
- Säkerhetsinformation. Uppgifter om säkerhetsåtgärder och rekommendationer.
- Kontextuell information. Uppgifter om kontexten kring cyberhot/cyberfenomen (till exempel uppgifter om pågående händelser och trender).

Informationsdelningen kan också behöva ske rörande mer strategiska frågor som exempelvis olika former av EU-arbete, drabbade målgrupper samt organisations- och samhällskonsekvenser. Även informa-

tion om digital infrastruktur kan behöva delas mellan NCSC 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 NCSC ska kunna identifiera vilka aktörer som befinner sig i riskzonen för exempelvis cyberhot.

Enligt 4 § NCSC-förordningen ska FRA organisera, leda och planera verksamheten som bedrivs inom NCSC. FRA ska i den verksamhet som bedrivs inom ramen för NCSC samverka med Försvarets materielverk, Försvarsmakten, MSB, Polismyndigheten, Post- och telestyrelsen samt Säkerhetspolisen. Dessa myndigheter betecknas som samverkansmyndigheter (4 § NCSC-förordningen). Samverkansmyndigheterna ska, inom ramen för sina respektive befintliga ansvarsområden, löpande bistå NCSC med kunskap, kompetens och information. NCSC ska 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 (5 § NCSC-förordningen).

Myndigheter har enligt 8 § förvaltningslagen (2017:900) en skyldighet att inom sina verksamhetsområden samverka med andra myndigheter. I 6 kap. 5 § offentlighets- och sekretesslagen (2009:400), förkortad 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.

Ofta lyfts synpunkten fram att en förutsättning för att myndigheter ska kunna samverka med varandra på ett ändamålsenligt sätt är att det finns ett fungerande informationsutbyte mellan myndigheterna. Det finns många aspekter att beakta när det gäller informationsutbyte. 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 uppgifter som är sekretessreglerade och där tjänstepersoner är, eller upplever sig vara, förhindrade att lämna ut information. En annan aspekt är vad informationsutbytet ska leda fram till, som till exem-

pel effektivare åtgärder mot ett visst samhällsproblem. Informationsutbyte för sakens skull behöver inte i sig vara eftersträvänsvärt.

I del 2 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) har vissa faktorer lyfts fram som utmanande när det kommer till informationsdelning. En faktor som framgått är att personal från de olika myndigheterna inte i tillräckligt stor omfattning har kunskap om regelverket kring sekretess. Det medför att personal inte delar information med de övriga myndigheterna i den utsträckning som egentligen är möjlig enligt gällande lagstiftning. Denna omständighet har också lyfts fram i flera lagstiftningsarbeten (se bland annat betänkandet *Ökat informationsflöde till brottsbekämpningen*, SOU 2023:69). Ofta påpekas att det inte enbart handlar om utökade rättsliga förutsättningar att dela information för att man ska åstadkomma ett utökat uppgiftslämnande. Regelverket för offentlighet och sekretess beskrivs som komplicerat att tillämpa för enskilda tjänstemän.

En annan fråga som måste beaktas är den omständigheten att vissa myndigheter som samverkar inom ramen för NCSC är under rättelsemyndigheter medan andra inte är det. Lagen (2019:547) om förbud mot användning av vissa uppgifter för att utreda brott förbjuder att uppgifter från FRA:s underrättelseverksamhet används för att utreda brott. Även detta kan försvåra informationsutbytet eftersom såväl Polismyndigheten som, i viss utsträckning, Säkerhetspolisen utreder brott.

Den bestämmelse som i huvudsak får relevans för informationsutbytet mellan NCSC och samverkansmyndigheterna är den så kallade generalklausulen i 10 kap. 27 § OSL. Enligt den får en sekretessbelagd uppgift lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Vid utlämnande enligt generalklausulen måste det för var och en av uppgifterna vara uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Det kan innebära svåra intresseavvägningar i enskilda fall. I lagstiftningsarbetet har generalklausulen upprepade gånger pekats ut som svårtillämpad och det har sagts att den ger upphov till svåra avvägningar om vilken typ av information som ska lämnas över. Särskilt uppenbarhetsrekvisitet framstår som svårt att tillämpa (se bland annat betänkandena SOU 2023:69, SOU 2024:63 och SOU 2024:87). Det informationsutbyte som ska förekomma

hos NCSC ska kunna ske rutinmässigt och löpande. I NCSC-förordningen anges uttryckligen att NCSC och samverkansmyndigheterna löpande ska bistå varandra med kunskap och information. Generalklausulen kan visserligen användas för rutinmässigt informationsutbyte, men bestämmelsen bygger på att sådant informationsutbyte i regel ska vara författningsreglerat (prop. 1979/80:2 Del A s. 327). I många lagstiftningsärenden avseende rutinmässigt informationsutbyte har bestämmelsen också ersatts med mer specifik lagstiftning. Ett exempel på detta är 35 kap. 10 c § OSL.

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 så framstår inte generalklausulen som en lämplig reglering för informationsutbytet mellan NCSC och samverkansmyndigheterna.

I sammanhanget kan nämnas att den möjlighet som finns att lämna ut annars sekretessbelagda uppgifter med förbehåll (10 kap. 14 § OSL) endast omfattar utlämnande till enskilda. Utlämnande med förbehåll är alltså inte aktuellt när det gäller informationsdelning mellan myndigheter inom ramen för NCSC:s verksamhet.

De uppgifter som behöver kunna delas inom ramen för NCSC:s verksamhet kan omfattas av sekretess, antingen till skydd för enskilda eller allmänna intressen. Som exempel kan nämnas att uppgifter om olika typer av tekniska funktioner och som lämnas in i samband med incidentrapporter kan omfattas av sekretess avseende säkerhets- eller bevakningsåtgärd enligt 18 kap. 8 § OSL. NCSC kan också behöva hantera uppgifter som omfattas av sekretess till skydd för risk- och sårbarhetsanalyser (18 kap. 13 § OSL). En annan typ av uppgifter som kan omfattas av sekretess och därmed kan vara svår att dela är sådana som omfattas av underrättelsesekretess (18 kap. 2 § OSL). Det kan inte uteslutas att samma uppgifter i ett enskilt fall kan vara sekretessbelagda enligt fler än en sekretessbestämmelse. Det finns ett stort samhällsintresse av att NCSC kan bedriva sin verksamhet under effektiva former. En tydlig reglering av informationsutbytet mellan NCSC och samverkansmyndigheterna kan bidra till detta. Utredningen bedömer inte att det är tillräckligt med

utbildningsinsatser för att komma till rätta med svårigheterna att dela information.

Regeringen har nyligen beslutat om en nationell strategi för cybersäkerhet (*Nationell strategi för cybersäkerhet 2025–2029*, skr. 2024/25:121). Av denna framgår, gällande önskat läge 2030, att det ska finnas väletablerade metoder för internationellt och privat-offentligt samarbete. Även plattformar för att dela säkerhetsrelaterad information ska etableras, både inom och mellan offentlig och privat sektor, som möjliggör ökad delning och analys av realtidsinformation på teknisk och operativ nivå. Vidare framgår en önskan om att arbetet bidrar till utvecklade och ändamålsenliga lägesbilder från NCSC till gagn för olika målgrupper samt vidareutvecklad samverkan mellan relevanta myndigheter om attribueringsfrågor. Informationsdelning ska ske, utifrån lagstiftning och etablerade processer, till gagn för alla inblandade parter och stärker bland annat förmågan att identifiera, hantera och utreda incidenter och angrepp. Utifrån att NCSC ska utgöra navet i det nationella cybersäkerhetsarbetet anser utredningen att en förenklad reglering av uppgiftsutbytet mellan NCSC och samverkansmyndigheterna kan bidra till att det målet uppnås.

Ny rättslig reglering av informationsutbyte innebär svåra avvägningar mellan det allmänna intresset av att bedriva ett effektivt och ändamålsenligt cybersäkerhetsarbete, upprätthålla förtroendet för myndigheter, skyddet för den personliga integriteten och andra rättssäkerhetsaspekter. Rättslig reglering bör därför utformas så att informationsutbytet är effektivt samtidigt som rättssäkerheten upprätthålls och intrånget i den personliga integriteten inte blir oproportionerligt.

4.2.2 Den utökade möjligheten att dela information ska formuleras som en ny lag om uppgiftsskyldighet

Utredningen har övervägt om den utökade möjligheten att dela information ska formuleras som en sekretessbrytande bestämmelse som innebär att en uppgift *får* lämnas ut eller en uppgiftsskyldighet, som innebär att sekretess bryts enligt 10 kap. 28 § OSL och att en uppgift *ska* lämnas ut. Utredningens ståndpunkt är att behovet bäst tillgodoses genom en uppgiftsskyldighet som skapar en utgångspunkt för att information ska delas. Utredningen anser också att uppgiftsskyldigheten ska regleras i särskild ordning och inte i OSL.

Vid avvägningen mellan en sekretessbrytande bestämmelse och en uppgiftsskyldighet finns det ett antal aspekter som har betydelse. En sekretessbrytande bestämmelse i OSL har fördelen att den innebär en mer sammanhållen reglering av de sekretessbestämmelser som en myndighet har att förhålla sig till. Eftersom det är fråga om myndigheter som är fristående från varandra måste de också kunna beakta sina egna intressen. En omständighet som är högst relevant i sammanhanget är att FRA, Försvarsmakten, Säkerhetspolisen och Polismyndigheten är underrättelsemyndigheter, vars underrättelseverksamhet till stor del bygger på att aktörer har förtroende för att information inte sprids vidare. Dessa omständigheter talar för att formulera lagstiftningen som en sekretessbrytande bestämmelse.

En sekretessbrytande bestämmelse med generell tillämpning inom ramen för NCSC:s verksamhet hade kunnat utformas enligt följande. *Secretess hindrar inte att en uppgift lämnas till en annan myndighet, om det behövs för samverkan inom ramen för verksamhet inom det nationella cybersäkerhetscentret vid Försvarets radioanstalt.* Bestämmelsen hade även behövt innehålla en intresseavvägning.

Det finns dock stora fördelar med att formulera förutsättningarna för informationsdelning som en uppgiftsskyldighet i egen lagstiftning som kan tillämpas av FRA och samverkansmyndigheterna inom ramen för NCSC:s verksamhet. Ofta lyfts synpunkten fram att en uppgiftsskyldighet framstår som enklare att tillämpa för de enskilda tjänstemän som ska pröva om en uppgift ska lämnas över eller inte. Om målsättningen är att fler uppgifter ska kunna delas än vad som är fallet i dag så kan en uppgiftsskyldighet få en mer handlingsdirigerande effekt än en sekretessbrytande bestämmelse.

Eftersom en sekretessbrytande uppgiftsskyldighet kan formuleras med en så kallad ventil, ska inte heller skillnaden i förhållande till sekretessbrytande bestämmelser överdrivas.

Den ovan skissade sekretessbrytande bestämmelsen träffar inte heller uppgifter som inte är sekretessbelagda, vilket kan innebära att den inte fullt ut tillgodoser behovet av att kunna utbyta information inom ramen för NCSC:s verksamhet. Utredningen har i avsnitt 4.2.1 identifierat flera andra aspekter utöver sekretesslagstiftningen som kan utgöra hinder mot informationsdelning mellan myndigheter. En uppgiftsskyldighet som även omfattar uppgifter som inte är sekretessbelagda kan därför förväntas leda till en mer utvecklad samverkan än den alternativa sekretessbrytande bestäm-

melsen. Utifrån dessa överväganden anser utredningen att behovet av informationsdelning inom ramen för NCSC:s verksamhet bäst tillgodoses genom en uppgiftsskyldighet i en egen lag. Utredningen återkommer i viss utsträckning till skillnaden mellan sekretessbelagda uppgifter och uppgifter som inte omfattas av sekretess i avsnitt 4.2.4.

En fråga som utredningen identifierat är huruvida det framstår som lämpligt att knyta en lag om uppgiftsskyldighet till en verksamhet (NCSC) som regleras i förordning i stället för i lag. I sammanhanget kan nämnas lagen (2016:774) om uppgiftsskyldighet vid samverkan mot grov organiserad brottslighet (LUS). Enligt den lagen kan en sekretessbrytande uppgiftsskyldighet utlösas av särskilda beslut hos myndigheter om samverkan. NCSC:s verksamhet är författningsstyrd och det framgår av förordning vilka myndigheter som ingår i centret och vilka uppgifter det ska utföra. Så länge det framgår av förordning vilka myndigheter som ingår i NCSC så uppstår inte heller oklarheter rörande tillsyn av hur uppgiftsskyldigheten tillämpas. Utredningens uppfattning är att den omständigheten att NCSC är reglerat på förordningsnivå inte hindrar att en lag om uppgiftsskyldighet kan knytas till centret.

När det gäller utformningen av lagtexten kan det hävdas att det typiskt sett inte är en god ordning att en författning för sin tillämpning är beroende av en annan författning, som dessutom ligger på lägre nivå i normhierarkin. Det framstår därför inte som lämpligt att lagtexten hänvisar till NCSC-förordningen. Utredningen har i stället övervägt att i lagtexten uttryckligen ange den samverkansskyldighet som framgår av NCSC-förordningen. Samverkansskyldigheten är brett formulerad. Samverkansmyndigheterna ska, inom ramen för sina befintliga ansvarsområden, löpande bistå NCSC med kunskap, kompetens och information. NCSC ska löpande bistå samverkansmyndigheterna med kunskap och information (5 § första stycket NCSC-förordningen). En mer specifik samverkansskyldighet gäller vid ett antagonistiskt cyberhot eller annan it-incident som har vållat eller som kan antas ha potential att vålla betydande skada (se 5 § andra stycket NCSC-förordningen). Mot bakgrund av risken för att lagtexten blir alltför otymplig och svåräst förordar utredningen dock inte en sådan lösning. Det är i stället utredningens uppfattning att en tillräckligt hög grad av precision och förutsebarhet kan uppnås genom att lagens tillämpning knyts till att det är fråga om samverkan i verksamhet inom NCSC.

Utredningen har övervägt om uppgiftsskyldigheten kan regleras genom en bestämmelse i NCSC-förordningen. Bestämmelsen i 2 kap. 2 § andra stycket tryckfrihetsförordningen, som avser begränsningar i enskildas rätt att ta del av allmänna handlingar, uppställer inget hinder mot att informationsutbytet mellan myndigheter regleras utanför OSL (prop. 1979/80:2 Del A s. 121). Eftersom uppgiftsskyldigheten ska gälla mellan myndigheter kan frågan anses falla under regeringens så kallade restkompetens enligt 8 kap. 7 § regeringsformen (RF). Något formellt hinder mot att frågan regleras i lag finns dock inte. Av 8 kap. 8 § RF framgår att den omständigheten att regeringen får meddela föreskrifter i ett visst ämne inte hindrar att riksdagen meddelar föreskrifter i samma ämne. Utredningen bedömer att det av tydlighetsskäl och mot bakgrund av rättssäkerhetsaspekter finns skäl att i detta fall reglera uppgiftsskyldigheten i lag.

4.2.3 Den nya lagen ska utgöra en balans mellan effektivitet och integritet

Vid övervägande om en ny uppgiftsskyldighet ska införas ska det beaktas vilka intressen som sekretessen avser att skydda. De sekretessbestämmelser som i huvudsak tillämpas av de myndigheter som samverkar inom ramen för NCSC:s verksamhet beskrivs närmare i del 2 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785). I huvudsak är det fråga om sekretess till skydd för allmänna intressen (exempelvis 15 kap. 1–2 §§ OSL). Det handlar i mindre omfattning om sekretess till skydd för enskilda intressen.

Sekretess mellan myndigheter syftar i första hand till att värna om enskildas integritet. En utgångspunkt är därför att information som omfattas av sekretess inte ska vidarebefordras utanför den verksamhet i vilken den hämtats in.

Det finns dock en förväntan på NCSC om att centret ska kunna utföra sitt uppdrag och bedriva ett så effektivt arbete som möjligt, samt vara en nationell plattform för samverkan och informationsutbyte rörande cybersäkerhet. Uppdelningen av arbetsuppgifter och ansvarsområden mellan NCSC och de olika samverkansmyndigheterna riskerar att begränsa möjligheten till samverkan inom ramen för den verksamhet som bedrivs i NCSC.

Utredningen har tidigare redovisat de invändningar som kan göras mot att stödja ett mer återkommande informationsutbyte på generalklausulen i 10 kap. 27 § OSL. Till detta kommer att uppenbarhetsrekvisitet i bestämmelsen inte i tillräckligt hög grad tillgodoser det behov av informationsutbyte som finns. Den nya lagstiftningen bör därmed innebära en lättnad för NCSC och samverkansmyndigheterna när det gäller att göra en avvägning kring om uppgifter ska lämnas ut eller inte, jämfört med vad som gäller enligt generalklausulen i 10 kap. 27 § OSL. Den bör också utformas så att den bättre motsvarar behovet för NCSC och samverkansmyndigheterna att dela information som annars skulle ha omfattats av sekretess.

Det kan noteras att tanken med uppgiftsskyldigheten inte är att myndigheterna ska samla in fler uppgifter om enskilda. De uppgifter som ska kunna delas är också sådana uppgifter som redan finns hos någon myndighet.

För att tillgodose behovet av integritet bör uppgiftsskyldigheten avgränsas på ett tydligt sätt. Med en koppling till de krav på samverkan mellan NCSC och samverkansmyndigheterna som ställs upp i NCSC-förordningen så begränsas kretsen av personer som kan få del av uppgifter. Det kommer att röra sig om de personer som deltar i NCSC:s verksamhet, oftast i form av anställda eller uppdrags-tagare.

Syftet med uppgiftsskyldigheten är inte att möjliggöra ett fritt uppgiftsutbyte utan att åstadkomma en sekretesslättnad i förhållande till vad som gäller enligt framför allt generalklausulen i 10 kap. 27 § OSL. Den utlämnande myndigheten bör därför även med tillämpning av den nya uppgiftsskyldigheten göra en intresseavvägning innan en uppgift lämnas ut.

Utöver dessa begränsningar bör regleringen av uppgiftsskyldigheten endast gälla vissa särskilt utpekade myndigheter.

De begränsningar som nämns, och som utvecklas nedan, innebär att den föreslagna regleringen utgör en balans mellan effektivitet och integritet.

4.2.4 Utformningen av uppgiftsskyldigheten

Uppgiftsskyldigheten ska utformas på samma sätt för alla myndigheter som samverkar inom ramen för NCSC:s verksamhet

Uppgiftsskyldigheten bör gälla oavsett vilken av de aktuella myndigheterna som förfogar över uppgiften. Uppgiftsskyldigheten bör också gälla oavsett vilken typ av sekretess som gäller för uppgiften. Eftersom syftet med lagen är att underlätta informationsdelningen vid samverkan inom ramen för NCSC:s verksamhet och skapa förutsättningar för NCSC att bedriva en effektiv verksamhet, behöver samtliga myndigheter ha en enhetlig lagstiftning att tillämpa. Ett gemensamt och enhetligt regelverk kan förväntas skapa tydligare praxis kring vilka uppgifter som kan och ska delas vid samverkan inom ramen för NCSC:s verksamhet. Även tillsynen över tillämpningen förenklas betydligt med ett enhetligt regelverk.

Det ska finnas ett behov av uppgiften inom ramen för NCSC:s verksamhet

Det är FRA som ska organisera, leda och planera verksamheten som bedrivs inom ramen för NCSC. Samverkansmyndigheterna kommer också ha viktiga arbetsuppgifter och roller i centrets verksamhet att utveckla och stärka arbetet med informations- och cybersäkerhet. Med anledning av den balans mellan effektivitet och integritet som ska finnas så bör uppgiftsskyldigheten endast vara tillämplig när behovet av ett effektivt informationsutbyte är starkt och därmed särskilt motiverat.

För att en myndighet ska kunna delta i verksamheten på olika sätt, exempelvis närvara vid möten, bidra med information eller vidta åtgärder inom den egna myndighetens verksamhetsområde som är relevanta för den samverkan som ska ske inom ramen för NCSC:s verksamhet, krävs ibland att myndigheten får del av exempelvis sekretessbelagd information från en annan myndighet. 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 verksamheten vid NCSC. Detta för att en rimlig avvägning mellan å ena sidan intresset av sekretess och personlig integ-

ritet och å andra sidan intresset av att NCSC ska kunna bedriva ett så effektivt och kunskapsbaserat arbete som möjligt.

Utredningen har övervägt om det ska gälla ett strängare krav på behovet hos mottagaren, som att uppgiften ska vara *nödvändig* för mottagarens deltagande i samverkan. Ett sådant rekvisit riskerar dock att skapa en omotiverat restriktiv tillämpning. En annan styrka på behovsrekvisitet som övervägts är att uppgiften *kan antas* behövas. Det hade inneburit en större flexibilitet i tillämpningen. Många sekretessbrytande bestämmelser är formulerade på så sätt att uppgifter kan lämnas ut om det kan antas att uppgifterna behövs eller är av betydelse för mottagaren (till exempel 10 kap. 18 a-c §§, 26 kap. 14 d §, 32 kap. 6 a § och 35 kap. 10 c § OSL). Men när det gäller uppgiftsskyldigheter är det vanligt att det i stället anges att skyldigheten gäller för uppgifter som behövs. Som exempel på sådan lagstiftning kan nämnas 2 § LUS, 4 a kap. 3 § lagen (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism och 2 § lagen (2024:307) om uppgiftsskyldighet för att motverka felaktiga utbetalningar från välfärdssystemen samt fusk, regelöverträdelser och brottslighet i arbetslivet. Uppgiftsskyldigheten bör vara tydligt avgränsad och det bör inte råda någon osäkerhet kring när en uppgift omfattas av skyldigheten. I stället bör myndigheterna kunna förväntas bedöma vilka uppgifter som behövs inom ramen för den samverkan som ska ske i NCSC, och göra en rimlig avvägning i fråga om vilka uppgifter som ska lämnas över. Uppgiftsskyldigheten bör därför gälla om uppgiften *behövs* för den mottagande myndighetens deltagande i samverkan.

Nästa fråga som utredningen behöver ta ställning till är hur uppgiftsskyldigheten ska avgränsas. Utredningen bedömer att det är tillräckligt att uppgiftsskyldigheten avgränsas genom att den gäller när samverkan sker mellan myndigheter i verksamhet inom NCSC. Samverkansskyldighetens närmare utformning går att utläsa i 4–5 §§ NCSC-förordningen. Så länge som samverkansskyldigheten framgår av författning så är tillämpningsområdet tillräckligt tydligt avgränsat.

Utredningen har övervägt om uppgiftsskyldigheten behöver avgränsas ytterligare, på så sätt att den uttryckligen knyts till vissa av NCSC:s arbetsuppgifter, så som de anges i NCSC-förordningen. Till exempel hade uppgiftsskyldigheten kunnat avgränsas till att gälla vid samverkan enligt 5 § NCSC-förordningen. Första stycket

innehåller en generell skyldighet att dela information på så sätt att NCSC och samverkansmyndigheterna ska löpande bistå varandra med kunskap och information. Skyldigheten är dock inte knuten till någon närmare angiven arbetsuppgift. Mer specifik är då skyldigheten att utbyta information enligt bestämmelsens andra stycke. Där framgår att 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* (utredningens kursivering).

Uppgiftsskyldigheten hade också kunnat knytas till centrets uppgift enligt 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt (FRA:s instruktion). Även den varianten riskerar att leda till osäkerhet i tillämpningen eftersom det kan framstå som oklart om uppgiftsskyldigheten gäller när NCSC utför de nya uppgifter som utredningen i kap. 3 föreslagit att FRA ska utföra enligt de nya bestämmelserna i FRA:s instruktion. Dessa uppgifter torde visserligen kunna inordnas under NCSC:s övergripande uppdrag så som det framgår av 4 a § FRA:s instruktion, varför det hade kunnat vara ett alternativ att uttryckligen ange det uppdrag som framgår av den bestämmelsen.

En alltför snäv avgränsning riskerar dock att leda till tillämpningssvårigheter om centret rör sig mellan olika arbetsuppgifter. Som exempel på en uppgift som riskerar att leda till tillämpningssvårigheter är NCSC:s uppgift enligt 3 § 1 och 3 NCSC-förordningen att bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet samt att lämna råd och stöd till privata och offentliga aktörer vid it-incidenter. Inom ramen för den verksamhet som NCSC ska utföra bör informationsutbytet kunna ske tämligen enkelt. Ett alltför högt ställt krav på när information ska utbytas riskerar helt enkelt att innebära att lagstiftningen inte får önskad effekt. Det är alltså mest ändamålsenligt att knyta uppgiftsskyldigheten till samtliga krav på samverkan enligt NCSC-förordningen.

Eftersom uppgiftsskyldigheten bryter all typ av sekretess behöver något sägas om sekretess som omfattar särskilt integritetskänsliga uppgifter, exempelvis uppgifter som omfattas av socialtjänstsekretess (26 kap. OSL) eller hälso- och sjukvårdssekretess (25 kap. OSL).

Även om uppgiftsskyldigheten är tillämplig på uppgifter som omfattas av den typen av sekretess torde det ytterst sällan finnas ett behov av att dela sådana uppgifter inom ramen för NCSC:s verksamhet. Utredningen har inte identifierat någon sådan situation. Om inte behovsrekvisitet är uppfyllt kan inte heller den annars sekretessbelagda uppgiften lämnas ut med stöd av uppgiftsskyldigheten.

Uppgifter bör kunna lämnas ut med stöd av uppgiftsskyldigheten dels efter begäran, dels på eget initiativ. Avsikten är inte att en myndighet ska leta efter omständigheter som ger upphov till ett behov hos mottagaren. Uppgiftsskyldigheten inträder först när det kan konstateras att det finns ett visst behov och att övriga förutsättningar för utlämnande av uppgifter är uppfyllda. Om det uppstår tveksamheter kring vilka uppgifter som behövs hos mottagaren får det förutsättas att NCSC och samverkansmyndigheterna i samråd med varandra verkar för att endast relevanta uppgifter lämnas över. Detta är också viktigt eftersom myndigheterna måste förhålla sig till principen om uppgiftsminimering i 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 (EU:s dataskyddsförordning). Enligt denna princip krävs att uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

En intresseavvägning ska göras

Utredningen bedömer att en intresseavvägning ska göras innan en uppgift lämnas ut. Eftersom det är fråga om en uppgiftsskyldighet finns det en presumtion för att en uppgift ska lämnas ut, om förutsättningarna är uppfyllda. Det finns starka skäl för att NCSC ska kunna bedriva sin verksamhet på ett effektivt sätt. Ett välfungerande informationsutbyte är en förutsättning för detta. Samtidigt kan uppgifter som är sekretessreglerade vara känsliga och av olika anledningar särskilt skyddsvärda. Därför bör uppgiftsskyldigheten utformas så att det finns en möjlighet att i varje enskilt fall beakta intressen som talar för att uppgiften inte ska lämnas ut. Intresseavvägningen ska 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 möjligheter att hemlighålla såväl skyddsvärda uppgifter om enskilda som skyddsvärda uppgifter om en myndighets verksamhet.

Ett annat alternativ hade varit att utforma intresseavvägningen som att det krävs övervägande skäl som talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Det kan dock diskuteras hur en sådan intresseavvägning förhåller sig till sekretessbrytande bestämmelser i OSL. Enligt detta alternativ synes det vara en förutsättning för intresseavvägningen att uppgiften *omfattas av sekretess*. Det innebär i så fall att i de fallen OSL innehåller en tillämplig sekretessbrytande bestämmelse blir den för uppgiftsskyldigheten föreskrivna intresseavvägningen inte aktuell. I de situationerna omfattas ju uppgiften inte av sekretess, och någon intresseavvägning ska då inte ske. Om intresseavvägningen görs beroende av att det finns en sekretessbestämmelse som är tillämplig på uppgiften framstår det snarare som att det intresse som den aktuella sekretessbestämmelsen ska skydda ska tjäna som utgångspunkt för intresseavvägningen, oavsett om det finns en tillämplig sekretessbrytande bestämmelse i OSL. Intresseavvägningen som ska göras enligt uppgiftsskyldigheten blir då fristående från en prövning av eventuella sekretessbrytande bestämmelser i OSL.

Både för- och nackdelar kan identifieras med de olika alternativen. Om det är en förutsättning att uppgiften omfattas av sekretess kommer tillämparen fullt ut att kunna beakta alla de möjligheter som de respektive lagarna erbjuder vid utlämnande. Det framstår också som rimligt att en intresseavvägning inte ska vara nödvändig i de fall där lagstiftaren i tidigare lagstiftningsärenden har bedömt att det ska vara möjligt att bryta sekretessen. Lösningen riskerar dock att göra tillämpningen än mer komplicerad. Om intresseavvägningen förutsätter att man redan konstaterat att det i det enskilda fallet gäller sekretess riskerar regleringen 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. I praktiken innebär en sådan lösning att den enskilda tjänstemannen först ska pröva om skaderekvisitet i den tillämpliga bestämmelsen är uppfyllt gentemot den myndighet som ska ta emot uppgiften. Därefter måste man ta ställning till om det finns några särskilda sekretessbrytande bestäm-

melser som är tillämpliga i det aktuella kapitlet i OSL. Sedan kan de allmänna sekretessbrytande bestämmelserna i 10 kap. OSL behöva beaktas. Det innebär att innan man ens kan påbörja intresseavvägningen enligt uppgiftsskyldigheten så kommer i många fall en prövning enligt generalklausulen behöva göras.

Enligt utredningens mening är risken stor att lagstiftningen blir kontraproduktiv i förhållande till syftet att underlätta informationsutbytet mellan myndigheterna. Att välja det andra alternativet – *det finns en sekretessbestämmelse som är tillämplig på uppgiften* – bör innebära att det uppfattas som att utgångspunkten för intresseavvägningen är det sekretessintresse som bestämmelsen avser att skydda. En sådan intresseavvägning blir fristående från tillämpningen av OSL.

Det bör dock beaktas att en nackdel med regleringen är att det krävs en intresseavvägning även i de fall då sekretess inte föreligger. Det innebär i sin tur att prövningen kan – när det är fråga om utlämnande på eget initiativ – resultera i att en skyldighet att lämna ut uppgifter inte föreligger trots att uppgiften i det enskilda fallet inte omfattas av sekretess. Den föreslagna regleringen av uppgiftsskyldigheten hindrar dock inte att uppgiften då lämnas ut enligt 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 den myndighet som förfogar över den aktuella uppgiften som ska pröva om det finns förutsättningar för att lämna över uppgiften till en annan myndighet. Kravet på övervägande skäl innebär att behovet av informationsutbyte inom ramen för NCSC:s verksamhet normalt sett har företräde framför andra intressen; det råder således en presumtion för att uppgiften ska lämnas ut.

Det krävs inte att det alltid görs en prövning i varje enskilt fall utan en bedömning kan göras utifrån de behov av sekretess som typiskt sett finns för en viss kategori av uppgifter (jfr prop. 1979/80:2 Del A s. 80–81 och s. 326–327).

Uppgiftsskyldigheten hindrar inte heller ett rutinmässigt utlämnande av en större mängd uppgifter, men det är viktigt att NCSC tar fram lämpliga former för att se till att endast relevanta uppgifter utbyts. Vid rutinmässigt utlämnande av uppgifter kan den bedömning som ska göras enligt uppgiftsskyldigheten göras på förhand och den behöver inte avse en prövning i varje enskilt fall.

Som exempel på uppgifter som ofta skyddas av sekretess och som det kan finnas starka skäl att inte lämna ut kan nämnas 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 uppgifter om myndighetens egna säkerhets- och bevakningsåtgärder. Det är viktigt att myndigheterna kan utbyta relevant information och samverka inom ramen för NCSC:s verksamhet. Men informationsutbytet får inte inskränka en myndighets möjlighet att utföra sitt primära uppdrag eller i övrigt försvåra myndighetens arbete och verksamhet. 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. Uppgifter av särskilt integritetskänslig art kan utgöra sådana uppgifter. Det kan röra sig om känsliga personuppgifter om hälsa eller politisk övertygelse. 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 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.

En omständighet som 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.

Vid intresseavvägningen ska också sekretesskyddet hos den mottagande myndigheten vägas in i bedömningen. Om uppgiften får ett svagare sekretesskydd hos mottagande myndighet kan intresseavvägningen utmynna i att en uppgift inte lämnas ut. Det kan dock diskuteras hur stor betydelse ett svagare sekretesskydd har. Det har uttalats att det i praktiken spelar mycket liten roll att sekretessen hos den mottagande myndigheten ibland är något svagare (prop. 1979/80:2 Del A s. 76–77). Även med ett rakt skaderekvisit gäller sekretess

för uppgifter som till sin art typiskt sett är känsliga (prop. 2009/10:165 s. 616).

4.2.5 Lagen omfattar endast myndigheter som regeringen bestämmer

Behovet av tydlighet och förutsägbarhet för exempelvis enskilda vars personuppgifter kan komma att utbytas vid myndighetssamverkan inom ramen för NCSC:s verksamhet innebär att det måste stå klart mellan vilka myndigheter uppgiftsskyldigheten ska gälla. Ett alternativ hade varit att uttryckligen ange samverkansmyndigheterna i lagen. Kretsen av samverkansmyndigheter framgår av NCSC-förordningen men kretsen behöver inte nödvändigtvis vara statisk. I del 1 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) lämnades förslag om att exempelvis Myndigheten för psykologiskt försvar ska delta i NCSC.

Det är dock viktigt att lagens tillämpningsområde enbart gäller inom ramen för NCSC:s verksamhet. Det framstår inte som en tillfredsställande lösning att ange samverkansmyndigheterna i lagen, eftersom det kan uppkomma behov av att utöka eller begränsa antalet myndigheter som NCSC ska samverka med. Lagen ska därför hänvisa till att regeringen bestämmer vilka myndigheter som ska dela uppgifter eller får ta emot uppgifter. I praktiken är det dock i NCSC-förordningen som det kommer att framgå vilka myndigheter som omfattas av den föreslagna lagen om uppgiftsskyldighet.

Den flexibilitet som en uppräknings i förordning innebär är viktig för att snabbt och effektivt kunna möta upp samhällsbehov som kan uppstå.

4.2.6 Det behövs inget ytterligare sekretesskydd för överlämnade uppgifter

Utredningens bedömning: Det behöver inte införas några nya sekretessbestämmelser till skydd för de uppgifter som lämnas mellan myndigheterna inom ramen för NCSC:s verksamhet. Befintlig lagstiftning, i kombination med utredningens förslag i avsnitt 4.3 om en ny bestämmelse i OSL innebär ett tillräckligt skydd för uppgifterna.

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.

Hos de olika myndigheter som deltar i NCSC:s verksamhet kan ett antal olika sekretessbestämmelser aktualiseras. Dels är det fråga om sekretessbestämmelser till skydd för enskilda intressen, som exempelvis 30 kap. 23 § (inklusive offentlighets- och sekretessförordningen [2009:641], förkortad OSF och bilagan till den), 35 kap. 1 § och 38 kap. 4 § OSL. Dels är det fråga om sekretessbestämmelser som skyddar allmänna intressen, som exempelvis 15 kap. 1 och 2 §§, 17 kap. 1 och 2 §§ samt 18 kap. 1, 2, 8 och 13 §§ OSL.

En bestämmelse som ofta kan aktualiseras är underrättelsesekretessen i 18 kap. 2 § OSL. Bestämmelsen 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, oavsett om de lämnats till en annan brottsbekämpande myndighet eller till en icke brottsbekämpande myndighet. Även uppgifter som lämnas från en icke brottsbekämpande myndighet till en brottsbekämpande myndighet kan hos den senare myndigheten skyddas av underrättelsesekretess.

Inom ramen för NCSC:s verksamhet samverkar såväl myndigheter med brottsbekämpande uppdrag som myndigheter utan ett sådant uppdrag. Icke brottsbekämpande myndigheter kan inom ramen för NCSC:s verksamhet få del av uppgifter som rör de brottsbekämpande myndigheternas arbete med att förebygga, förhindra eller upptäcka brottslig verksamhet. Dessa uppgifter kan omfattas av underrättelsesekretess. Även om det inte lämnas över handlingar till de icke brottsbekämpande myndigheterna som blir allmänna handlingar i deras verksamhet, uppstår en tystnadsplikt för den personal från de icke brottsbekämpande myndigheterna som får del

av informationen. Bestämmelser om sekretess innebär nämligen enligt 1 kap. 1 § OSL både ett förbud att lämna ut handlingar med sekretesskyddad information och tystnadsplikt för myndigheten och medarbetare.

Även om underrättelsesekretessen gäller till skydd för allmänna intressen, och inte direkt syftar till att skydda enskilda intressen, så kan bestämmelsen ändå ha till effekt att uppgifter om enskilda indirekt skyddas, så länge uppgifterna hänför sig till underrättelseverksamhet.

När det gäller enskilda intressen så bedömer utredningen vidare att den sekretessbestämmelse som föreslås i avsnitt 4.3 erbjuder ett ytterligare förstärkt skydd för uppgifter hos NCSC. Något behov av ytterligare skydd för uppgifterna har inte framkommit.

Det bör i sammanhanget noteras att frågan om sekretesskydd för uppgifter som lämnats inom ramen för olika typer av samverkan även är aktuell utifrån befintlig samverkan och det regelverk som tillämpas i dagsläget, som exempelvis generalklausulen i 10 kap. 27 § OSL.

4.2.7 Förhållandet mellan den nya lagen och annan lagstiftning

Utredningens bedömning: Den föreslagna lagen påverkar inte tillämpningen av andra bestämmelser.

Den föreslagna lagen om uppgiftsskyldighet mellan myndigheter inom ramen för NCSC:s verksamhet syftar till att underlätta det informationsutbyte som behövs för att uppfylla centrets uppdrag. Den påverkar inte tillämpningen av andra bestämmelser, till exempel uppgifter som en myndighet har fått i det internationella samarbetet. Enligt 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. Enligt bestämmelsens tredje stycke får exempelvis den sekretessbrytande bestämmelsen i 10 kap. 28 § OSL inte tillämpas i strid med det aktuella avtalet. Eftersom den reglering utredningen föreslår utgör en sådan uppgiftsskyldighet som

bryter sekretess enligt 10 kap. 28 § OSL så kan inte uppgifter som omfattas av 15 kap. 1 a § OSL lämnas vidare inom NCSC med stöd av den föreslagna lagen. Liknande bestämmelser om internationella avtal finns även i 27 kap. 5 §, 30 kap. 24 § och 34 kap. 4 § OSL.

I prop. 2024/25:180, *Ökat informationsutbyte mellan myndigheter – en ny sekretessbrytande bestämmelse*, som överlämnades till riksdagen den 28 maj 2025, föreslås en ny generell sekretessbrytande bestämmelse mellan myndigheter. Bestämmelsen föreslås bryta sekretessen enligt 21–40 kap. OSL, det vill säga sekretess till skydd för enskilda. Den generella sekretessbrytande bestämmelsen omfattar därmed inte sekretess till skydd för allmänna intressen. Behovet av en möjlighet att bryta den typen av sekretess kvarstår således för informationsdelning mellan myndigheter inom ramen för NCSC:s verksamhet, även om det förslaget införs. Den generella sekretessbrytande bestämmelsen anger vidare att sekretess får brytas i vissa syften, vilka är brett formulerade. Det går dock inte att utesluta att den informationsdelning som är aktuell inom ramen för NCSC:s verksamhet kan anses ske med andra syften. Som exempel kan nämnas att samverkan inte behöver ha koppling till brottslig verksamhet i den mening som avses i förslaget till den generella sekretessbrytande bestämmelsen.

Det kan uppstå situationer då samma information behöver hanteras och delas i olika syften. Som exempel kan nämnas att NCSC eller någon samverkansmyndighet fått del av sårbarhetsinformation som en underrättelseuppgift. Samma information kan också lämnas in till NCSC inom ramen för den sårbarhetsrapportering som görs till FRA i dess egenskap av CSIRT-enhet enligt 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). Det kan då framstå som oklart hur uppgiften ska hanteras utifrån sekretesslagstiftningen; till exempel vilken sekretessbestämmelse som ska tillämpas på uppgiften och om den kan lämnas ut eller inte. Det förekommer dock redan i dag att samma uppgift kan omfattas av flera olika typer av sekretessbestämmelser. Utredningen bedömer inte att den föreslagna uppgiftsskyldigheten i sig ger upphov till några nya oklarheter i rättstillämpningen jämfört med vad som gäller med det befintliga regelverket kring informa-

tionsdelning. Motsvarande problematik kan sägas gälla för delning av information enligt exempelvis generalklausulen respektive mer specifik reglering av informationsdelning.

Utredningen återkommer i avsnitt 4.5 med överväganden och förslag rörande personuppgiftsbehandlingen inom NCSC. Men när det gäller den föreslagna uppgiftsskyldigheten kan det konstateras att myndigheterna vid tillämpningen behöver förhålla sig till befintlig reglering rörande personuppgiftsbehandling, som den allmänna dataskyddsregleringen och eventuella sektorsspecifika registerlagar.

4.3 En ny sekretessbestämmelse hos NCSC

Utredningens bedömning: Uppgifter rörande enskildas personliga och ekonomiska förhållanden bör skyddas av sekretess. Uppgifterna är i dag delvis skyddade av sekretess. Ett mer heltäckande sekretesskydd bör dock införas.

Utredningens förslag: En ny sekretessbestämmelse ska införas i OSL. Syftet med bestämmelsen är att ge ett skydd för uppgift om enskildas personliga och ekonomiska förhållanden som förekommer hos FRA. Bestämmelsen ska ha ett omvänt skaderekvisit.

4.3.1 Det finns utmaningar med informationsdelning med näringslivet

I Riksrevisionens rapport *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig* (RiR 2023:8) framgår att näringslivsföreträdare anser att myndigheterna saknar intresse för samarbete och förståelse för vad näringslivet kan bidra med. Näringslivet upplever också att det offentliga inte delar med sig av tillräcklig information. Det saknas också standardisering eller tydliga riktlinjer för vilken information som är aktuell att dela mellan myndigheterna och näringslivet. Riksrevisionen har bedömt att avsaknaden av standardisering har gjort informationsdelning svårare både internt och externt. Myndigheten har rekommenderat att hinder för informationsutbyte identifieras och att det finns strukturer som medger nödvändigt informationsutbyte mellan myndigheter

såväl som mellan det offentliga och det privata för att arbetet med samhället informations- och cybersäkerhet ska fungera effektivt (RiR 2023:8).

Företrädare för näringslivet som utredningen pratat med har framfört bristen på återkoppling som problematisk. Enskilda företag kan lämna information om till exempel sårbarheter till myndigheterna, men får inte veta hur informationen tas om hand. Det skapar också en oro kring hur informationen sprids. Samtidigt finns det ett samhällsintresse av att uppgifter om incidenter och sårbarheter, som IP-adresser som har använts vid dataintrång, sprids för att olika aktörer ska kunna vidta skyddsåtgärder och utveckla arbetet med cybersäkerhet och informationssäkerhet.

Regeringen har uttryckt att privat-offentligt samarbete kring cybersäkerhetsincidenter behöver utvecklas och nyttja den incidenthanteringskompetens som finns i privat sektor. Utvecklat och bristande samarbete mellan det privata och offentliga, nationellt såväl som internationellt, utgör enligt regeringen en sårbarhet. Det finns också en strävan mot väletablerade metoder för internationellt och privat-offentligt samarbete (skr. 2024/25:121). 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.

4.3.2 NIS 2-direktivet ställer krav på anonymitet

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 utsetts till samordnare för den samordnade delgivningen av information om sårbarheter. Det rör sig alltså om en möjlighet till frivillig och, om så begärs, anonym rapportering av sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska enligt samma artikel säkerställa att skyndsamma uppföljningsåtgärder vidtas med avseende på den rapporterade sårbarheten och ska 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.

Kopplat till den rapporteringsskyldighet som finns i artikel 23 i NIS 2-direktivet för de entiteter som omfattas av direktivet finns också krav på konfidentialitet. Av artikel 23.6 framgår nämligen följande. När så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa viss typ av information som 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.

Artikel 30.1 i NIS 2-direktivet föreskriver 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 *dels* väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud, *dels* andra entiteter än de som avses ovan, oberoende av om de omfattas av direktivet, vad gäller om betydande incidenter, cyberhot och tillbud. Av artikel 30.2 följer vidare att medlemsstaterna ska behandla dessa frivilliga underrättelser i enlighet med vad som följer av artikel 23. Enligt samma artikel ska CSIRT-enheterna, och i tillämpliga fall, de behöriga myndigheterna vid behov informera de gemensamma kontaktpunkterna om underrättelser som mottagits i enlighet med artikeln, och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt.

Det finns alltså vissa krav i NIS 2-direktivet på att uppgifter ska behandlas med konfidentialitet och att den som rapporterar sårbarheter ska säkerställas anonymitet.

4.3.3 Vissa uppgifter om enskilda bör omfattas av sekretess hos NCSC

Utredningen bedömer att det är nödvändigt att sekretess gäller för uppgifter om enskildas affärs- och driftförhållanden. Det är viktigt att en öppen dialog kan förekomma i kontakterna mellan NCSC och företrädare för näringslivet. En förutsättning för en öppen dia-

log är att representanter för företag inte undanhåller viktig information av rädsla för att uppgifterna ska spridas vidare eller utnyttjas i konkurrenssyfte. Därtill innebär NIS 2-direktivet även att enskilda ska kunna lämna in sårbarhetsrapporter och vara anonyma. Skydd för anmälarens identitet är i regel inte något som täcks av en bestämmelse som skyddar uppgifter om enskildas affärs- och driftförhållanden. Därför måste utredningen överväga ett sekretessskydd som sträcker sig längre än enskildas affärs- och driftförhållanden, och alltså även täcker in enskildas personliga och ekonomiska förhållanden.

Eftersom utgångspunkten i svensk rätt är handlingsoffentlighet måste det övervägas hur det befintliga sekretessskyddet ser ut för den typen av uppgifter som nämns ovan.

4.3.4 Befintliga sekretessbestämmelser är inte tillräckliga för enskildas personliga och ekonomiska förhållanden

Sekretessen rörande säkerhets- eller bevakningsåtgärd är inte tillräcklig

Enligt 18 kap. 8 § 3 OSL gäller sekretess 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 exempelvis telekommunikation eller system för automatiserad behandling av information (tredje punkten). Bestämmelsen avser sekretess för olika brottsförebyggande åtgärder som i huvudsak hänför sig till annan verksamhet än den som bedrivs av Polismyndigheten (Lenberg m.fl. 2024, kommentaren till 18 kap. 8 § OSL). I betänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64) görs bedömningen att det inte kan uteslutas att det kan finnas uppgifter i en incidentrapport som, även om uppgifterna är mycket känsliga, inte skulle omfattas av sekretess enligt bestämmelsen. Den utredningen bedömde därför att en ny sekretessbestämmelse behövs för uppgifter i incidentrapporter. I avsnitt 4.4 återkommer utredningen med överväganden kring den bestämmelsen.

Utredningen delar bedömningen att 18 kap. 8 § OSL inte ger ett tillräckligt skydd för uppgifter i incidentrapporter. Därutöver kan det noteras att skaderekvisitet i den befintliga bestämmelsen innebär att sekretess gäller om det kan antas att syftet med åtgärden

motverkas om uppgiften röjs. Bestämmelsens syfte är alltså inte att skydda enskilda intressen. Utredningen bedömer att ett sekretess-skydd behöver omfatta enskilda intressen.

Förslaget om sekretess för uppgift i incidentrapporter är inte tillräckligt

I betänkandet SOU 2024:64 lämnas förslag om en ny sekretessbestämmelse för uppgift i incidentrapporter i 18 kap. 8 d § OSL. Bestämmelsen omfattar de tvingande incidentrapporteringar som ska göras av kritiska verksamhetsutövare enligt CER-direktivet (se utredningens förslag till 5 kap. 1 § lag om motståndskraft hos kritiska verksamhetsutövare). Bestämmelsen omfattar även den tvingande incidentrapporteringen som ska göras av verksamhetsutövare enligt NIS 2-direktivet (se utredningens förslag till 3 kap. 5–7 §§ lag om cybersäkerhet). Sekretess föreslås gälla för uppgift i incidentrapport samt för uppgift om åtgärd som följer av en sådan incident om det inte står klart att uppgiften kan röjas utan att den rapporterade verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas. Sekretess föreslås alltså gälla med ett omvänt skaderekvisit. Enligt förslaget författningskommentar kan skada för verksamheten till exempel vara negativa konsekvenser för verksamhetsutövarens pågående och framtida säkerhetsarbete, negativa ekonomiska effekter för enskilda verksamhetsutövare och bristande rapporteringsvilja.

Den tvingande incidentrapporteringen är dock endast en av flera situationer då privata aktörer kan komma att lämna uppgifter till myndigheter. Som framgått ovan ska medlemsstaterna säkerställa en möjlighet att anonymt rapportera sårbarheter till samordnande CSIRT-enhet (artikel 12.1 i NIS 2-direktivet). Även när det gäller frivillig incidentrapportering ska entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet bevaras (artikel 30 och artikel 23.6 i NIS 2-direktivet). Det förslag som lämnats i ovan angivet betänkande täcker inte de uppgifter som kan inkomma till myndigheter i de två senare situationerna.

Sekretessen rörande risk- och sårbarhetsanalyser är inte tillräcklig

Enligt 18 kap. 13 § OSL gäller sekretess för uppgift som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, om det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs. Med begreppet fredstida krissituationer avses mycket allvarliga kriser, alltså inte olyckor och andra händelser av mer vardaglig karaktär. Eftersom sekretessen enligt bestämmelsen gäller för uppgifter som *hänför sig till* nämnda verksamhet följer sekretessen med en uppgift som lämnas till en annan myndighet. Denna omständighet medför att det inte kan antas att det allmännas möjligheter att förebygga eller hantera fredstida krissituationer motverkas om uppgiften lämnas till den mottagande myndigheten (prop. 2004/05:5 s. 266).

Vidare framgår av förarbetena att uppgifter som omfattas av sekretess kan behöva lämnas ut till sammanslutningar och berörda näringsidkare. Ett sådant utlämnande kan ske med förbehåll enligt nuvarande 10 kap. 14 § OSL. Om det inte är möjligt att lämna ut uppgiften med förbehåll och ett utlämnande bedöms vara nödvändigt för att den utlämnande myndigheten ska kunna utföra analys-, förberedelse- eller planeringsarbetet så kan ett utlämnande ske med stöd av bestämmelsen i 10 kap. 2 § OSL (jfr prop. 2004/05:5 s. 266).

Det sekretesskydd som ges av bestämmelsen skulle kunna bli tillämpligt för viss del av NCSC:s verksamhet om det blir fråga om att göra en risk- och sårbarhetsanalys rörande att samhället på bred front kan utsättas för exempelvis cyberattacker som riskerar att lamslå samhällsviktiga verksamheter. När det gäller exempelvis incidentrapporter och sårbarhetsrapporter av mer vardaglig karaktär kan det inte vara fråga om sådana allvarliga kriser som ligger i begreppet fredstida krissituationer. Utredningen bedömer således att bestämmelsen inte lämnar ett tillfredsställande skydd för de uppgifter som bör vara sekretesskyddade.

Bestämmelsen i 18 kap. 13 § OSL syftar till att skydda allmänna intressen varför den inte täcker det behov av sekretess som kan finnas för att skydda enskilda intressen, även om det inte kan uteslutas

att bestämmelsen i vissa situationer kan ge ett indirekt skydd för enskilda intressen.

I samband med att bestämmelsen infördes väcktes frågan om sekretess till skydd för enskildas affärs- och driftförhållanden. Regeringen hänvisade till dåvarande 8 kap. 6 § sekretesslagen (nuvarande 30 kap. 23 § OSL) och anförde att för statliga myndigheters verksamhet torde ett eventuellt behov av sekretess till skydd för enskilda i första hand kunna täckas genom att nya bestämmelser förs in i sekretessförordningen (nuvarande OSF) och dess bilaga (prop. 2004/05:5 s. 261). Utredningen återkommer nedan till 30 kap. 23 § OSL.

Minimiskyddet är inte tillräckligt

I 21 kap. OSL finns bestämmelser om sekretess till skydd för uppgift om enskilds personliga förhållanden oavsett i vilket sammanhang uppgiften förekommer. Kapitlet innehåller bestämmelser om skydd för uppgifter om hälsa och sexualliv (21 kap. 1 § OSL), adress, telefon och skyddad folkbokföring avseende förföljda personer (21 kap. 3 och 3 a §§ OSL) samt uppgifter kopplade till utlännings säkerhet i vissa fall (21 kap. 5 § OSL). Det finns också en bestämmelse om sekretess för personuppgift, om det kan antas att uppgiften efter ett utlämnande kommer att behandlas i strid med dataskyddsregleringen (21 kap. 7 § OSL).

Det minimiskydd som finns i 21 kap. OSL omfattar vissa närmare angivna personliga förhållanden. Begreppet personliga förhållanden anses visserligen omfatta även ekonomiska förhållanden. Men det begreppet används inte i 21 kap. OSL. Dels innehåller bestämmelserna alltså inget skydd för uppgifter om ekonomiska förhållanden, dels kan inte juridiska personer anses omfattas av bestämmelserna. Även om personuppgifter i viss mån kan skyddas om det finns risk för att de kommer att behandlas i strid med dataskyddsregleringen så ger inte bestämmelserna i 21 kap. OSL ett tillfredsställande skydd för de uppgifter som utredningen anser behöver ett sekretesskydd.

Sekretessen för tillsyn, stödverksamhet m.m. är inte tillräcklig

Enligt 30 kap. 23 § OSL gäller sekretess, i den utsträckning regeringen meddelar föreskrifter om det, 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. Sekretessen gäller dels för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs, dels för uppgift om andra ekonomiska eller personliga förhållanden än som avses ovan för den som har trätt i affärsförbindelse eller liknande förbindelse med den som är föremål för myndighetens verksamhet.

Bestämmelsen ger inte i sig upphov till sekretess, utan kräver att regeringen meddelar föreskrifter som närmare anger vilka uppgifter som omfattas av sekretessen. Så har regeringen gjort i 9 § OSF samt i bilagan till förordningen. Det framgår av punkten 13 i bilagan till OSF att utredning, planering, tillsyn och stödverksamhet hos MSB omfattas av den sekretess som stadgas i 30 kap. 23 § OSL.

Med tillståndsgivning och tillsyn menas det område som i 1937 års sekretesslag beskrevs med ordet kontroll. Ordet tillsyn ska inte ges en alltför snäv tolkning utan får anses omfatta alla de fall där en myndighet har en övervakande eller styrande funktion i förhållande till näringslivet. Som exempel kan nämnas den samhälleliga verksamhet som regleras i marknadsföringslagen (1995:450), lagen (1994:1512) om avtalsvillkor i konsumentförhållanden och konsumentkreditlagen (1992:830). Även sådan rådgivning som sker som ett led i en myndighets tillsynsverksamhet omfattas av begreppet tillsyn. I flera lagstiftningsärenden har det framgått att tillsynsbegreppet på förvaltningsområdet med tiden kommit att bli snävare än tillsynsbegreppet i tryckfrihetsförordningen (TF) och OSL. En verksamhet som inte benämns som tillsyn i exempelvis myndighetsinstruktionen kan därmed anses som tillsyn i TF:s och OSL:s mening (prop. 2008/09:150 s. 355–356 och Lenberg m.fl. 2024, kommentaren till 30 kap. 23 § OSL).

Även med beaktande av att ordet tillsyn inte ska ges en alltför snäv innebörd finns det verksamhet som bedrivs med anledning av reglering i NIS 2-direktivet, som inte kan anses som tillsyn i bestämmelsens avseende. Till exempel ska verksamhetsutövare rapportera

incidenter till CSIRT-enheten. Denna skyldighet kan inte anses utgöra tillsyn, även om det kommer att finnas tillsynsmyndigheter som utövar tillsyn över rapporteringsskyldigheten. Inte heller den sårbarhetsrapportering som föreskrivs torde omfattas av bestämmelsen i 30 kap. 23 § OSL.

Utredningen har i kap. 3 betonat att den överföring av arbetsuppgifter från MSB till FRA som föreslås inte innebär att FRA kommer att utöva något tillsynsansvar. Det finns alltså en skiljelinje mellan NCSC:s stödjande verksamhet och tillsynsmyndigheternas faktiska tillsynsarbete.

Med *stödverksamhet* enligt 30 kap. 23 § OSL avses exempelvis sådan verksamhet som åsyftas i förordningen (1980:803) om regionalpolitiskt transportbidrag, presstödsförordningen (1990:524), stöd enligt förordningen (1996:1559) om statligt bidrag till svensk sjöfart och de olika stödförfattningarna på jordbruksområdet. Dessa verksamheter framgår av punkterna 28, 55, 71 och 75 i bilagan till OSF (Lenberg m.fl. 2024, kommentaren till 30 kap. 23 § OSL). Utredningen noterar att samtliga nämnda förordningar har upphävts. Men det kan konstateras att den stödverksamhet som avses synes hänföra sig till olika typer av statligt stöd eller bidrag. Som exempel på aktuell författning kan nämnas punkten 99 i bilagan till OSF. I punkten anges bland annat stöd enligt förordningen (2018:1300) om statligt stöd för driftsäkra och robusta elektroniska kommunikationer samt förordningen (2020:266) om statligt stöd för utbyggnad av bredbandsinfrastruktur. Begreppet stödverksamhet torde därför inte omfatta den verksamhet som utförs av NCSC.

Sekretess på grund av internationella avtal gäller inte

Enligt 30 kap. 24 § OSL gäller sekretess, i den utsträckning riksdagen godkänt ett avtal om detta med en annan stat eller med en mellanfolklig organisation, hos en statlig myndighet i verksamhet som avses i 23 §, för sådan uppgift om en enskilds ekonomiska eller personliga förhållanden som myndigheten förfogar över på grund av avtalet. Ekonomiska förhållanden innefattar även uppgifter om affärs- och driftförhållanden, uppfinningar och forskningsresultat (prop. 1992/93:120 s. 17–18). För att bestämmelsen ska bli tillämplig krävs att en myndighet, i den verksamhet som avses i 30 kap.

23 § OSL, förfogar över uppgift om en enskilda personliga eller ekonomiska förhållanden på grund av ett internationellt avtal som riksdagen har godkänt. I begreppet avtal anses bland annat rättsakter som gäller till följd av Sveriges medlemskap i EU ingå. De rättsakter som avses är anslutningsfördragen samt förordningar och direktiv som utfärdas av EU:s institutioner. Bestämmelsen förutsätter att det aktuella avtalet/rättsakten innehåller en klausul/artikel om att uppgiften inte får lämnas vidare i det aktuella fallet (Lenberg m.fl. 2024, kommentaren till 30 kap. 24 § OSL).

Bestämmelsen föreskriver så kallad absolut sekretess, vilket innebär att sekretess gäller för uppgifterna oberoende av en prövning av den risk för skada som ett utlämnande kan medföra (prop. 1992/93:120 s. 17).

Bestämmelsens tillämpning har berörts i andra lagstiftningsärenden. I samband med införande av Europaparlamentets och rådets direktiv 2003/42/EG av den 13 juli 2003 om rapportering av händelser inom civil luftfart resonerade regeringen kring tillämpligheten av 30 kap. 24 § OSL med koppling till artikel 8.1 i direktivet som överlämnade åt medlemsstaterna att säkra ”lämplig sekretess” (på engelska *appropriate confidentiality*). Regeringen bedömde att den artikeln inte innebar att 30 kap. 24 § OSL (dåvarande 8 kap. 6 § andra stycket sekretesslagen) var tillämplig (prop. 2006/07:110 s. 38).

I ett annat lagstiftningsärende bedömde regeringen att en artikel i ett direktiv som hänvisade till nationell rätt inte kan anses tillräckligt preciserad för att falla under 30 kap. 24 § OSL (prop. 2009/10:213 s. 31). Den artikel som avsågs var formulerad så att medlemsstaterna, i enlighet med gemenskapslagstiftning eller nationell lagstiftning, ska vidta nödvändiga åtgärder för att säkerställa sekretessen för de uppgifter som överlämnas till dem enligt direktivet och de ska endast använda uppgifterna i överensstämmelse med direktivet (artikel 24.1 Europaparlamentets och rådets direktiv 2009/17/EG av den 23 april 2009 om ändring av direktiv 2002/59/EG om inrättande av ett övervaknings- och informationssystem för sjötrafiken i gemenskapen).

I avsnitt 4.3.2 redogör utredningen för de artiklar i NIS 2-direktivet som handlar om konfidentialitet och anonymitet. Dessa artiklar är något mer preciserade än de som inte bedömts som tillräckliga i de ovan redovisade lagstiftningsärendena. Bland annat framgår att anonymiteten hos den rapporterande personen ska säkerställas och att berörda entiteters säkerhets- och affärsintressen ska skyddas.

Men artikel 23.6 hänvisar till unionsrätten eller nationell rätt i fråga om att bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet. Utredningen bedömer inte att de artiklar som behandlar konfidentialitet i NIS 2-direktivet är tillräckligt preciserade för att 30 kap. 24 § OSL ska vara tillämplig.

4.3.5 Sekretessintresset väger tyngre än insynsintresset

En avvägning mellan intresset av sekretess och insynsintresset ska göras i samband med att man överväger om en ny sekretessbestämmelse ska införas. Rätten att ta del av allmänna handlingar är en medborgerlig rättighet som utgör en viktig del av vårt demokratiska statsskick. Syftet med den rätten, som den kommer till uttryck i 2 kap. 1 § TF, är att främja ett fritt meningsutbyte och en allsidig upplysning. Genom tillgången till allmänna handlingar underlättas en fri åsiktsbildning, en fri debatt i olika samhällsfrågor samt den medborgerliga kontrollen av den offentliga maktutövningen.

Behovet av sekretess för en uppgift är oftast detsamma oavsett i vilket sammanhang uppgiften förekommer. Allmänintresset av insyn kan dock variera beroende på vilken typ av verksamhet det handlar om.

När det gäller NCSC:s verksamhet kan allmänintresset av insyn konkretiseras som att enskilda kan ha ett intresse av att få reda på om det föreligger sårbarheter i olika it-system, för att på så sätt själva kunna vidta säkerhetsåtgärder. NCSC:s verksamhet utgör till största delen inte myndighetsutövning och centret fattar få självständiga beslut. Utredningen gör vidare bedömningen i avsnitt 4.3.7 att den ärendehandläggning som NCSC ska ägna sig åt ska undantas från sekretessbestämmelsens tillämpningsområde. Intresset av insyn utifrån aspekten att allmänheten ska kunna granska myndigheters verksamhet är inte så stort i den del av NCSC:s verksamhet som inte utgör ärendehandläggning. Den delen av verksamheten utgör också huvuddelen av NCSC:s verksamhet.

Mot allmänintresset av insyn står 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 informations- och cybersäkerhetsområdet i ett antagonistiskt syfte. Att mängden information som

ska hanteras ökar innebär i sig en större risk för att antagonistiska aktörer kan använda informationen för att kunna utföra cyberattacker. Ur enskilda aktörers perspektiv är det viktigt i konkurrenshänseende att information om exempelvis arbetssätt inte sprids på ett omotiverat sätt. Det finns en risk att enskilda aktörer inte rapporterar sårbarheter eller lämnar in incidentrapporter av rädsla för att uppgifterna kommer att lämnas vidare, vilket kan skada den egna verksamheten. Vidare finns det ett konkret behov av att införliva NIS 2-direktivets krav på konfidentialitet rörande frivillig rapportering till NCSC. Om det inte gäller sekretess för dessa uppgifter finns också risken att informationsdelningen mellan FRA, i egenskap av CSIRT-enhet, och CSIRT-enheter i andra EU-medlemsstater försvåras.

Sekretessbehovet väger i detta fall tyngre än allmänhetens intresse av insyn i NCSC:s verksamhet.

4.3.6 Det behövs en ny sekretessbestämmelse

Utredningen har övervägt några olika alternativ för att reglera sekretessen för uppgift om enskildas personliga och ekonomiska förhållanden. Ett alternativ hade varit att utvidga tillämpningsområdet för den bestämmelse i 18 kap. 8 d § OSL som föreslagits i SOU 2024:64. Ett annat alternativ är att, med koppling till 30 kap. 23 § OSL, lägga till NCSC:s verksamhet till bilagan till OSF. Ett tredje alternativ är att införa en ny sekretessbestämmelse till skydd för enskildas personliga och ekonomiska förhållanden. Utredningen har kommit fram till att sekretessen bör regleras i enlighet med det senare alternativet.

En uppenbar skillnad mellan förslaget till 18 kap. 8 d § OSL och bestämmelsen i 30 kap. 23 § OSL är att bestämmelserna föreskriver olika skaderekvisit. Den förstnämnda bestämmelsen innehåller ett omvänt skaderekvisit medan den sistnämnda innehåller ett rakt skaderekvisit. Det kan uppstå tillämpningssvårigheter för FRA om olika sekretessbestämmelser ska tillämpas beroende på om uppgifterna härrör från en incidentrapportering eller från ett uppgiftslämnande inom ramen för NCSC:s övriga verksamhet.

I SOU 2024:18 görs bedömningen att frivillig rapportering inte behöver regleras särskilt, eftersom en enskild enligt 19 § förvaltningslagen formlost kan inleda ett ärende hos en myndighet genom en ansökan, anmälan eller annan framställning. Utredningen ifrågasät-

ter inte denna bedömning. Problemet med att utvidga tillämpningsområdet för förslaget till 18 kap. 8 d § OSL är dock att den frivilliga incidentrapporteringen inte föreslås regleras i lag. En hänvisning till förslaget till lag om cybersäkerhet täcker därmed inte behovet av sekretess till skydd för uppgifter som lämnas frivilligt. Det föreslagna skaderekvisitet i 18 kap. 8 d § OSL indikerar vidare att bestämmelsen inte direkt tar sikte på att skydda anmälarens anonymitet.

Enligt 30 kap. 23 § OSL gäller sekretess, i den utsträckning regeringen meddelar föreskrifter om det, 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.

I bilagan till OSF finns i punkt 13 ett sekretesskydd avseende utredning, planering, tillsyn och stödverksamhet hos MSB. Ett alternativ hade varit att lägga till en likalydande punkt avseende utredning, planering, tillsyn och stödverksamhet hos FRA/NCSC. Men som utredningen konstaterat tidigare så torde inte all den verksamhet som ska bedrivas av NCSC omfattas av tillämpningsområdet för 30 kap. 23 § OSL. Detta framstår därför inte som en tillfredsställande lösning.

Det tredje alternativet som identifierats är att föreslå en ny sekretessbestämmelse i OSL. Utredningen bedömer att det är det mest ändamålsenliga alternativet.

4.3.7 Utformningen av sekretessbestämmelsen

Utredningens förslag: En ny bestämmelse om sekretess införs i 40 kap. OSL. Sekretess ska gälla hos FRA i verksamhet som bedrivs inom 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. För uppgift i en allmän handling ska sekretessen gälla i högst sjuttio år.

Sekretessen ska inte gälla i ärende om stöd enligt förordning (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning.

Tystnadsplikten som följer av den nya sekretessbestämmelsen ska ha företräde framför meddelarfriheten.

Utredningens bedömning: NCSC utgör inte en självständig verksamhetsgren hos FRA, i den mening som avses i offentlighets- och sekretesslagstiftningen.

Allmänna utgångspunkter

Vid utformandet av en ny sekretessbestämmelse är det viktigt att beakta att handlingsoffentligheten inte inskränks mer än vad syftet med sekretessen kräver. Sekretessbestämmelser består av tre rekvisit, som reglerar sekretessens föremål, räckvidd och styrka. Sekretessbestämmelser ska utformas så specifikt som möjligt när det gäller både sekretessens föremål och dess räckvidd.

Sekretessens föremål och räckvidd

Sekretessens föremål utgörs av vilka uppgifter som ska omfattas av bestämmelsen. Sekretess är ett undantag från huvudregeln om offentlighet varför föremålet för sekretessen måste avgränsas så snävt som möjligt. Det kan vara fråga om en stor mängd uppgifter av varierande slag som kommer att behandlas i NCSC:s verksamhet. Detta innebär att det är svårt att på förhand avgränsa sekretessens föremål alltför mycket utan att samtidigt riskera att skyddsvärda uppgifter faller utanför bestämmelsens tillämpningsområde.

Utredningen har ovan konstaterat att sekretessen bör gälla till skydd för enskilda intressen. Ofta används formuleringen ”uppgift om enskilda personliga och ekonomiska förhållanden” i sekretessbestämmelser. Uppgifter om en persons ekonomi kan falla under begreppet personliga förhållanden, men eftersom bestämmelsen också bör gälla juridiska personer, som inte kan sägas ha några personliga förhållanden, så bör det anges uttryckligen att ekonomiska förhållanden omfattas (jfr prop. 1979/80:2 Del A s. 84). I begreppet ”ekonomiska förhållanden” ingår uppgifter om affärs- och driftförhållanden.

Uttrycket ”enskild” avser såväl en fysisk som en juridisk person, precis som i övrigt i OSL (se prop. 1979/80:2 Del A s. 329 och prop. 2008/09:150 s. 349).

Sekretessens räckvidd måste också begränsas så att den inte blir större än vad som är motiverat utifrån det behov av sekretess som

identifierats. Nedan redogör utredningen för några alternativa sätt att reglera sekretessen. Frågan om sekretessens styrka behandlas i nästa avsnitt.

För att täcka behovet av sekretess för enskildas identitet och uppfylla kravet i artikel 12.1 i NIS 2-direktivet, så hade en bestämmelse kunnat utformas enligt följande.

Sekretess gäller i verksamhet som avser det nationella cybersäkerhetscentret för uppgift om en enskilds personliga och ekonomiska förhållanden i en anmälan eller utsaga, om uppgiften kan avslöja anmälarens identitet och det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Om anmälaren varit rapporteringsskyldig enligt 3 kap. 5–7 §§ förslaget till lag om cybersäkerhet i SOU 2024:18 så skulle dock inte sekretessen gälla. Utredningen bedömer i så fall att den sekretessbestämmelse som föreslås i SOU 2024:64 borde tillämpas. En liknande bestämmelse finns i 30 kap. 4 b § OSL, vilken ursprungligen infördes för att genomföra en del av EU:s kapitaltäckningsdirektiv (Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om särskild tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG). Formuleringen täcker visserligen uppgifter om enskildas affärs- och driftförhållanden, men en förutsättning för att sekretessen ska gälla är att uppgiften kan avslöja anmälarens identitet. Formuleringen täcker därmed inte det behov som identifierats.

Ett annat alternativ hade varit att utforma en sekretessbestämmelse enligt följande.

Sekretess gäller hos Försvarets radioanstalt för uppgift som lämnats i en incidentrapport enligt cybersäkerhetslagen (2025:000), om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Konstruktionen påminner om den bestämmelse som föreslås i SOU 2024:64. Problemet med den lösningen är att varken den frivilliga incidentrapporteringen eller sårbarhetsrapporteringen enligt NIS 2-direktivet är reglerad i förslaget till lag om cybersäkerhet, vilket också framgår i avsnitt 4.3.6. Dessa frågor hade då fallit utanför tillämpningsområdet för bestämmelsen.

Ett ytterligare alternativ är att utforma en sekretessbestämmelse enligt följande modell.

Sekretess gäller i verksamhet hos Försvarets radioanstalt som avser det nationella cybersäkerhetscentrets uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Sekretessen enligt första stycket gäller för uppgifter om 1. en enskilds personliga eller ekonomiska förhållanden i en anmälan eller utsaga, om uppgiften kan avslöja anmälarens identitet, om det kan antas att den enskilde lider skada eller men om uppgiften röjs, och 2. en enskilds affärs- eller driftförhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

En sådan bestämmelse innehåller visserligen en precisering av vilken typ av uppgifter som omfattas av bestämmelsen. På så sätt minskar risken för att uppgifter hålls hemliga utan att det finns ett konkret behov av det. Bestämmelsen har också den fördelen att det går att föreskriva olika skaderekvisit för olika typer av uppgifter, om det finns behov av det, vilket ytterligare minskar denna risk. Utformningen riskerar dock att leda till tillämpningssvårigheter. Till exempel kan det förekomma situationer då det framstår som oklart om uppgifterna lämnats i en anmälan eller utsaga.

Ett mer heltäckande skydd kan uppnås av en bestämmelse som skyddar enskildas personliga eller ekonomiska förhållanden i verksamhet hos FRA som avser NCSC:s uppgift enligt 4 a § FRA:s instruktion, det vill säga uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Den formuleringen täcker in många typer av uppgifter om enskilda som kan förekomma hos NCSC. Utredningens bedömning är dock att de nya arbetsuppgifter som FRA ska utföra genom ändringar i instruktionen ska kunna utföras inom ramen för NCSC:s verksamhet. En uttrycklig hänvisning till NCSC:s uppgifter såsom de framkommer av 4 a § FRA:s instruktion riskerar dock att innebära att skyddsvärda uppgifter faller utanför tillämpningsområdet för sekretessbestämmelsen om uppgifterna hänför sig till verksamhet enligt exempelvis 4 c § FRA:s instruktion.

Utredningen har i stället landat i att bestämmelsens räckvidd ska avse verksamhet som bedrivs inom NCSC. Risken att uppgifter om enskilda som borde skyddas faller utanför framstår med en sådan reglering som liten. Nackdelen med en så heltäckande räckvidd är

att bestämmelsen i vissa fall träffar fler uppgifter än vad som är nödvändigt. Det kan ifrågasättas om det verkligen finns ett behov av en sekretessbestämmelse med så bred räckvidd. En klar fördel är dock att bestämmelsen inte ger upphov till svåra tillämpningsproblem, som kan uppkomma om sekretessens föremål anges alltför preciserat och avgränsat. En alltför detaljerad bestämmelse innebär också en risk att enskilda undviker att rapportera incidenter och sårbarheter eftersom det framstår som osäkert om uppgifterna skyddas av sekretess eller inte. Denna risk bör få genomslag i utformningen av sekretessens föremål och räckvidd.

När det gäller bestämmelsens räckvidd så uppnås en balans mellan intresset av offentlighet och intresset av att skydda uppgifter om enskilda genom att räckvidden knyts till verksamhet som bedrivs inom NCSC.

Viss ärendehandläggning ska undantas från tillämpningen

Utredningen föreslår i kapitel 3 att FRA ska pröva frågor om stöd enligt förordningen (2024:664) om stöd till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning. Enligt 4 § i den förordningen får stöd lämnas i form av bidrag till åtgärder för cybersäkerhet inom näringsliv, teknik och forskning, om det finns medel. Stöd får inte lämnas till privatpersoner.

Någon sekretessbestämmelse särskilt avsedd för tillämpning vid handläggning av sådana ärenden finns inte i dag. Att det skulle finnas några tydliga skäl för att uppgifter i dessa ärenden ska hemlighållas generellt har inte framkommit, även om det kan tänkas att ansökningar innehåller uppgifter om enskildas affärs- och driftförhållanden.

Till skillnad från merparten av den verksamhet som NCSC ska bedriva så är det i detta sammanhang fråga om att pröva om enskilda ska få ta del av stöd som finansieras av offentliga medel. Det innebär att allmänintresset av insyn är starkt. Utredningen bedömer avseende denna ärendehandläggning att enskildas intresse av att uppgifter hemlighålls inte överväger insynsintresset. Därför föreslår utredningen att ärendehandläggningen i detta avseende ska undantas från tillämpningsområdet för den föreslagna sekretessbestämmelsen. Det bör dock betonas att den omständigheten inte påverkar tillämpligheten av andra sekretessbestämmelser i OSL. Till exempel skulle

31 kap. 16 § OSL möjligtvis kunna vara tillämplig. Enligt den bestämmelsen gäller sekretess för uppgift om en enskilds affärs- eller driftförhållanden när denne i vissa fall har trätt i affärsförbindelse med en myndighet, om det av särskild anledning kan antas att den enskilde lider skada om uppgiften röjs. Om det framöver uppkommer behov av att skydda uppgifter som förekommer i ärendehandläggningen så kan frågan regleras på förordningsnivå, genom tillägg i bilagan till OSF. På så sätt kan uppgifter, i den omfattning det behövs, omfattas av tillämpningsområdet för 30 kap. 23 § OSL.

Sekretessens styrka

Även vid utformningen av sekretessens styrka så är utgångspunkten att inte mer än bara det som är oundgängligen nödvändigt ska sekretessbeläggas för att skydda det intresse som har föranlett bestämmelsen. Detta görs genom skaderekvisit (prop. 1979/80:2 Del A s. 78–79).

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 (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 uppgiften (prop. 1979/80:2 Del A s. 84).

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.

Den sekretessbestämmelse i 18 kap. OSL som föreslås i SOU 2024:64 har ett omvänt skaderekvisit. Som skäl för detta

anges att behovet av tilltro till systemet är avgörande, att innehållet i en incidentrapport kan orsaka en stor skada om den röjs samt att konsekvenserna av ett röjande kan få betydande negativa effekter i verksamheten hos den aktör som genomför rapporteringen. Sekretessens föremål och räckvidd är dock begränsade till uppgifter i incidentrapporter som aktörer är tvingade att lämna in. Sekretessbestämmelsen träffar således en mer begränsad krets av uppgifter än den bestämmelse som föreslås i detta betänkande. Den är knuten till vissa uppdrag som NCSC har och innebär ett bredare tillämpningsområde.

De omständigheter som anges som skäl för det omvända skaderekvisitet i SOU 2024:64 gör sig även i viss mån gällande när det handlar om den frivilliga incidentrapportering som ska kunna göras enligt NIS 2-direktivet. Om uppgifter om enskilda, särskilt enskildas affärs- och driftförhållanden, sprids kan det möjliggöra för antagonister att rikta cyberattacker. När det kommer till sårbarhetsrapporteringen så kräver direktivet att det ska finnas en möjlighet att vara anonym när en sådan rapportering görs. Det krävs också att den fysiska eller juridiska personen har begärt att få vara anonym. Sekretessintresset rörande den typen av uppgifter talar för att föreslå en sekretessbestämmelse med ett rakt skaderekvisit. Vissa anslutande sekretessbestämmelser, som 18 kap. 8 och 13 §§ samt 30 kap. 23 § OSL innehåller raka skaderekvisit. När det gäller insynsintresset så kan det konstateras att det torde finnas ett lågt allmänintresse av att få del av uppgifter om enskilda som förekommer hos NCSC. Insynsintresset bör i stället anses handla om frågor på en mer allmän nivå, och omfatta förekomsten av exempelvis cyberhot och cyberattacker. När det gäller uppgifter om enskilda så kan det dock finnas ett journalistiskt intresse av att få ut uppgifter om individer kopplade till exempelvis organiserade cyberattacker.

Sammantaget bedömer utredningen att sekretessintresset väger tyngre än insynsintresset. Bestämmelsen bör innehålla ett omvänt skaderekvisit. På så sätt uppnås också viss enhetlighet med det förslag om sekretess som lämnas i SOU 2024:64.

Begreppet ”skada” avser enbart ekonomisk skada (prop. 1979/80:2 Del A s. 83). Begreppet ”men” har dock en mycket vid innebörd. I första hand avses att någon blir utsatt för andras missaktning om hans eller hennes personliga förhållanden blir kända. Redan den omständigheten att vissa personer känner till en för någon enskild

ömtålig uppgift kan i många fall anses tillräckligt för att medföra men. Utgångspunkten för en bedömning av om men föreligger är den berörda personens egen upplevelse. Bedömningen måste dock i viss utsträckning kunna korrigeras på grundval av gängse värderingar i samhället. Enbart det faktum att en person anser att det i största allmänhet är obehagligt att andra vet var personen bor kan till exempel inte anses innebära men. Begreppet ”men” kan i vissa sammanhang även innefatta ekonomiska konsekvenser för en enskild (prop. 1979/80:2 Del A s. 83).

Sekretesstid och bestämmelsens placering

En sekretessbestämmelse bör innehålla en yttersta begränsning i tid. När det gäller sekretess till skydd för enskilda personliga förhållanden är sekretesstiden i regel bestämd till högst 70 år med utgångspunkt i att sekretessen bör gälla under större delen av den enskildes livstid (prop. 1979/80:2 Del A s. 459–460 och 493–494). Sekretessbestämmelser som skyddar uppgifter om affärs- eller driftförhållanden innehåller vanligen en sekretesstid om högst 20 år (se exempelvis 30 kap. 4, 10 och 11 §§ samt 31 kap. 5 a § och 38 kap. 6 § OSL).

I den sekretessbestämmelse för uppgifter i incidentrapporter som föreslås i SOU 2024:64 föreslås en sekretesstid om 40 år, i enlighet med den sekretesstid som gäller i övrigt för incidentrapporter i domstolar, med mera. Det kan diskuteras om de enskilda intressen som skyddas av den föreslagna bestämmelsen motiverar en längre sekretesstid än så, i enlighet med vad som anförts ovan om enskildas personliga förhållanden. Visserligen bör uppgifter om enskildas personliga förhållanden inte förekomma i stor omfattning hos NCSC. Men det kan förekomma sådana personuppgifter som betraktas som känsliga i EU:s dataskyddsförordnings mening, vilket utredningen återkommer till nedan. Sekretesstiden bör bestämmas till högst 70 år mot bakgrund av detta och då enskildas personliga förhållanden som utgångspunkt ska skyddas under så lång tid.

Den föreslagna bestämmelsen skyddar enskilda intressen. Den bör därför placeras i OSL:s femte avdelning (kap. 21–40). Kap. 30 innehåller sekretess till skydd för enskild i verksamhet som avser tillsyn m.m. i fråga om näringslivet. Ett alternativ hade varit att

placera bestämmelsen där. NCSC ska dock inte bedriva tillsyn. Det breda uppdrag som NCSC ska ha medför att bestämmelsen inte passar in i det kapitlet. Bestämmelsen bör i stället införas i 40 kap. OSL som reglerar sekretess till skydd för enskild hos övriga myndigheter och i övriga verksamheter.

Rätten att meddela och offentliggöra uppgifter bör begränsas

Rätten att meddela och offentliggöra uppgifter följer av TF och yttrandefrihetsgrundlagen. OSL innehåller begränsningar av den rätten i vissa fall. Eftersom en ny sekretessbestämmelse föreslås måste det även utredas om den tystnadsplikt som följer av bestämmelsen bör inskränka rätten att meddela och offentliggöra uppgifter eller om den rätten ska ha företräde. En allmän utgångspunkt är att stor återhållsamhet ska iakttas vid prövningen av om undantag ska göras från rätten att meddela och offentliggöra uppgifter i det särskilda fallet. Meddelarfriheten ska bara begränsas om det är särskilt motiverat. Sekretessbestämmelsens konstruktion kan ge visst stöd för bedömningen. Om sekretessbestämmelsen föreskriver absolut sekretess kan det finnas större anledning att överväga undantag från rätten att meddela och offentliggöra uppgifter. I viss utsträckning gäller samma resonemang när det är fråga om ett omvänt skaderekvisit. Det kan också få betydelse om uppgiften har lämnats av en enskild i en förtroendesituation eller om uppgiften hänför sig till myndighetsutövning. Som utgångspunkt bör rätten att meddela och offentliggöra uppgifter inskränkas i fall som avser en uppgift som lämnats i förtroende, medan denna rätt i stället bör ha företräde när det är fråga om uppgifter som hänför sig till myndighetsutövning (prop. 1979/80:2 Del A s. 111–112).

Den sekretessbestämmelse som föreslås innehåller ett omvänt skaderekvisit, vilket talar för att rätten att meddela och offentliggöra uppgifter bör begränsas. Det kommer dock inte som regel att vara fråga om att uppgifter lämnas till NCSC i en förtroendesituation av den enskilde själv, även om det skulle kunna förekomma. NCSC kommer att ha ett brett uppdrag att erbjuda stöd till olika samhällsaktörer i olika situationer som rör cybersäkerhet och informationssäkerhet. Det torde alltså inte vara fråga om en sådan förtroendesituation som avses i offentlighets- och sekretesslagstiftningens

förarbeten. Sekretessbestämmelsen ska inte omfatta den myndighetsutövning som NCSC kommer att utföra varför insynsintresset inte är särskilt starkt med anledning av det. Utredningen bedömer sammantaget att det framkommit tillräckligt starka skäl för att meddelarfriheten ska begränsas. Rätten att meddela och offentliggöra uppgifter (1 kap. 1 och 7 §§ TF samt 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen) bör därmed inte ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen. Detta ska komma till uttryck i 40 kap. 8 § OSL.

NCSC utgör inte en självständig verksamhetsgren inom FRA

Enligt utredningens förslag till ny sekretessbestämmelse ska sekretess gälla hos FRA i verksamhet som bedrivs inom NCSC. Med anledning av att NCSC är en del av FRA måste frågan om sekretessgränser gentemot FRA:s övriga verksamhet analyseras. Utgångspunkten är att ett tillfredsställande integritetsskydd för information som hanteras av en myndighet förutsätter att sekretesskyddade uppgifter inte vidarebefordras utanför den egna verksamheten där de har inhämtats. En sekretesskyddad uppgift får därför inte utan stöd i OSL lämnas till enskilda, andra myndigheter eller mellan olika verksamhetsgrenar inom en myndighet när de är att betrakta som självständiga i förhållande till varandra (se 8 kap. 1 och 2 §§ OSL). För att det ska uppstå en sekretessgräns inom en myndighet krävs två saker. För det första ska de olika delarna av en myndighets verksamhet tillämpa helt olika set av sekretessbestämmelser. I så fall är det fråga om olika verksamhetsgrenar i OSL:s mening. För det andra krävs det att de olika verksamhetsgrenarna ska vara organiserade på ett sådant sätt att verksamheterna är självständiga i förhållande till varandra. Först om båda dessa förutsättningar är uppfyllda uppkommer en sekretessgräns inom en myndighet (prop. 2008/09:150 s. 360).

FRA:s huvuduppdrag utgör att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning (1 § FRA:s instruktion). FRA ska särskilt följa förändringen av signalmiljön i omvärlden, den tekniska utvecklingen och signalskyddet, fortlöpande utveckla den teknik och metodik som behövs för att bedriva verksamheten, samt utföra matematiska bedömningar av kryptosystem (2 § FRA:s

instruktion). Även inom informationssäkerhetsområdet har FRA specifika uppdrag, enligt 4 § FRA:s instruktion. Myndigheten har även andra uppdrag rörande kryptologi, signalspaningssystem och att stötta Försvarsmakten rörande den myndighetens cyberförsvarsförmåga.

NCSC är organiserat som en egen avdelning inom FRA. I 4 a § FRA:s instruktion är centrets verksamhet särskilt reglerad och verksamheten leds av en chef som anställs genom beslut av regeringen (7 a § FRA:s instruktion). Vidare finns kompletterande reglering av NCSC:s verksamhet i NCSC-förordningen. Den föreslagna sekretessbestämmelsen kommer bara att vara tillämplig inom NCSC:s verksamhet. Men centret kan även komma att hantera uppgifter som omfattas av andra typer av sekretess, som 18 kap. 2, 8 och 13 §§ OSL. Även andra delar av FRA kan behöva tillämpa den typen av sekretessbestämmelser. Det framstår som tveksamt om NCSC:s verksamhet och FRA:s verksamhet i övrigt ska tillämpa helt olika set av sekretessbestämmelser, förutom när det gäller den föreslagna bestämmelsen. Huruvida FRA:s verksamhet är organiserad så att NCSC ska anses utgöra en självständig verksamhetsgren i OSL:s mening är inte alldeles enkelt att avgöra eftersom det ännu inte är helt klarlagt hur NCSC ska arbeta. Utredningen bedömer dock att verksamheten inte är organiserad så att NCSC ska anses utgöra en sådan självständig verksamhetsgren inom FRA. Det innebär att det inte råder någon sekretessgräns mellan NCSC och FRA i övrigt. Dataskyddslagstiftningen kan dock medföra begränsningar av informationsflödet inom myndigheten.

Det kan i sammanhanget noteras att utredningen övervägt om NCSC *borde* utgöra en självständig verksamhetsgren i förhållande till FRA:s övriga verksamhet. Något förhållande som talar för det har dock inte framkommit. Som exempel kan nämnas att FRA inte bedriver någon operativ tillsynsverksamhet som påverkar lämpligheten i att uppgifter lämnas mellan olika typer av verksamheter inom myndigheten (jfr prop. 2006/07:108 s. 43–46).

Behovet av en snabb lösning

Utredningen har uppmärksammat på behovet av en sekretessbestämmelse till skydd för enskilda intressen under tiden som uppstår innan arbetsuppgifterna har förts över till FRA. Den sekretessbestämmelse som föreslås har utformats med hänsyn till att utredningen föreslår att vissa arbetsuppgifter ska utföras av FRA. Under en övergångsperiod kommer dock MSB att utföra arbetsuppgifterna och därmed ta emot och hantera de uppgifter som kan behöva skyddas av sekretess. Oavsett om den föreslagna sekretessbestämmelsen knyts till FRA:s verksamhet eller exempelvis gäller i all offentlig verksamhet så är det oundvikligt att beredningen av utredningens förslag kommer att innebära att det under en viss tid inte finns en sekretessbestämmelse på plats.

En bestämmelse som knyter sekretessen till exempelvis den myndighet som ska vara gemensam kontaktpunkt, CSIRT-enhet och/eller cyberkrishanteringsmyndighet (för beskrivning se 20–32 §§ förslaget till förordning om cybersäkerhet i SOU 2024:18) har i sammanhanget övervägts. Det framstår dock inte som en tillfredsställande lösning. En sådan bestämmelse hade visserligen kunnat tillämpas av MSB under en övergångsperiod, innan FRA övertar dessa uppdrag. Men mot bakgrund av begreppsanvändningen och systematiken i OSL, samt med beaktande av att FRA och NCSC:s uppdrag i fråga om cybersäkerhet är bredare än dessa specifika funktioner förordar utredningen inte en sådan lösning.

Som utredningen konstaterat tidigare så finns det vissa sekretessbestämmelser som, åtminstone delvis, kan vara tillämpliga på de uppgifter om enskilda som behöver hanteras. I avvaktan på att det finns en sekretessbestämmelse på plats får därför uppgifterna hanteras inom befintligt regelverk.

4.3.8 En bestämmelse om tystnadsplikt för enskilda kan övervägas

Utredningens bedömning: Informationsdelningen med näringslivet hade underlättats om enskilda åläggs en lagstadgad tystnadsplikt rörande uppgifter som enskilda får del av från NCSC. Det finns dock i nuläget inte förutsättningar att föreslå en sådan bestämmelse.

Utredningen har övervägt behovet av att införa en bestämmelse om tystnadsplikt för enskilda som deltar i NCSC:s verksamhet. En bestämmelse med innebörden att enskilda som deltar eller har deltagit i NCSC:s verksamhet inte obehörigen får föra vidare eller utnyttja uppgifter som han eller hon har fått del av har i sammanhanget övervägts. En liknande bestämmelse finns i 1 kap. 15 § lagen (2022:482) om elektronisk kommunikation. Men den bestämmelsen grundar sig i att regleringsmyndigheten har en laglig möjlighet att ålägga en aktör att delta i bland annat planeringsarbete, se 1 kap. 13 § nämnda lag. Av 44 kap. 4 § OSL framgår vidare att bestämmelsen i 1 kap. 15 § lagen om elektronisk kommunikation innebär att rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks, när det är fråga om uppgift om förhållanden av betydelse för att förebygga eller hantera fredstida krissituationer.

Även 7 kap. 1 § lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap innehåller en bestämmelse om tystnadsplikt. Enligt bestämmelsen får inte den som deltar eller har deltagit i en kommuns eller en regions verksamhet med beredskap för eller åtgärder under extraordinära händelser i fredstid och höjd beredskap, obehörigen röja eller utnyttja vad han eller hon därigenom har fått veta om vissa förhållanden. Bland annat omfattas uppgifter om ett företags affärs- eller driftsförhållanden.

Som exempel på en situation då enskilda deltar i verksamhet enligt lagen kan nämnas bestämmelsen i 2 kap. 7 §. Av den framgår bland annat att kommuner under vissa förutsättningar ska verka för att olika aktörer i kommunen samverkar och uppnår samordning i planerings- och förberedelsearbetet. Det kan handla om statliga

myndigheter, regioner, organisationer och företag (prop. 2005/06:133 s. 159).

Av förslaget till förordning om cybersäkerhet i SOU 2024:18 framgår att CSIRT-enheten ska upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet (29 § 11 i förslaget). CSIRT-enheten ska alltså bedriva verksamhet som innefattar samverkan, och därmed informationsdelning, med näringslivet.

NCSC kommer dock inte att ha möjlighet enligt författning att ålägga enskilda aktörer att delta i verksamheten. Centret ska visserligen vara en nationell plattform för samverkan och informationsutbyte mellan aktörer, såväl privata som offentliga, i frågor som rör cybersäkerhet (2 § NCSC-förordningen). Informationsutbytet inom ramen för den samverkan hade underlättats av att enskilda ålagts tystnadsplikt. Huruvida det är lämpligt att knyta en lagstadgad tystnadsplikt för enskilda till uppgifter som regleras i förordning samt andra frågor med koppling till detta är något som får utredas i annat sammanhang.

Det kan också noteras att NCSC:s verksamhet kan innefatta hantering av säkerhetsskyddsklassificerade uppgifter. För det fall att sådana uppgifter skulle förekomma så gäller följande. Enligt 1 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585) så utgörs säkerhetsskyddsklassificerade uppgifter av uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL eller *som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig* (utredningens kursivering). Det kan konstateras att, för det fall att enskilda aktörer skulle få del av säkerhetsskyddsklassificerade uppgifter vid samverkan med NCSC, så är säkerhetsskyddslagstiftningen tillämplig även för den enskilda aktören (se prop. 2017/18:89 s. 51–52).

4.3.9 Konkurrens med andra sekretessbestämmelser

Det går inte att utesluta att den föreslagna sekretessbestämmelsen kan vara tillämplig samtidigt som någon annan sekretessbestämmelse. Som exempel kan nämnas 18 kap. 8 och 13 §§ samt 30 kap. 24 § OSL. Konkurrensen mellan olika sekretessbestämmelser regleras i 7 kap. 3 § OSL. Av den bestämmelsen följer att det är den eller de

bestämmelser enligt vilken uppgiften är sekretessbelagd som har företräde. Det innebär att det är resultatet av sekretessprövningen som är avgörande och inte skaderekvisitens konstruktion (prop. 2008/09:150 s. 318–320 och RÅ 2007 ref. 45).

Beredningen av den sekretessbestämmelse som föreslås i SOU 2024:64 pågår varför utredningen utgår från den formulering som föreslagits i betänkandet. Den bestämmelsen är avgränsad till uppgifter i incidentrapporter enligt viss lagstiftning, och avser den tvingande incidentrapporteringen som ska göras. Det går inte att utesluta att det med den i detta betänkande föreslagna sekretessbestämmelsen uppstår en överlappning mellan dessa båda bestämmelser. Detta förhållande får beaktas i den fortsatta beredningen av utredningens förslag.

Utredningen redogör nedan för vissa andra förslag som lagts fram i SOU 2024:64. Det kan inte uteslutas att det uppstår viss överlappning mellan den bestämmelse som föreslås i detta betänkande och den föreslagna 15 kap. 3 c § OSL i SOU 2024:64. Rörande den senare bestämmelsen så uttalade den utredningen att det är nödvändigt att uppgifter som regleras i bland annat NIS 2-direktivet ska kunna hanteras av andra myndigheter i Sverige än den myndighet som är primär mottagare. Det handlar om att tillgodose behovet av ett ömsesidigt uppgiftsutbyte rörande sådana uppgifter som härrör från andra EU-medlemsstater och EU:s institutioner oberoende av vilken myndighet som har fått uppgiften. Som exempel kan nämnas uppgifter i incidentrapporter och uppgifter som delges i samverkan med andra medlemsstaters tillsynsmyndigheter enligt NIS 2-direktivet.

Utredningen har övervägt om det går att begränsa sekretessens föremål i den nu föreslagna sekretessbestämmelsen till att den bara ska täcka uppgifter som härrör från den enskilde själv. En nackdel med den formuleringen att den kan vålla tillämpningssvårigheter och innebära att i och för sig skyddsvärda uppgifter faller utanför tillämpningsområdet. Dessa förhållanden får beaktas i den fortsatta beredningen av utredningens förslag.

4.3.10 Befintliga sekretessbestämmelser är tillräckliga för det allmännas affärs- och driftförhållanden

Utredningens bedömning: Befintlig reglering i 19 kap. 1 och 2 §§ OSL ger ett tillräckligt sekretesskydd för uppgifter om det allmännas affärs- och driftförhållanden.

Utredningen har övervägt om uppgifter som rör det allmännas affärs- och driftförhållanden skyddas i tillräcklig omfattning av befintlig reglering. Såväl myndigheter som bolag och andra aktörer där det allmänna utövar ett bestämmande inflytande kommer att omfattas av krav och möjligheter att rapportera incidenter och sårbarheter. Utredningen bedömer att det inte behöver införas något ytterligare sekretesskydd för uppgifter om offentlig verksamhets affärs- och driftförhållanden.

Enligt 19 kap. 1 § OSL gäller sekretess i en myndighets affärsverksamhet för uppgift om myndighetens affärs- eller driftförhållanden, om det kan antas att någon som driver likartad rörelse gynnas på myndighetens bekostnad om uppgiften röjs. Under motsvarande förutsättning gäller sekretess hos en myndighet för uppgift om affärs- eller driftförhållanden hos bolag, förening, samfällighet eller stiftelse som driver affärsverksamhet och där det allmänna genom myndigheten utövar ett bestämmande inflytande eller bedriver revision. Affärsverksamhet är antingen i sin helhet eller i en viss avgränsad del affärsinriktad och begreppet ska inte uppfattas alltför snävt. I första hand är det de statliga affärsdrivande verken som hör till myndigheter med affärsverksamhet, som Affärsverket svenska kraftnät, Luftfartsverket och Sjöfartsverket. Även myndigheter som i konkurrens med andra myndigheter eller enskilda åtar sig uppdrag omfattas. Även tillverkningsindustrin som bedrivs inom kriminalvården omfattas. På den kommunala sidan omfattas exempelvis affärsverk och hamnrörelser. Utlåningsverksamhet som bedrivs i affärsmässiga former, till exempel av Riksbanken och Allmänna pensionsfonden omfattas också (Lenberg m.fl., 2024, kommentaren till 19 kap. 1 § OSL).

I allmänhet ska verksamheten bedrivas utifrån krav på att den ska gå med vinst eller åtminstone gå ihop ekonomiskt. Det kan också vara affärsverksamhet om den är delvis subventionerad. I allmänhet ska det vara en verksamhet som inte kan sägas bestå i fullgörande

av en förvaltningsuppgift i snäv bemärkelse (Lenberg m.fl., 2024, kommentaren till 19 kap. 1 § OSL).

I 19 kap. 2 § OSL finns en bestämmelse om överföring av sekretess som innebär att om en myndighet får en uppgift som är sekretessreglerad i 19 kap. 1 § OSL från en annan myndighet, blir 1 § tillämplig på uppgiften också hos den mottagande myndigheten. Sekretessen gäller dock inte om uppgiften ingår i ett beslut av den mottagande myndigheten.

Med anledning av att dessa båda bestämmelser skyddar uppgifter om myndigheters affärs- eller driftförhållanden som synes täcka det behov av sekretess som finns för dessa uppgifter när de lämnas från en myndighet till en annan, behöver inte något ytterligare sekretesskydd införas.

4.4 Det finns behov att ändra vissa tidigare föreslagna bestämmelser

4.4.1 En sekretessbrytande bestämmelse

Utredningens förslag: Den i SOU 2024:64 föreslagna bestämmelsen i 15 kap. 3 c § OSL ändras så att hänvisningen till lagen (2025:000) om cybersäkerhet tas bort.

En ny sekretessbrytande bestämmelse förs in i 15 kap. OSL med följande lydelse.

Sekretessen enligt 1 a § hindrar inte att Försvarets radioanstalt lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om cybersäkerhet om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

Detsamma ska gälla när en tillsynsmyndighet lämnar sådana uppgifter till Försvarets radioanstalt.

En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

I avsnitt 13.3 i SOU 2024:64 lämnas ett förslag om en sekretessbrytande bestämmelse som ska bryta sekretessen enligt 15 kap. 1 a § OSL. Bestämmelsen skyddar uppgifter som en myndighet har fått från ett utländskt organ på grund av exempelvis en bindande

EU-rättsakt, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämrats om uppgiften röjs. Den utredningen bedömde att det behövs en sekretessbrytande bestämmelse för att möjliggöra ett informationsutbyte mellan MSB och tillsynsmyndigheterna, för att myndigheterna ska kunna fullgöra sina uppgifter.

Det saknas möjlighet för utredningen att göra en närmare självständig analys av behovet av en sådan bestämmelse. Utredningen ställer sig dock bakom de skäl som ligger till grund för förslaget i SOU 2024:64. Med anledning av att utredningen i kap. 3 föreslår att FRA ska utföra de uppgifter enligt NIS 2-direktivet som tidigare bedömts ska ligga på MSB så behöver en justering göras av den i SOU 2024:64 föreslagna bestämmelsen, för det fall att man överväger att gå vidare med det förslaget. Det mest ändamålsenliga sättet att reglera frågan är att bryta ut lagen om cybersäkerhet ur bestämmelsen och lägga till en ny bestämmelse direkt efter den tidigare föreslagna bestämmelsen, i 15 kap. OSL. Alternativet att göra justeringar i det tidigare förslaget framstår som mindre lämpligt då det riskerar att skapa otydlighet. Innebörden av bestämmelsen bör vara densamma som den som föreslås i SOU 2024:64, förutom att den gäller för FRA:s verksamhet (enligt den föreslagna lagen om cybersäkerhet).

4.4.2 Ytterligare ett förslag behöver ses över

Utredningens bedömning: Förslaget om en ny bestämmelse i 3 § OSF rörande diarium i SOU 2024:64 behöver ses över i samband med att FRA ska ta över uppgifter enligt förslaget till lag om cybersäkerhet.

I avsnitt 13.5 i SOU 2024:64 lämnas förslag om en ny bestämmelse i 3 § OSF rörande uppgifter i diarium som innehåller uppgifter om incidentrapportering enligt lagen om cybersäkerhet ska omfattas av sekretess. Det kan övervägas om det finns behov av en liknande bestämmelse för sådant diarium hos FRA. Behovet är kopplat till uppgifter som förekommer i diariet. Om utredningens förslag genomförs och FRA ska ta emot incidentrapporter enligt lagen om

cybersäkerhet torde samma överväganden göra sig gällande i fråga om det diarium som kommer att föras av FRA.

Denna omständighet får beaktas i den fortsatta beredningen av denna utrednings förslag och förslagen i SOU 2024:64.

4.5 Personuppgiftsbehandlingen hos NCSC

4.5.1 Olika regelverk styr personuppgiftsbehandlingen hos FRA

Utredningens bedömning: FRA:s behandling av personuppgifter inom NCSC styrs av EU:s dataskyddsförordning och lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Förhållandet mellan FRA-PuL och EU:s dataskyddsförordning

Det finns i huvudsak två olika regelverk som kan vara tillämpliga när FRA behandlar personuppgifter inom ramen för NCSC:s verksamhet. Det första regelverket är EU:s dataskyddsförordning med kompletterande nationella bestämmelser. Det andra regelverket utgörs av FRA:s egen registerlag, lag (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt (FRA-PuL), med tillhörande förordning (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt.

Enligt 2 § FRA-PuL tillämpas den lagen vid behandling av personuppgifter i försvarsunderrättelse- och utvecklingsverksamheten samt informationssäkerhetsverksamheten vid FRA. 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 in-

blandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser och ge annat tekniskt stöd. FRA ska även samverka med andra organisationer inom informations-säkerhetsområdet såväl inom som utom landet. FRA har vidare till uppgift enligt förordningen (2015:1053) om totalförsvaret och höjd beredskap att tilldela säkra kryptografiska funktioner till ett antal civila myndigheter och organisationer.

Det står klart att FRA-PuL ska tillämpas vid personuppgiftsbehandling inom FRA:s ovan nämnda verksamheter. Frågan är vilken lagstiftning som är tillämplig när NCSC, som finns inom FRA, behandlar personuppgifter. NCSC:s övergripande uppgift regleras i 4 a § FRA:s instruktion. Av bestämmelsen framgår att det inom FRA finns ett nationellt cybersäkerhetscenter med uppgift att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Utredningen föreslår vidare i kap. 3 att det ska införas en ny 4 b § i FRA:s instruktion om att FRA ska stödja och samordna arbetet med samhällets informationssäkerhet, med vissa närmare angivna uppgifter. Om det förslaget genomförs kommer även det innebära ett uppdrag som avser informationssäkerhet.

Om det generella regelverket för personuppgiftsbehandling ska tillämpas av NCSC så kan det i FRA:s verksamhet uppstå gränsdragningsfrågor när det kommer till arbetsuppgifter inom informationssäkerhetsområdet.

I den utredning som låg till grund för FRA-PuL uttrycktes följande rörande FRA:s informationssäkerhetsverksamhet.

Försvarets radioanstalt möjlighet att hantera de allvarligaste it-angrepen mot de mest skyddsvärda verksamheterna kräver en förmåga att upptäcka dessa samt att kartlägga bakomliggande aktörer. Signalspaning har en avgörande betydelse för att Försvarets radioanstalt ska kunna förse uppdragsgivare med unika underrättelser kring it-relaterade hot mot Sverige och svenska intressen. Samma underrättelser kan inom Försvarets radioanstalts informationssäkerhetsverksamhet om-sättas till indirekt och direkt skydd som omfattar såväl tekniska tjänster (exempelvis signalskydd, sensorsystem och informationssäkerhetsanalyser) som rådgivning och utbildning (SOU 2018:63 s. 102).

Utredningen bedömer att den dataskyddslagstiftning som är tillämplig inom NCSC:s verksamhet är den som grundar sig i EU:s dataskyddsförordning. För detta talar uttalanden i den utredning som låg till grund för FRA-PuL samt den omständigheten att 4 a § FRA:s

instruktion omfattar andra målgrupper än uppdraget enligt 4 § FRA:s instruktion. En omständighet som pekar i den riktningen är också att den verksamhet som bedrivs av NCSC, och tidigare i betänkan- det föreslås ska bedrivas av NCSC, till stor del utgörs av EU-reglerad verksamhet. Av artikel 2.12 i NIS 2-direktivet framgår att direktivet inte påverkar tillämpningen av bland annat EU:s dataskyddsförordning. Entiteter, behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av NIS 2-direktivet och i enlighet med EU:s dataskyddsförordning. I synnerhet ska behandlingen baseras på artikel 6 i EU:s dataskyddsförordning. Detta framgår uttryckligen av artikel 2.14 i NIS 2-direktivet. Även detta talar för att den personuppgiftsbehandling som NCSC ska utföra omfattas av EU:s dataskyddsförordning och regelverket kring den förordningen.

När det gäller förutsättningarna för personuppgiftsbehandling åligger det FRA att hålla isär den verksamhet som bedrivs på informationssäkerhetsområdet och omfattas av FRA-PuL:s tillämplighet 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 civila 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.

Förhållandet mellan brottsdatalagen och EU:s dataskyddsförordning

Utredningen har övervägt om brottsdatalagen (2018:1177) kan komma att bli tillämplig inom NCSC:s verksamhet. Utredningen bedömer dock att FRA inte ska anses vara en behörig myndighet i brottsdatalagens mening, då NCSC inte har sådana uppgifter att centret behandlar personuppgifter för syftena brottsbekämpning, lagföring, straffverkställighet eller upprättande av allmän ordning och säkerhet.

Vid viss behandling av personuppgifter gäller 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, nedan kallat dataskyddsdirektivet. I svensk rätt är dataskyddsdirektivet infört genom brottsdatalagen och brottsdataförordningen (2018:1202). Brottsdatalagen gäller vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. Den gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet (1 kap. 2 § brottsdatalagen).

Med behörig myndighet avses en myndighet som har till uppgift att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott, verkställa straffrättsliga påföljder, eller upprätthålla allmän ordning och säkerhet, när den behandlar personuppgifter för ett sådant syfte, eller en annan aktör som har anförtrots myndighetsutövning för ett syfte som anges i 1 kap. 1 §, när den behandlar personuppgifter för ett sådant syfte (1 kap. 6 § brottsdatalagen).

Avgörande för bedömningen av om en myndighet är behörig är om myndigheten har sådana uppgifter att den behandlar personuppgifter för syftena brottsbekämpning, lagföring, straffverkställighet eller upprättande av allmän ordning och säkerhet. Polismyndigheten, Tullverket, Kustbevakningen, Skatteverket, Ekobrottsmyndigheten, Åklagarmyndigheten, de allmänna domstolarna och Kriminalvården är behöriga myndigheter, men enbart när de behandlar personuppgifter för sådana syften (prop. 2017/18:232 s. 429). En myndighet kan därmed vara både behörig och icke behörig i lagens mening beroende på vilka uppgifter som utförs (ibid. s. 434).

När det gäller gränsdragningsfrågor mellan EU:s dataskyddsförordning och brottsdatalagen har regeringen uttalat att det är en fråga för rättstillämpningen att slutligt avgöra vilket regelverk för dataskydd som gäller i ett enskilt fall och att det inte är möjligt att inom ramen för lagstiftningsärendet rörande brottsdatalagen att ge klara svar på om vissa enskilda verksamheter eller arbetsuppgifter ska omfattas av brottsdatalagens tillämpningsområde eller inte. Det finns dock vissa utgångspunkter för bedömningen av när brottsdatalagen ska tillämpas. Om en myndighet har en skyldighet att anmäla

misstänkt brottslighet medför inte detta att anmälaren ska betraktas som behörig myndighet i brottsdatalagens mening, om anmälaren varken har ett brottsbekämpande uppdrag eller utövar myndighet för de syften som ramlagen omfattar (prop. 2017/18:232 s. 110–111).

Den verksamhet som NCSC ska bedriva enligt författning innebär inte att FRA ska anses vara en behörig myndighet i brottsdatalagens mening, när myndigheten behandlar personuppgifter för det syftet. De samverkansmyndigheter som i övrigt finns representerade hos NCSC kan i huvudsak inte anses som behöriga myndigheter i brottsdatalagens mening. Polismyndigheten betraktas dock i sin ordinarie verksamhet som en behörig myndighet. Beroende på om antalet deltagande myndigheter utökas i framtiden kan situationen uppkomma att det finns fler behöriga myndigheter representerade hos NCSC. I dag kan det vara så att vissa personuppgifter som behandlas av Polismyndigheten hos den myndigheten omfattas av brottsdatalagen, men kan komma att behandlas även av NCSC i samband med att information utbyts. Det kan konstateras att EU:s dataskyddsförordning är tillämplig redan på de behöriga myndigheternas behandling för att tillhandahålla personuppgifter till andra myndigheter, om ändamålet med behandlingen ligger utanför brottsdatalagens tillämpningsområde (prop. 2017/18:232 s. 132).

4.5.2 FRA behöver behandla personuppgifter inom ramen för NCSC:s verksamhet

Utredningens bedömning: FRA behöver behandla personuppgifter för att på ett ändamålsenligt sätt kunna utföra de uppdrag som ska utföras inom ramen för NCSC:s verksamhet.

FRA behöver utföra nödvändig behandling av uppgifter om brott.

Utredningen har ovan gjort bedömningen att EU:s dataskyddsförordning är tillämplig för NCSC:s verksamhet. Förordningen 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 prin-

ciper (se artikel 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 lokaliseringssuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

NCSC behöver behandla personuppgifter som avser utomstående personer som berörs av eller kommer i kontakt med NCSC. Det kan behöva ske inom ramen för samverkansforum med näringslivet eller deltagande vid konferenser och andra event som NCSC arrangerar. Personuppgifter kan också behöva behandlas i samband med extern information om NCSC:s verksamhet som en del av centrets uppdrag att förmedla råd och stöd avseende hot, sårbarheter och risker. Exempel på vilken typ av personuppgifter som NCSC behöver kunna behandla är namn, befattning, adressuppgifter, telefonnummer, e-postadresser, användarnamn, organisations-tillhörighet, foton, matallergier (kopplat till konferenser), IP-adresser samt kakor (cookies). En aktör kan också komma att lämna information om vilka personuppgifter som läckt ut i samband med en incident.

NCSC kan även komma att behandla sådana personuppgifter som omfattas av artikel 10 i EU:s dataskyddsförordning, alltså uppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott samt uppgifter om misstankar om brott. Som exempel kan nämnas att de incidentrapporter som lämnas in till NCSC kan innehålla uppgifter om cyberattacker. Dessa uppgifter kan falla inom tillämpningsområdet för brotten dataintrång eller försök till

dataintrång. Integritetsskyddsmyndigheten (IMY) har i beslut bedömt att uppgifter om IP-adresser i kombination med uppgift om att adressen använts dels vid försök till intrång eller genomförda intrång i internetbanker, dels i samband med intrångs- eller angreppsförsök eller tillgänglighets- och överbelastningsattacker mot en banks internetbank eller publika webbsidor, är sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning (IMY:s beslut den 18 mars 2008 i dnr 1402–2007 och den 20 januari 2015 i dnr 905–2014). FRA ska, i egenskap av CSIRT-enhet, övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå, vilket kan aktualisera behandling av sådana uppgifter om IP-adresser. Även realtidsövervakning av nätverks- och informationssystem kan aktualisera behandling av uppgifter om IP-adresser som kan utgöra sådana personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning (se artikel 11.3 i NIS 2-direktivet).

Enligt utredningens förslag till ändring av 14 § fjärde stycket förordningen (2022:524) om statliga myndigheters beredskap ska FRA, 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 (se avsnitt 3.3.5). Detta kan åtminstone utgöra en uppgift om misstanke om brott. Misstankar om brott omfattas vanligen av artikel 10 i EU:s dataskyddsförordning (se IMYRS 2021:1).

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

Utredningens förslag: Det ska införas en ny lag om behandling av personuppgifter i viss verksamhet vid FRA. Den nya lagen ska möjliggöra att FRA på ett ändamålsenligt sätt kan behandla personuppgifter samt säkerställa att EU:s dataskyddsförordnings krav på proportionalitet samt lämpliga och särskilda åtgärder för den registrerades grundläggande rättigheter och intressen efterlevs vid sådan behandling.

Det finns behov av en ny reglering

Utredningen har ovan gjort bedömningen att personuppgiftsbehandlingen i NCSC:s verksamhet sker med stöd av de generellt tillämpliga dataskyddsreglerna, med utgångspunkt i EU:s dataskyddsförordning. När det ska bedömas om den befintliga regleringen är tillräcklig för att ge stöd för personuppgiftsbehandlingen är utgångspunkten EU:s dataskyddsförordnings krav på proportionalitet (artikel 6.3) samt tydlighet, precision och förutsebarhet för de registrerade (skäl 41). Vid denna bedömning 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.

NCSC ska utgöra en nationell plattform för samverkan och informationsutbyte mellan såväl privata som offentliga aktörer i cybersäkerhetsfrågor. NCSC har också relativt breda uppdrag om att lämna råd och stöd till såväl privata som offentliga aktörer i frågor om cybersäkerhet. NCSC ska vidare genomföra bland annat utbildningar och övningar inom informations- och cybersäkerhetsområdet. Även i arbetet med att ta fram samlade lägesbilder kan personuppgifter behöva behandlas. Vidare kan kraven på samverkan innebära att personuppgifter behöver behandlas (2–3 och 5 §§ NCSC-förordningen). Uppdraget för centret är brett och det är därför svårt att fastställa vilka personuppgifter som NCSC behöver behandla. Generellt kan det dock sägas att IP-adresser, kontaktuppgifter till enskilda och uppgifter om hälsa behöver behandlas. Behandling av uppgifter om hälsa kan aktualiseras i exempelvis utbildnings- och övningssituationer. Uppgifter om hälsa utgör känsliga personuppgifter i EU:s dataskyddsförordnings mening. Uppgifter om IP-adresser eller liknande utgör inte känsliga personuppgifter. Men e-postadresser och användarnamn kan innehålla känsliga personuppgifter. Det kan också bli fråga om en relativt omfattande personuppgiftsbehandling 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 NCSC kommer också att ta del av personuppgifter som samlats in av andra aktörer. Som exempel kan nämnas uppgifter som ska lämnas enligt den föreslagna uppgiftsskyldigheten. Incidentrapporter från en aktör kan också innehålla uppgifter om exempelvis enskildas IP-adresser.

Utredningen anser att det utifrån EU:s dataskyddsförordnings krav på bland annat tydlighet och förutsebarhet för de registrerade, är lämpligt att NCSC:s behandling av personuppgifter regleras i en ny lag. För detta talar också effektivitetsskäl. Det finns en risk för att arbetet i NCSC inte kan bedrivas på önskvärt sätt om NCSC 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 NCSC får behandla vissa typer av personuppgifter. Eftersom NCSC behöver behandla känsliga personuppgifter, vilket utredningen återkommer till nedan, så behövs en särskild reglering som föreskriver anpassade skyddsåtgärder. Det generella regelverket föreskriver inte några sådana anpassade skyddsåtgärder.

I del 2 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) gjordes visserligen bedömningen att det inte behöver införas något nytt författningsstöd för behandlingen av personuppgifter i NCSC. Denna bedömning ifrågasattes av IMY i myndighetens remissvar till promemorian. Av remissvaret framgår att exempelvis en för myndigheterna gemensam och enhetlig ändamålsbestämmelse, antingen i en särskild registerförfattning eller i respektive myndighets registerförfattning innebära en ökad förutsägbarhet och tydlighet. IMY pekar i remissvaret också på att det i en särskild registerlag bland annat kan särregleras frågor om vilka kategorier av personuppgifter som får behandlas, hur länge de får sparas och vem som får ha åtkomst till dessa. Oavsett dessa påpekanden kan det konstateras att den tidigare bedömningen om behovet av utökad reglering av personuppgiftsbehandlingen baserades på att FRA skulle ta över huvudmannaskapet för NCSC. Men i detta betänkande föreslås att ett antal specifika arbetsuppgifter ska föras över till FRA och utföras inom centret, som exempelvis uppgiften att vara nationell CSIRT-enhet. Dessa omständigheter, tillsammans med omständigheten att den tidigare bedömningen baserades på delvis andra

förutsättningar om NCSC:s konstruktion talar ytterligare för att det behövs en ny registerlag.

Lagens syfte ska framgå

Utredningens förslag: Syftet med den nya lagen är dels att FRA får möjlighet att behandla personuppgifter på ett ändamålsenligt sätt, dels att skydda människor mot att deras personliga integritet kränks vid sådan behandling. Lagens dubbla syften ska framgå direkt av författningstexten.

Den nya lagstiftningen ska ha dubbla syften. Dels ska den möjliggöra en ändamålsenlig personuppgiftsbehandling när NCSC utför sina författningsreglerade uppdrag. Dels ska den skydda enskilda mot integritetsintrång. Även om syftesbestämmelsen saknar eget materiellt innehåll menar utredningen att den fyller en viktig funktion eftersom den ger vägledning gällande hur de materiella bestämmelserna ska tolkas. Syftesbestämmelsen innebär också ett tydliggörande av den rättsliga grunden för behandling av personuppgifter, det vill säga arbetsuppgifter som FRA utför inom ramen för NCSC.

Lagens tillämpningsområde

Utredningens förslag: Lagen ska gälla vid behandling av personuppgifter vid FRA när myndigheten utför uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter inom NCSC.

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

Bestämmelserna i lagen ska inte gälla vid behandling av personuppgifter som omfattas av lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt.

NCSC:s övergripande uppgifter framgår av 4 a § FRA:s instruktion. Centrets uppgifter beskrivs närmare i NCSC-förordningen. Det är

vidare utredningens uppfattning att de arbetsuppgifter som framgår av förslagen till 4 b-e §§ FRA:s instruktion ska utföras inom NCSC. Även i övrigt ska de nya arbetsuppgifter som föreslås utföras av FRA kunna utföras inom NCSC (se avsnitt 1.7–1.9). Utredningen har övervägt om den nya lagen enbart ska gälla när vissa arbetsuppgifter utförs. Det framstår dock inte som ändamålsenligt att avgränsa tillämpningen på det sättet. För att säkerställa att FRA kan utföra en ändamålsenlig personuppgiftsbehandling bör lagen gälla inom ramen för all verksamhet som bedrivs av NCSC. Med den skrivning som utredningen valt omfattas alla ovan nämnda arbetsuppgifter av den föreslagna registerlagen.

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. I detta avseende bedömer utredningen att den föreslagna lagen bör ha samma tillämpningsområde som EU:s dataskyddsförordning. Detta bör komma till uttryck i lagen.

I avsnitt 4.5.1 berörs förhållandet mellan FRA-PuL och EU:s dataskyddsförordning. I 1 kap. 4 § FRA-PuL 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 FRA-PuL bör det framgå av lagen att den inte ska tillämpas när FRA-PuL är tillämplig.

Lagen ska komplettera den allmänna dataskyddsregleringen

Utredningens förslag: Lagen ska innehålla bestämmelser som klargör att den kompletterar EU:s dataskyddsförordning. 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.

EU:s dataskyddsförordning är direkt tillämplig i svensk rätt. 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 enligt utredningen den nya lagens förhållande till förordningen och klargör att lagen inte kan tillämpas fristående, utan att den ska tillämpas tillsammans med förordningen.

Utredningen har övervägt behovet av en bestämmelse om att specialbestämmelser enligt den föreslagna lagen ska ges företräde framför de generella bestämmelserna i dataskyddslagen. Av 1 kap. 6 § dataskyddslagen följer dock direkt att dataskyddslagens bestämmelser är subsidiära i förhållande till annan lag eller förordning. Någon uttrycklig bestämmelse om detta behövs därför inte i den föreslagna lagen. Däremot finns det skäl att införa 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. Utredningen föreslår därför att detta framgår av den föreslagna lagen.

FRA ska vara personuppgiftsansvarig

Utredningens förslag: Det ska framgå av den nya lagen att FRA är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför enligt 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. FRA är personuppgiftsansvarig för den personuppgiftsbehandling som myndigheten utför inom ramen för NCSC:s verksamhet. Av tydlighetsskäl, inte minst i förhållande till enskilda, ska detta framgå direkt av lagen.

Ändamålen med behandlingen ska avgränsas

Utredningens förslag: FRA ska få behandla personuppgifter om det är nödvändigt för att FRA ska kunna utföra uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-inciden-ter inom NCSC.

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 bedömning: Att personuppgifter som omfattas av artikel 10 i EU:s dataskyddsförordning får behandlas behöver inte framgå av lagen.

Av 2 kap. 2 § 1 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 generellt vara uppgifter av allmänt intresse (prop. 2017/18:105 s. 56–57). FRA:s uppgifter inom ramen för NCSC utgör alltså uppgifter av allmänt intresse och det finns därför rättslig grund enligt artikel 6.1 e i EU:s dataskyddsförordning för sådan behandling av personuppgifter som är nödvändig för att utföra någon av dessa uppgifter. Det krävs också att personuppgiftsbehandlingen uppfyller de grundläggande principerna i artikel 5 i EU:s dataskyddsförordning. Dessa innebär bland annat 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 utgör därmed en form av åtgärd till skydd för personuppgif-

ter 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. Syftet 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. 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.

De primära ändamålen formuleras relativt brett 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 inte ett krav på att behandlingsåtgärden ska vara oundgänglig. Om behandlingen leder till effektivitetsvinster kan den anses nödvändig (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 (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 § 1 dataskyddslagen, inte fyller någon egentlig funktion i den föreslagna lagen. Det finns dock ett värde i att ändamålen anges uttryckligen. Bestämmelsen fungerar också som ett förtydligande för de registrerade, på så sätt att det framgår uttryckligen för vilka ändamål personuppgifter får behandlas. Vidare framstår det inte som önskvärt att avgränsa ändamålen i större utsträckning och ange mer konkreta,

uttryckliga ändamål än vad utredningen gjort. Anledningen till detta är att NCSC:s arbete spänner över ett brett område och måste kunna utföras så situationsstyrt och varierande som möjligt. En bred formulering innebär också att nya arbetsuppgifter som kan komma att aktualiseras 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 man inför bestämmelser som innebär att uppgifter ska eller får lämnas ut så 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 (2023:457) 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 bara 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 dem. 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 rymms inom den ram som den primära ändamålsbestämmelsen ställer upp.

Utredningen bedömer också att det ska 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 den så kallade finalitetsprincipen (artikel 5.1 b i EU:s dataskyddsförordning). Det följer av artikel 5.1 b i förordningen 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. Principen kommer även till uttryck i artikel 6.4, där det bland annat anges vad som i vissa fall ska beaktas vid en bedömning av om behandling för andra ändamål är förenlig med de ändamål för vilka personuppgifterna ursprungligen samlades in. Även den bestämmelsen ska därmed beaktas vid bedömningen av om behandlingen är förenlig med finalitetsprincipen. 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).

Även om EU:s dataskyddsförordnings bestämmelser om finalitetsprincipen är direkt tillämpliga i NCSC:s verksamhet talar tydlighetsskäl för att införa en bestämmelse som ger uttryck för principen (jfr prop. 2022/23:34 s. 128). Bestämmelsen ska ha samma innebörd som EU:s dataskyddsförordnings bestämmelse i artikel 5.1 b och bör 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 tillåta att insamlade personuppgifter behandlas för andra ändamål än det ursprungliga ändamålet. Det bör framhållas att det ytterst är FRA som personuppgiftsansvarig som måste bedöma om en behandling av personuppgifter är förenlig med finalitetsprincipen.

Av avsnitt 4.5.2 framgår att NCSC kan komma att behandla personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder (artikel 10 i EU:s dataskyddsförordning). Redan genom bestämmelsen i 3 kap. 8 § dataskyddslagen har NCSC rättslig grund för behandling av den typen av uppgifter. Det har inte framkommit något behov av att inskränka den möjligheten att behandla personuppgifter hos NCSC i förhållande till vad som gäller enligt den

allmänna regleringen. Därför finns inget behov av att reglera personuppgiftsbehandlingen i den delen särskilt i den föreslagna lagen.

Tillgången till personuppgifter ska begränsas

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

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 förordningens artikel 25.2 ska den personuppgiftsansvarige också genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, 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.

En fysisk person som utför arbete under den personuppgiftsansvariges överinseende, och som får tillgång till personuppgifter, får som utgångspunkt endast behandla dessa på instruktion från den personuppgiftsansvarige (artikel 29 i EU:s dataskyddsförordning). Den personuppgiftsansvarige ska vidta åtgärder för att säkerställa att personuppgifter inte behandlas utöver vad denne har gett instruktion om (artikel 32.4 i EU:s dataskyddsförordning). Den personuppgiftsansvarige har alltså ett ansvar för att anställda och andra uppdragstagare inte behandlar personuppgifter utöver vad denne har bedömt lämpligt.

Vilken spridning av personuppgifter som en viss behandling innebär har av naturliga skäl stor inverkan på integritetsriskerna med behandlingen. 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

FRA säkerställs att personuppgifter i NCSC:s 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 ska omfatta såväl tillsvidareanställd personal som exempelvis personer med tidsbegränsad anställning eller uppdragstagare. NCSC kan ha personal som deltar i centrets verksamhet och som kommer från någon av samverkansmyndigheterna. Alla dessa kategorier omfattas av uttrycket ”var och en”.

FRA ska 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 handläggnings-system eller motsvarande åtgärder. Ytterst är det FRA som i egen-skap av personuppgiftsansvarig har ansvar för att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att personuppgifter inte sprids i större omfattning än som är nödvändigt.

Känsliga personuppgifter får behandlas

Utredningens förslag: FRA ska få behandla känsliga personuppgifter, om det är nödvändigt med hänsyn till ändamålet med behandlingen.

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, biometrisk uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (artikel 9.1 i förordningen).

Förbudet kompletteras dock av ett antal undantag. Som exempel kan nämnas 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 förenlig med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättig-

heter och intressen (artikel 9.2 g). Den nu nämnda artikeln är direkt tillämplig, men det är möjligt för medlemsstaterna att i nationell rätt införa mer specifika bestämmelser avseende känsliga personuppgifter (artikel 6.2 och skäl 10 till EU:s dataskyddsförordning). Enligt artikel 9.4 får medlemsstater också behålla eller införa ytterligare villkor, även begränsningar, för behandlingen av genetiska eller biometriskt uppgifter eller uppgifter om hälsa.

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 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.

Utredningen bedömer att NCSC kan komma att behöva behandla känsliga personuppgifter, i en inte ringa omfattning. NCSC kommer att ha ett 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 indirekt avslöja en företrädares etniska ursprung. Anmälaren kan också vara en politisk eller religiös organisation. Även i en sådan situation kan NCSC 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.

Däremot är det bara under vissa förutsättningar som foton på människor utgör en känslig personuppgift, eftersom sådana foton bara är biometriskt uppgifter när de behandlas med teknik som möjliggör identifiering eller autentisering av en person (skäl 51 till EU:s dataskyddsförordning). Som exempel kan nämnas teknik för ansiktsigenkänning.

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 är ett allmänt intresse (alltså uttrycket som används i artikel 6.1 e i förordningen), respektive ett viktigt allmänt intresse (som används i artikel 9.2 g i förordningen), är inte definierat i EU:s dataskyddsförordning. 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 (prop. 2017/18:105 s. 83).

NCSC:s uppgifter framgår av dels FRA:s instruktion, dels NCSC-förordningen. Syftet med NCSC:s behandling av personuppgifter, i vilken känsliga personuppgifter kan ingå, är att utföra de författningsreglerade arbetsuppgifterna. När 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. Behandlingen av känsliga personuppgifter är därmed motiverad med hänsyn till ett viktigt allmänintresse.

När det gäller myndigheternas materiella verksamhetsreglering som fastställts i svensk rätt bör utgångspunkten vara att denna uppfyller kraven på proportionalitet i artikel 6.1 c och e i EU:s dataskyddsförordning (prop. 2017/18:105 s. 50). Artikel 9.2 g ställer krav på att behandlingen av känsliga personuppgifter av hänsyn till ett viktigt allmänt intresse ska ske på grundval av unionsrätten eller medlemsstaternas nationella rätt, vilken ska stå i proportion till det eftersträfvade syftet. Regeringen har tidigare uttalat att detta innebär att den rättsliga grunden för behandlingen typiskt sett kommer att vara någon av de som avses i artikel 6.1 c eller e (a. prop. s. 84). Det innebär att artikel 9.2 g bör tolkas så att det är den materiella verksamhetsregleringen vilken reglerar myndigheternas uppgifter, och

därmed det viktiga allmänna intresset, som ska ligga till grund för behandlingen och vara proportionerlig, vilket den som utgångspunkt kan anses vara i svensk rätt.

EU:s dataskyddsförordning ställer också krav på det rättsliga stödet, vilket måste vara förenligt med det väsentliga innehållet i rätten till dataskydd. Regeringen har 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. 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 (prop. 2017/18:105 s. 84). 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. Utredningen föreslår bestämmelser om olika former av 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 utredningen föreslår utgör en sådan skyddsåtgärd.

Sammantaget innebär det att den behandling som FRA behöver utföra av känsliga personuppgifter uppfyller kraven i artikel 9.2 g i EU:s dataskyddsförordning. Att FRA får behandla känsliga personuppgifter ska framgå av den föreslagna lagen.

Hänvisningar till en EU-rättsakt kan göras antingen statiska eller dynamiska. En dynamisk hänvisning innebär att hänvisningen avser EU-rättsakten i den vid varje tidpunkt gällande lydelsen. En statisk hänvisning innebär att hänvisningen avser EU-rättsakten i en viss angiven lydelse. Bestämmelsens hänvisning till EU:s dataskyddsförordning bör vara dynamisk för att säkerställa att änd-

ringar i EU-regleringen får omedelbart genomslag (jfr prop. 2017/18:105 s. 25–26).

Det ska vara förbjudet att utföra vissa sökningar

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

Utredningens bedömning: Behandling av personuppgifter som omfattas av artikel 10 i EU:s dataskyddsförordning och som FRA behöver utföra inom ramen för NCSC:s verksamhet bör inte begränsas.

Sökningar som tar sikte på känsliga personuppgifter är typiskt sett förknippade med särskilda risker i integritetshänseende (jfr prop. 2018/19:33 s. 132). Det finns ett generellt förbud mot att utföra sökningar i syfte att få fram ett urval av personer grundat på känsliga personuppgifter i 3 kap. 3 § andra stycket dataskyddslagen. 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 (a. prop. s. 132).

Det har inte framkommit något behov för NCSC att använda sökbegrepp som avser känsliga personuppgifter. Som utgångspunkt gäller att NCSC inte ska få utföra den typ av sökningar som syftar att få fram ett personurval grundat på känsliga personuppgifter. Det ska därför framgå av lagen att det är förbjudet att utföra sökningar i syfte att få fram detta. 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 dessa uppgifter.

Det bör noteras att bestämmelsen inte hindrar sökningar som görs i ett annat syfte än att få fram ett urval av personer. Som exempel kan nämnas att sökningar görs med syftet att ta fram verksamhetsstatistik eller för registervård.

Utredningen har även övervägt om det bör införas en sökbegränsning för uppgifter om lagöverträdelser enligt artikel 10 i EU:s data-

skyddsförordning. Något motsvarande generellt förbud mot att utföra sökningar i syfte att få fram ett urval av personer grundat på den typen av uppgifter finns dock inte. Utredningen vill också betona att behandling av personuppgifter ska vara nödvändig, och uppgifterna ska vara adekvata och relevanta i förhållande till ändamålet (artikel 5 i EU:s dataskyddsförordning). Utrymmet för FRA att behandla personuppgifter som omfattas av artikel 10 i EU:s dataskyddsförordning inom ramen för NCSC:s verksamhet är således avgränsat.

Utredningen har i avsnitt 4.5.2 konstaterat att FRA behöver utföra nödvändig behandling av uppgifter om lagöverträdelser. Det kan till exempel handla om uppgifter om IP-adresser i kombination med uppgifter om att adressen använts vid ett dataintrång. Det går dock inte fullt ut att förutse eller i författning avgränsa den behandling som FRA behöver kunna göra för att utföra sina författningsreglerade uppdrag inom NCSC.

Därtill gäller begränsningar enligt den föreslagna registerlagen, som tillgången till personuppgifter. Utredningen gör bedömningen att de grundläggande krav på personuppgiftsbehandlingen som anges i den allmänna dataskyddsrättsliga regleringen och den föreslagna registerlagen är en tillräcklig begränsning för FRA:s möjlighet att behandla uppgifter om lagöverträdelser inom ramen för NCSC:s verksamhet. I sammanhanget kan nämnas att de aktuella personuppgifterna också kommer att säkerställas ett skydd genom befintlig och föreslagen sekretessreglering.

Personuppgifter får lämnas ut elektroniskt

Utredningens förslag: Personuppgifter får lämnas ut elektroniskt på annat sätt än genom direktåtkomst om det inte är olämpligt.

NCSC behöver ha effektiva och tidsenliga former för utlämnande av information, inklusive personuppgifter. 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, andra interna-

tionella aktörer och vid kommunikation med det privata näringslivet. Det finns stora effektivitetsvinster med att låta 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 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 nationellt 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 (även kallat utlämnande på medium för automatiserad behandling). Dessa två former av elektroniskt utlämnande får ur integritetssynpunkt olika effekter.

Det finns inte någon legaldefinition av begreppet 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 kan generellt sägas öka riskerna för intrång i den personliga integriteten, eftersom den typiskt sett innebär att uppgifterna blir tillgängliga för fler personer och att den utlämnande myndighetens möjlighet att kontrollera utlämnandet minskar.

Uttrycken ”annat elektroniskt utlämnande” och ”utlämnande på medium för automatiserad behandling” har samma innebörd. Det förra 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 (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. Direktåtkomst innebär dels en större integritetsrisk, dels att uppgifter i en allmän handling som en myndighet har åtkomst till blir del av allmänna handlingar hos den myndigheten. Att reglera en möjlighet till direktåtkomst bör endast komma i fråga om det finns ett tydligt behov av det. Det har inte framkommit något sådant tydligt behov. 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 bestämmelsen formuleras som att utlämnande får 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 har betydelse för om ett utlämnande är olämpligt. Typiskt sett kan det inte anses olämpligt att lämna ut uppgifter elektroniskt till en myndighet. När det gäller utlämnandet till andra än svenska myndigheter krävs en mer nyanserad bedömning med hänsyn till bland annat innehållet i handlingen och vem (till exempel en organisation eller ett företag) som är mottagare. Om FRA bedömer att det finns en risk för att uppgifterna missbrukas om de lämnas ut elektroniskt kan det vara olämpligt att lämna ut dem på det sättet. Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informations-säkerheten, det vill säga säkerheten hos mottagaren, vägas in. Att FRA som personuppgiftsansvarig är skyldig att säkerställa att bland annat adekvata tekniska och organisatoriska åtgärder har vidtagits följer vidare 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.

Utredningen vill också peka på bestämmelsen i 21 kap. 7 § OSL som innebär att det gäller sekretess för uppgifterna om mottagaren kan antas komma att behandla uppgifterna på ett sätt som står i strid med bland annat EU:s dataskyddsförordning. I ett sådant fall får uppgifterna inte lämnas ut över huvud taget, vare sig i analog form eller elektroniskt.

Tiden som personuppgifter får behandlas ska begränsas

Utredningens förslag: Personuppgifter får inte behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Detta hindrar inte att FRA arkiverar och bevarar allmänna handlingar eller att arkivmaterial lämnas till en arkivmyndighet.

Gallring enligt registerförfattningar syftar till att skydda enskildas personliga integritet genom att det föreskrivs när den automatiserade behandlingen av personuppgifter ska upphöra. Vid all personuppgiftsbehandling är det ett grundläggande krav 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. Utredningen bedömer att det bör införas sådana bestämmelser i den nya lagen.

Det är svårt att på ett generellt plan uttala sig om hur länge det kan vara nödvändigt att lagra uppgifter i NCSC:s verksamhet. När det är fråga om konferenser eller liknande event kan det vara så att det inte längre är nödvändigt att behandla deltagares uppgifter om allergier eller liknande i samband med att konferensen är avslutad. När det gäller exempelvis IP-adresser kopplade till incidenter, kan det finnas behov av att lagra uppgifterna under en längre tid. Även om ingen faktisk längsta tid för personuppgiftsbehandling anges i lagen så finns det ett värde i att lagen anger att personuppgifter inte får behandlas längre än vad som är nödvändigt med hänsyn till ändamålet. Det som avses då 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 behovet kvarstår. Den generella bestämmelsen säkerställer att personuppgifter inte behandlas under en längre tid än vad som är nödvändigt utifrån de ändamål som NCSC får behandla personuppgifter.

EU:s dataskyddsförordning innehåller ett undantag från principen om lagringsminimering, som innebär att personuppgifter får lagras under längre perioder i den mån som 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 därför 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.

Rätten att göra invändningar ska inte gälla

Utredningens 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 den nya lagen eller föreskrifter som har meddelats i anslutning till lagen.

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. Den personuppgiftsansvarige får då inte längre behandla personuppgifterna om inte denne kan visa avgörande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter (artikel 21.1 i EU:s dataskyddsförordning). 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 denna rätt 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 syfte att säkerställa olika uppräknade intressen, bland annat den allmänna säkerheten, förebyggande eller förhindrande av brott eller andra viktiga mål av generell 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. 122–123 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 FRA utför för att fullgöra uppgiften enligt 4 a § FRA:s instruktion genomförs för att utföra en uppgift av allmänt intresse. EU:s dataskyddsförordnings bestämmelse 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 de författningsreglerade uppdrag som ålagts myndigheten inom ramen för NCSC. FRA kan därmed behöva hantera personuppgifter oavsett den registrerades inställning. Så länge personuppgiftsbehandlingen sker för de ändamål som stadgas i den föreslagna registerlagen 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 registre-

rade att invända mot behandling av personuppgifter kan dock ändå tänkas påverka effektiviteten i NCSC:s verksamhet.

För att säkerställa förutsättningarna för NCSC 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. Utredningen bedömer därför att den föreslagna lagen uppfyller även de krav som uppställs i artikel 23.1 i EU:s dataskyddsförordning.

Hänvisningen till EU:s dataskyddsförordning bör vidare vara dynamisk för att säkerställa att ändringar i regleringen får omedelbart genomslag.

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

Utredningens 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 från någon annan än den registrerade själv. Det saknas behov av ytterligare bestämmelser som begränsar rätten.

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, se 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 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 (prop. 2017/18:298 s. 110).

Den uppgiftsdelning som kommer att ske från myndigheter till NCSC inom ramen för centrets verksamhet kommer att grunda sig på den uppgiftsskyldighet som föreslås av utredningen, när det handlar om annars sekretessbelagda uppgifter som lämnas av myndigheter som samverkar med centret. Ytterst grundar sig uppgiftslämnandet 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 (prop. 2017/18:298 s. 111–112).

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 och prop. 2017/18:115 s. 25). 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. Det finns också ett antal bestämmelser som skyddar den registrerades personliga integritet när NCSC behandlar personuppgifter, till exempel genom bestämmelser om sök-

och behörighetsbegränsningar. Uppgifterna kan också komma att vara sekretessbelagda enligt den sekretessbestämmelse som föreslås. 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 inom lagens tillämpningsområde. Det behövs därför inte någon ytterligare lagstiftningsåtgärd för att NCSC ska kunna tillämpa undantaget.

Ibland kan personuppgifter som lämnas till NCSC av en annan aktör, som 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 detta andra syfte. I den mån utlämnandet av personuppgifter till 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 NCSC ha en skyldighet att upplysa den person som uppgifterna avser om detta. Huruvida denna omständighet är problematisk eller inte har inte framkommit. Det är inte heller möjligt att, inom ramen för den här utredningen, 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.

Rätten att meddela föreskrifter behöver inte framgå

Utredningens bedömning: Det finns inte skäl att införa en bestämmelse som upplyser om att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter som kompletterar den nya lagen.

Utredningen har inte identifierat något konkret behov av att komplettera lagen med bestämmelser i förordning eller föreskrifter. Det kan dock inte uteslutas att ett sådant behov uppkommer. Bestämmelser om myndigheternas personuppgiftsbehandling anses normalt falla in under regeringens så kallades restkompetens i 8 kap. 7 § regeringsformen. Regeringen eller den myndighet som regeringen bestämmer har alltså möjlighet att meddela kompletterande bestämmelser till den föreslagna lagen, så länge de inte är sådana som avses i 2 kap. 6 § andra stycket regeringsformen (jfr prop. 2017/18:105 s. 26). Utredningen har övervägt om det finns behov av att införa en upplysningsbestämmelse om regeringens rätt att meddela föreskrifter men har kommit fram till att det inte är behövligt.

IMY är tillsynsmyndighet

IMY är tillsynsmyndighet enligt FRA-PuL. Myndigheten har samma roll när det gäller EU:s dataskyddsförordning och dataskyddslagen. Detta framgår av 2 a § förordning (2007:975) med instruktion för IMY samt 3 § förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. Myndigheten kommer alltså även att utöva tillsyn när det gäller FRA:s personuppgiftsbehandling inom ramen för NCSC.

4.6 Integritetsrisker

4.6.1 En integritetsanalys ska göras i lagstiftningsarbetet

En viktig del av integritetsanalysen i lagstiftningsarbetet är bedömningen av om konsekvenserna för den personliga integriteten är nödvändiga och proportionerliga i förhållande till det man avser att uppnå med lagstiftningsåtgärden. För att utredningen ska kunna

göra en proportionalitetsbedömning måste integritetsriskerna kartläggas. Utredningen har använt sig av IMY:s vägledning för integritetsanalys i lagstiftningsarbete (IMY-2022-10835). Utredningen redogör i det följande för de risker för enskilda som förslagen medför. Det författningsförslag som är viktigast att analysera i sammanhanget är det om en ny lag om uppgiftsskyldighet. Men även förslaget om en så kallad registerlag för FRA:s personuppgiftsbehandling inom NCSC:s verksamhet genererar personuppgiftsbehandling. Utredningens analys avser samtliga förslag som lämnas. I de fall bedömningarna gäller något specifikt förslag så anges det särskilt i texten.

4.6.2 Förslagen medför en utökad behandling av personuppgifter

Utredningens bedömning: Förslagen medför en utökad behandling av personuppgifter.

Förslaget om en uppgiftsskyldighet inom ramen för NCSC innebär inte i sig att myndigheter kommer att vara skyldiga att utföra någon ny eller utökad personuppgiftsbehandling. Uppgifter kan också lämnas ut anonymiserat eller utan att personuppgifter över huvud taget förekommer. Det är dock rimligt att anta att uppgiftsskyldigheten kommer att innebära att fler personuppgifter utbyts mellan de i NCSC samverkande myndigheterna. När det gäller förslaget om en registerlag för personuppgiftsbehandlingen inom NCSC så kan även detta sägas innebära en utökad personuppgiftsbehandling. Exempelvis ges ett uttryckligt stöd för behandlingen av känsliga personuppgifter. Som utredningen återkommer till nedan så utgör registerlagen också en skyddsåtgärd för enskilda.

För att myndigheter ska kunna lämna ut uppgifter med stöd av lagen om uppgiftsskyldighet behöver de behandla personuppgifter i större utsträckning än vad de gör i dag. Förutom själva utlämnandet av uppgifter kan till exempel strukturering, kontroll, bearbetning och justering av uppgifter behöva göras, vilket alltsammans innebär personuppgiftsbehandling.

När myndigheter tar emot personuppgifter behöver de i sin tur behandla personuppgifter i större utsträckning än vad de gör i dag

eftersom de kommer att samla in och därefter bearbeta uppgifterna som de får från andra myndigheter. I sammanhanget kan det arkivrättsliga regelverket nämnas, vilket bland annat medför att mottagande myndigheter som utgångspunkt måste behandla inkomna uppgifter i sina arkiv.

Myndigheter kan alltså behöva behandla personuppgifter i flera led när uppgifter utbyts med stöd av uppgiftsskyldigheten. I vissa fall kan det vara fråga om en utökad behandling i jämförelse med den behandling i form av informationsutbyte och annan behandling som är förknippad med utbytet, som sker i dag. Som exempel kan nämnas informationsutbyte som sker med stöd av befintlig reglering. I andra fall, där själva informationsutbytet i dag inte får ske med stöd av befintlig reglering, kommer det att vara fråga om en helt ny personuppgiftsbehandling som myndigheterna inte tidigare haft någon rättslig grund för att utföra genom utbyte med andra myndigheter.

Sammantaget kommer personuppgiftsbehandlingen att öka när myndigheter tillämpar uppgiftsskyldigheten.

Förslaget om en registerlag för NCSC:s verksamhet innebär också att FRA får utökade möjligheter att behandla personuppgifter, jämfört med vad som gäller i dag. Det kan dock konstateras att myndigheter redan med befintlig reglering kan behandla personuppgifter. Med tanke på att registerlagen utökar FRA:s möjligheter att behandla personuppgifter får det dock förutsättas att personuppgiftsbehandlingen kommer att öka även med anledning av det förslaget.

4.6.3 Integritetsrisker aktualiseras som en följd av förslagen

Utredningens bedömning: Utökade skyldigheter att utbyta information mellan myndigheter innebär en generellt förhöjd risk för intrång i den personliga integriteten (integritetsrisk).

Förslaget om en uppgiftsskyldighet innebär att olika typer av personuppgifter kommer att behandlas. Det rör sig i begränsad omfattning om integritetskänslig personuppgiftsbehandling. Behandling av känsliga personuppgifter och uppgifter om lagöverträdelse kommer att aktualiseras. Det finns därmed integritetsrisker med behandlingen.

Det finns en generell förhöjd integritetsrisk med förslaget om uppgiftsskyldighet

Förslaget om en ny lag om uppgiftsskyldighet innebär att myndigheter kommer att utbyta fler sekretessreglerade uppgifter med varandra. Det kan dock konstateras att det i större utsträckning kommer att utbytas uppgifter som omfattas av sekretess till skydd för allmänna intressen, än till skydd för enskilda intressen. Detta utesluter dock inte att det kan vara fråga om att behandla personuppgifter. Uppgiftsskyldigheten möjliggör alltså utbyte av personuppgifter, det vill säga upplysningar som avser en identifierad eller identifierbar fysisk person (artikel 4.1 i EU:s dataskyddsförordning). Insamlande och utlämnande är exempel på åtgärder som utgör behandling av personuppgifter. Personuppgiftsbehandling är dock ett vidsträckt begrepp som även omfattar registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring av personuppgifter (artikel 4.2 i EU:s dataskyddsförordning).

Vid personuppgiftsbehandling måste flera regelverk följas för att värna den personliga integriteten. Någon enhetlig definition av begreppet 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 begreppet 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 lagöverträdelse anges också särskilt. Det anges också kunna föreligga integritetsrisker om det sker behandling 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 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.

Att avgöra omfattningen av den personuppgiftsbehandling som aktualiseras av förslaget om uppgiftsskyldighet är förenat med viss osäkerhet. Syftet är att information ska delas i större utsträckning mellan NCSC och samverkansmyndigheterna än vad som sker i dag.

Bestämmelsen om uppgiftsskyldighet innehåller inte någon avgränsning till en eller flera särskilda uppgiftskategorier utan endast en avgränsning till i vilket syfte uppgiften behövs hos mottagande myndighet. 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 vilken/vilka myndighet/er som tar del av vilka uppgifter, syftet med informationsutbytet, eventuell sekretess hos mottagaren eller NCSC samt eventuella skyldigheter för mottagaren att i sin tur lämna uppgifter vidare till andra aktörer.

Spridningen av personuppgifter kommer att ske inom den offentliga sektorn. Myndigheterna är genom dataskyddsreglerna och legalitetsprincipen förhindrade att behandla andra eller fler uppgifter än de som krävs för att utföra sina författningsreglerade verksamheter. De fysiska personer som kommer att kunna ta del av uppgifterna är vidare i första hand personer som arbetar inom den offentliga sektorn. Myndigheter har i det sammanhanget en skyldighet att se till att dess medarbetare inte behandlar personuppgifter på annat sätt än på instruktion av myndigheten (artikel 32.4 i EU:s dataskyddsförordning).

Behandling av känsliga personuppgifter och uppgifter om lagöverträdelser innebär en särskild risk

En viss del av personuppgiftsbehandlingen som behöver utföras med anledning av såväl förslaget om en uppgiftsskyldighet som förslaget om en ny registerlag kommer att avse känsliga person-

uppgifter och uppgifter om lagöverträdelser. En stor del av informationsutbytet inom ramen för NCSC:s verksamhet kommer dock att kunna ske i anonymiserad form. Även om förslagen inte utesluter att uppgifter som rör särskilt skyddsvärda grupper kan komma att behandlas, som personer med skyddade personuppgifter och barn, så har inte utredningen identifierat några särskilda situationer där förslagen skulle kunna leda till sådan behandling. Sådan personuppgiftsbehandling torde därmed ske i begränsad omfattning till följd av förslagen.

Som utredningen identifierat tidigare så kan det vara aktuellt med behandling av personuppgifter som avser uppgifter om lagöverträdelser (artikel 10 i EU:s dataskyddsförordning). Uppgiftsskyldigheten innebär dock inte i sig att myndigheter som saknar legitima skäl att behandla uppgifter om lagöverträdelser ges en rättslig möjlighet att göra det.

Även om behandling av känsliga personuppgifter och uppgifter om lagöverträdelser kan förväntas ske i begränsad omfattning så innebär förslagen ändå en särskild risk i detta avseende.

4.6.4 Omfattningen av personuppgiftsbehandlingen

Utredningens bedömning: Den personuppgiftsbehandling som möjliggörs genom förslagen kan bli omfattande och avse uppgifter om ett stort antal personer.

Den föreslagna uppgiftsskyldigheten innebär att NCSC och samverkansmyndigheterna får en helt ny och förenklad reglering av när uppgifter får utbytas inom centret. Uppgiftsskyldigheten är dock begränsad till när det finns ett behov hos den mottagande myndigheten för att den ska kunna delta i centrets verksamhet. Regleringen förväntas inte i första hand träffa uppgifter om enskilda, men att en sådan reglering kan medföra en omfattande personuppgiftsbehandling är tydligt. Någon närmare beskrivning av den förväntade totala omfattningen av personuppgiftsbehandlingen som uppgiftsskyldigheten kan ge upphov till är dock svår att göra. Även om förutsättningarna för utlämnande i och för sig är uppfyllda enligt det första steget i prövningen kan den intresseavvägning som ska göras innebära att uppgifterna ändå inte lämnas ut. Uppgiftsskyldigheten

syftar dock till att på ett tydligt sätt förenkla förutsättningarna för att lämna information mellan de i NCSC samverkande myndigheterna. Att personuppgiftsbehandlingen kan komma att öka måste dock förutsättas.

Uppgiftsskyldigheten har ett relativt brett tillämpningsområde. Men den är avsedd att tillämpas i särskilda situationer då uppgifterna behövs för att NCSC ska kunna bedriva sin verksamhet och närmare bestämt för att mottagande myndighet ska kunna delta i samverkan inom ramen för NCSC. Behovet är kopplat till ett konkret behov hos mottagaren. Tanken är inte att informationsdelning ska 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 NCSC:s verksamhet.

När det gäller förslaget om en lag om personuppgiftsbehandling så kommer även den ge ökade möjligheter att behandla personuppgifter, och det kan förutsättas att omfattningen av FRA:s personuppgiftsbehandling ökar med anledning av förslaget.

4.6.5 Det finns skyddsåtgärder

Utredningens bedömning: Det finns skyddsåtgärder som begränsar integritetsriskerna.

Begreppet skyddsåtgärder förekommer i olika sammanhang i EU:s dataskyddsförordning. Begreppet 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 (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.

Den nya uppgiftsskyldigheten uppställer villkor som inskränker skyldigheten att dela information. De specifika kraven som ställs för ett utlämnande begränsar på det sättet integritetsintrånget och är att betrakta som en skyddsåtgärd. Det är endast i situationer då en myndighet har behov av uppgiften för sitt deltagande i den reglerade samverkan som ska ske inom ramen för NCSC:s verksamhet som uppgiften ska lämnas ut. Den intresseavvägning som ska göras inför ett utlämnande av uppgifter innebär en ytterligare begränsning till skydd för enskildas personliga integritet. Som utgångspunkt kommer de uppgifter som lämnas mellan myndigheterna inom ramen för NCSC:s verksamhet att omfattas av sekretess – antingen sekretess som är tillämplig oavsett var uppgiften förekommer, eller sekretess till följd av den bestämmelse som föreslås. Detta utgör också en skyddsåtgärd som begränsar integritetsintrånget. Den föreslagna lagen som reglerar FRA:s personuppgiftsbehandling inom ramen för NCSC:s verksamhet utgör ytterligare en skyddsåtgärd. I den föreslås särskilda villkor för behandling av känsliga personuppgifter och en bestämmelse om sökbegränsningar.

Det finns alltså flera skyddsåtgärder som begränsar integritetsriskerna. I den slutliga proportionalitetsbedömningen görs också bedömningen att skyddsåtgärderna är tillräckliga och adekvata.

4.6.6 Ny rättslig grund för personuppgiftsbehandling

Utredningens bedömning: Förslaget om uppgiftsskyldighet inom ramen för NCSC:s verksamhet utgör ett fastställande av den rättsliga grunden rättslig förpliktelse och uppgift av allmänt intresse (artikel 6.1 c och e i EU:s dataskyddsförordning) för den personuppgiftsbehandling som ett utlämnande mellan myndigheter i enlighet med bestämmelsen utgör.

De rättsliga grunderna fastställs i svensk rätt på det sätt som krävs enligt artikel 6.3 första stycket punkten b i EU:s dataskyddsförordning, 2 kap. 1 och 2 §§ dataskyddslagen och skäl 41 i EU:s dataskyddsförordning. Bestämmelsen uppfyller ett mål av allmänt intresse och är proportionell mot det legitima mål som eftersträvas i enlighet med artikel 6.3 andra stycket sista meningen i EU:s dataskyddsförordning.

En grundläggande förutsättning för att behandling av personuppgifter ska vara laglig och tillåten är att det finns en rättslig grund för den behandling som utlämnandet innebär enligt EU:s dataskyddsförordning. Begreppet rättslig grund används i två betydelser; dels som en benämning av de villkor för laglighet som anges i artikel 6.1 i EU:s dataskyddsförordning, dels som en benämning av den reglering i unionsrätt eller nationellt rätt som fastställs enligt artikel 6.3 i förordningen.

Den föreslagna uppgiftsskyldigheten har för det första stöd i den rättsliga grunden behandling som är nödvändig för att utföra en rättslig förpliktelse (artikel 6.1 c i EU:s dataskyddsförordning). Enligt artikel 6.3 andra stycket första meningen i förordningen ska syftet med behandlingen fastställas i den rättsliga grunden då denna grundar sig på en rättslig förpliktelse. Det ska alltså vara möjligt för såväl den personuppgiftsansvarige som den registrerade att förstå varför behandlingen av personuppgifter ska ske (prop. 2017/18:105 s. 54). Av utredningens förslag framgår att syftet med uppgiftsskyldigheten är att uppgiftslämnande ska ske om uppgiften behövs för att en myndighet ska kunna delta i NCSC:s verksamhet. Förslaget uppfyller därmed kravet på ett fastställt syfte.

I 2 kap. 1 § dataskyddslagen tydliggörs att personuppgifter får 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. Den föreslagna uppgiftsskyldigheten uppfyller även detta krav.

Personuppgiftsbehandlingen som ett utlämnande innebär uppfyller även kravet på att vara nödvändig för att utföra en uppgift av allmänt intresse. Syftet med den föreslagna uppgiftsskyldigheten är att betydelsefull information ska kunna lämnas mellan NCSC och samverkansmyndigheterna. Alla uppgifter som riksdag eller regering gett i uppdrag åt statliga myndigheter att utföra är av allmänt intresse (prop. 2017/18:105 s. 57). Förslaget har därmed även stöd i den rättsliga grunden i artikel 6.1 e i EU:s dataskyddsförordning.

Gällande kraven enligt skäl 41 i EU:s dataskyddsförordning så är det tydligt för de enskilda som kan beröras av uppgiftsskyldigheten att uppgifter som lämnats till en myndighet kan komma att lämnas ut till en annan myndighet om förutsättningarna enligt uppgiftsskyldigheten är uppfyllda. Bestämmelsen är tillräckligt tydlig och precis och tillämpningen av den är tillräckligt förutsebar.

Den föreslagna uppgiftsskyldigheten är också proportionell mot det legitima mål som eftersträvas i enlighet med artikel 6.3 andra stycket sista meningen i EU:s dataskyddsförordning. Utredningen återkommer till frågan om proportionalitet i avsnitt 4.6.9.

4.6.7 Förslaget innebär att vidarebehandling av personuppgifter kommer att ske

Utredningens bedömning: Den vidarebehandling som följer av att uppgifter lämnas ut enligt förslaget om uppgiftsskyldighet utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda ett mål som avses i artikel 23.1 i EU:s dataskyddsförordning.

Inför ett utlämnande av uppgifter med stöd av den föreslagna uppgiftsskyldigheten behöver en myndighet inte pröva om ett utlämnande är förenligt med de ändamål för vilken uppgiften ursprungligen samlades in.

För att myndigheter ska kunna lämna ut information med stöd av uppgiftsskyldigheten behöver de behandla personuppgifter i större utsträckning än vad de gör i dag. Med hänsyn till den breda definitionen av personuppgiftsbehandling är det inte bara själva utlämnandet av information till en annan myndighet som utgör en behandling av personuppgifter. Även en rad åtgärder som behöver vidtas inför ett utlämnande kommer att medföra personuppgiftsbehandling, till exempel strukturering, kontroll, bearbetning och justering av uppgifter.

När myndigheter inom ramen för NCSC:s verksamhet tar emot personuppgifter behöver de i sin tur behandla personuppgifter i större utsträckning än vad de gör i dag eftersom de kommer att samla in och därefter bearbeta uppgifterna som de får från andra myndigheter.

Myndigheterna kommer att behandla personuppgifter i flera led när uppgifter utbyts med stöd av uppgiftsskyldigheten. I många fall kommer det inte att vara fråga om någon ny personuppgiftsbehandling, utan en utökad behandling i jämförelse med den behandling, i form av informationsutbyte och annan behandling som är förknippad med utbytet, som sker i dag. I andra fall, där informationsutbytet som sådant inte är tillåtet i dag, kommer det att röra sig om

en helt ny personuppgiftsbehandling av uppgifter som myndigheterna tidigare inte haft rättslig grund för att behandla på detta sätt, det vill säga genom utbyte med andra myndigheter.

Centralt för bedömningen är finalitetsprincipen som kommer till uttryck i artikel 5.1 b i EU:s dataskyddsförordning. Där framgår att personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. I artikel 6.4 i EU:s dataskyddsförordning anges de kriterier som den personuppgiftsansvarige måste beakta för att fastställa om behandling för nya ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in (det så kallade förenlighetstestet). I skäl 50 till förordningen anges att den personuppgiftsansvarige särskilt bör beakta den registrerades rimliga förväntningar på hur dennes uppgifter kommer att användas. Utgångspunkten är att den registrerade inte ska bli överraskad av den nya behandlingen.

Det finns dock möjligheter för lagstiftaren att införa undantag till den personuppgiftsansvariges skyldighet att utföra förenlighetstestet. Av artikel 6.4 i EU:s dataskyddsförordning framgår motsatsvis att en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in är tillåten, om den grundar sig på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1 i förordningen.

Den nationella rätten kan därmed ange en rättslig grund för vidarebehandling av uppgifter, och någon särskild prövning av förenlighetstestet behöver då inte göras. Om behandlingen är nödvändig för att fullgöra en uppgift av allmänt intresse eller som ett led i myndighetsutövning som den personuppgiftsansvarige har fått i uppdrag att utföra, kan unionsrätten eller medlemsstaternas nationella rätt fastställa och närmare ange för vilka uppgifter och syften ytterligare behandling bör betraktas som förenlig och laglig (skäl 50 andra meningen). Om behandlingen grundar sig på unionsrätten eller på nationell rätt som utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle, speciellt om det sker i syfte att säkerställa viktiga mål av allmänt intresse, bör den personuppgiftsansvarige dessutom tillåtas att behandla personuppgifterna ytterligare oavsett om det är förenligt med insamlingsändamålen eller inte (skäl 50 andra stycket första meningen).

Sekretessbrytande bestämmelser om att insamlade personuppgifter får eller ska lämnas ut, oberoende av för vilka ändamål de har samlats in, är ett exempel på en sådan lagstiftningsåtgärd som är tillåten enligt artikel 23 i förordningen. Lagstiftningsåtgärden bör vara tydlig och precis och dess tillämpning bör vara förutsägbar för personer som omfattas av den (skäl 41).

Ett av de ändamål som anges i artikel 23.1 i EU:s dataskyddsförordning är unionens eller en medlemsstats viktiga mål av generellt allmänt intresse. Regeringen har uttalat att verksamhet som innefattar myndighetsutövning utgör ett viktigt allmänt intresse. När det gäller myndigheters behandling är det också ett viktigt allmänt intresse att svenska myndigheter, även utanför området för myndighetsutövning, kan bedriva den verksamhet som tydligt faller inom ramen för deras befogenheter på ett korrekt, rättssäkert och effektivt sätt (prop. 2017/18:105 s. 83).

Den uppgiftsskyldighet som föreslås kommer inte lämna något utrymme för prövning av förenlighetstestet i det enskilda fallet. Det innebär att det bör prövas om regleringen utgör en nödvändig och proportionerlig åtgärd i ett demokratiskt samhälle för att skydda ett sådant mål som avses i artikel 23.1 i EU:s dataskyddsförordning. Syftet med uppgiftsskyldigheten kan sägas vara att NCSC, som är en del av en myndighet, ska kunna bedriva den verksamhet som centret är ålagt i författning att bedriva. Regleringen skyddar därmed ett sådant mål som avses i artikel 23.1 i förordningen, alltså ett viktigt allmänt intresse.

Kravet på nödvändighet innebär att det berättigade intresse som eftersträvas med behandlingen av personuppgifter inte rimligen kan uppnås på ett lika effektivt sätt genom andra medel som är mindre ingripande i de registrerades grundläggande fri- och rättigheter (dom av den 4 juli 2023, Meta Platforms m.fl. C-252/21, punkt 109). Kravet på att behandlingen ska vara nödvändig för ändamålet innebär alltså inte att behandlingsåtgärden måste vara oundgänglig. Behandlingen kan också anses nödvändig om den leder till effektivitetsvinster (jfr dom den 16 december 2008, Huber, mål C-524/06).

Kravet på proportionalitet torde som utgångspunkt innebära att skälen för att personuppgifterna behandlas för det nya ändamålet ska väga tyngre än det intrång som behandlingen innebär för den enskilde (jfr prop. 2017/18:232 s. 128).

Det berättigade intresse som eftersträvas med behandlingen av personuppgifter är att NCSC ska kunna utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Utifrån detta bedömer utredningen att såväl kravet på nödvändighet som kravet på proportionality är uppfyllt. Eftersom det är fråga om en uppgiftsskyldighet ska inte utlämnande myndighet därutöver pröva om utlämnandet är förenligt med finalitetsprincipen (se HFD 2021 ref. 10).

4.6.8 Förslagen innebär inte övervakning eller kartläggning

Utredningens bedömning: Förslagen innebär inte någon ny möjlighet till personuppgiftsbehandling som innebär övervakning eller kartläggning av enskildas personliga förhållanden.

Genom förslaget om uppgiftsskyldighet vid samverkan inom ramen för NCSC:s verksamhet möjliggörs för de deltagande myndigheterna att få 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 bör alltså i sig självt utgöra en integritetsrisk.

Enligt 2 kap. 6 § andra stycket RF måste en myndighet emellertid ha stöd i lag för sådan personuppgiftsbehandling som sker utan samtycke och som innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är enligt motiven till bestämmelsen 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 (prop. 2009/10:80 s. 177). Rätten till skydd mot betydande intrång i den personliga integriteten kan alltså begränsas, vilket framgår av 2 kap. 20 § RF. Det finns vissa krav som måste uppfyllas för att en sådan begränsning ska vara godtagbar, vilket framgår av 2 kap. 21 § RF. En begränsning får

enligt den nyss nämnda bestämmelsen göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningen får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får vidare inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning. Bestämmelsen i 2 kap. 6 § andra stycket RF innebär inte ett hinder mot sådan lagstiftning som behövs till skydd för viktiga samhällsintressen eller lagstiftning som utgör ett led i anpassningen av normerna till den fortgående samhällsutvecklingen, utan att det grundlagsskyddade området bör avgränsas på ett sådant sätt att det enbart omfattar de mest ingripande intrången (prop. 2009/10:80 s. 182).

Uppgiftslämnande som kan ske enligt den lag om uppgiftsskyldighet som föreslås av utredningen utgör inte i sig en kartläggning eller övervakning av enskildas personliga förhållanden. Hur personuppgifterna behandlas inom mottagande myndighets verksamhet regleras av den lagstiftning som gäller för respektive myndighet, samt den lag om personuppgiftsbehandling som föreslås. Uppgiftsskyldigheten som föreslås ger alltså inte myndigheterna stöd för att behandla personuppgifter på ett sådant sätt att det innebär övervakning eller kartläggning av enskildas personliga förhållanden i större utsträckning än vad den gällande lagstiftningen tillåter. Förslaget utgör således inte i sig självt någon inskränkning av det skydd för den personliga integriteten som följer av 2 kap. 6 § andra stycket RF.

När det gäller registerlagen så bedömer utredningen att omfattningen av behandlingen av uppgifter om enskildas personliga förhållanden inte kommer att ske i sådan omfattning att det blir fråga om sådan övervakning eller kartläggning som avses i 2 kap. 6 § andra stycket RF. I arbetet med att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter torde det inte vara nödvändigt att behandla personuppgifter i sådan omfattning att behandlingen ska anses utgöra övervakning eller kartläggning enligt RF.

4.6.9 Slutlig proportionalitets- och nödvändighetsbedömning

Utredningens bedömning: Förslagen är nödvändiga och proportionerliga och förenliga med det dataskyddsrättsliga regelverket.

Förslagen är nödvändiga

Kravet på nödvändighet innebär att det berättigade intresse som eftersträvas med behandlingen av personuppgifter inte rimligen ska kunna uppnås på ett lika effektivt sätt genom andra medel som är mindre ingripande i de registrerades grundläggande fri- och rättigheter.

Ett första led i bedömningen är således att avgöra om förslagen utgör en effektiv lösning på en konkret och tydliggjord problematik. Det är ett mycket angeläget och viktigt samhällsintresse att det myndighetsgemensamma arbetet inom NCSC med cybersäkerhet och informationssäkerhet kan fungera 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 dem emellan. Det är ett angeläget intresse att samverkan inom ramen för NCSC:s verksamhet fungerar tillfredsställande.

Utredningens bedömning är att förslaget om en uppgiftsskyldighet svarar mot ett angeläget behov av utökade rättsliga förutsättningar för informationsdelning inom ramen för NCSC:s verksamhet. Det finns fog för slutsatsen att förslaget kommer att bidra till en effektivare samverkan. Även om informationsdelning inte är ensamt avgörande för att NCSC:s arbete bedrivs framgångsrikt så är förslaget nödvändigt för att NCSC ska kunna bedriva en effektiv samverkan.

När det gäller förslaget om en lag om personuppgiftsbehandling så är även den nödvändig för att uppnå det eftersträlvade behovet, att FRA ska kunna behandla personuppgifter på ett tillfredsställande sätt.

Förslagen är proportionerliga

Kravet på proportionalitet innebär som utgångspunkt att skälen för åtgärden väger tyngre än det intrång som den innebär för den enskilde och att integritetsintrånget ska begränsas till det som är absolut nödvändigt för det eftersträlvade målet.

De integritetsrisker som följer av förslagen, och de skyddsåtgärder som i viss mån minskar integritetsriskerna framgår ovan. I den slutliga proportionalitetsavvägningen måste det prövas om det integritetsintrång som följer av förslagen är motiverat av det eftersträlvade målet, om det finns alternativa – mindre ingripande åtgärder – som skulle kunna uppnå samma syfte, eller om det behövs ytterligare skyddsåtgärder för att garantera proportionaliteten.

Samhällsintresset av ett effektivt cybersäkerhets- och informationssäkerhetsarbete måste anses ytterst angeläget. Det finns därmed fog för slutsatsen att vissa integritetsintrång är godtagbara om de leder till att detta arbete förbättras.

Informationsdelning hindras av sekretesslagstiftningen eftersom sekretess gäller mellan de myndigheter som förväntas samverka inom ramen för NCSC:s verksamhet. Den problematiken kan inte hanteras på annat sätt än genom bestämmelser som tillåter att annars sekretessbelagd information lämnas ut. Det finns inga alternativa sätt att möjliggöra informationsdelning som undviker detta integritetsintrång.

Uppgiftsskyldigheten är utformad utifrån en avvägning mellan intresset av att värna enskildas integritet och intresset av att möjliggöra samverkan mellan myndigheter. Det är naturligtvis en svår avvägning att göra. Det är viktigt att uppgiftsskyldigheten är tillräckligt flexibel för att möjliggöra ett ändamålsenligt uppgiftsutbyte i den enskilda situationen. Samtidigt finns det ett starkt intresse av att det informationsutbyte som möjliggörs ska vara förutsebart och att endast information som motsvarar ett verkligt behov i myndigheternas verksamhet ska lämnas över.

Som redovisats ovan finns det skyddsåtgärder som begränsar det integritetsintrång som följer av ett uppgiftsutbyte enligt uppgiftsskyldigheten. Regleringen är vidare utformad med hänsyn tagen till kraven på tydlighet, precision och förutsebarhet. Avgränsningen till NCSC:s uppdrag innebär ett tillräckligt specifikt tillämpningsområde.

Förslaget om en registerlag för NCSC begränsas vidare på så sätt att NCSC kan behandla personuppgifter endast i den utsträckning som är nödvändig för att utföra sina uppgifter. Dessutom föreslås en rad säkerhetsåtgärder, som en bestämmelse om sökbegränsningar och begränsad tillgång till personuppgifterna samt en ny sekretessbestämmelse till skydd för enskilda inom ramen för NCSC:s verksamhet. Förslagen är vidare förenliga med Europakonventionen. Att förhindra cyberattacker och skydda samhället mot betydande it-incidenter är viktiga ur ett samhällsperspektiv och möjligheten att effektivt bidra till detta begränsas om NCSC inte har möjlighet att behandla personuppgifter i den utsträckning som lagförslagen innebär. Inskränkningen som förslagen innebär av rätten till integritet och respekt för privat- och familjeliv samt skydd av personuppgifter enligt EU:s stadga om de grundläggande rättigheterna är därför nödvändig.

Sammantaget bedömer utredningen att de bestämmelser som föreslås uppfyller kraven på nödvändighet och proportionalitet och att förslagen är förenliga med de dataskyddsrättsliga regler som gäller.

5 Konsekvenser

5.1 Krav på konsekvensanalysen

Vilka konsekvenser som utredningen ska beskriva framgår av kommittéförordningen (1998:1474), förordningen (2024:183) om konsekvensutredningar och av utredningens direktiv. Om förslagen i ett betänkande medför kostnadsökningar eller intäktsminskningar för staten, kommuner eller regioner, ska förslag lämnas om finansiering som i första hand har anknytning till utredningens område. Skäl för den föreslagna finansieringen ska också lämnas (15 § kommittéförordningen). Konsekvensutredningen ska innehålla en redogörelse för

1. det aktuella problemet och vilken förändring som eftersträvas,
2. vilka konsekvenser som bedöms uppstå om ingen åtgärd vidtas,
3. de olika alternativ som finns för att uppnå förändringen och de fördelar respektive nackdelar som bedöms finnas med dessa, och
4. det eller de alternativ som bedöms lämpligast och av vilka skäl.

Konsekvensutredningen ska även innehålla en analys av det förslag som lämnas eller det beslut som avses att fattas. Analysen ska bestå av

1. en beskrivning och beräkning av förslagets eller beslutets kostnader och intäkter för staten, kommuner, regioner, företag och andra enskilda,
2. en beskrivning och, om möjligt, en beräkning av andra relevanta konsekvenser än sådana som anges i 1,
3. en redogörelse för vilka åtgärder som har vidtagits för att förslaget eller beslutet inte ska medföra mer långtgående kostnader

eller begränsningar än vad som bedöms vara nödvändigt för att uppnå dess syfte,

4. en bedömning av om särskild hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser, och
5. en beskrivning av hur och när konsekvenserna av förslaget eller beslutet kan utvärderas.

Av kommittédirektivet framgår att utredaren särskilt ska beakta de konsekvenser för Myndigheten för samhällsskydd och beredskap (MSB) och Försvarets radioanstalt (FRA) som en överföring av arbetsuppgifter får för respektive myndighets övriga uppdrag. Utredaren ska också klargöra vad en överföring av uppgifter medför för konsekvenser när det kommer till hanteringen av säkerhetsskyddsfrågor inom verksamheten. Det ska göras en analys av vilka rättsliga konsekvenser, både nationella och EU-rättsliga, som en överföring av arbetsuppgifterna innebär. Utredaren ska vidare särskilt beakta konsekvenserna i förhållande till genomförandet av 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). Slutligen ska utredaren analysera och redovisa de verksamhetsmässiga och personella konsekvenserna av förslagen som lämnas.

5.2 Utgångspunkter för konsekvensanalysen

Utredningen jämför förslagen mot ett nollalternativ. Nollalternativet avseende verksamhetsöverföringen innebär att MSB behåller sitt befintliga uppdrag på informations- och cybersäkerhetsområdet och att genomförandet av NIS 2-direktivet motsvarar de förslag som lades fram i betänkandet *Nya regler om cybersäkerhet* (SOU 2024:18). Nollalternativet för förslagen avseende informationsdelning, sekretess och personuppgiftsbehandling utgörs av att några författningsändringar inte sker, oaktat verksamhetsöverföringen från MSB. I kapitel 3 och 4 framgår flera av de övervägan-

den som krävs enligt 6 § förordning (2024:183) om konsekvensutredningar.

5.3 Regleringsalternativ

5.3.1 Förslagen uppfyller syftena med uppdraget men skapar nya utmaningar

I kapitel 3 föreslås en modell för en ny ansvarsfördelning inom centrala delar av statens arbete med Sveriges informations- och cybersäkerhet. Utredningen bedömer att verksamhetsöverföringen medför ett tydligare och större ansvar för FRA där statens resurser kan få en högre strategisk och operativ effekt. Genom överföringen blir det bland annat tydligt vilken aktör som har det primära ansvaret för att tillgodose regeringens behov av underlag och för att agera vid cyberhot eller andra it-incidenter. Det nationella cybersäkerhetscentrets (NCSC) befintliga uppdrag omfattar uppgiften att utgöra en plattform för privat-offentlig samverkan. Förslaget att NCC-SE ska samlokaliseras i NCSC stärker centret i detta uppdrag och ger därtill förutsättningar för ett nära samarbete mellan myndigheter, forskare och privata aktörer i utvecklingen av nya tekniska lösningar. NCSC blir därmed den naturliga samlingspunkten för samordningen av det nationella arbetet kopplat till EU:s forsknings- och innovationsfinansiering på informations- och cybersäkerhetsområdet. Sammantaget anser utredningen därför att samhällets motståndskraft på informations- och cybersäkerhetsområdet kommer att öka genom förslagen.

Förslagen ligger även i linje med visionen i regeringens nationella strategi för cybersäkerhet 2025–2029 där ett välfungerande NCSC bidrar till att samordna samhällets arbete med att stärka den nationella cybersäkerhetsförmågan och kommer de sektorsansvariga myndigheter till gagn i deras arbete med att ta fram välanpassade krav (se skr. 2024/25:121 s. 4). Det ska dock framhållas att uppgifterna inom informations- och cybersäkerhet alltså kommer vara delade mellan ett flertal myndigheter och departement. Samordningen mellan dessa aktörer kommer även fortsättningsvis att vara av avgörande betydelse för att åstadkomma ett effektivt arbete med informations- och cybersäkerhetsfrågorna.

Modellen medför samtidigt nya utmaningar genom att informations- och cybersäkerhetsarbetet i större utsträckning skiljs organisatoriskt från resten av arbetet med krisberedskap och det civila försvaret, som alltjämt är organiserat kring MSB som huvudman. FRA utgör inte heller en beredskapsmyndighet och tillhör således inte denna struktur. Arbetet på informations- och cybersäkerhetsområdet kommer dock även fortsättningsvis vara en viktig del av det civila försvaret. Det är därför av stor vikt att FRA och MSB gemensamt ser till att ett löpande samarbete kommer till stånd i dessa frågor så att en effektökning inom informations- och cybersäkerhetsarbetet inte sker på bekostnad av ett svagare civilt försvar i stort. Utredningen återkommer särskilt till frågan om samordningen av Sveriges krisberedskap avseende genomförandet av 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) i avsnitt 5.5.3.

5.3.2 Andra modeller har övervägts

Avvägningarna som har gjorts för varje enskild uppgift framgår av förslagen. Det finns dock andra lösningar som i varierande grad hade kunnat tillgodose motsvarande behov. Nollalternativet skulle innebära att MSB behåller sitt befintliga uppdrag och tilldelas ytterligare uppgifter enligt förslaget i SOU 2024:18. Detta alternativ skulle dock inte lösa ut frågan om överlappande uppgifter mellan NCSC och MSB. Ansvaret skulle således fortsatt vara delat mellan myndigheterna.

Ett annat alternativ vore att låta den operativa delen av arbetet med informations- och cybersäkerhet hos MSB överföras till FRA, medan MSB behåller sin strategiska verksamhet på området. Denna lösning skulle bland annat underlätta samordningen av NIS 2- och CER-regleringarna, eftersom MSB skulle ha ett strategiskt ansvar som innefattar båda direktiven. Vid en sådan uppdelning mellan operativ och strategisk verksamhet skulle de dubbla ansvaren mellan MSB och NCSC dock kvarstå eftersom även centret genom förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt har ett strategiskt ansvar på informations- och cybersäkerhetsområdet. Det hade även försvårat genomföran-

det av NIS 2-direktivet eftersom ansvarsområden i direktivet i det scenariot hade delats upp på två myndigheter, där CSIRT-enheten separeras från strategiska funktioner. Andra modeller där uppgifter som föreskrifter och tillsynssamordning förs över till en tredje myndighet skulle visserligen renodla NCSC:s uppdrag men påtagligt komplicera genomförandet av både NIS 2- och CER-direktiven samt inte åstadkomma den kraftsamling på området som utredningen har i uppdrag att åstadkomma.

Även andra uppdelningar av uppdrag, till exempel där flera CSIRT-funktioner för olika typer av incidenter upprättas och fördelas på centret och MSB har övervägts. MSB har till exempel i remissvar till förslagen i del 1 av promemorian *Ett nytt nationellt cybersäkerhetscenter* (Fö2024/00785) gett förslag på en sådan uppdelning där MSB utgör huvudman för CSIRT-enheten enligt NIS 2-direktivet medan en separat cyberförsvars-CSIRT byggs upp inom FRA och NCSC. Även dessa modeller har dock gemenensamt att de inte bidrar till den koncentration av ansvar och resurser som varit ett av syftena med utredningen.

5.4 Verksamhetsmässiga konsekvenser

5.4.1 FRA får ett bredare samhällsuppdrag

Genom förslagen samlas kompetens och ansvar i arbetet med Sveriges informations- och cybersäkerhet i större utsträckning hos FRA och NCSC. De nya uppgifterna kommer verksamhetsmässigt utföras i NCSC. För att arbetet i centret ska kunna fungera effektivt krävs att denna del av arbetet på myndigheten 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. Öppenheten är även en förutsättning för att Sverige ska kunna dra nytta av de stora ekonomiska satsningar som EU aviserat på området. Det är dessutom en förutsättning för att centret ska kunna verka i unionssamarbetet och ta till vara Sveriges intressen på ett ändamålsenligt sätt. Utöver centrets verksamhet kommer FRA även fortsatt bedriva signalspaning och verka inom cyberförsvaret. Det är av avgörande vikt att dessa delar av myndighetens verksamhet fortsätter utföras utan extern insyn. Denna nya dualitet i myndighetens uppdrag ställer höga krav

på myndighetens organisationsförmåga och ledning. En överhängande risk med förslagen är annars att även NCSC blir en sluten verksamhet på ett sådant sätt att Sverige inte kan uppfylla sina förpliktelser mot EU. Det vore även mycket skadligt för det nationella arbetet, där en samverkan mellan samtliga aktörer i samhället med NCSC som en samlingspunkt är nödvändig för Sveriges förmåga att möta aktuella och framtida hot på informations- och cybersäkerhetsområdet.

Av kommittédirektivet framgår att utredningen ska analysera och föreslå hur rapportering och uppföljning av informations- och cybersäkerhetsverksamheten vid en överföring av uppgifter kan struktureras så att verksamheten blir möjlig för regeringen att följa upp över tid. Utredningen föreslår i avsnitt 3.3.1 att FRA genom NCSC ska få ett samlat rapporteringsuppdrag till regeringen. Utredningen anser att förslaget ger NCSC tillräckligt författningsstöd för att kunna uppfylla regeringens krav på uppföljning. Genom att de dubbla uppdragen hos NCSC och MSB samlas på en myndighet bör regeringens tillgång till samlade och fullständiga underlag för politiska beslut förbättras. Det är av stor vikt att centret och regeringen kontinuerligt utvecklar formerna för denna uppföljning så att den är anpassad till det rådande omvärldsläget och tillförsäkrar regeringen ett fullgott underlag vid situationer när behov av brådskande politiska åtgärder uppstår.

En överföring av uppgifter som regleras i NIS 2-direktivet till FRA innebär även att myndigheten binds till att fullgöra dessa uppgifter oaktat övriga prioriteringar inom myndigheten. Därtill kommer andra EU-rättsakter medföra ytterligare uppgifter som ska utföras, vilket utredningen återkommer till i avsnitt 5.5.3. Sammantaget innebär detta att myndighetens självständiga handlingsutrymme att prioritera uppgifter inom verksamheten kommer att minska. För att FRA samtidigt ska kunna utföra sitt kärnuppdrag inom försvarsunderrättelseverksamhet på ett ändamålsenligt sätt krävs det att myndigheten beviljas adekvata resurser för att både finansiera underrättelseverksamheten och den tillkommande verksamheten i NCSC.

5.4.2 MSB får ett mer koncentrerat uppdrag

För MSB innebär förslagen organisatoriskt att verksamheterna för strategisk och operativ cybersäkerhet överförs till FRA. Däremot kommer MSB även fortsättningsvis bedriva verksamhet inom samhällsviktiga kommunikationstjänster. Myndigheten får därmed ett mer koncentrerat uppdrag för samordningen av frågor om skydd mot olyckor, krisberedskap och civilt försvar. Genom förslagen i betänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64) om genomförandet av CER-direktivet stärks myndighetens roll i dessa avseenden ytterligare. Samtidigt förlorar myndigheten kompetensen att samordna frågor om informations- och cybersäkerhet med andra frågor inom beredskapssystemet och det civila försvaret. MSB kommer till exempel bli beroende av ett informationsutbyte med NCSC för att komplettera lägesbilder till regeringen. MSB kommer dock även fortsättningsvis utgöra en samverkansmyndighet i NCSC och på så vis utgöra en viktig länk mellan arbetet med informations- och cybersäkerhet och övriga delar av det civila försvaret.

5.5 EU-rättsliga konsekvenser

Utredningen har bland annat haft i uppdrag att analysera och lämna förslag på hur en överföring av uppgifter kan ske utan att Sveriges möjligheter att uppfylla sina EU-rättsliga förpliktelser eller få del av EU-rättsligt stöd påverkas. Utredningen anser att förslagen kan genomföras utan någon sådan påverkan. Det är därutöver även av vikt att så långt det är möjligt beakta andra pågående arbeten inom EU-rätten som kan komma att få en påtaglig påverkan på NCSC:s verksamhet.

5.5.1 Förslagen hindrar inte Sverige från att uppfylla sina förpliktelser mot EU

Utredningens bedömning: Förslagen om överföring av uppgifter till FRA hindrar inte Sverige från att uppfylla sina förpliktelser mot EU.

Utredningen har i kapitel 3 gjort bedömningen att en överföring av uppgifter till FRA inte medför ett hinder för Sverige att uppfylla sina EU-rättsliga förpliktelser enligt NIS 2-direktivet eller 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). I kapitel 4 har utredningen lagt fram författningsförslag som medför att nödvändig informationsdelning kommer att kunna ske i enlighet med såväl offentlighets- och sekretesslagen (2009:400), förkortad OSL, som EU:s dataskyddsförordning. Därutöver tillkommer ytterligare internationella åtaganden som i nuläget utförs av MSB och som har en nära anknytning till arbetet i nätverken enligt NIS 2-direktivet. MSB deltar exempelvis som representant för Sverige i National Liaison Officers Network (NLO), som är ett samarbetsorgan mellan unionsmedlemsstaterna och Europeiska unionens cybersäkerhetsbyrå (Enisa). För att Sveriges inflytande inte ska minska genom en verksamhetsöverföring till FRA är det av vikt att representanter från NCSC utses till sådana övriga nätverk.

5.5.2 Förslagen påverkar inte Sveriges möjligheter att ta emot EU-rättsligt stöd

Utredningens bedömning: Förslagen om överföring av uppgifter till FRA påverkar inte Sveriges möjligheter att ta emot EU-rättsligt stöd.

Det åligger FRA att organisera sin verksamhet på ett sådant sätt att unionsrättsliga krav på insyn kan tillgodoses.

Allmänt om hantering av EU-medel och befintliga stöдавtal

EU avsätter genom både direktförvaltning och delad förvaltning medel för utvecklingen av unionens cybersäkerhet. Förmedling av medel sker bland annat genom programmet för ett digitalt Europa (DIGITAL), vars syfte är att föra ut digital teknik till företag, medborgare och offentliga förvaltningar. MSB har redan beviljats visst EU-stöd för en andel av kostnaderna hänförliga till utvecklingen av

uppdragen att utgöra CSIRT-enhet, gemensam kontaktpunkt och cyberkrishanteringsmyndighet. Myndigheten har även tagit emot stöd för tillsynssamordning och föreskriftsarbete. Stödet har mottagits i projektet ENIAC (Enhanced NIS2 Implementation And Cooperation) som finansieras genom DIGITAL-programmet. Avtalet om finansiering löper ut i maj 2027 och revisionsrätten kvarstår fem år efter slutlig betalning. Därutöver har MSB tagit emot stöd i utvecklingen av NCC-SE. Det stödet löper ut under 2025. Förslagen om överföring av uppgifter med sin grund i EU-rätten till FRA innebär därför även att myndigheten behöver ha rättsliga förutsättningar för att hantera EU-medel.

För att en myndighet ska kunna hantera EU-medel krävs inledningsvis att den omfattas av ramverket för intern styrning och kontroll (SOU 2024:22). Detta innebär att myndigheten ska omfattas av

- myndighetsförordningen (2007:515),
- internrevisionsförordningen (2006:1228),
- förordningen (2007:603) om intern styrning och kontroll, samt
- förordningen (2000:605) om årsredovisning och budgetunderlag.

FRA omfattas av samtliga av dessa förordningar. Några nationella författningsförändringar är därför inte nödvändiga för att möjliggöra för myndigheten att hantera EU-stöd. Frågan är därefter om hinder finns i förhållande till EU-rättslig reglering.

Rättigheter och skyldigheter som gäller enligt avtalen om finansiellt stöd överförs vid en överlåtelse av avtalet till en ny mottagare. Vid en överföring av uppgifterna enligt NIS 2-direktivet till FRA från MSB bör det finnas en avtalsmässig möjlighet för att även låta avtalen gå över till FRA. MSB har i detta avseende framhållit vikten av att kommissionen tidigt involveras i detta arbete. Överlåtelsen av avtalen medför vidare ett behov av att nationella avtal eller upphandlingar för tjänster som förbrukas i projekteten är ordnade inför överföringen. Utredningen gör därför bedömningen att det är möjligt för FRA att ta över avtalen i samband med verksamhetsöverföringen, men att detta kräver förberedelser i form av bland annat dialog med EU-kommissionen.

En överföring av avtalen medför krav på insyn

Enligt kommittédirektivet får en överföring av uppgifter till FRA inte medföra en ökad insyn i myndighetens arbete med nationell säkerhet. Vid en överlåtelse av avtalen blir FRA bunden av den revisionsrätt som i dag gäller gentemot MSB som stödmottagare. Någon möjlighet att inskränka denna insyn genom att utse NCSC till formell stödmottagare finns inte eftersom FRA gentemot EU utgör en enhet. Frågan är därför om det finns juridiskt utrymme för att ändå undanta information från granskning utan att samtidigt bryta mot nuvarande finansieringsavtal.

De grundläggande bestämmelserna om kraven för mottagande av unionsmedel framgår av EU:s budgetförordning (Europaparlamentets och rådets förordning 2018/1046 av den 18 juli 2018 om finansiella regler för unionens allmänna budget, om ändring av förordningarna (EU) nr 1296/2013, (EU) nr 1301/2013, (EU) nr 1303/2013, (EU) nr 1304/2013, (EU) nr 1309/2013, (EU) nr 1316/2013, (EU) nr 223/2014, (EU) nr 283/2014 och beslut nr 541/2014/EU samt om upphävande av förordning (EU, Euratom) nr 966/2012). Förordningen är numera ersatt, men gäller för avtal ingångna före den 23 september 2024.

Av artikel 129 i förordningen framgår att varje person eller enhet som mottar unionsmedel ska samarbeta till fullo för att skydda unionens ekonomiska intressen. Som ett villkor för mottagande av medel ska enheten därför bevilja de rättigheter och den tillgång som krävs för att den behöriga utanordnaren, Eppo, Olaf, revisionsrätten och, i tillämpliga fall, relevanta nationella myndigheter ska kunna utöva sina respektive befogenheter på ett heltäckande sätt. När det gäller Olaf ska dessa rättigheter innefatta rätten att genomföra utredningar, däribland kontroller på plats och inspektioner.

De allmänna bestämmelserna i EU:s budgetförordning och fördragen ska läsas tillsammans med regleringen för varje stödprogram, där mer detaljerade krav på mottagaren av stöd framgår. Därutöver regleras ytterst ett flertal frågor i stöдавtalet som ingås mellan EU och mottagaren.

Till hjälp för stödmottagare har kommissionen tagit fram en vägledning med kommentarer som gäller för de stöдавtal som ingåtts inom stödprogrammen under perioden 2021–2027 (AGA – Annotated Grant Agreement, EU Funding Programmes 2021–2027 ver-

sion 2.0 1 April 2025). Av artikel 25.1.3 i vägledningen framgår bland annat att eventuella revisioner omfattar finansiell, teknisk och juridisk granskning av hur bidraget används. Kommissionen har även rätt att när som helst under projektets gång genomföra kontroller på plats för att säkerställa att EU-medel används korrekt. En sådan platskontroll innefattar en fysisk inspektion av stödmottagarens verksamhet för att granska projektets genomförande. Det kan även innefatta en dokumentationsgranskning där alla relevanta dokument måste vara tillgängliga, så som kontrakt, kvitton och personalregister. Av artikel 13.2 i vägledningen framgår samtidigt att parterna i avtalet måste hantera klassificerad information i enlighet med tillämplig EU-rätt, internationell rätt eller nationell lagstiftning om skydd av klassificerad information. Leverabler, till exempel i ett projekt, som innehåller klassificerad information måste lämnas in enligt särskilda procedurer som överenskommits med bidragsmyndigheten. Det har framförts till utredningen att det inom ramen för dessa särskilda procedurer finns ett utrymme att sekretessmarkera delar av rapporter, men att detta sker enligt överenskommelse från fall till fall.

Av artikel 346.1 i fördraget om Europeiska unionens funktions-sätt (FEUF) anges vissa undantagsregler vars tillämpning inte ska hindras av bestämmelserna i fördragen. Enligt artikel 346.1 a) ska ingen medlemsstat vara förpliktad att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. Av artikel 346.1 b) anges därefter att varje medlemsstat får vidta åtgärder, som den anser nödvändiga för att skydda sina väsentliga säkerhetsintressen i fråga om tillverkning av eller handel med vapen, ammunition och krigsmateriel; sådana åtgärder får inte försämra konkurrensvillkoren på den inre marknaden vad gäller varor som inte är avsedda speciellt för militärändamål.

Det saknas vägledande avgöranden kring i vilken mån undantag kan göras från EU-rätten med stöd av artikel 346.1 a i FEUF. Avseende artikel 346.1 b finns däremot vägledande avgöranden från EU-domstolen på upphandlingsområdet som ger för handen att undantaget ska tolkas restriktivt och att avsteg måste vara proportionerliga och ska bedömas på en case-by-case basis (Friton. P and Wolf. F, s. 93).

Sammantaget gör utredningen bedömningen att utrymmet för att undanta eller maskera uppgifter i handlingar som är relevanta

för projektets genomförande vid en eventuell revision är begränsat och kommer behöva bedömas från fall till fall. En sådan åtgärd skulle kunna bedömas som ett avtalsbrott. FRA är samtidigt som utgångspunkt inte skyldig att utöver handlingar med en direkt koppling till projektet ge tillgång till information vars avslöjande myndigheten anser strida mot Sveriges väsentliga säkerhetsintressen. Information som har koppling till FRA:s verksamhet inom signalspaning utgör sådan information. För att åstadkomma en tillräcklig grad av insyn i arbetet i NCSC för att nuvarande och framtida avtal om finansiering ska kunna fullföljas krävs det att FRA organiserar sin verksamhet på ett sådant sätt att extern revision av NCSC möjliggörs. Detta bör kunna åstadkommas genom att till exempel ekonomisk redovisning för centret hålls tydligt åtskilt från information om myndighetens övriga verksamhet. Detta så att en extern granskning av myndighetens användning av EU-medel kan ske utan att informationen är sammanblandad med säkerhetsskyddsklassificerad information. Något utlämnande av information som kan skada Sveriges säkerhet bör givetvis inte komma i fråga. Inte heller ett agerande i strid med ingångna avtal med EU är önskvärt. Även i detta avseende är det således avgörande att verksamheten i NCSC bedrivs på ett öppet sätt och särskiljs från myndighetens befintliga uppdrag.

Särskilt om NCC-SE

Driften av NCC-SE medför i huvudsak inga ytterligare krav på insyn utöver den som följer av det stödavtal som har ingåtts mellan MSB och EU för att ta emot medel i utvecklandet av NCC-SE.

För att kunna förvalta EU-medel genom direkt stöd måste samordningscentret göra en begäran om erkännande till kommissionen. En sådan begäran kan enligt artikel 6.2 eller 6.6 i CCCN-förordningen antingen göras innan myndigheten nomineras till att utgöra samordningscenter eller närsomhelst därefter. Kommissionen har därefter att återkomma med ett beslut inom tre månader. Närmare förutsättningar för att få ett sådant erkännande framgår av kommissionens vägledning (Guidelines on the assessment of the capacity of National Coordination Centres to manage funds to fulfil the mission and objectives laid down in Regulation (EU) 2021/887) som utfärdats med stöd av artikel 6.6 tredje stycket CCCN-förordningen. Det

finns inget krav på att ett nationellt samordningscenter ska beviljas ett sådant erkännande för att utgöra ett nationellt samordningscenter. Utredningen konstaterar att det däremot vore fördelaktigt att kunna utnyttja EU-stöd för att bygga ut landets kapacitet på informations- och cybersäkerhetsområdet genom NCC-SE.

Med hänsyn till ovanstående anser utredningen att en överföring av NCC-SE till FRA inte försämrar Sveriges förmåga att ta emot EU-stöd. Precis som med befintliga finansieringsavtal är FRA dock beroende av ett godkännande från kommissionen.

5.5.3 Konsekvenser i förhållande till genomförandet av andra EU-rättsakter

NIS 2-regleringen utgör en bas för ytterligare rättsakter på informationssäkerhetsområdet, där flera initiativ redan är i olika genomförandestadier. Detta medför att uppdrag som tilldelats enligt NIS 2-direktivet kan komma att utökas med fler uppgifter än vad som framgår av NIS 2-direktivet. Någon fullständig bild av denna utveckling kan inte ges i detta sammanhang. Det finns dock vissa centrala rättsakter utöver NIS 2-direktivet som kommer påverka arbetet i NCSC. Utredningen redogör för dessa rättsakter i den fortsatta framställningen i detta avsnitt. Det är av vikt att ta höjd för dessa och andra regleringar från EU i det fortsatta arbetet med utvecklingen av NCSC.

Samordningen av NIS 2- och CER-direktiven förutsätter ett fortsatt nära samarbete mellan FRA och MSB

Parallellt med NIS 2-direktivet införs CER-direktivet som syftar till att öka motståndskraften hos kritiska verksamhetsutövare. Förslaget i SOU 2024:64 är att MSB genom förordning ska ges ansvaret för att ta emot incidentrapporter, utgöra kontaktpunkt samt utfärda föreskrifter. Eftersom MSB även tilldelats motsvarande uppgifter i förslaget till förordning om cybersäkerhet i SOU 2024:18 har någon analys inte tidigare gjorts av hur dessa regleringar ska samordnas när uppgifterna enligt direktiven fördelas på olika myndigheter. Det finns dock flera aspekter som medför ett behov av ett fortsatt

nära samarbete mellan FRA och MSB vid en överföring av uppgifter till FRA.

Inledningsvis medför uppdelningen av incidentrapporteringsfunktionen enligt NIS 2- och CER-direktiven på olika myndigheter avvägningar för verksamhetsutövarna kring om en incidentrapport ska lämnas enligt ett eller flera regelverk. För att förenkla förfarandet för verksamhetsutövarna har MSB påbörjat ett projekt för att skapa en gemensam plattform för rapportering enligt både NIS 2- och CER-direktiven med ”intelligenta” formulär som utifrån svar på inledande frågor endast ställer sådana frågor som organisationen behöver besvara för att lämna en korrekt rapport. Applikationen sköter även förmedlingen av den information som respektive ansvarig myndighet ska ha. Utredningen ser positivt på projektet och understryker vikten av att en myndighetsgemensam lösning kan åstadkommas efter det att incidentrapporteringen enligt NIS 2-direktivet förs över till FRA.

Genom att FRA blir cyberkrishanteringsmyndighet kommer även vissa gränsdragningsproblem uppkomma om vilken myndighet som är ansvarig vid storskaliga incidenter. MSB har till utredningen anfört att en konsekvens av den föreslagna uppdelningen mellan NIS 2- och CER-regleringarna innebär att MSB som ytterst ansvariga myndighet inom beredskapssystemet kommer att ha ansvaret för samordningen av samhällets insatser vid en störning i en samhällskritisk verksamhet tills det konstateras att störningen har sin grund i en it-incident. Oavsett övriga effekter av incidenten medför detta att FRA som cyberkrishanteringsmyndighet då blir ansvarig för samordningen. Utredningens bedömning är att FRA och NCSC saknar förmågan att ensamt kunna hantera de samlade effekterna av en sådan större incident. Det är därför av yttersta vikt att FRA och MSB upprättar rutiner för ett nära samarbete kring hanteringen av sådana incidenter.

Som utredningen konstaterat i avsnitt 3.3.2 har FRA fått i uppdrag att presentera en nationell operativ plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. En del av detta uppdrag utgörs enligt artikel 9.4 c i NIS 2-direktivet av en analys av cyberkrishanteringsförfaranden, inbegripet deras integrering i den allmänna nationella ramen för krishantering och kanaler för informationsutbyte. Utredningen ser positivt på att detta uppdrag innefattar en dialog med MSB.

Därutöver åligger det Sverige enligt artikel 4 i CER-direktivet att senast den 17 januari 2026 anta en strategi för att stärka kritiska entiteters motståndskraft. Strategin ska innehålla strategiska mål och policyåtgärder, som bygger på relevanta befintliga nationella och sektorsspecifika strategier, planer eller liknande dokument, för att uppnå och upprätthålla en hög grad av motståndskraft hos kritiska entiteter, och ska åtminstone omfatta de sektorer som anges i bilagan. Av artikel 4.2 g framgår att strategin bland annat ska innehålla en policyram för samordning mellan de behöriga myndigheterna enligt CER- respektive NIS 2-direktivet för att dela information om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter och utföra tillsynsuppgifter. Det finns även krav i direktiven på att behöriga myndigheter enligt respektive reglering har ett samarbete (se artikel 13.5 och 9.6 i NIS 2- respektive CER-direktivet).

Utredningen konstaterar utifrån ovanstående att det även finns krav i respektive EU-direktiv på en nära samordning av implementeringen av de två direktiven. Det åligger således myndigheterna att få till stånd ändamålsenliga arbetssätt för en god integrering av de två regelverken när implementeringen sker på två separata myndigheter.

Nätkoderna och cyberresiliensförordningen medför ytterligare uppgifter för CSIRT-funktionen

Nätkoderna

Kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden (Nätkoderna) är en sektorsspecifik förordning som enligt artikel 1 innehåller sektorspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden, bland annat regler om gemensamma minimikrav, planering, övervakning, rapportering och krishantering.

Enligt förordningen ska CSIRT-enheterna som utsetts enligt NIS 2-direktivet bland annat bistå i tillhandahållandet av en bedömning på medlemsstatsnivå av cybersäkerhetsrisker till Entso för el

och EU DSO-enheten, motta incidentrapporter utifrån regleringen samt skyndsamt informera Enisa om alla ej avhjälpna sårbarheter som den blir varse om hos organisationer som omfattas av regleringen. Även cyberkrishanteringsmyndigheten får tillkommande samordningsuppgifter enligt förordningen. Behörig myndighet enligt förordningen är Statens energimyndighet. Förordningen trädde i kraft den 13 juni 2024.

Cyberresiliensförordningen

Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828) (Cyberresiliensförordningen) syftar till att skapa förutsättningar för utveckling av säkra produkter med digitala element genom att säkerställa att hård- och mjukvara släpps ut på marknaden med färre sårbarheter och att tillverkare ska ta större ansvar för produkters cybersäkerhet genom deras livscykel. Förordningen syftar vidare till att konsumenter ska få tillräcklig information om cybersäkerheten för de produkter med digitala element som de köper och använder. Ekonomiska operatörer, vilka i huvudsak är tillverkare, importörer och distributörer, ska följa de cybersäkerhetskrav förordningen anger för alla produkter med digitala element, för att de ska kunna tillhandahållas på den inre marknaden (jfr dir. 2024:119 s. 2).

I artikel 14 i förordningen finns en obligatorisk rapporterings-skyldighet för tillverkarna att till den samordnande CSIRT-enheten anmäla alla aktivt utnyttjade sårbarheter i produkter med digitala element. Enligt artikel 15 finns även en möjlighet till frivillig rapportering för såväl tillverkare som andra om sårbarheter i produkter. Eftersom uppdraget att utgöra CSIRT-enhet ska föras över till FRA kommer myndigheten därmed även ansvara för hanteringen av rapporter enligt Cyberresiliensförordningen. FRA får som CSIRT-enhet även en rad andra uppgifter genom förordningen rörande informationsdelning till EU och stöd till tillverkare. Genomförandet kommer även innefatta krav på ett nära samarbete mellan NCSC och den eller de myndigheter som utses till marknadskontrollmyn-

dighet. Frågan om vilken eller vilka myndigheter som ska utses till marknadskontrollmyndighet omfattas av utredningen om kompletterande bestämmelser till Cyberresiliensförordningen. Utredaren ska redovisa uppdraget senast den 15 december 2025. Regleringen ska därefter tillämpas från och med 11 december 2027. Den obligatoriska rapporteringsskyldigheten för tillverkare ska dock tillämpas redan från och med den 11 september 2026.

Cybersolidaritetsförordningen kan innebära krav på ökad integrering i det unionsgemensamma arbetet

Europaparlamentets och rådets förordning (EU) 2025/38 av den 19 december 2024 om åtgärder för att stärka solidariteten och kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cybersäkerhetsincidenter och om ändring av förordning (EU) 2021/694 (Cybersolidaritetsförordningen) syftar till att stärka kapaciteten i unionen att upptäcka, förbereda sig inför och hantera cyberhot och cyberincidenter. Genom förordningen instiftas ett europeiskt nätverk av cybernav (det europeiska systemet med cybersäkerhetsvarningar) för att bygga upp och förbättra samordnad kapacitet för upptäckt och gemensam kapacitet för situationsmedvetenhet. Den instiftar även en cybernödsmekanism och en europeisk mekanism för utvärdering av cybersäkerhetsincidenter för att utvärdera och analysera betydande cybersäkerhetsincidenter eller storskaliga cybersäkerhetsincidenter. För närvarande pågår även arbete med att etablera regional samverkan mellan cybernav.

Det är frivilligt för medlemsstaterna att delta i systemet för cybersäkerhetsvarningar. Skulle Sverige välja att delta i ett fördjupat samarbete inom unionen i enlighet med förordningen ska ett nationellt cybernav utses. Kraven för att utses till cybernav framgår av artikel 4 i Cybersolidaritetsförordningen och ger för handen att FRA skulle kunna vara lämplig för denna uppgift i egenskap av CSIRT-enhet och cyberkrishanteringsmyndighet.

DORA-förordningen medför behov av samordning med finansinspektionen

DORA-förordningen (Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011) syftar till att uppnå en hög gemensam nivå av digital operativ motståndskraft i nätverks- och informationssystem som stöder finansiella entiteters affärsprocesser. Förordningen tillämpas sedan den 17 januari 2025. I svensk rätt kompletteras förordningen främst av lagen (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn. Enligt detta regelsystem ska finansiella entiteter rapportera allvarliga IKT-relaterade incidenter till finansinspektionen. Ett liknande system som i NIS 2-direktivet finns även för att på frivillig basis rapportera betydande cyberhot. Finansinspektionen har att lämna närmare uppgifter om allvarliga IKT-relaterade incidenter till behöriga myndigheter, den gemensamma kontaktpunkten eller CSIRT-enheten som inrättats enligt NIS 2-direktivet. Centret kommer således via Finansinspektionen även behöva hantera information som lämnas in enligt DORA-förordningen.

5.6 Personella konsekvenser och lokaler

5.6.1 Personella konsekvenser

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 idag.

MSB är organiserad i avdelningar som i sin tur består av flera verksamheter med underliggande enheter. Arbetet med informations- och cybersäkerhet återfinns främst hos avdelningen för cybersäkerhet och samhällsviktiga kommunikationer. Inom avdelningen finns fyra verksamheter; verksamheten för strategisk cybersäkerhet, verksamheten för operativ cybersäkerhet, verksamheten för stöd

till ledning och samverkan, samt verksamheten för samhällsviktiga kommunikationstjänster. Det är personalen från verksamheten för strategisk cybersäkerhet och från verksamheten för operativ cybersäkerhet som kommer att omfattas av en eventuell verksamhetsövergång. Vid tidpunkten för verksamhetsöverföringen uppskattas förslagen omfatta 85–100 personer.

För arbetstagaren innebär det att anställningen automatiskt övergår till den nya arbetsgivaren men att arbetstagaren kan motsätta sig övergången. Rättigheter och skyldigheter enligt anställningsavtalet, till exempel avseende lön och arbetstid följer under dessa omständigheter med till den nya arbetsgivaren.

Utredningen bedömer att NCSC vid en verksamhetsöverföring kommer att ha tillgång till adekvat personal för att uppfylla kraven i NIS 2-direktivet och för att utföra de övriga uppgifter som omfattas av verksamhetsöverföringen. Ytterligare rekryteringar kan dock komma att behövas för att möta centrets växande uppdrag.

5.6.2 Lokaler

NCSC:s verksamhet bedrivs nu i MSB:s lokaler. Nya lokaler avsedda för NCSC är under uppbyggnad. Den myndighetsgemensamma projektgruppen har uppgett till utredningen att centret även fortsättningsvis kommer att vara placerat där i avvaktan på att nya lokaler färdigställs. Preliminärt kommer verksamheten att kunna flytta till nya lokaler under 2028. Under förutsättning att MSB fortsätter att tillhandahålla it-lösningar för NCSC:s verksamhet fram till att FRA får egna sådana på plats gör utredningen bedömningen att befintliga lokaler uppfyller de tekniska kraven enligt NIS 2-direktivet och i övrigt är ändamålsenliga för verksamheten. Det är dock centralt att en flytt till de nya lokalerna kommer till stånd så snart som möjligt.

5.7 Ekonomiska konsekvenser

5.7.1 Ekonomiska konsekvenser av förslagen om överföring av uppgifter från MSB till FRA

Utredningens bedömning: Förslagen om att FRA ska utföra nya arbetsuppgifter leder till ökade kostnader för myndigheten. Förslagen kan i huvudsak finansieras genom en omfördelning av medel i anslagen 2:6.

Förslagen bör i huvudsak finansieras genom överföring av anslag från MSB till FRA

Förslagen innebär att uppgifter och personal förs över från MSB till FRA. En konsekvens av detta kommer vara att en omfördelning av anslag behöver göras från 2026 och framåt för att täcka FRA:s ökade kostnader för den överförda verksamheten. MSB kommer på motsvarande sätt att få minskade anslag, men kommer samtidigt få minskade kostnader för lön och andra verksamhetskostnader för den personal som förs över till FRA.

Driften av verksamheterna för strategisk och operativ informationssäkerhet hos MSB beräknas uppgå till 225 000 000 kronor. Utgångspunkten för beräkningarna är budget för 2025 med stöd av utfallet för 2024. Kostnaderna avser den del som finansieras av myndighetens förvaltningsanslag 2:6. I totalen ingår lokalkostnader, som dock inte redovisas särskilt. Den myndighetsgemensamma projektgruppen har till utredningen inkommit med underlag utifrån uppskattningen att verksamhetsöverföringen kommer att omfatta 85 medarbetare. Personalstyrkan förväntas dock öka det kommande året till närmare 100 medarbetare varför personalkostnaderna kan förväntas bli högre. Även kostnaderna för EU-projektet ENIAC framgår. Det är detta EU-projekt som har omfattat utvecklingen av uppgifter enligt NIS 2-direktivet. Projektet kommer föras över till FRA och pågå fram till halvårsskiftet 2027. Däremot har bidragsdelen från EU-projektet inte räknats med. I beräkningarna ingår inte medlen för utlysningar inom NCC-SE eftersom dessa varierar från år till år och även kan innefatta EU-stöd. Fördelningen av kostnaderna framgår av tabellen nedan.

Tabell 5.1 Kostnader för driften av verksamheterna operativ och strategisk cybersäkerhet

Utgiftsposter	Kostnader i tkr
Lönekostnader	85 000
Generella OH-kostnader	1 400
Utbildning	5 000
Resekostnader	1 600
Varuinköp	5 900
Övriga driftskostnader	67 000
Köp av tjänster	59 000

Källa: Myndigheten för samhällsskydd och beredskap.

De generella OH-kostnader som redovisas avser endast de gemensamma kostnader på årsbasis som är direkt rörliga utifrån antal anställda så som licenskostnader för olika system, datorer, telefoner, lönespecifikation, och liknande kostnader. Andra OH-kostnader, exempelvis för medarbetare i central stödverksamhet ingår inte. Under övriga driftskostnader ingår bland annat en uppskattning av kvarvarande avskrivningar och löpande räntor på anläggningstillgångar, som kommer preciseras efter att en inventering har gjorts av MSB. Utöver anslagen i 2:6 har MSB för 2025 bland annat fått finansiering för tre utvecklingsprojekt från anslag 2:4 anslagspost 5 Krisberedskap och totalförsvar med koppling till cybersäkerhet. När verksamheten går över till FRA kan myndigheten söka medel för denna typ av utvecklingsprojekt från samma anslag. Därutöver mottar MSB även anslag för finansiering av sådan forskning och övning som behandlas i avsnitt 3.5. Sådana kostnader har inte heller räknats med. Underlaget ger således inte en sådan heltäckande bild att fullständiga beräkningar av verksamheternas totala kostnader kan göras.

Beräkningarna bygger på kostnaderna för att bedriva verksamheten i nuläget hos MSB. Som utredningen har pekat på kommer ytterligare unionsrättsliga rättsakter på området de kommande åren sannolikt medföra ytterligare uppdrag för FRA och NCSC. Dessa uppdrag kommer i en övergångsperiod att skötas av MSB fram till dess att verksamhetsöverföringen genomförs. Det är därför troligt att NCSC redan vid tidpunkten för överföringen kommer att kräva utökad finansiering.

Förslagen kan antas medföra merkostnader på kort sikt

På kort sikt kan förslagen antas medföra merkostnader för både MSB och FRA. Såväl planeringen av organisationsförändringen som sker i den myndighetsgemensamma projektgruppen, som tiden fram tills att en verksamhetsöverföring är genomförd kan beräknas medföra merkostnader. Bland annat kommer merkostnader uppstå för MSB för den personal som väljer att inte följa med vid en verksamhetsöverföring till FRA. FRA kommer samtidigt få ökade kostnader för personalrekrytering. Även andra praktiska aspekter som överföring av arkiv kommer medföra merkostnader. Utredningen har inte mottagit något underlag avseende kostnader för själva verksamhetsöverföringen, och det är svårt att redan nu uppskatta vad dessa kommer att uppgå till.

Statskontoret har i ett annat sammanhang konstaterat att myndighetssammanslagningar tenderar att temporärt öka trycket på stödfunktioner för att hantera sammanslagningen. Det tar även tid att överbrygga organisationskulturer och etablera en ny intern styrning med rutiner och processer, vilket ofta innebär utökade kostnader under en period (Statskontoret dnr 2023/171-5 samt dnr 2022/164-4). Utredningens förslag innebär visserligen endast en överföring av en del av MSB:s verksamhet och inte en sammanslagning av två myndigheter. Med hänsyn till omfattningen av verksamhetsöverföringen kan dock de erfarenheter som redovisats avseende sammanslagningar även antas bli aktuella för åren närmast före och efter verksamhetsöverföringen. Det är däremot svårt att göra någon närmare uppskattning om vad dessa merkostnader som är hänförliga till processer hos myndigheterna kommer att uppgå till.

De ökade kostnader som verksamhetsöverföringen kan medföra för MSB och FRA på kort sikt skulle eventuellt kunna finansieras genom omprioritering inom MSB och FRA. Ett annat alternativ är att det finansieras genom annan omfördelning av medel inom utgiftsområde 6. Denna fråga bör avgöras av regeringen efter dialog med MSB och FRA.

Förslagen kan medföra en mer kostnadseffektiv förvaltning på medellång till lång sikt

Förslagen bör på längre sikt leda till synergieffekter när kompetens koncentreras i en verksamhet. Den förslagna organisationsstrukturen innehåller även färre överlappande ansvarsområden. Mycket av det stödjande och samordnande uppdrag som omfattats av både MSB och NCSC:s uppdrag kommer nu koncentreras i centret. Detta gäller även ansvaret för rapporteringen till regeringen. Syftet med förslagen är i första hand att öka Sveriges strategiska och operativa förmåga att möta framtida hot och kriser på informations- och cybersäkerhetsområdet. Utredningen har således inte i första hand haft som utgångspunkt att minska kostnaderna i förvaltningen. Det framstår dock som sannolikt att dessa effekter på sikt kommer medföra en mer kostnadseffektiv förvaltning på området. Det är dock svårt att i nuläget närmare uppskatta storleken på dessa eventuella besparingar.

5.7.2 Ekonomiska konsekvenser av förslagen om informationshantering

Utredningens bedömning: De kostnader som kan uppstå för berörda statliga myndigheter bör inte vara större än att de kan hanteras inom befintliga ekonomiska anslag.

Förslagen rörande informationshantering berör vissa statliga myndigheter

Förslagen i kap. 4 rörande informationshantering berör i första hand FRA. Men även samverkansmyndigheterna Försvarets materielverk, Försvarmakten, MSB, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen kan behöva tillämpa framför allt förslaget om uppgiftsskyldighet.

Förslaget om en ny lag om uppgiftsskyldighet vid samverkan i verksamhet inom NCSC

Ett visst behov av utbildning kan antas uppkomma för tillämpning av den föreslagna lagen. 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 bör kunna rymmas inom befintliga ekonomiska ramar.

Förslaget om en registerlag för NCSC

Förslaget kan innebära behov av utbildning, vilket kan innebära kostnader för FRA. Den föreslagna lagen ska dock komplettera den allmänna dataskyddsregleringen. Utbildningsinsatser är därmed nödvändiga redan i dag till följd av den regleringen. Den eventuella tillkommande kostnaden för utbildning med anledning av förslaget om registerlag bedöms vara så låg jämfört med kostnaden i dag att den bör rymmas inom FRA:s befintliga ekonomiska ramar.

Förslagen om ändringar i OSL

Förslaget till en ny sekretessbestämmelse 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. Detta förhållande bör dock inte vara aktuellt i sådan omfattning som leder till mätbara kostnader, varken för FRA eller domstolarna. Förslaget om en sekretessbrytande bestämmelse rörande utrikessekretessen innebär också att det kan uppkomma en viss ökad hantering avseende utlämnande av uppgifter med stöd av bestämmelsen. Utlämnande av information torde dock ske inom ramen för system och rutiner som redan finns på plats. Den marginella ökning av arbetsbördan som de aktuella bestämmelserna kan ge upphov till bör kunna hanteras inom befintliga ekonomiska ramar.

5.8 Säkerhetsskydd

Säkerhetsskydd är ett system av förebyggande åtgärder för att skydda säkerhetsskyddsklassificerade uppgifter och övrig säkerhetskänslig verksamhet mot antagonistiska handlingar. Säkerhetsskydd innefattar också skydd i andra fall av säkerhetsskyddsklassificerade uppgifter, exempelvis mot att uppgifter röjs som en följd av bristande säkerhetsrutiner. Säkerhetskänslig verksamhet är sådan verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd. Uttrycket ”Sveriges säkerhet” tar sikte på förhållanden av grundläggande betydelse för Sverige. Det kan handla om både militär och civil verksamhet, så länge verksamheten har en sådan betydelse. Förutom militär verksamhet kan det exempelvis vara fråga om central statsförvaltning och diplomatisk verksamhet eller viktig civil infrastruktur som flygplatser, energianläggningar och informationssystem för elektronisk kommunikation. Säkerhetsskyddsklassificerade uppgifter är sådana uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt OSL, eller uppgifter som skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig.

Frågan om säkerhetsskydd i NCSC utreddes i samband med förslaget om att centret skulle bli en del av FRA, se del 2 av promemorian *Ett nytt Nationellt cybersäkerhetscenter* (Fö2024/00785). I promemorian gjordes bedömningen att FRA är verksamhetsutövare för centrets verksamhet och har det övergripande ansvaret för säkerhetsskyddet. Utredningen delar denna bedömning, särskilt som NCSC numera är placerat inom FRA. Detta medför vid verksamhetsöverföringen till centret att FRA blir ansvarig för informations-säkerheten och den fysiska säkerheten för den utökade verksamheten vid centret.

Genom förslagen om verksamhetsöverföring blir FRA även personalsäkerhetsansvarig för den personal som flyttas över till centret från MSB. Enligt 2 kap. 4 § säkerhetsskyddslagen (2018:585) innebär detta att myndigheten ska förebygga att personer som inte är pålitliga från säkerhetssynpunkt deltar i en verksamhet där de kan få tillgång till säkerhetsskyddsklassificerade uppgifter eller i en verksamhet som av någon annan anledning är säkerhetskänslig. Den ska även säkerställa att de som deltar i säkerhetskänslig verksamhet har tillräcklig kunskap om säkerhetsskydd. Detta medför att FRA blir

ansvarig för att genomföra en säkerhetsprövning av all personal som omfattas av en eventuell verksamhetsövergång. Myndigheten är även ansvarig för att personalen har tillräcklig utbildning om säkerhetsskydd.

NCSC:s arbetsformer är emellertid ännu inte fastslagna varför det kan uppkomma situationer där det inte är självklart att FRA är ansvarig för säkerhetsskyddet. Exempelvis kan nämnas situationen där personal från samverkansmyndigheterna deltar i centrets verksamhet men använder den egna myndighetens it-system. Det kan inte uteslutas att det uppkommer behov av att träffa någon form av säkerhetsskyddsöverenskommelse mellan berörda aktörer.

5.9 Övriga konsekvenser

Utredningens förslag medför inga konsekvenser för jämställdheten mellan män och kvinnor, det kommunala självstyret eller Sveriges möjlighet att uppnå klimatmålen. De förslag som lämnas i kapitel 4 har konsekvenser för den personliga integriteten. De närmare konsekvenserna i den delen framgår av det kapitlet.

5.10 Tidpunkt för utvärdering av förslagen

Utredningen föreslår i kapitel 6 att både förslagen om verksamhetsöverföring och informationshantering ska träda i kraft den 1 juli 2026. Det är viktigt att i detta sammanhang betona att konsekvenserna av förslagen avseende överföring av arbetsuppgifter till FRA endast kan utvärderas i sin helhet genom att de utvärderas tillsammans med övriga förslag på informations- och cybersäkerhetsområdet som har eller kommer tas fram i närtid, så som implementeringen av NIS 2- och CER-direktiven i övrigt som bereds i Regeringskansliet, DORA-förordningen, Cyberresiliensförordningen och Cyber-solidaritetsakten. På samma sätt är det nödvändigt vid en utvärdering av förslagen om informationsdelning att ta hänsyn till andra ändringar avseende sekretess och dataskydd som kommit eller ska komma på området de närmsta åren. En effekt kan annars uppstå där förslag som var för sig kan betraktas som ändamålsenliga och proportionerliga tillsammans får en oproportionerligt stor negativ inverkan i förhållande till enskildas integritet.

Regeringen har i sin nationella strategi för cybersäkerhet för 2025–2029 (skr. 2024/25:121) satt upp målsättningar för NCSC:s verksamhet samt för en ändamålsenlig informationsdelning på området. Bifogat till strategin finns en handlingsplan som ska uppdateras löpande. Handlingsplanen bör därför vara en god utgångspunkt för en årlig utvärdering av förslagens konsekvenser med start efter ikraftträdandet. Regeringen bör även göra en fördjupad utvärdering av förslagens konsekvenser som en del av det arbete som kommer föranleda den nya cybersäkerhetsstrategin för 2030 och framåt.

6 Ikraftträdande och övergångsbestämmelser

Utredningens förslag: Samtliga författningsförslag ska träda i kraft den 1 juli 2026.

Utredningens bedömning: Det saknas behov av övergångsbestämmelser.

Författningsändringarna bör komma till stånd snarast möjligt, bland annat för att inte försena arbetet med den nationella cybersäkerhetsstrategin. Innan ikraftträdandet behövs dock sedvanlig tid för remissbehandling och beredning inom Regeringskansliet. Den myndighetsgemensamma projektgruppen innefattande Myndigheten för samhällsskydd och beredskap (MSB) och Försvarets radioanstalt (FRA) har anfört till utredningen att en verksamhetsöverföring kan ske tidigast den 1 juli 2026. Prognosen är avhängig en effektiv behandling inom Regeringskansliet, bland annat för att myndigheterna ska kunna påbörja förhandlingar med kommissionen avseende överföring av stödaftal och utnämmande av nytt nationellt samverkanscenter. Det saknas skäl att ifrågasätta denna prognos. Även finansieringen av myndigheterna måste vara beslutad. För att centerverksamheten ska kunna bedrivas på ett ändamålsenligt sätt behöver även förslagen avseende sekretess och personuppgiftsbehandling träda i kraft i anslutning till att verksamhetsöverföringen verkställs. Dessutom är det av yttersta vikt av att CSIRT-enheten och övriga funktioner är fullt operativa i samband med det svenska riksdagsvalet den 13 september 2026. Utredningen anser därför att en rimlig tidpunkt för författningsändringarna att träda i kraft är 1 juli 2026.

Tidpunkten för ikraftträdande medför att MSB under 2025 kommer att fortsätta bedriva sin befintliga verksamhet. Myndigheten kommer sannolikt tilldelas ytterligare uppgifter genom den kommande förordningen om cybersäkerhet. Det är av vikt att FRA involveras och hålls informerad om utvecklingen av verksamheten under denna övergångsperiod.

Utredningen har inte funnit att det finns något behov av övergångsbestämmelser. Därför föreslås inte några sådana.

7 Författningskommentar

7.1 Förslaget till lag om uppgiftsskyldighet vid samverkan i verksamhet inom det nationella cybersäkerhetscentret

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

I paragrafen anges lagens tillämpningsområde. Övervägandena finns i avsnitt 4.2.2.

En förutsättning för att lagen ska vara tillämplig är att det är fråga om samverkan som sker mellan myndigheter i verksamhet inom det nationella cybersäkerhetscentret (NCSC) vid Försvarets radioanstalt (FRA). Myndigheternas samverkan är reglerad i förordningen (2025:237) om det nationella cybersäkerhetscentret vid Försvarets radioanstalt (NCSC-förordningen). Enligt 4 § NCSC-förordningen ska FRA organisera, leda och planera verksamheten som bedrivs inom ramen för NCSC. FRA ska i den verksamheten samverka med samverkansmyndigheterna Försvarets materielverk, Förvarsmakten, MSB, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen. Av 5 § NCSC-förordningen framgår att samverkansmyndigheterna ska, inom ramen för sina respektive befintliga ansvarsområden, löpande bistå NCSC med kunskap, kompetens och information. NCSC ska på samma sätt bistå samverkansmyndigheterna med kunskap och information. Av samma bestämmelse framgår också att 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.

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 behandlas i avsnitt 4.2.4 och innehåller en sekretessbrytande uppgiftsskyldighet för de myndigheter som omfattas av lagen. Av 3 § framgår att endast de myndigheter som regeringen bestämmer kan vara uppgiftsskyldiga enligt paragrafen.

Uppgiftsskyldigheten gäller endast inom ramen för samverkan inom ramen för NCSC:s verksamhet. Utbyte av uppgifter i andra sammanhang får ske med stöd av andra bestämmelser, till exempel generalklausulen i 10 kap. 27 § offentlighet- och sekretesslagen (2009:400), förkortad OSL.

Uppgiftsskyldigheten gäller endast då en myndighet har behov av att få en viss uppgift från en annan myndighet för att delta i samverkan. Behovet av uppgifter kan variera eftersom myndigheters deltagande i NCSC kan se ut på olika sätt. Till exempel kan det vara fråga om att närvara vid möten, bidra med information eller vidta andra åtgärder inom NCSC:s verksamhetsområde som är relevanta för den samverkan som ska ske inom ramen för verksamheten.

Som exempel på när en myndighet kan ha behov av uppgifter kan nämnas att såväl NCSC som samverkansmyndigheterna har behov av att få del av samma information vid till exempel ett gemensamt möte.

Uppgifter kan lämnas efter förfrågan men också på eget initiativ, om myndigheten vet vilka uppgifter en annan myndighet behöver. I de flesta fall torde behovet av information väckas i ett pågående projekt eller det dagliga arbetet och därmed föregås av en diskussion mellan de berörda myndigheterna om behovet av och lämpligheten i att lämna ut viss information.

Utgångspunkten är att uppgifter ska lämnas ut om förutsättningarna enligt paragrafen är uppfyllda. Det är den utlämnande myndigheten som prövar om förutsättningarna är uppfyllda.

Uppgiftsskyldigheten blir inte tillämplig när det till exempel gäller uppgifter som erhållits genom internationella avtal. I OSL

finns ett antal bestämmelser om sekretess med anledning av internationella förpliktelser. Exempel på sådana bestämmelser är 15 kap. 1 a §, 27 kap. 5 § och 34 kap. 4 § OSL. Av dessa bestämmelser framgår att den sekretessbrytande bestämmelsen i bland annat 10 kap. 28 § OSL inte får tillämpas i strid mot ett sådant avtal. Eftersom lagen innebär en sådan uppgiftsskyldighet som avses i 10 kap. 28 § OSL, innebär det att lagen inte ger stöd för utlämnande av uppgifter som härrör från tillämpning av sådana avtal och rättsakter.

Enligt *andra stycket* behöver en uppgift inte 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. Det krävs inte att det alltid görs en prövning i varje enskilt fall utan en bedömning kan göras utifrån de behov av sekretess som typiskt sett finns för en viss kategori av uppgifter (jfr prop. 1979/80:2 Del A s. 80–81 och 326–327). Intresseavvägningen ger ett förhållandevis stort utrymme för en myndighet att avstå från att lämna ut en uppgift.

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. Som exempel på uppgifter som ofta skyddas av sekretess och som det kan finnas starka skäl att inte lämna ut kan nämnas 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. Uppgifter om myndighetens egna säkerhets- och bevakningsåtgärder kan också nämnas. 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. Uppgifter av särskilt integritetskänslig art kan utgöra sådana uppgifter, så som känsliga personuppgifter om hälsa eller politisk övertygelse. Den samverkan som ska ske inom ramen för NCSC:s verksamhet får inte inskränka en myndighets möjlighet att utföra sitt

primära uppdrag eller i övrigt försvåra myndighetens arbete och verksamhet.

Vid intresseavvägningen ska, som utgångspunkt, sekretesskyddet hos mottagaren vägas in. Det faktum att styrkan i sekretessen skiljer sig åt hos den utlämnande och den mottagande myndigheten är dock inte av avgörande betydelse.

Bestämmelsen påverkar inte regler om partsinsyn. Det innebär bland annat att sekretess för uppgifter i ett mål eller ärende hos en myndighet kan få ge vika för en parts rätt till insyn i målet eller ärendet. Vid intresseavvägningen kan detta behöva beaktas, i synnerhet när det är fråga om uppgifter vars röjande kan skada eller motverka en myndighets verksamhet.

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

Av paragrafen framgår att regeringen bestämmer vilka myndigheter som ska vara uppgiftsskyldiga eller som kan vara mottagare av uppgifter vid uppgiftslämnande med stöd av lagen. Som utgångspunkt är det i NCSC-förordningen som detta framgår. Övervägandena finns i avsnitt 4.2.5.

7.2 Förslaget till lag om behandling av personuppgifter i viss verksamhet vid Försvarets radioanstalt

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 det övergripande syftet med lagen. Övervägandena finns i avsnitt 4.5.3.

Syftet med lagen är dubbelt. Lagen ska dels göra det möjligt för FRA att behandla personuppgifter på ett ändamålsenligt sätt, 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 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.

Paragrafen anger lagens tillämpningsområde. Övervägandena finns i avsnitt 4.5.3.

Av *första stycket* framgår att lagen gäller vid behandling av personuppgifter i viss verksamhet vid FRA. Uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter inom NCSC framgår av 4 a § förordningen (2007:937) med instruktion för Försvarets radioanstalt.

Av *andra stycket* framgår att lagens tillämpningsområde begränsas till att avse helt eller delvis automatiserad behandling av personuppgifter och behandling av personuppgifter som ingår i eller kommer att ingå i ett register. Den föreslagna lagens tillämpningsområde motsvarar i denna del helt tillämpningsområdet för 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 (EU:s dataskyddsförordning). Av artikel 2.1 i EU:s dataskyddsförordning framgår 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 i eller kommer att ingå i ett register. Ett register är enligt definitionen i artikel 4.6 i EU:s dataskyddsförordning 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. Det innebär att manuell behandling av personuppgifter som inte ingår eller kommer att ingå i ett register faller utanför lagens tillämpningsområde.

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

I paragrafen föreskrivs att lagen inte gäller vid behandling av personuppgifter som omfattas av lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt. Övervägandena finns i avsnitt 4.5.3.

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.

Paragrafen anger lagens förhållande till EU:s dataskyddsförordning. Övervägandena finns i avsnitt 4.5.3.

I paragrafen upplyses om att lagen kompletterar EU:s dataskyddsförordning. EU:s dataskyddsförordning är direkt tillämplig men förutsätter och tillåter i vissa avseenden nationella bestämmelser som kompletterar förordningen. Lagen innehåller de kompletterande bestämmelser som gäller i den verksamhet som avses i 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 (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) och föreskrifter som har meddelats i anslutning till den lagen. Övervägandena finns i avsnitt 4.5.3.

Dataskyddslagen, som kompletterar EU:s dataskyddsförordning på nationell generell nivå, är subsidiär i förhållande till lagen. Bestämmelsen innebär att om inte något annat följer av lagen eller föreskrifter som har meddelats i anslutning till lagen, gäller dataskyddslagen och föreskrifter som har meddelats i anslutning till den.

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 4.5.3.

FRA är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten, inom ramen för de uppgifter som ska utföras inom NCSC, utför enligt lagen. FRA ansvarar därmed för att behandlingen utförs i enlighet med gällande dataskyddsreglering.

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 §.

Paragrafen anger de primära ändamålen för vilka personuppgifter får behandlas. Övervägandena finns i avsnitt 4.5.3.

Personuppgifter får behandlas om det är nödvändigt för att FRA ska kunna utföra uppgiften att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter inom NCSC. Ändamålen är brett formulerade och FRA måste därför 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. Att behandlingen ska vara nödvändig innebär inte ett krav på att behandlingsåtgärden ska vara oundgänglig. Behandlingen kan anses nödvändig om den leder till effektivitetsvinster (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 (se prop. 2017/18:232 s. 117).

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.

Paragrafen anger de ytterligare ändamål för vilka personuppgifter får behandlas. Övervägandena finns i avsnitt 4.5.3.

Av *första stycket* framgår att personuppgifter som behandlas enligt 7 § även får behandlas för att fullgöra uppgiftslämnande som sker i överensstämmelse med lag eller förordning. Behandlingen förutsätter således att uppgifterna redan är föremål för behandling enligt den primära ändamålsbestämmelsen. Behandling får då ske både för uppgiftslämnande som görs på grund av en skyldighet att lämna ut uppgifter och för uppgiftslämnande som görs med stöd av bestämmelser som innebär att uppgifter får lämnas ut, till exempel den så kallade generalklausulen i 10 kap. 27 § OSL. Bestämmelsen omfattar uppgiftslämnande både till andra myndigheter och till andra aktörer, så länge uppgiftslämnandet sker med stöd av lag eller förordning.

Andra stycket tydliggör att den så kallade finalitetsprincipen gäller vid behandling av personuppgifter enligt lagen. Bestämmelsen är utformad i nära anslutning till artikel 5.1 b i EU:s dataskyddsförordning och bör tolkas på samma sätt. 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 tillgången till personuppgifter. Övervägandena finns i avsnitt 4.5.3.

Uttrycket var och en inkluderar tillsvidareanställd personal men även till exempel personer med en tidsbegränsad anställning eller uppdragstagare. Den personal som deltar i NCSC:s verksamhet från samverkansmyndigheterna omfattas av bestämmelsen. FRA ska aktivt ta ställning till vilket informationsbehov ett tjänsteåliggande eller uppdrag medför och tilldela 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

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 §.

Paragrafen reglerar behandlingen av känsliga personuppgifter. Övervägandena finns i avsnitt 4.5.3.

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 de är nödvändiga för fullgörandet av uppgiften som anges i 2 §. Nödvändighetsrekvisitet har samma innebörd som i 7 § (jfr prop. 2017/18:105 s. 75), se också kommentaren till den paragrafen. Hänvisningarna till EU:s dataskyddsförordning är dynamiska och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

Sökbegränsningar

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

Paragrafen förbjuder vissa integritetskänsliga sökningar. Övervägandena finns i avsnitt 4.5.3.

Det är 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 bestämmelsen 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.

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 uppgiftslämnande. Övervägandena finns i avsnitt 4.5.3.

Bestämmelsen tydliggör att elektroniskt utlämnande på annat sätt än genom direktåtkomst är tillåtet. Det kan vara fråga om att personuppgifter lämnas ut på usb-minne, genom e-post eller genom direkt överföring från ett datasystem till ett annat via elektroniska kommunikationsnät.

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 har betydelse för om ett utlämnande är olämpligt. Typiskt sett kan det inte anses olämpligt att lämna ut uppgifter elektroniskt till en myndighet. När det gäller utlämnandet till andra än svenska myndigheter krävs en mer nyanserad bedömning med hänsyn till bland annat innehållet i handlingen och vem (till exempel en organisation eller ett företag) som är mottagare. Om FRA bedömer att det finns en risk för att uppgifterna missbrukas om de lämnas ut elektroniskt kan det vara olämpligt att lämna ut dem på det sättet. Vid prövningen av om personuppgifter bör lämnas ut elektroniskt bör även informations-säkerheten, det vill säga säkerheten hos mottagaren, vägas in.

Även 21 kap. 7 § OSL kan få betydelse vid lämplighetsprövningen. Enligt den bestämmelsen gäller sekretess för uppgifter om mottagaren kan antas komma att behandla uppgifterna på ett sätt som står i strid med bland annat EU:s dataskyddsförordning.

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 4.5.3.

I *första stycket* föreskrivs att personuppgifter inte får behandlas under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det handlar om vad som är nödvändigt för att FRA ska kunna utföra uppgiften som anges i 2 §. Det som avses är ändamålet i det enskilda fallet. Om uppgiften behandlas för flera olika ändamål, får den dock fortsätta att behandlas för de andra ändamålen om behovet av behandling kvarstår för dessa.

Av *andra stycket* framgår att bestämmelserna om längsta tid för behandling inte hindrar att personuppgifterna arkiveras 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 innehåller ett undantag från den registrerades rätt att göra invändningar enligt EU:s dataskyddsförordning. Övervägandena finns i avsnitt 4.5.3.

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 (artikel 6.1 e). Undantaget utgör en sådan begränsning i den nationella rätten som är tillåten enligt artikel 23 i EU:s dataskyddsförordning. Hänvisningen till förordningen är dynamisk och avser alltså förordningen i den vid varje tidpunkt gällande lydelsen.

7.3 Förslaget till lag om ändring av lagen om ändring av offentlighets- och sekretesslagen (2009:400)

15 kap.

3 c §

Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Myndigheten för samhällsskydd och beredskap.

En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Paragrafen innehåller en sekretessbrytande bestämmelse för Myndigheten för samhällsskydd och beredskap och tillsynsmyndigheter enligt viss lagstiftning. Övervägandena finns i avsnitt 4.4.1.

Ändringen utgörs av att hänvisningen till lagen (2025:000) om cybersäkerhet tagits bort från *första stycket*.

7.4 Förslaget till lag om ändring av offentlighets- och sekretesslagen (2009:400)

15 kap.

3 d §

Sekretessen enligt 1 a § hindrar inte att Försvarets radioanstalt lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om cybersäkerhet om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Försvarets radioanstalt.

En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Paragrafen är ny och innehåller en sekretessbrytande bestämmelse för FRA och tillsynsmyndigheter enligt lagen om cybersäkerhet när det gäller sekretess i det internationella samarbetet. Övervägandena finns i avsnitt 4.4.1.

Första stycket gör det möjligt för FRA att lämna en uppgift som avses i 15 kap. 1 a § OSL till en tillsynsmyndighet om det behövs för att tillsynsmyndigheten ska kunna utföra sina uppgifter enligt den nämnda lagen. Det rör sig till exempel om uppgifter i incident-rapporter och uppgifter som delges i samverkan med andra medlems-staters tillsynsmyndigheter enligt NIS 2-direktivet.

Andra stycket gör det möjligt för en tillsynsmyndighet att på samma sätt lämna en uppgift som avses i 15 kap. 1 a § OSL till FRA.

Enligt *tredje stycket* bryts sekretessen endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Det ska alltså göras en intresseavvägning.

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.

Paragrafen, som är ny, reglerar sekretess i viss verksamhet vid FRA. Övervägandena finns i avsnitt 4.3.7.

Av *första stycket* framgår att sekretess gäller hos FRA i verksamhet som bedrivs inom NCSC. Sekretessen gäller för uppgift om en enskilds personliga eller ekonomiska förhållanden. Med enskild avses såväl en fysisk som en juridisk person. Det kan typiskt sett röra sig om uppgifter om enskildas affärs- och driftförhållanden, vilket omfattas av begreppet ekonomiska förhållanden. Men även uppgifter av mer personlig karaktär omfattas, som exempelvis uppgifter om identiteten på den som rapporterat en sårbarhet. Skaderekvisitet i bestämmelsen 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* framgår att för uppgift i allmän handling gäller sekretessen i högst sjuttio år.

Av *tredje stycket* framgår att uppgifter som förekommer vid handläggning av ärenden om stöd enligt den nämnda förordningen inte omfattas av bestämmelsens tillämpningsområde.

8 §

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.

Övervägandena finns i avsnitt 4.3.7.

Ändringen i paragrafen är en följd av införandet av den nya bestämmelsen i 7 g § och innebär att tystnadsplikten som följer av den bestämmelsen inskränker den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Referenser

Offentligt tryck

Propositioner

- Prop. 1979/80:2, Del A, med förslag till sekretesslag m.m.
- Prop. 1992/93:120, om ändring i sekretesslagen (1980:100) med anledning av EES-avtalet.
- Prop. 2004/05:5, Vårt framtida försvar.
- Prop. 2005/06:133, Samverkan vid kris – för ett säkrare samhälle.
- Prop. 2005/06:173, Översyn av personuppgiftslagen.
- Prop. 2006/07:110, Rapportering av händelser inom civil luftfart m.m.
- Prop. 2009/10:80, En reformerad grundlag.
- Prop. 2009/10:231, Tredje sjösäkerhetspaketet – Del I.
- Prop. 2016/17:58, Uppgifter på individnivå i arbetsgivardeklarationen.
- Prop. 2017/18:89, Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag.
- Prop. 2017/18:254, Anpassning av utlänningsdatalagen till EU:s dataskyddsförordning.
- Prop. 2017/18:105, Ny dataskyddslag.
- Prop. 2017/18:113, Anpassning av domstolsdatalagen till EU:s dataskyddsförordning.
- Prop. 2017/18:115, Anpassning till EU:s dataskyddsförordning av lagen om behandling av personuppgifter i verksamhet med val och folkomröstningar.
- Prop. 2017/18:232, Brottssdatalag.
- Prop. 2017/18:298, Behandling av personuppgifter för forskningsändamål.

- Prop. 2019/20:106, Stärkt integritet i Rättsmedicinalverkets verksamhet.
- Prop. 2019/20:123, Ett effektivare informationsutbyte mellan polis och socialtjänst vid samverkan mot terrorism.
- Prop. 2020/21:194, Ett starkare skydd för Sveriges säkerhet.
- Prop. 2020/21:226, Behandling av personuppgifter vid Försvarsmakten och Försvarets radioanstalt.
- Prop. 2022/23:34, Utbetalningsmyndigheten.
- Prop. 2024/25:1, Budgetproposition utgiftsområde 6; försvar och samhällets krisberedskap.

Statens offentliga utredningar

- SOU 2018:63, Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt.
- SOU 2024:18, Nya regler om cybersäkerhet.
- SOU 2024:22, En ny organisation för förvaltning av EU-medel.
- SOU 2024:64, Motståndskraft i samhällsviktiga tjänster.

Departementsserien och promemorior

- Ds 2023:34, Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret.
- Fö2024/00785, Ett nytt Nationellt cybersäkerhetscenter del 1, ändamålsenliga och effektiva former för ledning, organisering och styrning.
- Fö2024/00785, Ett nytt Nationellt cybersäkerhetscenter del 2, förutsättningar för en effektiv verksamhet.

Kommittédirektiv

- Kommittédirektiv dir. 2024:119, Kompletterande bestämmelser till EU:s cyberresiliensförordning.

Regeringsbeslut m.m.

Fö2025/00387, Uppdrag till myndigheten för samhällsskydd och beredskap att vara behörig myndighet gällande vissa uppgifter enligt NIS2-direktivet.

Fö2025/00388, Uppdrag till försvarets radioanstalt att utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser.

Regeringens faktapromemoria 2022/23:FPM87, Cybersolidaritetsinitiativet.

Regeringens skrivelse 2024/25:121, En ny era av cybersäkerhet. Nationell strategi för cybersäkerhet 2025–2029.

Rättsfall och myndighetspraxis

EU-domstolens dom den 16 december 2008, Huber, mål C-524/06.

EU-domstolens dom den 4 juli 2023, Meta Platforms m.fl., C-252/21.

HFD 2021 ref. 10.

Integritetsskyddsmyndighetens beslut den 18 mars 2008 i dnr 1402–2007.

Integritetsskyddsmyndighetens beslut den 20 januari 2015 i dnr 905–2014.

RÅ 2007 ref. 45.

Internationella dokument

EU Grants: AGA – Annotated Grant Agreement: 2.0 1 April 2025.

Litteratur, publikationer m.m.

Ekonomistyrningsverket och Statskontoret (2024), *Redovisning av uppdrag att lämna förslag om organisationsförändring*
https://www.statskontoret.se/siteassets/rapporter-pdf/2024/2024_4---utskriftsversion.pdf, senast hämtad 2025-05-28.

- Friton, P. & Wolf, F. (2020) *The Protection Of "Key Defence And Security Technology" Under The Revised German Public Procurement Law And Its Compatibility With Article 346 TFEU* <https://urt.cc/wp-content/uploads/2023/03/Friton-Pascal-Wolf-Florian-The-protection-of-key-defence-and-security-technology-UrT-2020-p.-89-1.pdf>, senast hämtad 2025-06-02.
- Integritetsskyddsmyndigheten, *Rättsligt ställningstagande – innebörden av begreppet "personuppgifter som rör lagöverträdelse som innefattar brott" i artikel 10 i dataskyddsförordningen*, IMYRS 2021:1.
- Lenberg, E., Tansjö, A. & Geijer, U. (2024) *Offentlighets- och sekretesslagen*, version 30, JUNO.
- Otter Johansen, T. (2024) *Krisjuridik; rättsliga befogenheter från olycka till höjd beredskap*, version 1, JUNO.
- Statskontoret (2023), *När myndigheter ställer om – Erfarenheter av snabba omställningar* https://www.statskontoret.se/siteassets/rapporter-pdf/2023/oos_48---utskriftsversion.pdf, senast hämtad 2025-05-28.
- Totalförsvarets forskningsinstitut, *Delat ansvar är ingens ansvar? – En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete*, FOI-R5546--SE, 2024.

Kommittédirektiv 2024:111

Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet

Beslut vid regeringssammanträde den 14 november 2024

Sammanfattning

I Försvarsberedningens rapport Kraftsamling – Inriktningen av totalförsvaret och utformningen av det civila försvaret (Ds 2023:34) ifrågasätts om dagens myndighetsstruktur är ändamålsenlig för att uppnå en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete. Mot denna bakgrund ges en särskild utredare i uppdrag att utreda hur en överföring av arbetsuppgifter inom informations- och cybersäkerhet från Myndigheten för samhällsskydd och beredskap (MSB) till Försvarets radioanstalt (FRA) kan genomföras.

Utredaren ska bl.a.

- utreda och redovisa förutsättningarna för och konsekvenserna av en överföring av arbetsuppgifterna,
- analysera och bedöma hur överföring av uppgifter och ansvar för dessa påverkar samhällets motståndskraft på informations- och cybersäkerhetsområdet,
- analysera och föreslå vilka av MSB:s uppgifter inom informations- och cybersäkerhet som bör föras över till FRA, och
- lämna nödvändiga författningsförslag.

Uppdraget ska redovisas senast den 1 juli 2025.

Behovet av att se över ansvaret för vissa delar av samhällets informations- och cybersäkerhet

Det svenska samhället har i mycket snabb takt digitaliserats och näringslivet och samhällsviktiga tjänster är i dag beroende av digitala lösningar. Det har inneburit nya sårbarheter eftersom automatisering och digitalisering av alltifrån betalfunktioner till vatten- och avlopps-system gjort oss mer utsatta för t.ex. systemfel i den digitala miljön och cyberattacker. Med hänsyn till det allvarliga säkerhetsläget behöver en förändring ske snabbt. Arbetet med att ständigt effektivisera den samhällsviktiga infrastrukturen måste i största möjliga utsträckning anpassas efter vilka säkra digitala lösningar som finns tillgängliga.

I takt med samhällets ökande digitalisering är det viktigt att inte tappa fart i arbetet med att förebygga, upptäcka, stå emot och hantera problem som uppkommer när informations- och cybersäkerheten brister. Regeringen bedömer att dagens befintliga myndighetsstruktur när det gäller informations- och cybersäkerhet inte är ändamålsenlig utan behöver ses över för att bli mer samlad och funktionell.

Uppdraget att föreslå en ny struktur för en samlad styrning av vissa delar av informations- och cybersäkerhet

Informations- och cybersäkerhet är en grundläggande del av samhällets funktionalitet och har stor inverkan på näringslivet och medborgarnas vardag som helhet. För att stärka samarbetet mellan myndigheter och näringsliv och förbättra kunskapen om hur samhället på bästa sätt kan värnas vid cyberangrepp, samt för att skydda samhället vid andra större störningar, krävs att det finns såväl förmåga som adekvat stöd för att motstå, hantera och snabbt agera på händelser i cybermiljön. Detta är särskilt viktigt när cyberangrepp sker vid en kris, höjd beredskap eller i krig.

MSB och FRA har båda omfattande uppgifter inom informations- och cybersäkerhet. Enligt sin instruktion ska FRA ha hög teknisk kompetens inom informationssäkerhetsområdet och får efter begäran stödja andra myndigheter och enskilda verksamhetsutövare på området, bl.a. genom att ge tekniskt stöd. MSB har i uppgift att stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra stat-

liga myndigheter, kommuner och regioner samt till företag och organisationer. Båda myndigheterna arbetar således med att stärka samhällets motståndskraft på cybersäkerhetsområdet.

År 2020 gav regeringen FRA, Försvarmakten, MSB och Säkerhetspolisen i uppdrag att fördjupa samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter (NCSC) (beslut den 10 december 2020, Fö nr 8). Regeringen angav att dessa myndigheter skulle ha en nära samverkan med Försvarets materielverk, Polismyndigheten och Post- och telestyrelsen. Syftet med uppdraget var att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot. En utredare har biträtt Försvarsdepartementet med att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av NCSC kan utformas och föreslår bl.a. att FRA ska få ett huvudmannaskap för NCSC (Fö2024/00785). Förslagen har remitterats. FRA har efter en ändring av myndighetens instruktion, som beslutades den 19 september 2024, huvudmannaskap för NCSC från och med den 1 november 2024. Övriga förslag bereds inom Regeringskansliet.

Det finns skäl att i större uträkning än i dag – och med en bredare ansats än den tidigare utredningen hade i uppgift att föreslå – samla uppdrag och arbetsuppgifter rörande informations- och cybersäkerhet hos en och samma myndighet i syfte att uppnå ett mer ändamålsenligt informations- och cybersäkerhetsarbete. För att åstadkomma detta ska centrala delar av de arbetsuppgifter inom informations- och cybersäkerhet som MSB har i dag föras över till FRA. Utredaren ska därför undersöka och lämna förslag på vilka av MSB:s uppgifter rörande informations- och cybersäkerhet som bör överföras till FRA. En utgångspunkt för utredaren ska vara att en organisatorisk åtskillnad mellan stödjande verksamhet och tillsynsverksamhet inom cybersäkerhetsområdet ska upprätthållas. Utredaren ska säkerställa en tydlig ansvarsfördelning, utan överlapp eller dubblering av uppgifter och ansvar, och att verksamheten kan bedrivas effektivt utifrån de behov som finns att samla informations- och cybersäkerhetsfrågorna.

Samhällets behov av snabb och säker information om pågående it-incidenter är omfattande och ökar i takt med digitaliseringen. FRA behöver därför vid en överföring av uppgifter ha möjlighet att förmedla råd och stöd avseende hot, sårbarheter och risker. Vid en överföring av uppgifter behöver dessa behov tillgodoses och utredaren ska

därför utreda vilka förutsättningar FRA behöver för att kunna genomföra denna uppgift, i fråga om t.ex. personalresurser och lokaler.

MSB är Sveriges nationella CSIRT (computer incident response team) vilket innebär att myndigheten bl.a. har i uppgift att ta emot och hantera incidentrapporter från leverantörer enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Eftersom verksamheten som CSIRT-enhet regleras av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet) omfattas den av tillsyn från Europeiska unionens revisionsrätt i enlighet med artikel 287 i fördraget om Europeiska unionens funktions sätt. Det finns även möjlighet för MSB att ta emot finansiering från EU för denna verksamhet.

EU har enligt artikel 4.2 i fördraget om Europeiska unionen som huvudregel inte kompetens inom områden som rör medlemsstaternas nationella säkerhet eller försvar. Den största delen av FRA:s verksamhet, signalspaning i försvarsunderrättelseverksamhet, är sådan verksamhet som inte omfattas av EU:s kompetens. Det är viktigt att denna verksamhet även fortsatt kan bedrivas utan krav på ytterligare reglering eller insyn från EU. De övriga uppgifter hos MSB som omfattas av EU-lagstiftning granskas också av Europeiska unionens revisionsrätt. Revisionsrätten kan ta del av granskningar av verksamheten som ansvarig tillsynsmyndighet har genomfört. Det gäller i synnerhet om verksamheten utvecklas med stöd av EU-finansiering. Dessa förhållanden kvarstår även om verksamheten flyttas till annan myndighet.

Det är viktigt att överföringen av uppgifter genomförs på ett sätt som möjliggör att de delar av FRA:s verksamhet som rör nationell säkerhet och försvar inte omfattas av krav på insyn från EU.

Både MSB och FRA, var för sig och inom ramen för NCSC, spelar en viktig roll för svensk utrikes- och säkerhetspolitik på cyberområdet. Bland annat utgör MSB svensk teknisk kontaktpunkt i cyberarbetet inom Organisationen för säkerhet och samarbete i Europa (OSSE). Utredaren bör beakta hur en överföring av arbetsuppgifter kan bidra till ett mer samlat internationellt företrädeskap i cyberfrågor på myndighetsnivå.

Utredaren behöver även analysera om informationshantering som krävs med anledning av överföringen av arbetsuppgifter till FRA och NCSC medför något behov av ändringar i offentlighet- och sekretess-

lagstiftningen eller av regelverket som gäller för personuppgiftsbehandling. Utredaren behöver bl.a. ta ställning till om det finns förutsättningar för nödvändigt utbyte av information mellan MSB och FRA i samband med och efter överföringen av arbetsuppgifter. Utredaren behöver även analysera om det finns förutsättningar för att genomföra nödvändigt informationsutbyte mellan FRA och privata aktörer. I uppdraget ingår därmed bland annat att ta ställning till om nu gällande regelverk innebär ett tillräckligt skydd för uppgifter som kommer att utbytas.

Utredaren ska därför

- analysera och föreslå vilka uppgifter på informations- och cybersäkerhetsområdet hos MSB som bör föras över till FRA eller NCSC vid FRA, och när en sådan överföring kan och bör genomföras,
- analysera och föreslå hur överföringen från MSB till FRA av aktuella uppgifter kan genomföras,
- analysera och lämna förslag på hur FRA efter en överföring av uppgifter kan tillgodose regeringens och samhällets behov av snabb och säker information om cyberincidenter,
- analysera och föreslå hur rapportering och uppföljning av informations- och cybersäkerhetsverksamheten vid en överföring av uppgifter kan struktureras så att verksamheten blir möjlig för regeringen att följa upp över tid,
- analysera och lämna förslag på hur en överföring av uppgifter kan ske utan att Sveriges möjligheter att uppfylla sina EU-rättsliga förpliktelser eller få del av EU-rättsligt stöd påverkas,
- analysera om det finns behov av ändringar i offentlighets- och sekretesslagstiftningen och regelverket som gäller för personuppgiftsbehandling,
- analysera vilka följder en överföring av uppgifter får när det gäller FRA:s behov av personalresurser och lokaler,
- vid behov föreslå åtgärder för en fördjupad samverkan inom ramen för NCSC, och
- lämna nödvändiga författningsförslag.

Utredaren ska i analys och förslag säkerställa att en överföring av uppgifter inte inverkar negativt på de delar av FRA:s verksamhet som rör nationell säkerhet och försvar.

Konsekvensbeskrivningar

Utredaren ska i enlighet med kommittéförordningen (1998:1474) och förordningen (2024:183) om konsekvensutredningar ange kostnadsberäkningar och andra konsekvensbeskrivningar för sina förslag.

Utredaren ska

- i sina överväganden och förslag särskilt beakta de konsekvenser för MSB respektive FRA som en överföring av uppgifter får för respektive myndighets övriga uppdrag,
- klargöra vad en överföring av uppgifter medför för konsekvenser när det kommer till hanteringen av säkerhetsskyddsfrågor inom verksamheten,
- analysera vilka rättsliga konsekvenser, både nationella och EU-rättsliga, som en överföring av arbetsuppgifterna innebär,
- särskilt beakta konsekvenserna i förhållande till genomförandet av Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet), samt
- analysera och redovisa de verksamhetsmässiga och personella konsekvenserna av förslagen som lämnas.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och kommittéväsendet. Utredaren ska särskilt beakta arbetet med att ta hand om förslagen i promemoriorna Ett nytt Nationellt cybersäkerhetscenter – Ändamålsenliga och effektiva former för ledning, organisering och styrning och Ett nytt Nationellt cybersäkerhetscenter, Förutsättningar för en effektiv verksamhet (Fö2024/00785). Utredaren ska också beakta arbetet med att ta om hand förslagen i betänkandena Nya regler om cybersäker-

het (SOU 2024:18) och Motståndskraft i samhällsviktiga tjänster (SOU 2024:64).

Utredaren ska ha en nära dialog med MSB och FRA och kontakter bör även tas med andra myndigheter och organisationer som på olika sätt berörs av de frågeställningar som uppdraget omfattar, bl.a. de myndigheter som är tillsynsmyndigheter enligt NIS-direktivet. Utredaren ska ha en nära dialog med Arbetsgivarverket i arbetsrättsliga frågor. Utredaren ska fortlöpande hålla Regeringskansliet (Försvarsdepartementet) informerat om det löpande arbetet.

Utredaren får även ta upp och lämna förslag i andra frågor än de som nämns i dessa direktiv om frågorna har samband med uppdraget och det ändå kan redovisas i tid.

Uppdraget ska redovisas senast den 1 juli 2025.

(Försvarsdepartementet)

Statens offentliga utredningar 2025

Kronologisk förteckning

1. Skärpta krav för svenskt medborgarskap. Ju.
2. Några frågor om grundläggande fri- och rättigheter. Ju.
3. Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskattereglerna. Fi.
4. Moderna och enklare skatteregler för arbetslivet. Fi.
5. Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. LI.
6. Plikten kallar! En modern personalförsörjning av det civila försvaret. Fö.
7. Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. KN.
8. Bättre förutsättningar för trygghet och studiero i skolan. U.
9. På språklig grund. U.
10. En förändrad abortlag – för en god, säker och tillgänglig abortvård. S.
11. Straffbarhetsåldern. Ju.
12. AI-kommissionens Färdplan för Sverige. Fi.
13. En effektivare organisering av mindre myndigheter – analys och förslag. Fi.
14. En skärpt miljöstraffrätt och ett effektivt sanktionssystem. KN.
15. Stärkta drivkrafter och möjligheter för biståndsmottagare. Volym 1 och 2. S.
16. Ett nytt regelverk för uppsikt och förvar. Ju.
17. Anpassning av svensk rätt till EU:s avskogningsförordning. LI.
18. Ett likvärdigt betygssystem. Volym 1 och 2. U.
19. Kunskap för alla – nya läroplaner med fokus på undervisning och lärande. U.
20. Kommunal anslutning till Utbetalningsmyndighetens verksamhet. Fi.
21. Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). KN.
22. Förbättrad konkurrens i offentlig och privat verksamhet. KN.
23. Ersättningsregler med brottsoffret i fokus. Ju.
24. Publiken i fokus – reformer för ett starkare filmland. Ku.
25. Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. A.
26. Tid för undervisningsuppdraget – åtgärder för god undervisning och läraryrkenas attraktivitet. U.
27. En socionomutbildning i tiden. U.
28. Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. A.
29. Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. A.
30. Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. Fi.
31. Utmönstring av permanent uppehållstillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. Ju.
32. Vissa förändringar av jaktlagstiftningen. LI.
33. Skärpta och tydligare krav på vandel för uppehållstillstånd. Ju.
34. Ett modernare konsumentskydd vid distansavtal. Ju.
35. Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. A.

36. Skydd för biologisk mångfald i havsområden utanför nationell jurisdiktion. UD.
37. Skärpta villkor för friskolesektorn. U.
38. Att omhänderta barn och unga. S.
39. Digital teknik på lika villkor.
En reglering för socialtjänsten och verksamhet enligt LSS. S.
40. Säkrare tivoli. Ju.
41. Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. S.
42. Säkerhetsskyddslagen – ytterligare kompletteringar. Ju.
43. Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. S.
44. Förbättrat stöd i skolan. U.
45. Ökat informationsutbyte mellan myndigheter – några anslutande frågor. Ju.
46. Tryggare idrottsarrangemang. Ju.
47. Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? KN.
48. Stärkt pandemiberedskap. S.
49. Säkerhetspolisens behandling av personuppgifter. Ju.
50. En ny nationell myndighet för viltförvaltning. LI.
51. Bättre förutsättningar för klimatanpassning. KN.
52. Ökad insyn i politiska processer. Ju.
53. Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. S.
54. Ett skärpt regelverk om utvisning på grund av brott. Ju.
55. En reformerad samhällsorientering för bättre integration. A.
56. Stärkt skydd för domstolarnas och domarnas oberoende. Ju.
57. Polisär beredskap i fred, kris och krig. Ju.
58. En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. LI.
59. Stärkt lagstiftning mot hedersrelaterat våld och förtryck. Ju.
60. En starkare fondmarknad. Fi.
61. Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. S.
62. Ansvar för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. S.
63. Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. S.
64. En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. LI.
65. En mer flexibel hyresmarknad. Ju.
66. En straffreform. Volym 1, 2, 3 och 4. Ju.
67. Arlanda – en viktig port för det svenska väståndet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. LI.
68. Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. KN.
69. Effektivare samverkan för djur- och folkhälsa. LI.
70. Längre liv, längre arbetsliv – förlängd rätt att kvarstå i anställningen. A.
71. Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. S.
72. Verktyg för en mer likvärdig resursfördelning till skolan. U.
73. En arbetsmiljöstrategi för ett förändrat arbetsliv. A.
74. Ny reglering för den arbetsmarknadspolitiska verksamheten. A.
75. Folkbokföringsverksamhet, biometri och brottsbekämpning. Fi.
76. Det handlar om oss – så bryter vi utanförskapet och bygger en starkare gemenskap. A.
77. En översyn av den statliga lönegarantin. A.
78. En reformerad underrättelseverksamhet. Fö.
79. Samlade förmågor för ökad cybersäkerhet. Fö.

Statens offentliga utredningar 2025

Systematisk förteckning

Arbetsmarknadsdepartementet

- Arbetslivskriminalitet – upplägg, verktyg och åtgärder, fortsatt arbete. [25]
- Frihet från våld, förtryck och utnyttjande. En jämställdhetspolitisk strategi mot våld och en stärkt styrning av centrala myndigheter. [28]
- Ökad kvalitet hos Samhall och fler vägar till skyddat arbete. [29]
- Etableringsboendelagen – ett nytt system för bosättning för vissa nyanlända. [35]
- En reformerad samhällsorientering för bättre integration. [55]
- Längre liv, längre arbetsliv – förlängd rätt att kvarstå i anställningen. [70]
- En arbetsmiljöstrategi för ett förändrat arbetsliv. [73]
- Ny reglering för den arbetsmarknads-politiska verksamheten. [74]
- Det handlar om oss
– så bryter vi utanförskapet
och bygger en starkare gemenskap. [76]
- En översyn av den statliga löne-garantin. [77]

Finansdepartementet

- Skatteincitament för forskning och utveckling. En översyn av FoU-avdraget och expertskatte-reglerna. [3]
- Moderna och enklare skatteregler för arbetslivet. [4]
- AI-kommissionens Färdplan för Sverige. [12]
- En effektivare organisering av mindre myndigheter – analys och förslag. [13]
- Kommunal anslutning till Utbetalnings-myndighetens verksamhet. [20]
- Enklare mervärdesskatteregler vid försäljning av begagnade varor och donation av livsmedel. [30]
- En starkare fondmarknad. [60]

- Folkbokföringsverksamhet, biometri och brottsbekämpning. [75]

Försvarsdepartementet

- Plikten kallar! En modern personal-försörjning av det civila försvaret. [6]
- En reformerad underrättelse-verksamhet. [78]
- Samlade förmågor för ökad cybersäkerhet. [79]

Justitiedepartementet

- Skärpta krav för svenskt medborgarskap. [1]
- Några frågor om grundläggande fri- och rättigheter. [2]
- Straffbarhetsåldern. [11]
- Ett nytt regelverk för uppsikt och förvar. [16]
- Ersättningsregler med brottsoffret i fokus. [23]
- Utmönstring av permanent uppehålls-tillstånd och vissa anpassningar till miniminivån enligt EU:s migrations- och asylpakt. [31]
- Skärpta och tydligare krav på vandel för uppehållstillstånd. [33]
- Ett modernare konsumentskydd vid distansavtal. [34]
- Säkrare tivoli. [40]
- Säkerhetsskyddslagen – ytterligare kompletteringar. [42]
- Ökat informationsutbyte mellan myndigheter – några anslutande frågor. [45]
- Tryggare idrottsarrangemang. [46]
- Säkerhetspolisens behandling av personuppgifter. [49]
- Ökad insyn i politiska processer. [52]

Ett skärpt regelverk om utvisning på grund av brott. [54]
Stärkt skydd för domstolarnas och domarnas oberoende. [56]
Polisiär beredskap i fred, kris och krig. [57]
Stärkt lagstiftning mot hedersrelaterat våld och förtryck. [59]
En mer flexibel hyresmarknad. [65]
En straffreform. Volym 1, 2, 3 och 4. [66]

Klimat- och näringslivsdepartementet

Ny kärnkraft i Sverige – effektivare tillståndsprövning och ändamålsenliga avgifter. [7]
En skärpt miljöstraffrätt och ett effektivt sanktionssystem. [14]
Miljömålsberedningens förslag om en strategi för hur Sverige ska leva upp till EU:s åtaganden inom biologisk mångfald respektive nettoupptag av växthusgaser från markanvändningssektorn (LULUCF). [21]
Förbättrad konkurrens i offentlig och privat verksamhet. [22]
Spänning i tillvaron – hur säkrar vi vår framtida elförsörjning? [47]
Bättre förutsättningar för klimatanpassning. [51]
Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap. [68]

Kulturdepartementet

Publiken i fokus – reformer för ett starkare filmland. [24]

Landsbygds- och infrastrukturdepartementet

Avgift för områdessamverkan – och andra åtgärder för trygghet i byggd miljö. [5]
Anpassning av svensk rätt till EU:s avskogningsförordning. [17]
Vissa förändringar av jaktlagstiftningen. [32]
En ny nationell myndighet för viltförvaltning. [50]

En stärkt hästnäring – för företagande, jämställdhet, jämlikhet och folkhälsa. [58]
En ny kontrollorganisation i livsmedelskedjan – för ökad effektivitet, likvärdighet och konkurrenskraft. [64]
Arlanda – en viktig port för det svenska välståndet. Åtgärder som stärker konkurrenskraften för Arlanda flygplats. [67]
Effektivare samverkan för djur- och folkhälsa. [69]

Socialdepartementet

En förändrad abortlag – för en god, säker och tillgänglig abortvård. [10]
Stärkta drivkrafter och möjligheter för biståndsmottagare Volym 1 och 2. [15]
Att omhänderta barn och unga. [38]
Digital teknik på lika villkor.
En reglering för socialtjänsten och verksamhet enligt LSS. [39]
Pensionsnivåer och pensionsavgiften – analyser på hundra års sikt. [41]
Säkerställ tillgången till läkemedel – förordnande och utlämnande i bristsituationer. [43]
Stärkt pandemiberedskap. [48]
Kvalificering till socialförsäkring och ekonomiskt bistånd för vissa grupper. [53]
Sveriges internationella adoptionsverksamhet – lärdomar och vägen framåt. Volym 1 och 2. [61]
Ansvar för hälso- och sjukvården. Volym 1 Bedömningar och förslag. Volym 2 Underlagsrapporter. [62]
Stärkt patientsäkerhet genom rätt kompetens – utifrån hälso- och sjukvårdens och tandvårdens behov. [63]
Fortsatt utveckling av en nationell läkemedelslista – en del i en ny nationell infrastruktur för datadelning. Del 1 och 2. [71]

Utbildningsdepartementet

Bättre förutsättningar för trygghet
och studiero i skolan. [8]

På språklig grund. [9]

Ett likvärdigt betygssystem
Volym 1 och 2. [18]

Kunskap för alla – nya läroplaner med
fokus på undervisning och lärande. [19]

Tid för undervisningsuppgiften – åtgärder
för god undervisning och läraryrkenas
attraktivitet. [26]

En socionomutbildning i tiden. [27]

Skärpta villkor för friskolesektorn. [37]

Förbättrat stöd i skolan. [44]

Verktyg för en mer likvärdig
resursfördelning till skolan. [72]

Utrikesdepartementet

Skydd för biologisk mångfald i
havsområden utanför nationell
jurisdiktion. [36]