

Lagrådsremiss

Ett mer effektivt informationsutbyte vid Nationellt centrum för terrorhotbedömning

Regeringen överlämnar denna remiss till Lagrådet.

Gävle den 7 september 2017

Heléne Fritzon

Jenny Ferm
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Regeringen föreslår att Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten, inom ramen för samarbetet vid Nationellt centrum för terrorhotbedömning, ska få lämna ut uppgifter till varandra elektroniskt genom direktåtkomst. Förslaget syftar till att effektivisera det informationsutbyte som redan förekommer inom samarbetet i dag för att skapa bättre förutsättningar för myndigheterna att göra korrekta bedömningar av terrorhot i rätt tid. Förslaget innebär att varje myndighet vid Nationellt centrum för terrorhotbedömning ska få medge de övriga myndigheterna inom samarbetet direktåtkomst till sådana uppgifter som behövs för att kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Direktåtkomsten ska inte omfatta fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra. För att möjliggöra utlämnandet föreslås att sekretessbrytande bestämmelser i form av uppgiftsskyldigheter införs.

Lagändringarna föreslås träda i kraft den 1 mars 2018.

Innehållsförteckning

1	Beslut	4
2	Lagtext	5
2.1	Förslag till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst	5
2.2	Förslag till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet	7
2.3	Förslag till lag om ändring i polisdatalagen (2010:361)	9
3	Ärendet och dess beredning	11
4	Nationellt centrum för terrorhotbedömning	12
5	Pågående arbete med översyn av registerförfattningar	14
6	Personuppgiftsbehandling vid Nationellt centrum för terrorhotbedömning	16
7	Ett effektiviserat informationsutbyte	19
7.1	Det behöver bli enklare att utbyta uppgifter inom ramen för samarbetet	19
7.2	Utformningen av direktåtkomsten	23
7.3	Sekretess och uppgiftsskyldighet	27
7.4	Flera sekretessbestämmelser skyddar de överlämnade uppgifterna	31
8	Ikraftträdande	32
9	Konsekvenser	32
10	Författningskommentar	35
10.1	Förslaget till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst	35
10.2	Förslaget till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet	38
10.3	Förslaget till lag om ändring i polisdatalagen (2010:361)	40
Bilaga 1	Sammanfattning av departementspromemorian Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning (Ds 2016:31)	43

Bilaga 2	Lagförslag i departementspromemorian Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning (Ds 2016:31)	44
Bilaga 3	Förteckning över remissinstanserna	50

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst,

2. lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet,

3. lag om ändring i polisdatalagen (2010:361).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Härigenom föreskrivs i fråga om lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

dels att 1 kap. 15 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 15 a §, och närmast före 1 kap. 15 a § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap. 15 §

Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar *ytterligare föreskrifter eller beslut i enskilda fall om*

Regeringen meddelar föreskrifter om vilka myndigheter som *i andra fall* får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar

1. ytterligare föreskrifter eller

omfattningen av direktåtkomsten.

beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Uppgiftsskyldighet

15 a §

Säkerhetspolisen och Försvarets radioanstalt har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Denna lag träder i kraft den 1 mars 2018.

2.2 Förslag till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Härigenom föreskrivs i fråga om lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

dels att 1 kap. 15 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 15 a §, och närmast före 1 kap 15 a § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

15 §

Säkerhetspolisen och Försvarmakten får medges direktåtkomst till uppgifter som utgör analysresultat i en uppgiftssamling för analyser och som behövs för att myndigheterna, inom ramen för myndighetsöverskridande

samverkan mellan Försvarets radioanstalt, Försvarmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar *ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten.*

Regeringen meddelar föreskrifter om vilka myndigheter som *i andra fall* får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Uppgiftsskyldighet

15 a §

Säkerhetspolisen och Försvarsmakten har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Denna lag träder i kraft den 1 mars 2018.

2.3 Förslag till lag om ändring i polisdatalagen (2010:361)

Härigenom föreskrivs i fråga om polisdatalagen (2010:361)

dels att 2 kap. 21 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 6 kap. 11 a och 11 b §§, och närmast före 6 kap. 11 a § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 kap.

21 §

Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag.

Regeringen meddelar föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, om detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 § samt 4 kap. 10 och 17 §§.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 §, 4 kap. 10 och 17 §§ *samt 6 kap. 11 a §.*

6 kap.

*Direktåtkomst
och uppgiftsskyldighet*

11 a §

Försvarets radioanstalt och Försvarmakten får medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina

arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet vid sådan åtkomst.

11 b §

Försvarets radioanstalt och Försvarsmakten har, trots sekretess enligt 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 11 a § första stycket.

Denna lag träder i kraft den 1 mars 2018.

3 Ärendet och dess beredning

Nationellt centrum för terrorhotbedömning (NCT) är en permanent myndighetsgemensam arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten vid Försvarsmakten (Must). Säkerhetspolisen har i en skrivelse till regeringen (Ju2015/05096/L4) pekat på ett behov av att effektivisera uppgiftsutbytet inom ramen för samarbetet vid NCT. Säkerhetspolisen har föreslagit att myndigheten ska ges möjlighet att medge Försvarsmakten och FRA direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga för NCT-samarbetet i Säkerhetspolisens verksamhet om uppgifterna behövs för strategiska bedömningar av terrorhotet mot Sverige och svenska intressen. Säkerhetspolisen har uppgett att många av de uppgifter som NCT:s bedömningar och rapporter bygger på kommer från Säkerhetspolisens underrättelseinformation. Säkerhetspolisen anser därför att det är viktigt för samarbetet att berörda tjänstemän från de två andra myndigheterna har direktåtkomst till relevant information från Säkerhetspolisen.

Regeringen har i strategin mot terrorism som presenterats i skrivelsen Förebygga, förhindra och försvåra – den svenska strategin mot terrorism (skr. 2014/15:146) angett att regeringen ska verka för att uppgiftsutbytet inom NCT effektiviseras.

Den 10 december 2015 ingick regeringen en överenskommelse om ytterligare åtgärder mot terrorism med Moderaterna, Centerpartiet, Liberalerna och Kristdemokraterna. I överenskommelsen anges bl.a. att arbetet vid NCT ska effektiviseras genom att en lagändring som ger de samarbetande myndigheterna möjlighet att dela information digitalt ska utredas.

Inrikesministern beslutade den 1 oktober 2015 att ge en utredare i uppdrag att biträda Justitiedepartementet med att beskriva den verksamhet som bedrivs inom ramen för NCT, analysera de rättsliga förutsättningarna för Säkerhetspolisens, Försvarsmaktens och FRA:s personuppgiftsbehandling inom ramen för NCT-samarbetet och klarlägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling som sker. Utredaren skulle vidare analysera hur informationsutbytet kan effektiviseras och särskilt i vilken utsträckning Säkerhetspolisen ska kunna medge övriga myndigheter inom NCT direktåtkomst till uppgifter som är gemensamt tillgängliga för NCT-samarbetet i Säkerhetspolisens verksamhet om uppgifterna behövs för att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen (Ju2015/07312/P). Uppdraget har även kommit att omfatta i vilken utsträckning FRA respektive Försvarsmakten ska kunna medge övriga myndigheter inom NCT-samarbetet direktåtkomst till relevanta uppgifter. Uppdraget redovisades i augusti 2016 i departementspromemorian *Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning* (Ds 2016:31). En sammanfattning av promemorian finns i *bilaga 1* och promemorians lagförslag finns i *bilaga 2*. Promemorian har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2016/06351/L4).

4 Nationellt centrum för terrorhotbedömning

Nationellt centrum för terrorhotbedömning (NCT) är en myndighetsgemensam arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten vid Forsvarsmakten (Must). NCT bildades 2005 och är sedan 2009 en permanent arbetsgrupp som regleras i en skriftlig överenskommelse mellan myndigheterna.

Arbetsgruppen har till uppgift att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt. NCT producerar även strategiska analyser av händelser, trender och omvärldsutveckling med koppling till terrorism som berör, eller kan komma att beröra, Sverige och svenska intressen. Samarbetet inom NCT ger möjligheter att ta tillvara den samlade kompetens som finns hos de tre myndigheterna. NCT är därigenom den funktion i Sverige som har en överblick över allt tillgängligt material av strategisk karaktär med bäring på terrorism och därmed en unik möjlighet att bedöma utvecklingen när det gäller hot mot Sverige och svenska intressen.

Vid NCT arbetar analytiker från de tre myndigheterna i gemensamma lokaler hos Säkerhetspolisen. Bedömningarna delges delar av Regeringskansliet, samt i de flesta fall även myndigheterna inom Samverkansrådet mot terrorism, och syftar till att ge tidig förvarning om förändringar som kan påverka hotbilden mot Sverige och svenska intressen och som kan kräva åtgärder.

I regeringens strategi mot terrorism (Förebygga, förhindra och försvåra – den svenska strategin mot terrorism) konstateras bl.a. att tillgång till information är en grundläggande förutsättning för myndigheternas möjligheter att förhindra terroristbrottslighet. Myndigheterna måste ha tillgång till adekvat information i rätt tid och de måste också ha möjlighet att bearbeta och analysera denna information. Enligt regeringen är därför möjligheten till samverkan och informationsutbyte, såväl på strategisk nivå som i den operativa verksamheten, av stor vikt (skr. 2014/15:146). I strategin nämns NCT som ett exempel på strategisk samverkan som fyller en viktig funktion.

Att motverka terrorism är ett angeläget samhällsintresse och förutsätter en effektiv samverkan

Samarbetet inom NCT möjliggör ett tillvaratagande av Forsvarsmaktens, FRA:s och Säkerhetspolisens samlade kompetens. Det är av största vikt att NCT har en god förmåga att ge tidig förvarning om förändringar i terrorhotet mot Sverige och svenska intressen. NCT har en central funktion för hotbedömningar mot Sverige och svenska intressen och det är viktigt att samarbetet fortsätter och effektiviseras. För att NCT ska kunna leverera relevanta och aktuella strategiska bedömningar krävs att samtliga medarbetare vid NCT på ett effektivt sätt kan ta del av och använda underrättelseinformation från de samarbetande myndigheterna. Sådan information kan inkludera personuppgifter. Den information som

medarbetarna lägger till grund för sina bedömningar måste även vara aktuell och uppdaterad.

NCT:s bedömningar och rapporter baseras på sekretessbelagd information från alla de tre samarbetande myndigheterna. NCT:s analyser och bedömningar presenteras i olika typer av rapporter. NCT producerar ungefär 20–30 underrättelserapporter per år.

Medarbetarna vid NCT är uppkopplade mot sina hemmamyndigheters it-system och Säkerhetspolisens it-system. Respektive myndighets medarbetare har tillgång till en myndighetsspecifik mapp i Säkerhetspolisens it-system, till vilken medarbetare från de andra myndigheterna inte har tillgång. I Säkerhetspolisens it-system finns även en gemensam NCT-mapp, som medarbetarna från alla tre myndigheter har tillgång till. Den gemensamma mappen innehåller utkastet till de rapporter som ännu inte färdigställts. I promemorian har redogjorts för vilka bestämmelser i respektive registerförfattning som är tillämpliga när medarbetarna behandlar uppgifter dels i sina egna it-system, dels i de myndighetsspecifika mapparna i Säkerhetspolisens it-system. I de allra flesta situationer framgår det alltså tydligt vem som är ansvarig för vilken personuppgiftsbehandling, t.ex. genom att det endast är en av myndigheterna som har tillgång till personuppgifterna eller it-systemet.

Författande av rapporter

Rapporterna skrivs i den gemensamma NCT-mappen av en grupp analytiker. Det ska finnas minst en analytiker från varje NCT-myndighet med i den grupp som skriver rapporten. En av analytikerna brukar vara huvudredaktör för rapporten och skriva det mesta av texten, men analytikerna diskuterar och planerar innehållet i rapporten tillsammans. Analytikerna sitter ofta tillsammans och arbetar i rapportutkastet, men det förekommer också att en analytiker arbetar ensam i ett dokument. Rapportutkastet innehåller fotnoter med hänvisning till de källor som ligger till grund för bedömningen eftersom informationen i rapporterna i så stor utsträckning som möjligt ska följas av referenser till ursprungsdokument. Det kan röra sig om både offentliga källor och källor som av olika anledningar är hemliga eller känsliga.

Eftersom NCT gör strategiska bedömningar innehåller rapporterna generellt relativt få personuppgifter. De personuppgifter som förekommer i rapporterna brukar röra personer som alla tre NCT-myndigheterna redan känner till och behandlar uppgifter om, t.ex. ledare för större internationella terrornätverk. Alla analytiker som arbetar med en rapport har möjlighet att lägga till, ändra eller ta bort personuppgifter i rapportutkastet.

När en rapport har färdigställts upprättas den i en eller flera olika versioner och skickas till de myndigheter som ska få del av rapporten, däribland de tre NCT-myndigheterna. I dessa versioner har fotnoterna med hänvisning till hemliga och känsliga källor tagits bort. De upprättade rapporterna sparas och diarieförs hos respektive NCT-myndighet.

Tillsyn över behandlingen av personuppgifter vid de aktuella myndigheterna

Datainspektionen är tillsynsmyndighet när det gäller den behandling av personuppgifter som sker vid Försvarmakten, FRA och Säkerhetspolisen. Detta framgår av respektive myndighets registerförfattning. Säkerhets- och integritetsskyddsnämnden (SIN) har tillsynsansvar över den behandling av personuppgifter som utförs av Säkerhetspolisen enligt polisdatalagen (2010:361; PDL). Vidare har Statens inspektion för försvarsunderrättelseverksamheten (Siun) till uppgift att granska den personuppgiftsbehandling som utförs av FRA och Försvarmakten inom ramen för lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

SIN granskade under 2015 delar av den personuppgiftsbehandling som Säkerhetspolisen utför inom ramen för NCT-samarbetet. Nämnden kunde vid sin granskning inte se att Säkerhetspolisen behandlade några personuppgifter i strid med PDL. Nämnden konstaterade dock i sin rapport den 6 maj 2015 att gällande reglering inte är anpassad för sådant samarbete mellan myndigheter som förekommer inom ramen för NCT och att det därför finns en risk för att den enskildes integritet åsidosätts. Nämnden pekade särskilt på frågan om myndigheternas personuppgiftsansvar och konstaterade att det också finns sekretessrelaterade problem i samarbeten av nu aktuellt slag. Nämnden ansåg därför att det fanns anledning att närmare analysera de rättsliga förutsättningar som gäller vid samarbete av det slag som förekommer inom NCT (SIN dnr 324-2014, s.13). Siun genomförde den 14 oktober 2014 en övergripande granskning avseende viss personuppgiftsbehandling hos Försvarmakten och FRA inom NCT-samarbetet. Inspektionen uppmärksammade vid sin granskning inte några felaktigt behandlade personuppgifter. I protokollet har dock Siun konstaterat att det finns frågeställningar avseende förutsättningarna för Försvarmaktens och FRA:s personuppgiftsbehandling inom NCT-samarbetet, särskilt när det gäller personuppgiftsansvar och grund för behandling, som kan behöva utredas (Utdrag ur protokoll från nämndsammanträde den 18 november 2015, dnr 51-2014H:11).

5 Pågående arbete med översyn av registerförfattningar

Europeiska unionen har enats om en genomgripande dataskyddsreform som ska vara genomförd under våren 2018. Reformen omfattar dels en

allmän dataskyddsförordning¹, dels ett dataskyddsdirektiv som behandlar dataskyddet vid bl.a. brottsbekämpning, lagföring och straffverkställighet². Från förordningens tillämpningsområde undantas personuppgiftsbehandling som utförs av behöriga myndigheter i syfte att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straff, inkluderande skydd mot samt förebyggande av hot mot den allmänna säkerheten. Personuppgiftsbehandling för dessa syften ligger i stället under det nya dataskyddsdirektivets tillämpningsområde. Viss behandling av personuppgifter undantas från både dataskyddsförordningens och dataskyddsdirektivets tillämpningsområden. Det gäller personuppgiftsbehandling i verksamhet som inte omfattas av unionsrätten, däribland området nationell säkerhet.

En konsekvens av reformen är att personuppgiftslagen (1998:204) kommer att upphävas och att all lagstiftning om personuppgiftsbehandling behöver ses över och anpassas. Dataskyddsutredningen (Ju 2016:04) fick i februari 2016 i uppdrag att föreslå den kompletterande reglering som dataskyddsförordningen kan kräva och utreda vissa andra generella frågor som dataskyddsreformen väcker. Uppdraget redovisades den 12 maj 2017 i betänkandet Ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39).

Vidare har en särskild utredare fått i uppdrag att föreslå hur det nya direktivet ska genomföras i svensk rätt (Utredningen om 2016 års dataskyddsdirektiv, Ju 2016:06). Uppdraget delredovisades den 1 april 2017. Utredaren har i delbetänkandet Brottsdatalag (SOU 2017:29) föreslagit att direktivet i huvudsak ska genomföras genom en ny ramlag, brottsdatalagen. Lagen föreslås – i likhet med personuppgiftslagen – vara generellt tillämplig inom det område som direktivet reglerar. Lagen ska även vara subsidiär. De myndigheter som bedriver verksamhet inom lagens tillämpningsområde har i allmänhet särskilda registerförfattningar som reglerar personuppgiftsbehandlingen. Utredningen kommer att i slutbetänkandet föreslå de anpassningar som krävs med anledning av ramlagen i de registerförfattningar som ingår i utredningens uppdrag (vilket bl.a. omfattar personuppgiftsbehandling inom Säkerhetspolisen). Registerförfattningarna kommer att gälla utöver brottsdatalagen. Uppdraget ska slutredovisas den 30 september 2017.

En särskild utredare har fått i uppdrag göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom Försvarmakten och FRA. Syftet med uppdraget är att säkerställa att lagstiftningen är anpassad till den tekniska och legala utvecklingen. Utredaren ska bland annat analysera om rådande lagstiftning är ändamålsenlig för Försvarmaktens och FRA:s verksamheter och om den

¹ 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.

² 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.

är tillräcklig i fråga om skyddet för enskildas personliga integritet (Fö 2017:03). Uppdraget ska redovisas senast den 31 maj 2018.

6 Personuppgiftsbehandling vid Nationellt centrum för terrorhotbedömning

Regeringens bedömning: Det behöver inte införas något förtydligande författningsstöd för Säkerhetspolisens, Försvarets radioanstalts och Försvarmaktens behandling av personuppgifter inom ramen för samarbetet.

Promemorians bedömning överensstämmer med regeringens. **Remissinstanserna:** De flesta remissinstanserna instämmer i eller har inget att invända mot bedömningen, bl.a. *Försvarmakten, Försvarets radioanstalt (FRA), Säkerhetspolisens, Åklagarmyndigheten, Migrationsverket, Justitiekanslern, Försvarsunderrättsdomstolen, Riksdagens ombudsmän (JO), Tullverket, Kammarrätten i Göteborg, Brottsförebyggande rådet, Transportstyrelsen och Ekobrottsmyndigheten. Datainspektionen, Statens inspektion för försvarsunderrättelseverksamheten (Siun), Advokatsamfundet och Förvaltningsrätten i Stockholm* ifrågasätter om inte myndigheterna inom ramen för samarbetet kan komma att behandla sådana uppgifter som de inte får behandla med stöd av sina egna registerförfattningar. De anser med anledning av detta att frågan om ett förtydligande författningsstöd bör övervägas ytterligare. Även *Säkerhets- och integritetsskyddsnämnden (SIN)* anser att i vart fall principerna för fördelningen av personuppgiftsansvaret bör framgå av en författning. *Uppsala universitet* anser att det finns behov av en tydlig reglering av myndigheternas inbördes och gemensamma personuppgiftsansvar. *Göteborgs universitet* och *Totalförsvarets forskningsinstitut (FOI)* anser att Nationellt centrum för terrorhotbedömning (NCT) lämpligen borde göras till ett eget rättssubjekt.

Skälen för regeringens bedömning

Behandling av personuppgifter i den gemensamma mappen

Till skillnad från många andra samarbeten handlar NCT-samarbetet inte enbart om att utbyta information. Handläggarna vid NCT-myndigheterna arbetar också tillsammans i en gemensam mapp där de, med hjälp av underlag från de tre myndigheterna, gemensamt skriver rapporter med bedömningar av terrorhotet mot Sverige och svenska intressen. I den gemensamma NCT-mappen lägger myndigheterna in uppgifter från sina egna mapper som används vid framtagandet av rapporter. Detta innebär att handläggarna, när de därefter arbetar i ett dokument eller rapportutkast, kan komma att behandla även uppgifter som handläggare från de andra myndigheterna har lagt in i dokumentet.

En viktig utgångspunkt vid denna form av samarbete är att det finns ett tydligt stöd för den personuppgiftsbehandling som sker och att det inte

råder någon tvekan om vem som är ansvarig för sådan behandling. De samverkande myndigheterna deltar i samarbetet utifrån sina respektive uppdrag och utifrån respektive myndighets rättsliga regleringar. Av de relevanta registerförfattningarna följer att var och en av NCT-myndigheterna är ansvariga för den behandling av personuppgifter som myndigheten utför.

Datainspektionen, Siun, Advokatsamfundet och Förvaltningsrätten i Stockholm ifrågasätter om inte myndigheterna vid författandet av rapporter kan komma att behandla sådana uppgifter som de inte får behandla med stöd av sina egna registerförfattningar. De anser med anledning av detta att frågan om ett förtydligande författningsstöd bör övervägas ytterligare. *Göteborgs universitet* och *FOI* anser att den nu beskrivna personuppgiftsbehandlingen medför att NCT lämpligen borde göras till ett eget rättssubjekt.

Även om olika registerförfattningar med lite olika lydelse är tillämpliga för de myndigheter som samverkar inom NCT, styrs myndigheterna enligt regeringens mening av ändamålsbestämmelser med liknande innebörd, dvs. att personuppgifter får behandlas för att motverka terrorism. Samtliga myndigheter får alltså behandla personuppgifter i syfte att producera strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt. Samarbetet inom ramen för NCT har pågått under mer än 10 års tid och varit föremål för granskning av tillsynsmyndigheterna. Granskningarna visade inte att någon av de deltagande myndigheterna behandlat personuppgifter utan stöd i sina respektive registerförfattningar. Regeringen ser inte heller att tillämpningen av tre olika registerförfattningar medför några större problem i praktiken eftersom flertalet bestämmelser ser likadana ut i alla tre författningarna. Alla tre registerförfattningar med tillhörande förordningar ses för närvarande över i anledning av EU:s dataskyddsreform, som ska börja tillämpas under våren 2018.

När det gäller personuppgiftsansvaret för uppgifterna som behandlas i rapportutkasterna i den gemensamma mappen görs i promemorian bedömningen att myndigheterna är gemensamt och solidariskt ansvariga för behandlingen i de fall det inte går att urskilja vilken myndighet som har utfört en specifik behandling i ett rapportutkast och det heller inte på annat sätt går att urskilja någon tydlig fördelning av ansvaret. *Uppsala universitet* anser att det finns behov av en tydlig reglering av myndigheternas inbördes och gemensamma personuppgiftsansvar. *SIN* anför att i vart fall principerna för fördelningen av personuppgiftsansvaret bör framgå av en författning.

Regeringen konstaterar att samarbete mellan myndigheter är en förutsättning för ett effektivt arbete mot terrorism. Sådana samarbeten kan se olika ut och vara mer eller mindre formaliserade. Ett samarbete mellan två eller flera myndigheter medför inte automatiskt ett gemensamt ansvar för behandlingen av personuppgifter. Det avgörande är i stället om de deltagande myndigheterna i någon mån tillsammans bestämmer ändamålen med och medlen för behandlingen. I många fall då myndigheter samarbetar framgår det av de faktiska omständigheterna vem som är ansvarig för vilken personuppgiftsbehandling, t.ex. genom att det endast är en myndighet som har tillgång till personuppgifterna

eller it-systemet, eller om myndigheterna agerar i olika skeden av en process. Det förhållandet att två myndigheter använder samma datasystem eller att en myndighet ger en annan myndighet direktåtkomst till ett visst datasystem innebär inte heller per automatik att det uppstår ett gemensamt personuppgiftsansvar. Ibland förekommer dock att flera myndigheter är ansvariga för samma behandling, om samarbetet innebär att de deltagande myndigheterna bestämmer tillsammans exempelvis vilka uppgifter som ska läggas in, lagras eller tas bort. I likhet med utredningen bedömer regeringen att det finns omständigheter som talar för att ett gemensamt personuppgiftsansvar skulle kunna finnas för delar av den behandling av personuppgifter som sker i NCT:s arbete.

Frågan är om det nu beskrivna personuppgiftsansvaret innebär en sådan otydlighet för enskilda att det av den anledningen finns behov av att införa förtydligande författningsstöd för behandlingen. Ett otydligt personuppgiftsansvar kan innebära svårigheter för den enskilde att veta vem han eller hon ska vända sig till för att få information om personuppgiftsbehandlingen eller för att göra eventuella anspråk gällande. För tillsynen är det vidare av avgörande betydelse att personuppgiftsansvaret är tydligt.

Den verksamhet som NCT-myndigheterna bedriver omgärdas av stark sekretess, vilket innebär att enskilda registrerade ofta inte kan få någon insyn i verksamheten och personuppgiftsbehandlingen och således inte själva kan bevaka sina rättigheter. De få personuppgifter som förekommer i den gemensamma mappen där rapporterna skrivs, rör också i de flesta fall utländska medborgare som inte befinner sig i Sverige och som i praktiken aldrig kommer att vända sig till någon av myndigheterna med anledning av personuppgiftsbehandlingen. I stället har tillsynsmyndigheterna ett ansvar att granska och kontrollera den personuppgiftsbehandling som sker.

I promemorian har det föreslagits hur personuppgiftsansvaret kan förtydligas genom ändring av den skriftliga överenskommelse om samarbetet som gäller mellan myndigheterna. Vid bedömningen av om ett gemensamt personuppgiftsansvar över huvud taget uppstår i samband med en viss behandling kan tydliga överenskommelser mellan de behandlande myndigheterna om roller och ansvar för behandlingen vägas in, förutsatt att de är utformade på sätt som tillgodoser de registrerades rättigheter. En tydlig överenskommelse kan också medföra att innebörden av respektive myndighets personuppgiftsansvar inom samarbetet blir tydligare internt för de samarbetande myndigheterna, för tillsynsorganen, och – i förekommande fall – för enskilda registrerade. Därmed garanteras att dataskyddsbestämmelserna följs. Det är NCT-myndigheternas ansvar att ta ställning till om deras överenskommelse bör ändras i enlighet med förslaget eller på annat sätt.

Regeringen kan konstatera att det inte framkommit annat än att personuppgiftsbehandlingen inom samarbetet fungerar bra och att myndigheterna är väl medvetna om vad som innefattas i deras respektive personuppgiftsansvar och hur detta ansvar i praktiken ska utövas och avgränsas mellan myndigheterna.

Mot denna bakgrund anser regeringen att det för närvarande inte finns ett sådant behov av tydligare lagstöd för den nuvarande personuppgiftsbehandlingen inom NCT-samarbetet att det finns anledning att föreslå

sådana bestämmelser. Med hänsyn till att samtliga NCT-myndigheters registerförfattningar nu ses över, bl.a. med anledning av dataskyddsreformen, är det även för tidigt att nu göra en helhetsbedömning av dessa frågor, eftersom det fortfarande är osäkert hur myndigheternas regleringar kan komma att utformas i samband med det pågående arbetet med dataskyddsreformen.

Regeringen vill i detta sammanhang framhålla att slutsatserna ovan endast avser frågan om det finns behov av tydligare lagstöd för den nuvarande personuppgiftsbehandlingen inom NCT-samarbetet. Det är i rättstillämpningen som frågan om personuppgiftsansvarets fördelning slutligt avgörs. Det kan slutligen konstateras att frågan om NCT borde göras till ett eget rättssubjekt inte omfattas av detta lagstiftningsärende.

7 Ett effektiviserat informationsutbyte

7.1 Det behöver bli enklare att utbyta uppgifter inom ramen för samarbetet

Regeringens bedömning: Det informationsutbyte som förekommer inom ramen för samarbetet behöver effektiviseras.

Regeringens förslag: Säkerhetspolisen, Försvarmakten och Försvarets radioanstalt ska under vissa förutsättningar ges möjlighet att utbyta uppgifter elektroniskt genom direktåtkomst.

Promemorians bedömning och förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna tillstyrker eller har inga invändningar mot bedömningen och förslaget. *Försvarsunderrättelsesdomstolen* delar bedömningen att det är angeläget att förutsättningar skapas för en effektiv samverkan inom ramen för samarbetet. *Statens inspektion för försvarsunderrättelseverksamheten (Siun)* anför att det med hänsyn till uppgifternas integritetskänsliga karaktär samt att de inte primärt rör försvarsunderrättelseverksamhet, inte har presenterats tillräckliga skäl för att Försvarmakten och Försvarets radioanstalt (FRA) ska medges direktåtkomst till Säkerhetspolisens uppgifter. *Dataskydd.net* delar inte bedömningen eftersom behov saknas. Även *Advokatsamfundet*, *Totalförsvarets forskningsinstitut (FOI)*, *Uppsala Universitet* och *Göteborgs universitet* anser att verksamheten inom Nationellt centrum för terrorhotbedömning (NCT) bör utredas vidare när det gäller möjligheten att göra NCT till ett eget rättssubjekt samt i fråga om den rättsliga styrningen av verksamheten och informationssäkerheten innan direktåtkomst medges.

Skälen för regeringens bedömning och förslag

Informationsutbytet behöver effektiviseras

NCT-samarbetet är beroende av att myndigheterna utbyter information med varandra. Inom samarbetet sker informationsutbytet för närvarande främst muntligen eller på papper, vilket är tidskrävande och ineffektivt. De handlingar som kan bli aktuella att visa för övriga myndigheter inom samarbetet förvaras i respektive myndighets säkerhetsskåp. Även om myndigheterna genom väl inarbetade rutiner och kompetent personal har uppnått ett fungerande arbetssätt, tar detta förfarande för utbyte av information viktig tid i anspråk för medarbetarna och hämmar effektiviteten inom samarbetet. Information i underrättelserapporter och andra handlingar som skrivs ut och sparas i pappersform kan heller inte uppdateras och blir fort inaktuell. Den pappersbaserade hantering av information som i dag förekommer kan därför medföra en risk för att den information som utbyts är inaktuell och till och med felaktig. Detta innebär en fara ur integritetssynpunkt och kan även påverka NCT:s förmåga att göra korrekta bedömningar.

Ett manuellt utbyte av information innebär också att det alltid måste finnas en medarbetare från varje myndighet på plats vid NCT. Om så inte är fallet fördröjs informationsöverföringen till medarbetarna från de andra myndigheterna, vilket också kan få konsekvenser för NCT:s förmåga att göra korrekta bedömningar. Det medför också en risk för att NCT:s förmåga att ge tidig förvarning om förändringar av terrorhotet mot Sverige och svenska intressen påverkas.

Medarbetarna vid NCT behöver ha snabb tillgång till relevant underrättelseinformation från de tre myndigheterna för att kunna leverera relevanta och aktuella strategiska bedömningar. Operativ och tidskritisk information utgör ett centralt underlag för strategiska bedömningar eftersom bedömningarna snabbt kan behöva revideras om ny information kommer in. Sådan information kan även inkludera personuppgifter. Det kan t.ex. handla om ny information om en aktörs avsikt och förmåga att begå attentat mot mål i Sverige eller mot svenska intressen. Det finns således ett behov hos samtliga medarbetare vid NCT att omedelbart och självständigt kunna ta del av och använda uppgifter från de samarbetande myndigheterna. Ett förbättrat informationsutbyte inom samarbetet gör att myndigheterna kan utnyttja de samlade resurserna mer effektivt. Detta ökar förutsättningarna för myndigheterna att göra korrekta bedömningar av terrorhotet i rätt tid, vilket i sin tur ökar möjligheterna för övriga myndigheter och aktörer i samhället att vidta lämpliga åtgärder i arbetet med att bekämpa terrorism. Ett väl fungerande och effektivt NCT-samarbete medför därför inte bara förbättringar för NCT-myndigheterna, utan ger också övriga myndigheter och aktörer i samhället bättre förutsättningar i deras arbete. I längden medför detta också en ökad nationell säkerhet. Mot denna bakgrund anser regeringen att det finns ett behov av ett effektiviserat informationsutbyte inom NCT. Som konstaterats finns det även en risk för att den information som lämnas ut på papper, eller muntligen genom att en pappershandling visas, inte alltid är uppdaterad och således inte heller korrekt. Om handläggarna vid NCT ges möjlighet att genom direktåtkomst självständigt söka efter och ta del

av information direkt från de tre myndigheterna kan detta undvikas. Handläggarna skulle då i princip alltid ha tillgång till uppdaterad och aktuell information från de tre myndigheterna och dessutom ha möjlighet att jämföra den med annan tillgänglig information för att på så sätt göra korrekta bedömningar.

Ett alternativ till direktåtkomst som bör övervägas är att informationen överförs elektroniskt i varje enskilt fall, t.ex. genom e-post. Att i stället få del av information genom annan elektronisk överföring ger dock inte samma möjligheter. Dels kan uppgifter som lämnas ut på detta sätt fort bli inaktuella då de inte uppdateras efter att de har lämnat systemet, dels förutsätter sådant utlämnande att det finns personal på plats från varje myndighet för att administrera utlämnandet. Ett sådant elektroniskt utlämnande medför därför inte någon större effektivitetsvinst i förhållande till det utlämnande som förekommer inom samarbetet i dag. Att myndigheterna inom NCT, i stället för pappershantering eller muntligt utlämnande, skulle ges bättre möjligheter att utbyta information elektroniskt via exempelvis e-post skulle således inte innebära en tillräcklig förbättring.

I jämförelse med annat elektroniskt utlämnande innebär direktåtkomst ofta fördelar för den mottagande myndigheten, eftersom handläggande tjänstemän inte behöver begära ut de uppgifter som behövs från den utlämnande myndigheten utan själva kan söka den information som behövs i den utlämnande myndighetens uppgiftssamling. På samma sätt innebär direktåtkomst också fördelar för den utlämnande myndigheten, eftersom den inte behöver avsätta resurser för att hantera de förfrågningar om utlämnande som kommer in från andra myndigheter. Ett utlämnande genom direktåtkomst kan även innebära fördelar ur informationssäkerhetssynpunkt, eftersom överföring av information vid direktåtkomst kan ske på ett säkrare sätt än genom e-post.

Sammanfattningsvis är regeringens bedömning att ett effektivare och mer ändamålsenligt informationsutbyte inom NCT-samarbetet bäst uppnås genom att myndigheterna inom samarbetet får möjlighet att genom direktåtkomst ta del av relevant information från varandra.

Avvägningen mellan behovet av effektivitet och skyddet för den personliga integriteten

Den 1 januari 2011 förstärktes integritetsskyddet i grundlagen genom införandet av 2 kap. 6 § andra stycket regeringsformen. Enligt den bestämmelsen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär kartläggning eller övervakning av den enskildes personliga förhållanden. Även 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. Införandet av en möjlighet till direktåtkomst skulle kunna anses medföra en ökad risk för intrång i den personliga integriteten. Mot NCT-myndigheternas behov av ett effektiviserat informationsutbyte måste således vägas hänsynen till den enskildes integritet.

Datainspektionen anser att man i det fortsatta lagstiftningsarbetet rimligen bör utgå från att uppgifter som kommer att behandlas inom ramen för den föreslagna direktåtkomsten omfattar integritetskänsliga uppgifter från Säkerhetspolisens operativa verksamhet och dess verksamhetssystem. Vilken effekt det får för den personliga integriteten behöver enligt *Datainspektionen* klarläggas och analyseras. *Siun* anför att det med hänsyn till uppgifternas integritetskänsliga karaktär samt att de inte primärt rör försvarsunderrättelseverksamhet, inte har presenterats tillräckliga skäl för att Försvarsmakten och FRA ska medges direktåtkomst till Säkerhetspolisens uppgifter.

Vid polisdatalagens (2010:361; PDL) tillkomst gjordes bedömningen att direktåtkomst inte skulle medges till uppgifter hos Säkerhetspolisen. Skälen som angavs var att de uppgifter som Säkerhetspolisen behandlar är särskilt känsliga (prop. 2009/10:85 s. 179). Det är naturligtvis fortfarande så att de uppgifter som Säkerhetspolisen behandlar är av känslig natur. Inom NCT-samarbetet arbetar myndigheterna enbart med att göra strategiska bedömningar av terrorhotet och bedriver således ingen operativ verksamhet. Säkerhetspolisens behov av ett effektivare informationsutbyte har dessutom ökat sedan polisdatalagens tillkomst, inte minst med anledning av den utveckling på terrorområdet som skett i världen de senaste åren. Denna utveckling har också medfört att NCT har fått en allt viktigare roll. Mot denna bakgrund anser regeringen att det numera finns starka skäl som talar för att direktåtkomst till uppgifter hos Säkerhetspolisen i vissa fall bör kunna medges.

En viktig princip inom NCT-samarbetet är dessutom att de tre myndigheterna deltar på lika villkor. Myndigheterna har även själva påtalat att det finns ett behov för samtliga handläggare vid NCT att kunna ta del av uppgifter från alla tre myndigheterna. För att arbetet ska fungera så bra och effektivt som möjligt är det därför enligt regeringens bedömning viktigt att handläggarna från alla tre myndigheterna ges samma möjlighet till elektronisk åtkomst.

Vid en bedömning av vilka konsekvenser det aktuella förslaget kan få för enskildas personliga integritet kan konstateras att ett regelbundet uppgiftsutbyte mellan myndigheterna sker redan i dag. När det gäller tillgången till uppgifter inom en myndighet framgår det av respektive myndighets registerförfattning att tillgången ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Därutöver kan konstateras att tillgången till de uppgifter som ska lämnas ut genom direktåtkomst kommer att vara begränsad till den personal som deltar i NCT-samarbetet. Det är således en mycket snäv krets som kommer att ha tillgång till de uppgifter som görs tillgängliga via direktåtkomst. De ökade integritetsrisker som en möjlighet till direktåtkomst skulle kunna medföra motverkas genom bestämmelser av annat slag, t.ex. bestämmelser om sekretess, om tillgång till uppgifter och om informationssäkerhet.

Sammantaget gör regeringen bedömningen att alla tre myndigheterna har lika stort behov av att få direktåtkomst till övriga myndigheters uppgifter och att behovet av ett effektivt informationsutbyte genom direktåtkomst inom samarbetet väger tyngre än den eventuella risk för intrång i den personliga integriteten som ett sådant utbyte kan medföra.

NCT-myndigheterna bör därmed ges möjlighet att genom direktåtkomst ta del av uppgifter som behandlas i respektive myndighets verksamhet.

7.2 Utformningen av direktåtkomsten

Regeringens förslag: Försvarets radioanstalt (FRA) och Försvarsmakten ska få medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att dessa myndigheter, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. En upplysningsbestämmelse ska införas som anger att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om omfattningen av direktåtkomsten och om behörighet och säkerhet vid sådan åtkomst.

Säkerhetspolisen och Försvarsmakten ska få medges direktåtkomst till uppgifter som utgör analysresultat i en uppgiftssamling för analyser hos FRA och som behövs för att dessa myndigheter, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

Säkerhetspolisen och FRA ska få medges direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet hos Försvarsmakten som behövs för att dessa myndigheter, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

Även för FRA:s och Försvarsmaktens del ska en upplysningsbestämmelse införas som anger att regeringen eller den myndighet som regeringen bestämmer kan meddela föreskrifter om behörighet och säkerhet vid direktåtkomst.

I samtliga fall ska tillgången till uppgifterna vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna.

Promemorians förslag överensstämmer med regeringens.

Remissinstanserna: En majoritet av remissinstanserna instämmer i förslaget eller har inget att invända mot det. *Datainspektionen* och *Säkerhets- och integritetsskyddsnämnden (SIN)* anser att det finns anledning att i det fortsatta lagstiftningsarbetet närmare analysera vilka uppgifter som ska omfattas av direktåtkomst och hur dessa uppgifter praktiskt ska avgränsas i myndigheternas respektive it-system och uppgiftssamlingar. *Advokatsamfundet* anser att det bör införas en sekretessgräns mellan handläggare och respektive myndighet.

Skälen för regeringens förslag

Behörighetsbegränsningar och avgränsningar – inledning

Från ett integritetsperspektiv är det viktigt att det tydligt framgår vilka uppgifter som får inhämtas genom direktåtkomst. Det bör därför i bestämmelser om direktåtkomst så långt som möjligt uttryckligen framgå vilka uppgifter som får göras tillgängliga på detta sätt. *Datainspektionen* anför att medarbetarna inom NCT tar del av stora mängder information från sina egna system och att det för respektive medarbetare torde vara svårt att bedöma och avgränsa den mängd information som direktåtkomsten ska omfatta, varför en viktig fråga blir hur myndigheterna praktiskt avser att lösa behörighetsbegränsningar och avgränsningar i de olika uppgiftssamlingarna.

Regeringen instämmer i *Datainspektionens* bedömning att de uppgifter som respektive myndighet inom samarbetet ska kunna medges direktåtkomst till måste vara väl avgränsade. I detta fall är det dock inte möjligt att ange exakt vilken typ av uppgifter som myndigheterna ska få ta del av hos varandra. Den verksamhet som bedrivs inom NCT är inte sådan att det på förhand går att avgöra närmare vilka uppgifter som är relevanta att ta del av. Tillgången får i stället så långt som möjligt avgränsas genom att det i författningstext pekats ut en specifik uppgiftssamling eller uppgiftstyp samt genom att det anges att direktåtkomst medges endast för vissa särskilt angivna ändamål. Direktåtkomsten omfattar dock i princip inte fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra på paper eller muntligen.

Säkerhetspolisen har uppgett att de uppgifter som myndigheten har för avsikt att lämna ut är sådana som redan har gjorts gemensamt tillgängliga i verksamheten. Någon ytterligare avgränsning till exempelvis en viss uppgiftssamling är inte möjlig att göra med hänsyn till hur den relevanta informationen är tillgänglig i Säkerhetspolisens system. Direktåtkomst bör därför för Säkerhetspolisens del endast få medges till gemensamt tillgängliga uppgifter. Dessa uppgifter utbyts redan i dag muntligen eller på paper.

Av promemorian framgår att de uppgifter hos Försvarsmakten som är relevanta för NCT-samarbetet finns i myndighetens uppgiftssamlingar för försvarsunderrättelseverksamhet. För FRA:s del förekommer de för samarbetet relevanta uppgifterna i myndighetens uppgiftssamlingar för analyser. I dessa uppgiftssamlingar har dock övriga myndigheter, enligt FRA, endast behov av att ta del av uppgifter som utgör analysresultat. Direktåtkomst bör således för Försvarsmaktens och FRA:s del endast få medges till angivna uppgifter i de ovan nämnda uppgiftssamlingarna.

Inom ramen för de begränsningar regeringen föreslår, får var och en av myndigheterna själv bedöma vilka uppgifter som är relevanta för arbetet inom NCT och som till följd av det bör göras tillgängliga för övriga myndigheter. Självfallet kan endast sådana uppgifter göras tillgängliga som den mottagande myndigheten får behandla i sin verksamhet. Eftersom informationsutbytet mellan de berörda myndigheterna förekommer redan i dag, både inom NCT-samarbetet och inom ramen för annat samarbete, är myndigheterna emellertid vana vid att göra dessa avvägningar. Myndigheterna har också uppgett att detta fungerar väl i praktiken.

Direktåtkomst bör medges enbart till uppgifter som har betydelse för myndigheternas möjligheter att, inom samarbetet, kunna göra strategiska terrorhotbedömningar

En första förutsättning för att en myndighet inom samarbetet ska kunna medges direktåtkomst till annan myndighets uppgifter är att uppgifterna är gemensamt tillgängliga i verksamheten eller har gjorts gemensamt tillgängliga i en uppgiftssamling hos den senare myndigheten. Åtkomsten bör vidare begränsas till sådana uppgifter som den mottagande myndigheten verkligen kan antas ha behov av för att kunna utföra den uppgift som åligger myndigheten inom samarbetet. De uppgifter som myndigheterna ska få ta del av hos varandra ska således behövas för det specifika ändamål som NCT-samarbetet syftar till och den uppgift som myndigheterna inom ramen för detta har att utföra. Direktåtkomst bör därför bara ges till uppgifter som har betydelse för myndigheternas möjligheter att, inom samarbetet, kunna göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen. Uppgifterna som görs tillgängliga ska vidare bara användas inom ramen för NCT-samarbetet till stöd för strategiska bedömningar avseende internationell terrorism och inte i myndighetsutövning mot någon enskild. Den föreslagna bestämmelsen ska därför ange vilken typ av uppgifter hos myndigheterna som avses samt vilket behov som måste föreligga för att dessa uppgifter ska få lämnas ut. Vidare bör upplysas om att regeringen eller den myndighet som regeringen bestämmer har möjlighet att meddela närmare föreskrifter om omfattningen av direktåtkomsten.

SIN anser att avgränsningen i författningsförslaget är för oprecis och kan innebära risker för att även andra uppgifter än sådana som strikt behövs för bedömningar på strategisk nivå görs tillgängliga för direktåtkomst. En sådan risk är särskilt allvarlig med tanke på den syn som i dag råder på informationsutbyte mellan framför allt FRA och Säkerhetspolisen. *SIN* anser därför att regeringen bör avgränsa direktåtkomsten och att det av rättssäkerhetsskäl förefaller lämpligt att Säkerhetspolisen skapar en från verksamheten i övrigt skild uppgiftssamling för de uppgifter som Säkerhetspolisen avser att göra tillgängliga inom NCT-samarbetet.

När det gäller tillgången till uppgifter inom de aktuella myndigheterna framgår av respektive myndighets registerförfattning att tillgången ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Regeringen föreslår att detta ska förtydligas i bestämmelserna om direktåtkomst. I detta sammanhang bör också betonas att de uppgifter som nu föreslås ska göras tillgängliga genom direktåtkomst utgör en mycket begränsad del av alla de uppgifter som myndigheterna behandlar i sina respektive verksamheter. Handläggarna vid NCT har även en begränsad tillgång till uppgifter i den egna myndighetens system utifrån sin placering och sina arbetsuppgifter vid NCT. De uppgifter hos respektive myndighet som därutöver via direktåtkomst ska göras tillgängliga för handläggarna vid de andra myndigheterna, kommer att vara än mer begränsade mot bakgrund av den specifika verksamhet som bedrivs inom NCT och de tydligt avgränsade ändamål som gäller för denna verksamhet. I praktiken har därför medarbetarna avgränsat de uppgifter som kan göras tillgängliga genom direktåtkomst på så sätt att

medarbetarna skapat en från sin respektive verksamhet i övrigt skild uppgiftssamling för de uppgifter som myndigheten avser att göra tillgängliga för övriga inom NCT-samarbetet. SIN:s synpunkt föranleder därför inte någon vidare åtgärd.

Som framgår av promemorian finns inte någon sekretessgräns mellan handläggarna vid NCT och deras respektive myndigheter. *Advokatsamfundet* anser att det bör införas en sekretessgräns mellan handläggare och respektive myndighet. Handläggarna vid de tre myndigheterna utbyter dock redan i dag de aktuella uppgifterna och den omständigheten att uppgifterna inte omfattas av sekretess i förhållande till den egna myndigheten har hittills inte ansetts innebära några problem. Vidare kan konstateras att det av respektive myndighets registerförfattning följer att uppgifter endast bör behandlas i den mån det krävs för att en tjänsteman ska kunna fullgöra sina uppgifter. Regeringen anser därför till skillnad från *Advokatsamfundet* att det inte behöver införas någon sådan sekretessgräns.

Val av regleringsform

När det gäller Säkerhetspolisen har lagstiftaren ansett att direktåtkomst till uppgifter i Polismyndighetens brottsbekämpande verksamhet ska regleras i lag (se 2 kap. 21 § PDL) och det finns inte anledning att göra någon annan bedömning när det gäller direktåtkomst till uppgifter hos Säkerhetspolisen.

När det gäller FRA och Försvarsmakten har man inte ansett det lämpligt att detaljreglera dessa myndigheters verksamheter i lag. Det har ansetts gälla även i fråga om regleringen av direktåtkomsten (prop. 2006/07:46 s. 80). Här måste emellertid beaktas den nya lydelsen av 2 kap. 6 § regeringsformen, (RF), vilken trädde i kraft den 1 januari 2011. Bestämmelsen innebär att enskilda är skyddade mot åtgärder från det allmänna som innefattar betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Sammantaget med bestämmelsen i 2 kap. 20 § RF innebär den nya lydelsen av 2 kap. 6 § att åtgärder som innebär betydande intrång i den personliga integriteten måste regleras i lag. Grundlagsbestämmelsen omfattar således endast vissa kvalificerade intrång i den personliga integriteten. I förarbetena till 2 kap. 6 § andra stycket RF framhåller regeringen att flera omständigheter ska vägas in vid bedömningen av vad som kan anses vara ett betydande intrång, bl.a. uppgifternas karaktär och omfattning. Ju känsligare uppgifterna är, desto mer ingripande måste det allmännas hantering av uppgifterna normalt anses vara. Vid bedömningen av intrångets karaktär är också ändamålet med behandlingen och omfattningen av utlämnandet av uppgifter till andra av betydelse. En hantering som syftar till att utreda brott kan normalt anses vara mer känslig än t.ex. en behandling som uteslutande görs för att ge en myndighet underlag för förbättringar av kvaliteten i handläggningen (prop. 2009/10:80 s. 183–185).

Frågan är om det förhållandet att direktåtkomst medges till uppgifter hos FRA och Försvarsmakten innebär ett sådant intrång i enskildas personliga integritet att det omfattas av grundlagsbestämmelsens skydd. De uppgifter som FRA och Försvarsmakten behandlar och som ska

lämnas ut genom direktåtkomst kan visserligen vara av relativt känslig art. Det utlämnande som föreslås förutsätter också att sekretessen i vissa fall bryts mellan myndigheterna, vilket kan ses som att sekretessen till viss del försvagas mellan myndigheterna. I det här fallet rör det sig emellertid om uppgifter som myndigheterna redan kan lämna ut till varandra i dag och i varierande omfattning också rent faktiskt lämnar ut. Den föreslagna möjligheten till direktåtkomst innebär därför huvudsakligen att formen för utlämnandet förändras. Samtidigt ges de mottagande myndigheterna möjlighet att själva söka information bland de avgränsade uppgifter som den utlämnande myndigheten medger tillgång till. Detta är i och för sig en nyhet. Det är dock fråga om en relativt begränsad mängd uppgifter som lämnas ut och det är endast ett fåtal personer som kommer att ges möjlighet att ta del av uppgifterna genom direktåtkomst. Här rör det sig också om myndigheter vars verksamheter, även om de skiljer sig åt, har nära anknytning till varandra och många gånger förutsätter ett visst uppgiftsutbyte för att respektive myndighet ska kunna utföra sina uppgifter. Säkerhetspolisen och Försvarmakten inriktar exempelvis, och bestämmer härmed till viss del, FRA:s verksamhet. Mycket talar därför för att direktåtkomsten till FRA:s och Försvarmaktens uppgifter inom ramen för NCT-samarbetet inte kan anses innebära ett sådant betydande intrång i enskildas integritet som avses i 2 kap. 6 § andra stycket RF. Regeringen anser emellertid ändå att det i det här fallet kan vara lämpligt att reglera direktåtkomsten i lag, främst mot bakgrund av den känsliga verksamhet som myndigheterna inom NCT-samarbetet bedriver samt då utlämnandet förutsätter att sekretessbrytande bestämmelser om uppgiftsskyldighet faktiskt införs. Här bör också beaktas att Säkerhetspolisens utlämnande i samma situation enligt regeringens förslag ska regleras i lag.

7.3 Sekretess och uppgiftsskyldighet

Regeringens bedömning: För att myndigheterna inom NCT-samarbetet ska kunna lämna ut uppgifter till varandra genom direktåtkomst behöver det införas sekretessbrytande bestämmelser i form av uppgiftsskyldigheter.

Regeringens förslag: Trots sekretess enligt 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400; OSL) ska Försvarmakten och FRA ha rätt att ta del av sådana uppgifter som avses i den föreslagna regeln i 6 kap. 11 a § första stycket PDL.

Trots sekretess enligt 38 kap. 4 § OSL, ska Säkerhetspolisen och FRA ha rätt att ta del av sådana uppgifter som avses i den föreslagna regeln i 1 kap. 15 § första stycket lagen om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Trots sekretess enligt 38 kap. 4 § OSL, ska Säkerhetspolisen och Försvarmakten ha rätt att ta del av sådana uppgifter som avses i den föreslagna regeln i 1 kap. 15 § första stycket lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Promemorians bedömning och förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna uttalar sig inte i frågan. *SIN* ifrågasätter om inte annan sekretess än den som följer av de av utredningen angivna sekretessbestämmelserna kan gälla och att dessa bestämmelser skulle kunna förhindra ett utlämnande.

Skälen för regeringens bedömning och förslag

Tillämpliga sekretessbestämmelser

Som framgår av promemorian finns det en rad sekretessbestämmelser som gäller dels till skydd för den verksamhet som NCT-myndigheterna bedriver, dels till skydd för enskilda personliga och ekonomiska förhållanden i dessa verksamheter. De uppgifter som myndigheterna behandlar inom ramen för samarbetet omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ OSL, dvs. utrikes- och försvarssekretess, och 18 kap. 2 § OSL, vilken reglerar sekretess för uppgifter som hänför sig till underrättelseverksamhet som bedrivs för att förebygga, förhindra eller upptäcka brott. Bestämmelserna är tillämpliga på uppgifter som hänför sig till eller rör en viss verksamhet. Bestämmelserna omfattar således hela det allmänna verksamhet där det finns uppgifter som hänför sig till eller rör den verksamhet som anges i bestämmelserna. Sekretessbestämmelserna är primära hos de tre myndigheterna.

Uppgifter om enskilda i Säkerhetspolisens verksamhet omfattas som regel av sekretess enligt 35 kap. 1 § OSL. Bestämmelsen reglerar uppgifter som rör en enskilda personliga och ekonomiska förhållanden och som förekommer i verksamhet för att t.ex. förebygga brott. Uppgifter om enskilda hos Säkerhetspolisen kan även omfattas av sekretess enligt 37 kap. 1 § OSL och 21 kap. 5 § OSL. Enligt 21 kap. 5 § OSL gäller sekretess till skydd för utlännings säkerhet i vissa fall. Enligt 37 kap. 1 § OSL gäller sekretess i verksamhet för kontroll över utlänningar och i ärenden om svenskt medborgarskap. Uppgifter om enskilda i Försvarsmaktens och FRA:s verksamhet omfattas som regel av sekretess enligt 38 kap. 4 § OSL. Där anges att sekretess gäller hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos FRA i underrättelse- och säkerhetsverksamheten. Därutöver gäller även bestämmelsen i 21 kap. 5 § OSL för Försvarsmakten och FRA.

Sekretessgenombrott mellan NCT-myndigheterna

De föreslagna bestämmelserna om direktåtkomst reglerar endast tillåtligheten av ett visst tillvägagångssätt för att lämna ut uppgifter. Bestämmelserna har alltså inte någon självständig sekretessbrytande effekt. Eftersom direktåtkomst innebär att den mottagande myndigheten fritt kan avgöra vilka uppgifter – inom ramen för den beviljade direktåtkomsten – den vill ta del av, blir uppgifterna att anse som utlämnade i och med att direktåtkomst medges. En myndighet kan därför inte tillåta en annan myndighet direktåtkomst till uppgifter som, vid en sekretessprövning, den senare myndigheten inte med säkerhet skulle ha rätt att ta del av (prop. 2008/09:160 s. 73). Eftersom de uppgifter som FRA, Försvars-

makten och Säkerhetspolisen inom ramen för NCT-samarbetet har för avsikt att lämna ut till varandra genom direktåtkomst omfattas av sekretess behöver sekretessen således på förhand brytas.

För Försvarmaktens och FRA:s del finns en bestämmelse om uppgiftsskyldighet intagen i 2 § lagen (2000:130) om försvarsunderrättelseverksamhet. Där anges att underrättelser ska rapporteras till berörda myndigheter. Denna uppgiftsskyldighet omfattar dock inte den typ av uppgifter som myndigheterna inom samarbetet har behov av att utbyta och som det nu föreslås att de ska få tillgängliggöra genom direktåtkomst. För Säkerhetspolisens del finns ingen uppgiftsskyldighet avseende sådana uppgifter som myndigheten enligt förslaget ska få lämna ut. Frågan är således om sekretessen mellan myndigheterna bör brytas genom införande av bestämmelser om uppgiftsskyldighet eller om gällande bestämmelser är tillräckliga i detta avseende.

Utlämnande av uppgifter mellan myndigheterna inom NCT sker i dag genom tillämpning av generalklausulen i 10 kap. 27 § OSL. Bestämmelsen innebär att en sekretessbelagd uppgift får lämnas till en annan myndighet om det är uppenbart att intresset av att uppgifterna lämnas har företräde framför det intresse som sekretessen ska skydda. Detsamma gäller överlämnande av uppgifter mellan olika verksamhetsgrenar inom samma myndighet. I promemorian görs bedömningen att ett sådant utlämnande förutsätter att det görs en bedömning i varje enskilt fall av om uppgifterna trots sekretess kan lämnas ut eller inte. Det torde således i princip inte vara möjligt att på förhand göra en intresseavvägning gällande sådana uppgifter i allmänhet. För att myndigheterna inom samarbetet ska kunna lämna ut den här typen av uppgifter till varandra genom direktåtkomst krävs det därför att sekretessen bryts på annat sätt. Även om det rör sig om en relativt begränsad mängd uppgifter i varje myndighets verksamhet som kommer att göras tillgängliga på detta sätt, innebär det ändå ett rutinmässigt uppgiftsutbyte mellan myndigheterna. Mot denna bakgrund anser regeringen att det bör införas sekretessbrytande regler i form av uppgiftsskyldigheter till stöd för det utlämnande av uppgifter genom direktåtkomst som föreslås.

Vilka sekretessbestämmelser ska uppgiftsskyldigheten omfatta?

De uppgifter som NCT-myndigheterna vill medge direktåtkomst till omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 2 § OSL. Dessa sekretessbestämmelser avser att skydda nationens intressen samt den verksamhet som myndigheterna bedriver. Som framgår ovan är sekretessbestämmelserna primära hos alla tre myndigheterna. I princip torde det inte kunna anses medföra fara för rikets säkerhet eller innebära någon skada för myndigheternas respektive verksamheter eller för nationen att sådana uppgifter som här är aktuella lämnas ut till övriga myndigheter inom NCT-samarbetet. De uppgifter som myndigheterna vill kunna lämna ut till varandra genom direktåtkomst kan därför lämnas ut oavsett regleringen i 15 kap. 1 och 2 §§ samt 18 kap. 2 § OSL. Detsamma synes gälla ifråga om uppgifter som är sekretessreglerade i 21 kap. 5 § OSL. Denna bestämmelse gäller till skydd för utlännings säkerhet i vissa fall och är primär hos alla tre myndigheterna. Sekretess

gäller om det kan antas att röjande av uppgiften skulle medföra fara för att någon utsätts för övergrepp eller lider annat allvarligt men som föranleds av förhållandet mellan utlänningen och en utländsk stat eller myndighet eller organisation av utläningar. Regeringens bedömning är att utlämnande av uppgifter inom NCT-samarbetet inte medför någon sådan fara för enskilda eftersom den aktuella sekretessbestämmelsen är tillämplig hos alla tre myndigheterna. Det medför inte heller någon sådan fara i sig för den enskilde att uppgifter inom ramen för samarbetet lämnas mellan de tre NCT-myndigheterna. Skaderekvisitet kan således inte anses vara uppfyllt i detta fall heller och bestämmelsen hindrar därmed inte ett utlämnande inom samarbetet. Något generellt behov av att bryta den sekretess som eventuellt skulle kunna gälla enligt 15 kap. 1 och 2 §§, 18 kap. 2 § samt 21 kap. 5 § OSL kan således inte anses föreligga.

Uppgifter om enskildas personliga och ekonomiska förhållanden omfattas hos Säkerhetspolisen av sekretess enligt 35 kap. 1 § och 37 kap. 1 § OSL och hos FRA och Försvarsmakten av sekretess enligt 38 kap. 4 § OSL. Dessa tre bestämmelser är alla försedda med ett omvänt skaderekvisit. Uppgifterna har således samma sekretesskydd hos alla tre myndigheterna. Utlämnande av uppgifter som rör enskildas personliga eller ekonomiska förhållanden torde i den aktuella situationen nästan alltid anses vara till skada eller men för den enskilde.

De bestämmelser om uppgiftsskyldighet som föreslås bör således för Säkerhetspolisens del bryta den sekretess som gäller enligt 35 kap. 1 § och 37 kap. 1 § OSL och för FRA:s och Försvarsmaktens del den sekretess som gäller enligt 38 kap. 4 § OSL. I den mån annan sekretess gäller för uppgifterna bör direktåtkomst inte komma i fråga. I sådana fall får det i stället, på samma sätt som nu, göras en bedömning i det enskilda fallet av huruvida sekretessen hindrar att uppgifterna lämnas ut till en annan myndighet inom samarbetet eller om uppgiften kan lämnas ut med stöd av någon annan sekretessbrytande bestämmelse, exempelvis 10 kap. 27 § OSL. *SIN:s* synpunkt föranleder ingen annan bedömning.

De sekretessbrytande bestämmelsernas placering

Sekretessbrytande bestämmelser kan tas in i både lag och förordning. Mot bakgrund av polisverksamhetens särskilda natur har regeringen ansett att andra myndigheters tillgång till uppgifter som behandlas av polisen normalt bör regleras i lag (se prop. 2009/10:85 s. 193). Samma bedömning har regeringen gjort när det gäller andra myndigheters tillgång till uppgifter hos Kustbevakningen, Åklagarmyndigheten och Ekobrottsmyndigheten (se prop. 2011/12:45 s. 148 och prop. 2014/15:63 s. 109). Regeringen anser, i likhet med vad som anges i promemorian, att samma bedömning bör göras för Säkerhetspolisens del. Den sekretessbrytande uppgiftsskyldigheten för Säkerhetspolisen bör därför, tillsammans med bestämmelsen om direktåtkomst, tas in i PDL och placeras i 6 kap., där Säkerhetspolisens behandling av personuppgifter i övrigt regleras.

Liksom när det gäller polisverksamheten bör Säkerhetspolisens tillgång till uppgifter som behandlas av FRA och Försvarsmakten i allmänhet regleras i lag. FRA:s och Försvarsmaktens verksamheter omgärdas generellt av höga sekretess- och säkerhetskrav. Av verksamhetens

karaktär följer också att det är ett grundläggande krav att myndigheternas information inom såväl försvarsunderrättelseverksamheten som säkerhetstjänsten inte sprids till obehöriga (se prop. 2006/07:46 s. 80). Som framgår ovan har regeringen också föreslagit att bestämmelserna om direktåtkomst för FRA:s och Försvarsmaktens del ska införas i lag. Bestämmelserna om uppgiftsskyldighet är så nära förknippade med bestämmelserna om direktåtkomst att de bör placeras på samma normgivningsnivå och i anslutning till varandra.

7.4 Flera sekretessbestämmelser skyddar de överlämnade uppgifterna

Regeringens bedömning: Det behöver inte införas några nya sekretessbestämmelser till skydd för de uppgifter som lämnas mellan myndigheterna som samverkar inom ramen för NCT-samarbetet.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna har inte yttrat sig i frågan, med undantag för *Svenska Journalistförbundet* och *Tidningsutgivarna*, som betonar att förslaget innebär att handlingar som inkommer till den mottagande myndigheten genom direktåtkomst blir att anse som inkomna där och därmed kan begäras ut och att detta bör beaktas i det fortsatta lagstiftningsarbetet.

Skälen för regeringens bedömning: En viktig fråga när det gäller utlämnande genom direktåtkomst är om de uppgifter som ska lämnas ut omfattas av sekretess hos den mottagande myndigheten. Av 11 kap. 4 § OSL framgår att om en myndighet har direktåtkomst till sekretessreglerade uppgifter hos en annan myndighet blir sekretessbestämmelsen tillämplig även hos den mottagande myndigheten. Enligt 11 kap. 8 § OSL har dock primär sekretess företräde framför överförd sekretess. Bestämmelsen i 11 kap. 4 § OSL ska således inte tillämpas om det finns en annan primär sekretessbestämmelse till skydd för samma intressen som är tillämplig på uppgiften hos den mottagande myndigheten.

De uppgifter som NCT-myndigheterna vill medge direktåtkomst till omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 2 § OSL. Dessa bestämmelser är primära sekretessbestämmelser hos alla tre myndigheterna och ska således tillämpas av alla. Uppgifter hos de tre myndigheterna kan också omfattas av sekretess enligt 21 kap. 5 § OSL. Även denna bestämmelse är primär hos alla tre myndigheterna och ska således tillämpas av alla tre.

Avseende bestämmelserna till skydd för enskilda personliga och ekonomiska förhållanden gäller hos Säkerhetspolisen sekretess till skydd för enskild enligt 35 kap. 1 § och 37 kap. 1 § OSL. Hos FRA och Försvarsmakten skyddas uppgifter om enskilda genom sekretessbestämmelsen i 38 kap. 4 § OSL. Bestämmelserna är primära hos respektive myndighet och har således företräde framför överförd sekretess. Bestämmelserna i 35 kap. 1 §, 37 kap. 1 § och 38 kap. 4 § OSL är alla

försedda med ett omvänt skaderekvisit, vilket innebär att uppgifterna har samma sekretesskydd hos Säkerhetspolisen, FRA och Försvarsmakten.

Det kan således konstateras att de uppgifter som Säkerhetspolisen, FRA och Försvarsmakten ges möjlighet att lämna ut till varandra genom direktåtkomst omfattas av sekretess till skydd för samma intressen och med samma styrka hos alla tre myndigheterna. Regeringens bedömning är därför att det inte behöver införas några kompletterande sekretessbestämmelser med anledning av förslaget om direktåtkomst. De synpunkter som framförts av *Tidningsutgivarna* och *Svenska Journalistförbundet* medför ingen annan bedömning i detta avseende.

8 Ikraftträdande

Regeringens förslag: Lagändringarna ska träda i kraft den 1 mars 2018.

Promemorians förslag innebär att lagändringarna ska träda i kraft den 1 januari 2018.

Remissinstanserna uttalar sig inte i frågan.

Skälen för regeringens förslag: De föreslagna författningsändringarna är angelägna och bör träda i kraft så snart som möjligt. Ett tidigare ikraftträdande än den 1 mars 2018 är inte möjligt. Regeringen bedömer att det inte behövs några övergångsbestämmelser.

9 Konsekvenser

Regeringens bedömning: Förslagen förväntas få positiva konsekvenser för förmågan att göra relevanta terrorhotbedömningar. Den risk för ökat integritetsintrång som förslagen kan medföra är acceptabel i förhållande till det samhällsintresse som bekämpningen av terroristbrottslighet utgör. Förslagen ger inte upphov till kostnader som inte kan täckas av myndigheternas befintliga anslag.

Promemorians bedömning överensstämmer med regeringens.

Remissinstanserna: *Uppsala Universitet* pekar på att Säkerhets- och integritetsskyddsnämndens (SIN) och Statens inspektion för försvarsunderrättelseverksamhetens (Siun) resurser bör förstärkas som en konsekvens av förslagen. Universitetet anför att den överlappande och splittrade regleringen av området innebär i sig en inte obetydlig svårighet för såväl övervakningsorganen som riksdagen att följa verksamheten, vilket försvårar förutsättningarna för ansvarsutkrävande. Enligt *Totalförsvarets forskningsinstitut (FOI)* är en särskild fråga vem som utövar tillsyn över NCT på informationssäkerhetsområdet när Försvarsmakten och Säkerhetspolisen var för sig är föreskrivande, deltagande och

tillsynsmyndigheter i samma verksamhet. Detta eftersom de i samarbetet ingående myndigheterna, med utgångspunkt i sin uppgift, lyder under två olika departement (Försvarsdepartementet och Justitiedepartementet). Försvarsmakten (Must) har enligt säkerhetsskyddsförordningen (1996:633) föreskriftsrätt angående verkställigheten av säkerhetsskyddslagen (1996:627) över de myndigheter som lyder under Försvarsdepartementet, medan Säkerhetspolisen har föreskriftsrätt över övriga myndigheter, utom Justitiekanslern. Försvarsmakten (Must) och Säkerhetspolisen utövar tillsyn över de myndigheter som de har föreskriftsrätt på säkerhetsskyddsområdet.

Skälen för regeringens bedömning

Konsekvenser för förmågan att göra relevanta terrorhotbedömningar och ekonomiska konsekvenser

Syftet med lagförslagen är att underlätta myndigheternas samverkan mot terroristbrottslighet. Förslagen innebär att Säkerhetspolisen, FRA och Försvarsmakten, inom ramen för NCT-samarbetet, ges rätt att lämna ut uppgifter till varandra genom direktåtkomst. NCT-myndigheterna lämnar redan i dag ut uppgifter till varandra i betydande omfattning. Förslagen innebär därför främst att de ges möjlighet att inrätta system där de själva kan söka efter dessa uppgifter och på elektronisk väg ta del av dem. Detta förväntas medföra en ytterligare effektivisering av verksamheten inom NCT, vilken i sin tur kan förväntas ge de samverkande myndigheterna bättre förutsättningar i arbetet mot terrorism.

De kostnader som förslagen kan komma att innebära är enligt regeringens bedömning marginella. Det rör sig bl.a. om kostnader för eventuella utbildningsinsatser och framtagande av riktlinjer för de tjänstemän som arbetar vid NCT. Myndigheterna måste också komma överens i frågor om t.ex. förutsättningarna för direktåtkomsten och de praktiska lösningarna. Vissa kostnader kan inledningsvis uppkomma till följd av detta. Ett elektroniskt utlämnande genom direktåtkomst bedöms kunna genomföras inom myndigheternas befintliga it-system och torde således inte kräva några nya tekniska lösningar. De kostnader som kan uppkomma för att man ska kunna lösa direktåtkomsten rent tekniskt rymms inom myndigheternas anslag.

Uppsala Universitet anför att SIN:s och Siuns resurser bör förstärkas som en konsekvens av förslagen. Ingen av tillsynsmyndigheterna har framfört några synpunkter avseende merkostnader till följd av förslagen. Det kan också konstateras att det informationsutbyte mellan NCT-myndigheterna som förslaget avser redan pågår – om än i annan form än den som nu föreslås – och därmed står under tillsyn.

Sammantaget gör regeringen bedömningen att kostnaderna för de inblandade myndigheterna – såväl NCT-myndigheterna som tillsynsmyndigheterna – bör bli marginella och därför kan rymmas inom respektive myndighets befintliga ekonomiska ramar.

Enligt *FOI* är en särskild fråga vem som utövar tillsyn över NCT på informationssäkerhetsområdet när Försvarsmakten och Säkerhetspolisen var för sig är föreskrivande, deltagande och tillsynsmyndigheter i samma verksamhet. Frågan om tillsyn över myndigheter på säkerhetsskyddsområdet omfattas av Utredningen om utkontraktering av

säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd (Ju 2017:08). Uppdraget ska redovisas senast den 1 maj 2018.

Konsekvenser för den personliga integriteten

I svensk rätt finns ingen definition av begreppet integritet. En kränkning av den personliga integriteten kan beskrivas 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 (prop. 2005/06:173 s. 15).

En annan aspekt på integritet är att medborgare kan kräva att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger att staten måste anstränga sig för att se till att brott förebyggs, förhindras och utreds och att gärningsmän ställs till svars för sina brottsliga handlingar. Staten har alltså ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. En väl fungerande samhällsorganisation kommer alltid att medföra vissa intrång i enskildas personliga integritet.

Vid en bedömning av förslagets konsekvenser för den personliga integriteten kan det inledningsvis konstateras att det rör sig om uppgiftsutbyte mellan myndigheter och inte uppgiftslämnande till enskild. Myndigheter har att förhålla sig till regler som sätter gränser för deras uppdrag och verksamhet, det finns regler för hantering och spridning av information och tjänstemän är underkastade tjänstefelsansvar.

Av stor betydelse för bedömningen är också det förhållandet att myndigheterna redan i dag kan utbyta och rent faktiskt också utbyter mycket av den information som direktåtkomsten tar sikte på. Förslagen innebär därför främst en möjlighet för myndigheterna att i fortsättningen själva söka efter dessa uppgifter och på elektronisk väg ta del av dem. Det kan emellertid inte uteslutas att direktåtkomsten kommer att medföra ett visst ökat uppgiftsutbyte, vilket i sig kan få konsekvenser för den personliga integriteten. Det har dessutom ansetts att direktåtkomst generellt medför vissa risker för integritetsintrång, jämfört med t.ex. ett manuellt utlämnande av uppgifter. För att myndigheterna inom NCT-samarbetet ska kunna utbyta uppgifter med hjälp av direktåtkomst krävs vidare vissa regler som gör att uppgifterna kan lämnas ut trots sekretess till skydd för den enskilde.

De ökade integritetsrisker som en möjlighet till direktåtkomst skulle kunna medföra motverkas genom bestämmelser av annat slag, t.ex. bestämmelser om sekretess, om tillgång till uppgifter och om informations-säkerhet. I myndigheternas registerförfattningar finns även regler som sätter gränser för behandlingen av personuppgifter, t.ex. regler om behandling av känsliga uppgifter, om gallring och om tillgång till och utlämnande av uppgifter. Det är vidare en mycket begränsad krets av tjänstemän vid respektive myndighet som kommer att ges möjlighet att ta del av uppgifter genom direktåtkomst. Genom utformningen av bestämmelserna har de uppgifter som direktåtkomsten ska få avse dessutom begränsats till vad som är nödvändigt för det specifika ändamålet med NCT-verksamheten och de uppgifter som myndigheterna har att utföra inom ramen för samarbetet.

En ytterligare konsekvens av förslaget om direktåtkomst för den enskilde är att förslaget gör det lättare för myndigheterna att få information om och kartlägga vissa individer som är intressanta för bedömningen av terrorhotet mot Sverige och svenska intressen. Det eventuella integritetsintrång som detta kan medföra för dessa personer är något som de enligt regeringens mening i och för sig får räkna med. Mot det integritetsintrång som utbytet av uppgifter riskerar att medföra ska ställas det starka samhälleliga intresset av att motverka och bekämpa terrorism. Detta ändamål innebär att vissa begränsningar av integritetsskyddet får anses vara godtagbara. Enligt regeringen är den avvägning mellan effektivitet och integritet som görs i promemorian på ett övergripande plan godtagbar.

Sammanfattningsvis kan konstateras att de föreslagna bestämmelserna i och för sig skulle kunna leda till en ökad risk för integritetsintrång. Genom de begränsningar som föreslås i bestämmelserna och de regler som i övrigt styr myndigheternas uppdrag och verksamhet, får den risken emellertid anses godtagbar i förhållande till samhällets intresse av att terrorism bekämpas.

Övriga konsekvenser

Förslagen bedöms inte ha några konsekvenser när det gäller kostnader och intäkter för kommuner, landsting, företag eller andra enskilda. Inte heller bedöms förslagen ha några konsekvenser för den kommunala självstyrelsen, sysselsättningen, den offentliga servicen i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företag. De föreslagna bestämmelserna bedöms inte heller ha någon påverkan på jämställdheten mellan män och kvinnor, möjligheterna att nå de integrationspolitiska målen eller miljön.

10 Författningskommentar

10.1 Förslaget till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

1 kap.

15 §

Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som i andra fall får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Paragrafen reglerar direktåtkomst till uppgiftssamlingar hos Försvarsmakten.

I *första stycket* har det införts en ny bestämmelse som ger Försvarsmakten möjlighet att lämna ut uppgifter genom direktåtkomst till Säkerhetspolisen och Försvarets radioanstalt (FRA) inom ramen för samarbetet i Nationellt centrum för terrorhotbedömning (NCT). Övervägandena finns i avsnitt 7.2.

Med direktåtkomst avses att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat eller på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I uttrycket direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle får del av. Bestämmelser om direktåtkomst har inte någon sekretessbrytande verkan.

Säkerhetspolisens och FRA:s direktåtkomst enligt paragrafen är begränsad till uppgifter som finns i en uppgiftssamling för försvarsunderrättelseverksamhet. Direktåtkomst får dessutom bara medges till uppgifter som bedöms nödvändiga för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Det är Försvarsmakten som avgör vilka uppgifter det finns behov av att lämna ut.

Bestämmelsen ger Försvarsmakten möjlighet att medge direktåtkomst, men innebär inte någon rätt för mottagarna att få sådan åtkomst. En bestämmelse om direktåtkomst anger endast i vilken form uppgifter får lämnas ut. Möjligheten att lämna ut vissa uppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Något utlämnande genom direktåtkomst får inte ske om utlämnandet förutsätter en sekretessprövning. I och med att det i 1 kap. 15 a § införs en sekretessbrytande bestämmelse kan dock uppgifter som omfattas av den bestämmelsen lämnas ut genom direktåtkomst.

Med utgångspunkt i paragrafens bestämmelser och eventuella föreskrifter får Försvarsmakten avgöra om myndigheten kan medge de angivna myndigheterna direktåtkomst och i så fall i vilken omfattning.

Av bestämmelsen framgår att tillgången till uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom ramen för samverkan behöver ha tillgång till uppgifterna. Den mottagande myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften. Att tillgången förutsätter att

personen har ett behov av uppgifterna inom ramen för samverkan innebär en ytterligare begränsning av tillgången utöver den allmänna begränsningen enligt 1 kap. 16 § i lagen.

Bestämmelsen reglerar enbart Försvarsmaktens möjlighet att lämna ut uppgifter genom direktåtkomst till Säkerhetspolisen och FRA inom ramen för viss myndighetsöverskridande samverkan myndigheterna emellan, och påverkar inte Försvarsmaktens möjlighet att i övrigt lämna ut uppgifter genom direktåtkomst till FRA enligt 8 § förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

I *andra stycket* har det gjorts en ändring med anledning av att bestämmelsen i första stycket har införts. Eftersom utlämnande genom direktåtkomst till Säkerhetspolisen och FRA inom ramen för NCT-samarbetet regleras i första stycket anger upplysningsbestämmelsen i andra stycket att regeringen i andra fall meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. Detta innebär att regeringen inte kan medge ytterligare myndigheter direktåtkomst inom ramen för NCT-samarbetet.

I *tredje stycket* har det i den befintliga bestämmelsen införts en ytterligare upplysning om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om behörighet och säkerhet vid direktåtkomst.

Uppgiftsskyldighet

15 a §

Säkerhetspolisen och Försvarets radioanstalt har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Paragrafen är ny och reglerar viss uppgiftsskyldighet för Försvarsmakten. Övervägandena finns i avsnitt 7.3.

I bestämmelsen anges att Säkerhetspolisen och FRA har rätt att ta del av sådana uppgifter som avses i 15 § första stycket. Myndigheterna ges genom bestämmelsen en rätt att ta del av samma uppgifter som de får medges direktåtkomst till. Detta innebär att FRA och Säkerhetspolisen, trots viss i paragrafen angiven sekretess till skydd för enskild, har rätt att ta del av sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Uppgiftsskyldigheten gäller bara inom ramen för NCT-samarbetet. Genom FRA:s och Säkerhetspolisens rätt att ta del av uppgifterna uppkommer en sådan uppgiftsskyldighet som enligt 10 kap. 28 § första stycket OSL bryter sekretessen enligt den angivna sekretessbestämmelsen.

10.2 Förslaget till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

1 kap.

15 §

Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till uppgifter som utgör analysresultat i en uppgiftssamling för analyser och som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom sådan samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som i andra fall får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, och

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Paragrafen reglerar direktåtkomst till uppgiftssamlingar hos FRA.

I första stycket har det införts en ny bestämmelse som ger FRA möjlighet att lämna ut uppgifter genom direktåtkomst till Säkerhetspolisen och Försvarsmakten inom ramen för samarbetet i NCT. Övervägandena finns i avsnitt 7.2.

Med direktåtkomst avses att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat eller på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I uttrycket direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle får del av. Bestämmelser om direktåtkomst har inte någon sekretessbrytande verkan.

Säkerhetspolisens och Försvarsmaktens direktåtkomst enligt paragrafen är begränsad till uppgifter som utgör analysresultat i en uppgiftssamling för analyser. Direktåtkomst får dessutom bara medges till uppgifter som bedöms nödvändiga för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Det är FRA som avgör vilka uppgifter det finns behov av att lämna ut.

Bestämmelsen ger FRA möjlighet att medge direktåtkomst, men innebär inte någon rätt för mottagarna att få sådan åtkomst. En bestämmelse om direktåtkomst anger endast i vilken form uppgifter får lämnas ut. Möjligheten att lämna ut vissa uppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Något

utlämnande genom direktåtkomst får inte ske om utlämnandet förutsätter en sekretessprövning. I och med att det i 1 kap. 15 a § införs en sekretessbrytande bestämmelse kan dock uppgifter som omfattas av den bestämmelsen lämnas ut genom direktåtkomst.

Med utgångspunkt i paragrafens bestämmelser och eventuella föreskrifter får FRA avgöra om myndigheten kan medge de angivna myndigheterna direktåtkomst och i så fall i vilken omfattning.

Av bestämmelsen framgår att tillgången till uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom ramen för samverkan behöver ha tillgång till uppgifterna. Den mottagande myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften. Att tillgången förutsätter att personen har ett behov av uppgifterna inom ramen för samverkan innebär en ytterligare begränsning av tillgången utöver den allmänna begränsningen enligt 1 kap. 16 § i lagen.

I *andra stycket* har det gjorts en ändring med anledning av att bestämmelsen i första stycket har införts. Eftersom utlämnande genom direktåtkomst till Säkerhetspolisen och Försvarmakten nu regleras i första stycket anger upplysningsbestämmelsen i andra stycket att regeringen i andra fall meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. Detta innebär att regeringen inte kan medge ytterligare myndigheter direktåtkomst inom ramen för NCT-samarbetet.

I *tredje stycket* har det i den befintliga bestämmelsen införts en ytterligare upplysning om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om behörighet och säkerhet vid direktåtkomst.

Uppgiftsskyldighet

15 a §

Säkerhetspolisen och Försvarmakten har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Paragrafen är ny och reglerar viss uppgiftsskyldighet för FRA. Övervägandena finns i avsnitt 7.3.

I bestämmelsen anges att Säkerhetspolisen och Försvarmakten har rätt att ta del av sådana uppgifter som avses i 15 § första stycket. Myndigheterna ges genom bestämmelsen en rätt att ta del av samma uppgifter som de får medges direktåtkomst till. Detta innebär att Försvarmakten och Säkerhetspolisen, trots viss i paragrafen angiven sekretess till skydd för enskild, har rätt att ta del av uppgifter som utgör analysresultat i en uppgiftssamling för analyser och som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan FRA, Försvarmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Uppgiftsskyldigheten gäller bara inom ramen för NCT-samarbetet. Genom Försvarmaktens och Säkerhetspolisens rätt att ta del av uppgifterna uppkommer en sådan uppgiftsskyldighet som enligt 10 kap.

28 § första stycket OSL bryter sekretessen enligt den angivna sekretessbestämmelsen.

10.3 Förslaget till lag om ändring i polisdatalagen (2010:361)

2 kap.

21 §

Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag.

Regeringen meddelar föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, om detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 §, 4 kap. 10 och 17 §§ samt 6 kap. 11 a §.

Paragrafen reglerar direktåtkomst. Bestämmelsen har endast ändrats på så sätt att det i *tredje stycket*, där det anges vilka övriga bestämmelser i lagen som reglerar direktåtkomst, har lagts till en hänvisning till bestämmelsen om direktåtkomst i 6 kap. 11 a §.

6 kap.

Direktåtkomst och uppgiftsskyldighet

11 a §

Försvarets radioanstalt och Försvarsmakten får medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet vid sådan åtkomst.

Paragrafen är ny och reglerar direktåtkomst till uppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet. Övervägandena finns i avsnitt 7.2.

Med direktåtkomst avses att någon har direkt tillgång till register, databaser eller andra samlingar av uppgifter som behandlas automatiserat

eller på egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen. I uttrycket direktåtkomst ligger också att den som är ansvarig för uppgiftssamlingen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst tillfälle får del av. Bestämmelser om direktåtkomst har inte någon sekretessbrytande verkan.

I *första stycket* regleras Säkerhetspolisens möjlighet att lämna ut uppgifter genom direktåtkomst till FRA och Försvarmakten inom ramen för samarbetet i NCT. Direktåtkomsten är begränsad till uppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet. Direktåtkomst får dessutom bara medges till uppgifter som bedöms nödvändiga för att myndigheterna, inom ramen för myndighetsöverskridande samverkan mellan FRA, Försvarmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Det är Säkerhetspolisen som avgör vilka uppgifter det finns behov av att lämna ut.

Bestämmelsen ger Säkerhetspolisen möjlighet att medge direktåtkomst, men innebär inte någon rätt för mottagarna att få sådan åtkomst. En bestämmelse om direktåtkomst anger endast i vilken form uppgifter får lämnas ut. Möjligheten att lämna ut vissa uppgifter genom direktåtkomst kan vara begränsad genom att uppgifterna är skyddade av sekretess. Något utlämnande genom direktåtkomst får inte ske om utlämnandet förutsätter en sekretessprövning. I och med att det i 6 kap. 11 b § införs en sekretessbrytande bestämmelse kan dock uppgifter som omfattas av den bestämmelsen lämnas ut genom direktåtkomst.

Med utgångspunkt i paragrafens bestämmelser och eventuella föreskrifter får Säkerhetspolisen avgöra om myndigheten kan medge de angivna myndigheterna direktåtkomst och i så fall i vilken omfattning.

Av *andra stycket* framgår att om en myndighet har beviljats direktåtkomst till personuppgifter som behandlas enligt lagen, ansvarar denna för att tillgången till uppgifterna inom den egna myndigheten begränsas. Myndigheten är alltså skyldig att se till att endast den som behöver en uppgift för att fullgöra sina arbetsuppgifter har möjlighet att få del av uppgiften. Bestämmelsen har formulerats på samma sätt som den generella bestämmelsen om direktåtkomst i 3 kap. 8 § andra stycket i lagen och är därmed inte likalydande med hur bestämmelsen formulerats i övriga lagförslag. Innebörden av bestämmelsen är dock densamma.

I *tredje stycket* informeras om att regeringen, eller den myndighet som regeringen bestämmer, kan meddela föreskrifter om bl.a. begränsningar i direktåtkomsten och om behörighet och säkerhet.

11 b §

Försvarets radioanstalt och Försvarmakten har, trots sekretess enligt 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 11 a § första stycket.

Paragrafen är ny och reglerar viss uppgiftsskyldighet för Säkerhetspolisen. Övervägandena finns i avsnitt 7.3.

I bestämmelsen anges att FRA och Försvarmakten har rätt att ta del av sådana uppgifter som avses i 6 kap. 11 a § första stycket. Myndigheterna

ges genom bestämmelsen en rätt att ta del av samma uppgifter som de får medges direktåtkomst till. Detta innebär att FRA och Försvarsmakten, trots viss i paragrafen angiven sekretess till skydd för enskild, har rätt att ta del av uppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Uppgiftsskyldigheten gäller bara inom ramen för NCT-samarbetet. Genom FRA:s och Försvarsmaktens rätt att ta del av uppgifterna uppkommer en sådan uppgiftsskyldighet som enligt 10 kap. 28 § första stycket OSL bryter sekretessen enligt de angivna sekretessbestämmelserna.

Sammanfattning av departementspromemorian Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning (Ds 2016:31)

Promemorian innehåller en beskrivning och analys av den personuppgiftsbehandling som de tre myndigheterna vidtar inom ramen för NCT-samarbetet.

I promemorian görs bedömningen att det inte finns något behov av förtydligande författningsstöd för den personuppgiftsbehandling som förekommer inom samarbetet. Merparten av de bestämmelser som aktualiseras vid myndigheternas behandling av personuppgifter i den gemensamma mappen ser likadana ut i myndigheternas respektive registerförfattningar. Myndigheternas verksamhet inom NCT-samarbetet styrs dessutom av ändamålsbestämmelser med samma övergripande innebörd. Säkerhetspolisen, FRA och Försvarmakten bedöms vara gemensamt personuppgiftsansvariga för merparten av de behandlingar av personuppgifter som utförs i den gemensamma mappen. Eftersom ett sådant gemensamt personuppgiftsansvar kan riskera att medföra vissa otydligheter görs det i promemorian bedömningen att den närmare innebörden av ett sådant ansvar bör tydliggöras, förslagsvis genom en överenskommelse mellan myndigheterna.

I promemorian föreslås vidare att Säkerhetspolisen, FRA och Försvarmakten, inom ramen för NCT-samarbetet, ska få lämna ut uppgifter till varandra elektroniskt genom direktåtkomst. Förslaget syftar till att effektivisera det informationsutbyte som förekommer inom samarbetet i dag och härigenom ge myndigheterna bättre förutsättningar att göra korrekta bedömningar av terrorhot i rätt tid. Förslaget innebär att varje myndighet inom NCT ska få medge de övriga myndigheterna inom samarbetet direktåtkomst till sådana uppgifter som behövs för att analytikerna vid myndigheterna ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Direktåtkomsten ska inte omfatta fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra på papper eller muntligen. Förslaget syftar således endast till att reglera formen för det utlämnande av uppgifter som redan förekommer inom samarbetet i dag. För att möjliggöra utlämnandet föreslås att sekretessbrytande bestämmelser i form av uppgiftsskyldigheter införs.

Förslagen föreslås träda i kraft den 1 januari 2018.

Lagförslag i departementspromemorian Behandling av personuppgifter inom Nationellt centrum för terrorhotbedömning (Ds 2016:31)

Förslag till lag om ändring i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Härigenom föreskrivs i fråga om lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

dels att 1 kap. 15 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 15 a §, och närmast före den paragrafen en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

15 §

Säkerhetspolisen och Försvarets radioanstalt får medges direktåtkomst till sådana uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom ramen för samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar ytterligare föreskrifter

Regeringen, eller den myndighet som regeringen bestämmer, kan med stöd av 8 kap. 7 §

eller beslut i enskilda fall om omfattningen av direktåtkomsten.

regeringsformen meddela

Bilaga 2

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, samt

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

Uppgiftsskyldighet

15 a §

Säkerhetspolisen och Försvarets radioanstalt har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Denna lag träder i kraft den...

Förslag till lag om ändring i lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Härigenom föreskrivs i fråga om lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

dels att 1 kap. 15 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 15 a §, och närmast före den paragrafen en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

1 kap.

15 §

Säkerhetspolisen och Försvarsmakten får medges direktåtkomst till uppgifter som utgör analysresultat i en uppgiftssamling för analyser och som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. Tillgången till sådana uppgifter ska vara förbehållen de personer inom myndigheterna som på grund av sina arbetsuppgifter inom ramen för samverkan behöver ha tillgång till uppgifterna.

Regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen kan med stöd av 8 kap. 7 § regeringsformen meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar.

Regeringen, eller den myndighet som regeringen bestämmer, meddelar ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten.

Regeringen, eller den myndighet som regeringen bestämmer, kan med stöd av 8 kap. 7 § regeringsformen meddela

1. ytterligare föreskrifter eller beslut i enskilda fall om omfattningen av direktåtkomsten, samt

2. föreskrifter om behörighet och säkerhet vid sådan åtkomst.

15 a §

Säkerhetspolisen och Försvarsmakten har, trots sekretess enligt 38 kap. 4 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 15 § första stycket.

Denna lag träder i kraft den...

Förslag till lag om ändring i polisdatalagen (2010:361)

Härigenom föreskrivs i fråga om polisdatalagen (2010:361)

dels att 2 kap. 21 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 6 kap. 11 a och 11 b §§, och närmast före 6 kap. 11 a § en ny rubrik av följande lydelse.

Nuvarande lydelse

Föreslagen lydelse

2 kap.

21 §

Utlämnande genom direktåtkomst är tillåtet bara i den utsträckning som följer av denna lag.

Regeringen meddelar föreskrifter om att en utländsk myndighet, Europol eller en mellanfolklig organisation får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet, om detta är nödvändigt för att fullgöra en internationell överenskommelse som Sverige efter riksdagens godkännande har tillträtt eller om det följer av en EU-rättsakt.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 § samt 4 kap. 10 och 17 §§.

Ytterligare bestämmelser om direktåtkomst finns i 3 kap. 8 §, 4 kap. 10 och 17 §§ samt 6 kap. 11 a §.

6 kap.

Direktåtkomst

och uppgiftsskyldighet

11 a §

Försvarets radioanstalt och Försvarsmakten får medges direktåtkomst till personuppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens brottsbekämpande verksamhet och som behövs för att myndigheterna, inom myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvarsmakten och Säkerhetspolisen, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen.

En myndighet som har medgetts direktåtkomst ansvarar för att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Regeringen eller den myndighet

som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om omfattningen av direktåtkomsten samt om behörighet och säkerhet vid sådan åtkomst.

11 b §

Försvarets radioanstalt och Försvarsmakten har, trots sekretess enligt 35 kap. 1 § och 37 kap. 1 § offentlighets- och sekretesslagen (2009:400), rätt att ta del av sådana uppgifter som avses i 11 a § första stycket.

Denna lag träder i kraft den...

Förteckning över remissinstanserna

Följande remissinstanser har inkommit med yttrande över departementspromemorian: Riksdagens ombudsmän, Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Stockholms tingsrätt, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Myndigheten för samhällsskydd och beredskap, Kustbevakningen, Migrationsverket, Datainspektionen, Inspektionen för strategiska produkter, Försvarmakten, Försvarets radioanstalt, Totalförsvarets forskningsinstitut, Statens inspektion för försvarsunderrättelseverksamheten, Försvarsunderrättsedomstolen, Tullverket, Skatteverket, Uppsala universitet (Juridiska fakulteten), Göteborgs universitet (Handelshögskolan, juridiska institutionen), Strålsäkerhetsmyndigheten, Post- och telestyrelsen, Transportstyrelsen, Sveriges Advokatsamfund, Tidningsutgivarna, Svenska Journalistförbundet och Dataskydd.net.

Försvårshögskolan har förklarat att de avstår från att yttra sig över promemorian.

Svenska avdelningen av Internationella Juristkommissionen och Civil Rights Defenders har inbjudits att lämna synpunkter men inte inkommit med svar.