Ds 2016:31

Behandling av personuppgifter inom NationellT centrum för terrorhotbedömning

REGERINGSKANSLIET
Justitiedepartementet

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Omslag: Regeringskansliets standard
Tryck: Elanders Sverige AB, Stockholm 2016

ISBN 978-91-38-24491-3
ISSN 0284-6012

Till Justitiedepartementet

Den 1 oktober 2015 beslutade statsrådet Anders Ygeman att uppdra åt hovrättsrådet, tillika vice ordförande på avdelning, Eva Lönqvist att biträda Justitiedepartementet med att analysera de rättsliga förutsättningarna för personuppgiftsbehandlingen inom Nationellt centrum för terrorhotbedömning (NCT) och hur informationsutbytet inom samarbetet kan effektiviseras. Som sekreterare anställdes samma dag hovrättsassessorn Maria Arnell.

Vi har under utarbetandet av denna promemoria arbetat i nära samråd och vi har därför valt att skriva i vi-form.

Med denna promemoria är uppdraget slutfört.

Göteborg i augusti 2016

Innehåll

Förkortningar m.m.

Förkortningar

DI	Datainspektionen
DIFS	Datainspektionens författningssamling
FRA	Försvarets radioanstalt
FRA-PuF	förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet
FRA-PuL	lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet
LSF	lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet
Must	Militära underrättelse- och säkerhetstjänsten
NCT	Nationellt centrum för terrorhotbedömning
OSL	offentlighets- och sekretesslagen (2009:400)
PDL	polisdatalagen (2010:361)
PuF	personuppgiftsförordningen (1998:1191)

PuL	personuppgiftslagen (1998:204)
PuF UNDSÄK	förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst
PuL UNDSÄK	lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst
RF	regeringsformen
SIN	Säkerhets- och integritetsskyddsnämnden
Siun	Statens inspektion för försvarsunderrättelseverksamheten
TF	tryckfrihetsförordningen

Kortformer för viss citerad litteratur

Lenberg m.fl.	Eva Lenberg, Ulrika Geijer och Anna Tansjö, Offentlighets- och sekretesslagen. En kommentar, 1 januari 2016, Zeteo
Öman/Lindblom	Sören Öman och Hans-Olof Lindblom, Personuppgiftslagen. En kommentar, 4 uppl. 2011

1 Promemorians huvudsakliga innehåll

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). NCT 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. NCT:s analyser och bedömningar presenteras i olika typer av rapporter.

Promemorian innehåller en beskrivning och analys av den personuppgiftsbehandling som de tre myndigheterna vidtar inom ramen för NCT-samarbetet. Analytikerna vid NCT arbetar i gemensamma lokaler, men använder sina egna myndigheters IT-system och har inte tillgång till varandras system. Det finns dock en gemensam NCT-mapp som medarbetarna från alla tre myndigheterna har tillgång till och där NCT:s rapporter arbetas fram och färdigställs. Informationsutbytet inom samarbetet sker främst muntligen eller på papper.

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 Försvarsmakten bedöms vara gemensamt personuppgifts-

ansvariga 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 Försvarsmakten, 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.

Promemorian innehåller också förslag till en teknikneutral bestämmelse som ska ge Säkerhetspolisen samma möjlighet som Försvarsmakten och FRA att lämna ut uppgifter elektroniskt på annat sätt inom samarbetet.

Förslagen föreslås träda i kraft den 1 januari 2018.

2 Författningsförslag

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 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 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.*
	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…

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 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.*
	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…

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 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…

2.4 Förslag till förordning om ändring i förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst

Härigenom föreskrivs att det i förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst ska införas en ny paragraf, 9 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	9 a §
	Försvarsmakten får meddela närmare föreskrifter om omfattningen av direktåtkomst och om vad som krävs i fråga om behörighet och säkerhet för att direktåtkomst till uppgifter ska kunna medges de myndigheter som anges i 1 kap. 15 § första stycket lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.
	Direktåtkomst till uppgifterna får inte medges innan Försvarsmakten har försäkrat sig om att den mottagande myndigheten uppfyller uppställda krav på behörighet och säkerhet.

Denna förordning träder i kraft den…

2.5 Förslag till förordning om ändring i förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet

Härigenom föreskrivs att det i förordningen (2007:261) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ska införas en ny paragraf, 9 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	9 a §
	Försvarets radioanstalt får meddela närmare föreskrifter om omfattningen av direktåtkomst och om vad som krävs i fråga om behörighet och säkerhet för att direktåtkomst till uppgifter ska kunna medges de myndigheter som anges i 1 kap. 15 § första stycket lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.
	Direktåtkomst till uppgifterna får inte medges innan Försvarets radioanstalt har försäkrat sig om att den mottagande myndigheten uppfyller uppställda krav på behörighet och säkerhet.

Denna förordning träder i kraft den…

2.6 Förslag till förordning om ändring i polisdataförordningen (2010:1155)

Härigenom föreskrivs ifråga om polisdataförordningen (2010:1155)

dels att 14 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 18 c § och 18 d §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
14 §[1]	
Polismyndigheten får meddela närmare föreskrifter om vad som krävs i fråga om behörighet och säkerhet för att myndigheten ska kunna medge direktåtkomst till uppgifter för de myndigheter som anges i 3 kap. 8 § polisdatalagen (2010:361).	
	Säkerhetspolisen får meddela närmare föreskrifter om vad som krävs i fråga om behörighet och säkerhet för att myndigheten ska kunna medge direktåtkomst till uppgifter för de myndigheter som anges i 6 kap. 11 a § polisdatalagen (2010:361).
Direktåtkomst till uppgifterna får inte medges innan Polismyndigheten har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.	Direktåtkomst till uppgifterna får inte medges innan Polismyndigheten *respektive Säkerhetspolisen* har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.
	18 c §
	Inom ramen för myndighetsöverskridande samverkan mellan Försvarets radioanstalt, Försvars-

[1] Senaste lydelse 2014:1181.

makten och Säkerhetspolisen får Säkerhetspolisen lämna ut fler personuppgifter än vad som anges i 2 kap. 20 § första meningen polisdatalagen (2010:361) på medium för automatiserad behandling till Försvarets radioanstalt och Försvarsmakten.

18 d §

Försvarsmaktens direktåtkomst enligt 6 kap. 11 a § polisdatalagen (2010:361) får endast avse personuppgifter som den myndigheten får behandla enligt 8 § lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Försvarets radioanstalts direktåtkomst enligt 6 kap. 11 a § polisdatalagen (2010:361) får endast avse personuppgifter som den myndigheten får behandla enligt 8 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Denna förordning träder i kraft den…

3 Utredningens uppdrag och arbete

3.1 Bakgrund

3.1.1 Nationellt centrum för terrorhotbedömning – NCT

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). NCT bildades 2005 och var inledningsvis en arbetsgrupp under Samverkansrådet mot terrorism. Sedan 2009 är arbetsgruppen dock permanent och direkt underställd Säkerhetspolisen, FRA och Försvarsmakten genom Must (NCT-myndigheterna).

NCT 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.

Vid NCT arbetar analytiker från de tre NCT-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. Samarbetet inom NCT ger större möjligheter att ta tillvara den samlade kompetens som finns hos de tre myndigheterna och syftar till att förbättra Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorangrepp mot Sverige och svenska intressen.

3.1.2 Regeringens strategi mot terrorism

I regeringens skrivelsen Ansvar och engagemang – en nationell strategi mot terrorism (skr. 2011/12:73, s. 18 f.) konstaterade regeringen att NCT har en central funktion för hotbedömningar avseende terrorism med bäring på Sverige och svenska intressen. I samma skrivelse framförde regeringen att en väl fungerande samordning på myndighetsnivå är en förutsättning för goda resultat och att regeringen förutsätter att myndigheterna samverkar. Regeringen noterade också att NCT-myndigheterna hade framfört ett behov av förbättrade möjligheter att utbyta information och konstaterade att det fanns anledning att följa frågan vidare.

I augusti 2015 presenterade regeringen en ny nationell strategi mot terrorism som nu ska vara utgångspunkten för Sveriges långsiktiga arbete på detta område (Regeringens skrivelse 2014/15:146 Förebygga, förhindra och försvåra – den svenska strategin mot terrorism). Den nya strategin ersätter den tidigare strategin från år 2012. Regeringen har i den nya strategin bl.a. konstaterat 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, s. 15).

I den nya strategin nämns NCT som ett exempel på strategisk samverkan och det konstateras återigen att NCT fyller en viktig funktion. Regeringen har vidare konstaterat att Säkerhetspolisen pekat på ett behov av att kunna medge övriga myndigheter inom NCT direktåtkomst till de uppgifter i myndighetens verksamhet som behövs för samarbetet, för att på så sätt effektivisera arbetet, och av strategin framgår att regeringen ska verka för att uppgiftsutbytet inom NCT effektiviseras (skr. 2014/15:146, s. 16 f.).

3.1.3 Behandling av personuppgifter inom NCT-samarbetet

NCT är ett samarbete mellan tre myndigheter och utgör inte ett eget rättssubjekt. Den verksamhet som bedrivs inom ramen för NCT-samarbetet grundas därför på den rättsliga reglering som

gäller för var och en av de samarbetande myndigheterna. NCT:s bedömningar och rapporter baseras huvudsakligen på sekretessbelagd information från de tre samarbetande myndigheterna. Denna information kan innehålla personuppgifter.

Säkerhetspolisens behandling av personuppgifter inom ramen för NCT-samarbetet sker med stöd av 6 kap. 1 § 1 b polisdatalagen (2010:361), PDL. Enligt denna bestämmelse får personuppgifter behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott.

FRA behandlar personuppgifter inom ramen för samarbetet med stöd av 1 kap. 8 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, FRA-PuL. Enligt bestämmelsen får personuppgifter behandlas i myndighetens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Vidare anges att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Försvarsmakten/Must behandlar personuppgifter inom ramen för samarbetet med stöd av 1 kap. 8 § lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, PuL UNDSÄK. Bestämmelsens lydelse motsvarar den som finns i 1 kap. 8 § FRA-PuL.

Regler om utlämnande av uppgifter från en myndighet till en annan finns dels i offentlighets- och sekretesslagen (2009:400), OSL, dels i de författningar som reglerar myndigheternas personuppgiftsbehandling. För att myndigheterna ska kunna utbyta information krävs att informationen inte omfattas av sekretess eller att sekretessen kan brytas. Det krävs också att det finns stöd för att uppgifterna får lämnas ut.

Datainspektionen (DI) är tillsynsmyndighet när det gäller den behandling av personuppgifter som sker vid de tre NCT-myndigheterna. Detta framgår av respektive myndighets registerförfattning. Därutöver har Säkerhets- och integritetsskyddsnämnden (SIN) ett tillsynsansvar över den behandling av personuppgifter som utförs av Säkerhetspolisen enligt PDL. Detta framgår av 1 §

lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet som PDL hänvisar till. Slutligen har också Statens inspektion för försvarsunderrättelseverksamheten (Siun) till uppgift att granska den personuppgiftsbehandling som utförs av FRA och Försvarsmakten.

SIN granskade under 2015 delar av den personuppgiftsbehandling som Säkerhetspolisen utför inom ramen för samarbetet i NCT. Nämnden kunde vid sin granskning inte se att Säkerhetspolisen behandlade några personuppgifter i strid med PDL. Nämnden konstaterade dock i sin rapport av den 6 maj 2015 att regleringen i PDL 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 det 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 FRA och Försvarsmakten 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 Försvarsmaktens och FRA:s personuppgiftsbehandling inom NCT-samarbetet, särskilt vad gäller personuppgiftsansvar och grund för behandling, som kan behöva utredas. Mot bakgrund av att regeringen har tillsatt en utredning för att se över personuppgiftsbehandlingen inom ramen för NCT-samarbetet beslutade nämnden den 18 november 2015 att avsluta ärendet utan vidare åtgärder (Utdrag ur protokoll för nämndsammanträde den 18 november 2015, dnr 51-2014H:11).

3.1.4 Behovet av en utredning

Olika former av samverkan mellan myndigheter har blivit allt vanligare. Bakgrunden till detta är bl.a. att regeringen genom regleringsbrev och separata regeringsuppdrag uppmanat myndigheterna att samverka och att effektivisera den samverkan som redan finns

etablerad. Ett viktigt led i alla former av samverkan är möjligheten att kunna utbyta information.

Arbetet med att motverka terrorism kräver ett nära myndighetssamarbete. Det samarbete som sker inom NCT möjliggör ett tillvaratagande av de tre myndigheternas samlade kompetens och syftar till att förbättra Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorangrepp mot Sverige och svenska intressen. Regeringen har konstaterat att NCT har en central funktion för hotbedömningar mot Sverige och svenska intressen och att det därför är viktigt att samarbetet fortsätter.

Säkerhetspolisen har i en skrivelse till regeringen (Ju2015/05096/L4) pekat på ett behov av att effektivisera uppgiftsutbytet inom 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.

Med hänsyn till SIN:s granskning och de uttalanden nämnden har gjort i sin rapport samt Säkerhetspolisens skrivelse har regeringen ansett att det finns anledning att närmare analysera dels de rättsliga förutsättningarna för det samarbete som sker inom NCT, dels hur samarbetet kan effektiviseras.

3.2 Uppdraget

Till grund för regeringsuppdraget ligger en av regeringskansliet utarbetad promemoria, se bilaga 1. Enligt promemorian ska vi beskriva den verksamhet som bedrivs inom ramen för NCT-samarbetet och analysera de rättsliga förutsättningarna för Säkerhetspolisens, Försvarsmaktens och FRA:s personuppgiftsbehandling inom ramen för NCT-samarbetet i syfte att klarlägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling

som sker. Vi ska 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.

Av promemorian framgår att vi ska lämna förslag på de författningsändringar som bedöms nödvändiga. Vi ska i detta arbete säkerställa att det blir en lämplig avvägning mellan intresset av ett effektiviserat informationsutbyte och skyddet för den personliga integriteten i de förslag som lämnas. Vi ska härvid redovisa hur skyddet av den personliga integriteten stärks genom en författningsreglering.

Vi ska därtill analysera och redovisa förslagens ekonomiska konsekvenser. Om kostnader bedöms uppkomma ska ett finansieringsförslag lämnas.

3.3 Uppdragets omfattning

Som framgår ovan har vi fått i uppdrag att 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. Mot bakgrund av hur uppdraget är formulerat har vi ansett oss oförhindrade att analysera även andra rättsliga åtgärder för ett effektiviserat informationsutbyte och då främst frågan om även Försvarsmakten och FRA ska kunna medge övriga myndigheter inom samarbetet direktåtkomst till uppgifter i sina respektive verksamheter. Det har emellertid inte ingått i vårt uppdrag att föreslå organisatoriska förändringar för samarbetet.

3.4 Arbetets bedrivande

Vårt arbete påbörjades i oktober 2015. Målsättningen har varit att skapa juridiska förutsättningar för ett effektivare och mer ändamålsenligt samarbete mellan myndigheterna inom NCT samtidigt

som skyddet för den personliga integriteten beaktas. Vårt mål har varit att så långt som möjligt finna lösningar inom ramen för befintliga regelverk.

Vi har under arbetes gång samrått med företrädare för Säkerhetspolisen, FRA och Försvarsmakten/Must samt företrädare för NCT. Vi har besökt NCT och där fått en inblick i verksamheten på plats. Vid besöken har vi inhämtat synpunkter på och information om det praktiska arbete som bedrivs inom samarbetet. I samband härmed har vi även diskuterat den praktiska tillämpningen av lagstiftningen och vilka konsekvenser den får för samarbetet. Vi har vidare tagit del av skriftligt material samt underrättelserapporter producerade av NCT. Vi har dessutom samrått med DI, SIN och Siun.

4 NCT och de samarbetande myndigheterna

4.1 Inledning

NCT är en permanent myndighetsgemensam arbetsgrupp med personal från Säkerhetspolisen, FRA och Must. Som tidigare redogjorts för bildades NCT 2005 och var inledningsvis en arbetsgrupp under Samverkansrådet mot terrorism. Sedan 2009 är arbetsgruppen permanent och direkt underställd Säkerhetspolisen, FRA och Försvarsmakten genom Must.

I detta kapitel följer en beskrivning av NCT:s organisation, syfte och uppgift. Vi beskriver också översiktligt den verksamhet som bedrivs inom samarbetet. Redogörelsen grundar sig på de överenskommelser som tecknats mellan myndigheterna och de interna arbetsdokument som reglerar verksamheten samt uppgifter hämtade från företrädare för NCT och de tre myndigheterna.

Som framgår ovan består NCT av tre separata myndigheter vars verksamhet och arbetsuppgifter skiljer sig åt. För att underlätta förståelsen för NCT:s arbete inleds därför detta kapitel med en genomgång av de tre NCT-myndigheternas ordinarie verksamhet.

4.2 Säkerhetspolisen

4.2.1 Uppgifter

Säkerhetspolisen är sedan den 1 januari 2015 en självständig myndighet. Säkerhetspolisens huvudsakliga uppgifter och ansvar framgår av 3 § polislagen (1984:387). Där anges att Säkerhetspolisen ska (1) förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott samt (2)

utreda och beivra sådana brott, (3) fullgöra uppgifter i samband med personskydd av den centrala statsledningen och andra som regeringen eller Säkerhetspolisen bestämmer, (4) fullgöra uppgifter enligt säkerhetskyddslagen (1996:627) samt (5) leda annan polisverksamhet om regeringen föreskriver det och i övrigt bedriva sådan verksamhet som framgår av lag eller förordning eller som regeringen uppdragit åt Säkerhetspolisen att i särskilda hänseenden ansvara för. I förordningen (2014:1103) med instruktion för Säkerhetspolisen samt i regleringsbrev från regeringen preciseras Säkerhetspolisens uppdrag närmare.

Gemensamt för Säkerhetspolisens olika verksamhetsområden är det förebyggande arbetet, dvs. att förhindra att brott över huvudtaget begås. Säkerhetspolisens verksamhet syftar till att skydda Sveriges demokratiska system, medborgarnas fri- och rättigheter och den nationella säkerheten. Detta sker genom att Säkerhetspolisen förebygger och avslöjar brott mot rikets säkerhet, bekämpar terrorism och skyddar den centrala statsledningen (Säkerhetspolisens årsbok 2015, s. 7).

4.2.2 Huvudsakliga verksamhetsområden

Säkerhetspolisens verksamhet kan i huvudsak delas in i fem områden; kontraspionage, kontraterrorism, säkerhetsskydd, författningsskydd och personskydd.

- *Kontraspionage* innebär att förebygga och avslöja spioneri och annan olovlig underrättelseverksamhet som kan rikta sig mot Sverige och svenska intressen utomlands samt mot utländska intressen i landet och mot flyktingar.
- *Kontraterrorism* innebär att förebygga och avslöja terrorism som riktas mot Sverige, svenska intressen i utlandet, utländska intressen i Sverige, terroristhandlingar i andra länder, förekomsten av internationella terroristnätverks förgreningar i Sverige samt stöd och finansiering av terroristverksamhet.
- *Författningsskydd* innebär att motverka verksamhet som genom otillåten påverkan som trakasserier, hot, våld, tvång eller korruption syftar till att påverka det demokratiska statsskickets funktioner.

– *Säkerhetsskydd* innebär att höja säkerhetsnivån i samhället genom analyser, registerkontroller, tillsyn och rekommendationer till myndigheter vars verksamhet har bäring på rikets säkerhet.
– *Personskydd* handlar om bevaknings- och säkerhetsarbete för den centrala statsledningen, främmande statsbeskickningsmedlemmar samt vid statsbesök och liknande händelser.

Därutöver arbetar Säkerhetspolisen även med ickespridning, vilket handlar om att förhindra spridning och anskaffning av produkter som kan användas för att producera massförstörelsevapen. I Säkerhetspolisens uppdrag ingår också att vara remissinstans till Migrationsverket och överklagandeinstanserna i fall där individer befaras utgöra ett säkerhetshot (Säkerhetspolisens årsbok 2015, s. 9).

4.2.3 Närmare om kontraterrorism

En av Säkerhetspolisens uppgifter är att förhindra att terroristattentat begås i Sverige. Konsekvenserna av ett terroristattentat kan bli mycket allvarliga för samhället och medborgarna. Därför är Säkerhetspolisens mål att förhindra terroristbrottslighet på ett tidigt stadium. Säkerhetspolisens uppgift är också att försvåra och reducera verksamheter som stödjer terrorism. Det kan röra sig om finansiering, logistiskt stöd, utbildning, rekrytering eller radikalisering.

Säkerhetspolisen arbetar brett för att förhindra all terrorism oavsett ideologisk motivering. Detta kräver bl.a. ett gediget och effektivt inriktat underrättelsearbete baserat på information från olika källor. Förutsättningen för Säkerhetspolisens underrättelsearbete inom kontraterrorism är inhämtning av relevant information. Inhämtningen sker genom spaning, personkällor, öppna källor, förhörsinformation, tvångsmedel samt kontakter och samverkan både nationellt och internationellt. Tvångsmedel beslutas av domstol och innefattar hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig rumsavlyssning, hemlig kameraövervakning och postkontroll. När uppgifterna har analyserats delges berörda inom Säkerhetspolisen som med utgångspunkt från informationen beslutar om åtgärder.

Samverkan med både nationella och internationella parter är en förutsättning för Säkerhetspolisens arbete med att förhindra terroristbrott i Sverige. Säkerhetspolisen arbetar kontinuerligt med att förbättra och utöka samarbetet med framför allt Polismyndigheten, Must, FRA och utländska underrättelse- och säkerhetstjänster. Säkerhetspolisen har även ett nära samarbete med Migrationsverket i syfte att identifiera säkerhetshot i migrationsströmmarna till Sverige. I Samverkansrådet mot terrorism är Säkerhetspolisen sammankallande. Rådet består av 14 svenska myndigheter som tillsammans arbetar i linje med de strategier på kontraterrorismområdet som EU och den svenska regeringen har (Säkerhetspolisens årsbok 2015, s. 32 f.).

4.2.4 Kontroll

Säkerhetspolisen granskas av SIN. SIN har till uppgift att bland annat kontrollera Säkerhetspolisens behandling av personuppgifter och om denna har skett i enlighet med gällande regler. SIN gör inspektioner på eget initiativ och kontrollerar på begäran av enskild om han eller hon har utsatts för hemliga tvångsmedel eller har varit föremål för Säkerhetspolisens personuppgiftsbehandling. Även DI utövar tillsyn över den personuppgiftsbehandling som Säkerhetspolisen utför.

4.3 Militära underrättelse- och säkerhetstjänsten

4.3.1 Allmänt

Must är en del av myndigheten Försvarsmakten. Must bedriver försvarsunderrättelseverksamhet och militär säkerhetstjänst och har till uppgift att identifiera, bevaka och bedöma yttre hot mot Sverige och svenska intressen i utlandet. Uppgifterna preciseras närmare i ett inriktningsbeslut från regeringen. Vidare inriktar överbefälhavaren (ÖB) Must beträffande Försvarsmaktens underrättelsebehov. Must har tillgång till information om utrikesförhållanden från en rad olika inhämtningsdiscipliner, alltifrån öppna källor till personbaserad underrättelseinhämtning och information som erhålls via Musts partnersamarbeten. Must är således en så kallad

Multi-Source organisation (Försvarsmakten, Årsöversikt 2015, Militära underrättelse- och säkerhetstjänsten, s. 25). Information om yttre hot bearbetas, analyseras och presenteras för uppdragsgivarna i form av underrättelserapportering innehållande såväl kortsiktiga som långsiktiga bedömningar. Bland de yttre hoten som Must bevakar och rapporterar om kan, enligt uppgift från myndigheten, nämnas militära hot och terrorism. Nedan beskrivs den huvudsakliga indelningen av Musts uppgifter under rubrikerna försvarsunderrättelseverksamhet och militär säkerhetstjänst. Inom ramen för försvarsunderrättelseverksamheten bedriver Must en omfattande och mångfacetterad verksamhet. Under delkapitlet nedan läggs fokus på hotet från terrorism, vilket är det relevanta för denna utredning.

4.3.2 Försvarsunderrättelseverksamhet vid Must

Musts uppgift vad gäller underrättelseverksamhet är att inhämta, bearbeta och delge underrättelser till stöd för svensk utrikes- och säkerhetspolitik samt i övrigt för kartläggning av yttre hot mot riket. Denna uppgift är reglerad i lagen (2000:130) om försvarsunderrättelseverksamhet.

I 1 § i lagen om försvarsunderrättelseverksamhet anges att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet och att den endast får avse utländska förhållanden. Begränsningen till utländska förhållanden innebär att försvarsunderrättelseverksamheten typiskt sett ska inhämta, bearbeta och delge sådan information om företeelser och förhållanden i andra länder som bl.a. ger svenska beslutsfattare ett förbättrat underlag för beslut och bedömningar i utrikes-, säkerhets- och försvarspolitiska frågor eller för att skydda svensk personal som deltar i internationella insatser. Verksamheten kan dock även avse vissa företeelser inom landet. Exempel på när utländska förhållanden anses sträcka sig innanför landets gränser är när en organisation med verksamhet som utgör ett hot mot landet har sitt ursprung i ett annat land men verkar genom representanter i Sverige eller genom att på annat sätt utnyttja resurser i Sverige. Det handlar då om att följa upp utländska förhållandens koppling till

Sverige för att kunna bedöma hotbilden mot landet. I sådana situationer är det viktigt att framhålla att mandatet för de myndigheter som bedriver försvarsunderrättelseverksamhet är begränsat till just underrättelseverksamhet; alla åtgärder som syftar till att hantera de hot av kriminell karaktär som kan identifieras inom landet är förbehållna de brottsbekämpande myndigheterna (prop. 2006/07:63 s. 43).

Försvarsunderrättelseverksamheten ska, enligt 2 § lagen om försvarsunderrättelseverksamhet, bedrivas genom inhämtning, bearbetning, analys och rapportering av underrättelser till berörda myndigheter. Inom Must är det framför allt underrättelsekontoret som levererar underrättelser till regeringen och Regeringskansliet. Rapporteringen sker kontinuerligt i form av föredragningar, dialoger och skriftliga rapporter. Musts underrättelserapportering delges vidare en rad andra myndigheter, exempelvis Säkerhetspolisen och FRA, i enlighet med dessa myndigheters behov. Delgivningen är reglerad i inriktningsbeslutet från regeringen (Försvarsmakten, Årsöversikt 2015, Militära underrättelse- och säkerhetstjänsten, s. 25).

För att lösa sina uppgifter har Must ett antal egna källor samt ett brett samarbete med internationella partners och organisationer. Must bedriver exempelvis personbaserad underrättelseinhämtning och bildunderrättelseinhämtning. Inom ramen för den nationella samverkan delges Must information från bland andra Säkerhetspolisen och FRA (samma källa, s. 25).

Musts underrättelseinhämtning och rapportering spänner över ett brett fält av såväl geografiska som funktionella områden. Urvalet regleras i de ovan nämnda inriktningarna från regeringen och överbefälhavaren. En central del av Musts uppgifter är att leverera underrättelser och bedömningar om hot mot rikets säkerhet. Enligt uppgift har Must successivt, sedan attentaten den 11 september 2001, på uppdrag från regeringen, ökat sin inhämtning och bearbetning av information om internationella terroristgrupper och deras nätverk. Syftet med detta, inom ramen för underrättelseverksamheten, är dels att förse regeringen och Regeringskansliet med underrättelser om och bedömningar av den internationella terrorismens utveckling, dels stödja de samverkande nationella myndigheterna i sitt arbete att motverka terrorism och avvärja terroristattentat mot Sverige och mot svenska intressen utomlands.

Sverige har som stat en rad internationella åtaganden i kampen mot terrorism. Målet med Musts rapportering på temat är, enligt uppgift från företrädare för myndigheten, att svenska regeringsföreträdare ska kunna ta del av underrättelser som är relevanta och rapporterade i tid för att bilda sig en självständig svensk uppfattning i frågor inom arbetet mot terrorism. Beträffande Musts stöd till samverkande myndigheter har Must i uppdrag att komplettera Säkerhetspolisens analys av terrorhotet inom riket med utvecklingen utomlands, i och med att dessa två arenor är sammanlänkade. Terrorism är ett gränsöverskridande hot och ska därför bemötas med gränsöverskridande samarbete (samma källa, s. 7). Utbyte av information med partnertjänster i andra länder utgör en väsentlig del i att bemöta hotet mot terrorism på internationell nivå.

4.3.3 Militär säkerhetstjänst

Av 3 b § förordningen (2007:1266) med instruktion för Försvarsmakten framgår att Försvarsmakten ska leda och bedriva militär säkerhetstjänst. I säkerhetsskyddslagen (1996:627) finns bestämmelser om säkerhetsskydd. Med säkerhetsskydd avses enligt 6 § säkerhetsskyddslagen dels skydd mot spionerі, sabotage och andra brott som kan hota rikets säkerhet, dels skydd i andra fall av uppgifter som omfattas av sekretess enligt OSL och som rör rikets säkerhet. Vidare avses med säkerhetsskydd även skydd mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, även om brotten inte hotar rikets säkerhet. Den militära säkerhetstjänstens uppgift är att upptäcka, identifiera och möta säkerhetshot som riktas mot Försvarsmakten och dess säkerhetsintressen såväl inom som utom landet. Säkerhetsintressena omfattar eller kan hänföras till personal, materiel, information, anläggningar och verksamhet i vid bemärkelse inklusive den internationella verksamhet som Försvarsmakten deltar i. Den säkerhetshotande verksamhet som riktas mot Försvarsmakten brukar delas in i underrättelseverksamhet, kriminalitet, sabotage, subversiv verksamhet samt terrorism. Den kan riktas mot hela eller delar av Försvarsmakten, viss funktion eller verksamhet och förband samt verksamhet inom

Försvarsmaktens intresseområde, t.ex. försvarsindustri (prop. 2006/07:46 s. 25).

Den militära säkerhetstjänsten omfattar säkerhetsunderrättelsetjänst, säkerhetsskyddstjänst och signalskyddstjänst. Säkerhetsunderrättelsetjänsten har till uppgift att klarlägga den säkerhetshotande verksamhetens omfattning, inriktning samt medel och metoder. Verksamheten syftar till att utifrån aktuella säkerhetsunderrättelsebehov lämna underlag för beslut om t.ex. säkerhetsskyddsåtgärder, beredskap eller förbandsproduktion. Säkerhetsunderrättelsetjänst sker i stort under samma arbetsformer och med utnyttjande av samma typ av källor som används i försvarsunderrättelseverksamheten.

Säkerhetsskyddstjänstens uppgift är att ta fram åtgärder som syftar till att hindra eller försvåra säkerhetshotande verksamhet. Den arbetar med att förebygga att hemliga uppgifter som rör rikets säkerhet obehörigen röjs, ändras eller förstörs. Säkerhetsskyddstjänsten skyddar också materiel och anläggningar mot sabotage och stöld samt personal, anläggningar och materiel mot terrorism. Säkerhetsskyddstjänsten omfattar informationssäkerhet inklusive IT-säkerhet, säkerhetsprövning, tillträdesbegränsning, utbildning och kontroll av säkerhetsskyddet (nämnda prop. s. 25).

Signalskyddstjänst syftar till att, med hjälp av kryptografiska metoder och övriga signalskyddsåtgärder, förhindra obehörig insyn i och påverkan av telekommunikations- och IT-system. Exempel på signalskyddsåtgärder är kryptering, täckning, omskrivning, radiotystnad, frekvenshopp, val av sambandsmedel, användning av digitala signaturer för säker verifiering av elektroniska dokument samt stark autentisering för skydd mot intrång. En del av signalskyddstjänsten är kontroll av signalskyddet i telekommunikations- och IT-system, s.k. signalkontroll. Signalkontroll syftar till att klarlägga riskerna för obehörig åtkomst till eller förvanskning av uppgifter eller störning av telekommunikation. Vidare kan signalkontroll klarlägga att systemen används enligt gällande regelverk.

Enligt 39 § 1 säkerhetsskyddsförordningen (1996:633) utövar Försvarsmakten även tillsyn vad avser säkerhetsskyddet vid Fortifikationsverket, Försvarshögskolan och de myndigheter som hör till Försvarsdepartementet. Inom Försvarsmakten kontrolleras detta av Must (se 6 kap. Försvarsmakens interna bestämmelser, FIB 2015:2, om säkerhetsskydd och skydd av viss materiel).

4.3.4 Kontroll

Försvarsunderrättelseverksamheten omgärdas av naturliga skäl av hög sekretess och begränsad insyn. I en verksamhet med sådan begränsad transparens är en väl fungerande kontroll mycket viktig. Siun är den myndighet som har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som bedrivs av Försvarsmakten sker i enlighet med det av riksdagen och regeringen fastställda regelverket. Därutöver granskar även DI den hantering av personuppgifter som sker inom Försvarsmakten.

4.4 Försvarets radioanstalt

4.4.1 Försvarsunderrättelseverksamhet vid FRA

FRA är en civil myndighet. FRA:s verksamhet regleras i 1 § förordningen (2007:937) med instruktion för Försvarets radioanstalt. Där anges att myndighetens uppgift är att bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet (LSF) och till lagen anslutande förordning. FRA bedriver således också försvarsunderrättelseverksamhet.

Försvarsunderrättelseverksamhet regleras, som framgår ovan, i lagen (2000:130) om försvarsunderrättelseverksamhet och tillhörande förordning. FRA:s signalspaning regleras vidare i ovan nämnda LSF och tillhörande förordning, i lagen (2003:389) om elektronisk kommunikation samt i FRA-PuL och tillhörande FRA-PuF.

Som redogjorts för ovan framgår det av 1 § lagen om försvarsunderrättelseverksamhet att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet och att den endast får avse utländska förhållanden. Verksamheten ska, enligt 2 § samma lag, bedrivas genom inhämtning, bearbetning, analys och rapportering av underrättelser till berörda myndigheter. All försvarsunderrättelseverksamhet vid FRA bedrivs efter inriktning från uppdragsgivare. Av 4 § LSF framgår att inriktning endast får anges av regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten.

FRA:s signalspaning är en betydelsefull del av Sveriges underrättelsetjänst och syftar till att ge kunskap, förvarning och djupare insikter i händelser och förhållanden i omvärlden. Den information som FRA rapporterar till uppdragsgivarna handlar inte alltid om något som utgör ett omedelbart hot mot Sverige i dag, utan är ofta ett mer strategiskt beslutsunderlag och stöd till regeringens utrikes- och säkerhetspolitik. FRA förser, enligt uppgift från företrädare för myndigheten, regeringen och övriga uppdragsgivare med information om exempelvis militär förmåga i andra länder, internationell terrorism, utvecklingen i krigs- och konfliktregioner eller om hur IT-angrepp sker i det globala nätet.

Av 1 § andra stycket LSF framgår de specifika försvarsunderrättelseändamål för vilka signalspaning får bedrivas (ändamålskatalogen). Signalspaning i försvarsunderrättelseverksamhet får ske endast i syfte att kartlägga

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen, eller
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

Av LSF följer att ingen inhämtning genom signalspaning får ske utan att företeelsen omfattas av regeringens inriktning och av tillstånd från Försvarsunderrättelsedomstolen. Domstolen ska enligt LSF pröva bl.a. det inhämtningsuppdrag för vilket inhämtning begärs, vilka signalbärare som FRA ska få tillgång till för att fullgöra uppdraget samt vilka sökbegrepp eller kategorier av sökbegrepp som ska få användas vid inhämtningen. Därutöver finns det i 1 kap. 8 § FRA-PuL krav på att personuppgifter som behandlas i FRA:s försvarsunderrättelseverksamhet ska ha anknytning till en preciserad inriktning och att behandlingen ska vara nödvändig för att fullfölja den inriktningen.

4.4.2 Kontroll

Precis som när det gäller Försvarsmakten är det Siun som har till uppgift att kontrollera att den försvarsunderrättelseverksamhet som FRA bedriver sker i enlighet med det av riksdagen och regeringen fastställda regelverket. Därutöver granskar även DI den hantering av personuppgifter som sker inom FRA.

4.5 Nationellt centrum för terrorhotbedömning – NCT

4.5.1 Bakgrund

Arbetet med att motverka terrorism följer inte traditionella gränsdragningar mellan myndigheter. För att bedöma hotet mot Sverige och svenska intressen, och tillgodose Sveriges strategiska underrättelsebehov, krävs samarbete mellan flera myndigheter. Mot denna bakgrund bildades år 2005 ett Nationellt centrum för terrorhotbedömning, NCT. NCT är en myndighetsgemensam arbetsgrupp som är beslutad av och styrs av cheferna för Säkerhetspolisen, FRA och Försvarsmakten/Must. Det är således myndigheterna själva som har tagit initiativ till samarbetet. NCT bemannas av medarbetare från dessa tre myndigheter och är sedan 2009 permanent och samlokaliserad i Säkerhetspolisens lokaler.

De tre myndigheterna deltar i samarbetet utifrån sitt respektive uppdrag. Samarbetet inom NCT ligger således inom ramen för

Säkerhetspolisens uppdrag att bekämpa terrorism. Det ligger också inom ramen för Försvarsmaktens och FRA:s uppdrag att bedriva försvarsunderrättelseverksamhet. Samarbetet inom NCT är formaliserat genom en överenskommelse mellan myndigheterna. Överenskommelsen reglerar bl.a. myndighetsansvar, ledning och styrning samt hantering av uppgifter. Nu gällande överenskommelse ingicks mellan myndigheterna den 5 maj 2014.

4.5.2 Syfte och uppgift

NCT:s uppgift är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt. Detta inkluderar strategiska analyser av händelser, trender, fenomen och omvärldsutveckling med koppling till terrorism. För att kunna göra detta följs och analyseras en mängd information inom olika bearbetningsområden. Det kan bl.a. röra sig om den nationella hotbedömningen i aktuella länder, svenska intressen, genomförda och avvärjda attentat, terrornätverk, rekrytering och stöd, ideologisk förankring samt logistik, vapentillgång och finansiering. NCT:s bedömningar syftar till att ge tidig förvarning om utveckling inom terrorism som berör, eller kan komma att beröra, Sverige och svenska intressen. NCT-samarbetet syftar således inte till att utreda brott. Vidare ska NCT bidra med rekommendationer för språkbruk och bearbetningsmetoder inom underrättelseområdet terrorism.

Syftet med verksamheten inom ramen för NCT är att stärka den samlade förmågan hos Säkerhetspolisen, Försvarsmakten/Must och FRA att genomföra strategiska bedömningar till stöd för Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorism. Denna ökade förmåga ska åstadkommas genom att information från de tre myndigheterna anlyseras av den samlade kompetensen hos NCT-representanterna från de tre myndigheterna. Samarbetet ger således större möjligheter att ta tillvara den samlade kompetensen som finns vid Säkerhetspolisen, Försvarsmakten/Must och FRA.

NCT:s bedömningar delges främst i rapporter till Regeringskansliet och de tre myndigheter som ingår i NCT-samarbetet (hemmamyndigheterna). I de flesta fall delges även berörda myn-

digheter inom Samverkansrådet mot terrorism. De analyser som tas fram av NCT är centrala för de strategiska beslutsunderlag som Regeringskansliet utarbetar rörande terrorism. Analyserna utgör även centrala beslutsunderlag för Säkerhetspolisen, Försvarsmakten och flera andra myndigheter i Sverige. NCT:s rapportering utgör en viktig del i att skapa samsyn kring hur terrorhotet mot Sverige och svenska intressen ser ut och utvecklas, vilket ökar Sveriges samlade förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorism. En återkommande rapport är NCT:s helårsbedömning av utvecklingen av terrorhotet under det kommande året och som delges en gång per år. Helårsbedömningen revideras löpande utifrån inkommande information. Det kan bl.a. handla om händelseutvecklingen i omvärlden eller attentatsplanering som påverkar hotet mot Sverige och svenska intressen.

NCT samverkar också internationellt med utländska motsvarigheter till NCT samt deltar i enlighet med önskemål från hemmamyndigheterna i deras respektive partnersamverkan.

4.5.3 Ledning och styrning

En styrgrupp bestående av cheferna för Säkerhetspolisen, Försvarsmakten/Must och FRA fastställer målen för NCT:s verksamhet med hänsyn till regeringens inriktning av respektive myndighet. Styrgruppen har ett övergripande ansvar för att skapa förutsättningar för och undanröja hinder för NCT:s uppdrag samt följa upp att målen nås och att säkerställa grunderna för samverkan. Styrgruppen fastställer årligen en verksamhetsplan där målen och de ekonomiska ramarna för verksamheten ska anges.

Styrgruppen beslutar vidare vilka myndigheter utanför Regeringskansliet som kan bli aktuella för delgivning av NCT:s rapporter samt vilka utländska motsvarigheter som NCT får samarbeta med. Det är också styrgruppen som utser chef och ställföreträdande chef för NCT. Styrgruppen har även till uppgift att identifiera och fastställa vilka strategiska uppgifter inom terrorism och kontraterrorism som NCT har fått i uppdrag att utföra, förtydliga vad detta uppdrag innebär, samt följa upp resultaten.

En av de tre NCT-myndigheterna är sammankallande och ordförande för styrgruppen. Ordförandeskapet roterar mellan myndig-

heterna var tredje år. Styrgruppen sammanträder normalt fyra gånger per år.

Till NCT finns det också knutet en beredningsgrupp bestående av en representant från varje myndighet. Beredningsgruppen ska underlätta och effektivisera samverkan mellan de tre NCT-myndigheterna. Beredningsgruppen ska vidare initiera och vid behov samordna arbetsgrupper med specifikt uppdrag att undanröja hinder och skapa så bra förutsättningar som möjligt för NCT:s arbete och utveckling. Till stöd för NCT finns således en juridisk grupp, en grupp som arbetar med personal- och kompetensförsörjning, en grupp som ser till NCT:s specifika tekniska och säkerhetsmässiga behov samt en grupp som hjälper till med kommunikation utöver ordinarie rapportering. Beredningsgruppen har vidare till uppgift att fastställa instruktioner och rutiner för NCT:s verksamhet samt i övrigt bereda de beslut som styrgruppen fattar.

4.5.4 Personal

Vid NCT arbetar personal från Säkerhetspolisen, Must och FRA. Personalen deltar i NCT-samarbetet under en begränsad tid och är då samlokaliserade i Säkerhetspolisens lokaler. I den överenskommelse som gäller mellan NCT-myndigheterna anges att NCT bör vara bemannat med fyra analytiker från Säkerhetspolisen, tre analytiker från Must och tre analytiker från FRA. Dessa ska vara placerade vid NCT under minst två år med möjlighet till förlängning till maximalt fem år. Därutöver finns det en administratör som kommer från Säkerhetspolisen och som är fast placerad vid NCT. Under sin tid på NCT behåller personalen sin anställning hos den ordinarie myndigheten. I överenskommelsen anges att de analytiker som placeras vid NCT ska ha lång erfarenhet och hög kompetens inom något av sakområdena underrättelseanalys eller terrorism och säkerhetspolitik.

En chef leder det dagliga arbetet inom NCT och ansvarar för genomförandet av verksamheten. Chefen för NCT ska komma från någon av de tre NCT-myndigheterna. Chefskapet roterar mellan myndigheterna och chefen ska vara placerad vid NCT i högst tre år. Vid NCT ska det även finnas en ställföreträdande chef som kommer från någon av de tre myndigheterna. Om chefen för NCT är

anställd hos Försvarsmakten/Must eller FRA ska den ställföreträdande chefen var anställd hos Säkerhetspolisen och tvärtom. Den ställföreträdande chefen ansvarar bl.a. för den dagliga analysverksamheten och produktionen.

4.5.5 Verksamheten

NCT är ett samarbete mellan tre myndigheter och utgör inte ett eget rättssubjekt. Den verksamhet som bedrivs inom ramen för NCT-samarbetet grundas därför på den rättsliga reglering som gäller för var och en av de samarbetande myndigheterna. Det betyder bl.a. att respektive myndighet gör en sekretessprövning innan uppgifter lämnas ut till övriga myndigheter och att respektive myndighet i princip är ansvarig för den egna behandlingen av personuppgifter. NCT:s bedömningar och rapporter baseras på sekretessbelagd information från alla tre samarbetande myndigheter. Utbytet av information mellan myndigheterna sker främst genom att handlingar lämnas ut till respektive myndighet eller att handlingar visas, utan att de lämnas ut, för medarbetarna från de andra myndigheterna. I överenskommelsen som reglerar NCT:s verksamhet anges att myndigheterna ska verka för att, inom ramen för gällande rätt, så mycket som möjligt av för NCT relevant information lämnas ut.

Den information som ligger till grund för NCT:s analyser och bedömningar hämtas in av tjänstemännen främst från deras respektive hemmamyndigheter. Informationen hämtas från flera olika typer av material och dokument. Relevant information kan exempelvis komma NCT-tjänstemännen till handa genom formella rapporter ställda till någon av NCT-myndigheterna eller till alla tre. Informationen kan även utgöras av bearbetat grundmaterial från någon av myndigheterna, dvs. bedömningar och underlag baserat på råmaterial, eller allmänna bedömningar baserade på analytikernas generella kunskap på området. Informationen hämtas från bl.a. olika register och databaser, myndighetsrapportering, FN- och EU-rapportering samt underrättelserapportering från exempelvis insatsområden, tvångsmedel, informatörer och källor. Information kan också komma in till Säkerhetspolisen för NCT:s räkning. NCT är ingen egen myndighet och handlingar kan således inte i juridisk

mening inkomma till NCT. Det begränsade antal handlingar som kommer NCT till del på detta sätt registreras därför som inkomna hos alla tre myndigheterna alternativt hos Säkerhetspolisen.

NCT:s analyser och bedömningar presenteras i olika typer av rapporter. En helårsrapport innehåller en regelbunden strategisk hotbedömning mot Sverige och svenska intressen för en period om tolv månader framåt medan en rapport om långsiktig hotbild behandlar en strategisk hotbild under en period om tre till fem år. Därutöver skriver NCT underrättelserapporter som innehåller löpande såväl strategisk som tidskritisk rapportering i samband med särskilda händelser eller strategiska trender, samt svar på frågor och begäran om information från någon av hemmamyndigheterna. NCT skriver också rapporter som inte är att bedöma som rena underrättelserapporter. Sådana rapporter kan exempelvis rikta sig till vissa myndigheter eller organisationer och ange hur dessa ska agera i vissa speciella situationer. NCT producerar ungefär 20–30 underrättelserapporter per år. En NCT-rapport kan initieras på flera olika sätt. Den kan grunda sig på en begäran om underlag eller ett förslag från någon av hemmamyndigheterna eller en begäran om information från Regeringskansliet eller Samverkansrådet mot terrorism. En rapport kan också ha sin bakgrund i NCT:s fastställda produktionsplan eller tas fram på grund av en särskild händelse. En rapportidé kan vidare utvecklas av en enskild eller en grupp av analytiker.

När en rapport har färdigställts upprättas den i en eller flera olika versioner och skickas till de myndigheter som ska få del av rapporten. En NCT-rapport är färdigställd när den har fastställts av chefen för NCT. Innan en rapport får fastställas ska den dock ha godkänts av en representant från varje myndighet inom NCT. Om en rapport innebär en förändrad bedömning av hotnivå ska rapportens färdigställande dessutom föregås av ett beslut av chefen för Säkerhetspolisen.

NCT använder en hotnivåskala i sina presentationer och rapporter för terrorhotbedömningar. Syftet är främst att rapportmottagaren på ett snabbt och enkelt sätt ska få en uppfattning om hur NCT bedömer terrorhotet mot Sverige och svenska intressen i utlandet och huruvida det skett en förändring sedan tidigare bedömning. NCT bedömer hotnivån dels för Sverige generellt, dels för svenska intressen i olika geografiska områden utanför Sverige.

Ett hot består av att en person, organisation eller främmande makt har en kombinerad avsikt och förmåga att utföra exempelvis ett terrorattentat. Vid en terrorhotbedömning görs således en sammanvägd bedömning avseende förmåga och avsikt att utföra attentat mot Sverige och svenska intressen. NCT bedömer terrorhotet enligt en femgradig skala från (1) inget hot till (5) mycket högt hot. Däremellan kan bedömningen göras att det föreligger (2) ett lågt hot, (3) ett förhöjt hot eller (4) ett högt hot.

NCT ska vara den funktion i Sverige som har den bästa överblicken över allt tillgängligt underrättelsematerial av strategisk karaktär med bäring på terrorism. NCT har därmed en unik möjlighet att bedöma utvecklingen vad gäller hot mot Sverige och svenska intressen. Hotnivån för Sverige har sedan hösten 2010 bedömts motsvara en trea på den femgradiga skalan, dvs. det har förelegat ett förhöjt hot mot landet. I november 2015 höjdes emellertid hotnivån till en fyra på skalan, dvs. ett högt hot. Den 2 mars 2016 beslutade chefen för Säkerhetspolisen att terrorhotnivån skulle återgå till den förhöjda hotnivå som rått i Sverige sedan hösten 2010 och terrorhotnivån sänktes därmed återigen till en trea på den femgradiga skalan. Beslutet fattades med utgångspunkt i strategiska bedömningar gjorda av NCT.

5 Rättsliga utgångspunkter

5.1 Inledning

Utbyte av information är en av de grundläggande förutsättningarna för ett fungerande samarbete mellan myndigheter. Regler om utlämnande av uppgifter från en myndighet till en annan finns dels i OSL, dels i myndigheternas registerförfattningar. För att myndigheter ska kunna utbyta information krävs dels att informationen inte omfattas av sekretess eller att sekretessen kan brytas, dels att bestämmelser om behandling av personuppgifter i myndigheternas registerförfattningar ger stöd för att uppgifter kan lämnas ut.

Bestämmelser om behandling av personuppgifter och andra regler till skydd för den personliga integriteten finns på såväl internationell som nationell nivå. På internationell nivå finns bestämmelser i form av olika internationella konventioner och rekommendationer samt regleringen inom EU. På nationell nivå finns dels grundläggande och allmänna regler, dels särskilda s.k. registerförfattningar.

Detta avsnitt innehåller en redogörelse för de bestämmelser om offentlighet och sekretess som aktualiseras vid samarbete av sådant slag som förekommer inom NCT. Vidare redogörs för allmänna bestämmelser om behandling av personuppgifter samt de bestämmelser som gäller specifikt för de myndigheter som samverkar inom ramen för NCT. Avsnittet innehåller också en översiktlig redogörelse för internationella överenskommelser med grundläggande bestämmelser om integritetsskydd och dataskydd.

5.2 Internationella överenskommelser

5.2.1 Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna m.m.

Förenta nationernas (FN) generalförsamling antog i december 1948 en universell deklaration om de mänskliga rättigheterna – Förenta nationernas allmänna förklaring om de mänskliga rättigheterna. Deklarationen är inte formellt bindande för medlemsstaterna, men har betydelse som ett uttryck för vad den internationella opinionen kräver. I artikel 12 sägs att ingen får utsättas för godtyckliga ingripanden i fråga om privatliv, familj, hem eller korrespondens och inte heller för angrepp på sin heder eller sitt anseende samt att var och en har rätt till lagens skydd mot sådana ingripanden eller angrepp. Vidare sägs i artikel 29 att endast sådana inskränkningar i de i deklarationen angivna fri- och rättigheterna är tillåtna som fastställts i lag. Ingrepp får dessutom enbart ske i syfte att trygga tillbörlig hänsyn till och respekt för andras fri- och rättigheter samt för att tillgodose ett demokratiskt samhälles berättigade krav på moral, allmän ordning och allmän välfärd.

Inom FN har det också utarbetats en internationell konvention om medborgerliga och politiska rättigheter (ICCPR), som antogs av generalförsamlingen år 1966. Sverige anslöt sig till konventionen år 1971, varefter den trädde i kraft år 1976. Av konventionens artikel 17 följer att var och en har rätt till lagens skydd mot godtyckliga eller olagliga ingripanden i sitt privat- och familjeliv, sitt hem eller sin korrespondens, liksom mot olagliga angrepp på sin heder och sitt anseende. De stater som har tillträtt konventionen åläggs därmed vissa skyldigheter. Ett särskilt inrättat organ benämnt Kommittén för de mänskliga rättigheterna (Human Rights Committee) övervakar att de till konventionen anslutna staterna efterlever sina skyldigheter.

FN:s generalförsamling antog år 1990 även riktlinjer om datoriserade register med personuppgifter.

5.2.2 Europakonventionen

Den europeiska konventionen av den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är från och med den 1 januari 1995 inkorporerad i svensk rätt och gäller här i landet som lag (lag [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Den har därmed inte getts ställning som grundlag. I 2 kap. 19 § regeringsformen har emellertid införts en bestämmelse om att lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. Kontrollen av efterlevnaden av konventionen sker huvudsakligen av Europadomstolen för mänskliga rättigheter.

Av betydelse för skyddet för den personliga integriteten är framför allt artikel 8 i konventionen. I artikel 8 stadgas att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. En offentlig myndighet får inte inskränka åtnjutande av denna rättighet annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter.

Behandling av personuppgifter kan falla inom tillämpningsområdet för artikel 8 i Europakonventionen. All slags behandling av personuppgifter omfattas dock inte, utan frågan måste gälla privatliv, familjeliv, hem eller korrespondens. Primärt innebär artikel 8 att staten ska avhålla sig från ingrepp i den skyddade rättigheten. Artikeln innebär även en skyldighet för staten att vidta positiva åtgärder för att skydda den enskildes privatsfär. Sådana positiva åtgärder kan utgöras av lagstiftning, men också ha till ändamål att på annat sätt tillförsäkra medborgarna skydd mot övergrepp isärskilda situationer. I sin praxis har Europadomstolen också framhållit att kravet på att ingreppet ska vara nödvändigt inte är synonymt med ”oundgängligt”. Vad som krävs är däremot att det finns ett ”angeläget samhälleligt behov”. Inskränkningen i den grundläggande rättigheten måste vidare stå i rimlig proportion till det syfte som ska tillgodoses genom inskränkningen. Varje konventionsstat har själv en viss frihet att avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att

övervaka om denna frihet utnyttjas på ett rimligt sätt. (Hans Danelius, Mänskliga rättigheter i europeisk praxis, 2015, s. 365 f.)

5.2.3 Europarådets dataskyddskonvention

Europarådets ministerkommitté antog i januari 1981 en konvention (CETS No 108) till skydd för enskilda vid automatisk databehandling av personuppgifter, den s.k. dataskyddskonventionen. Konventionen trädde i kraft den 1 oktober 1985 och har ratificerats av samtliga medlemsstater i EU.

Dataskyddskonventionens innehåll kan ses som en precisering av skyddet enligt artikel 8 i Europakonventionen för enskilda vid automatiserad databehandling. Dataskyddskonventionens syfte är att säkerställa den enskildes rätt till personlig integritet i samband med behandling av personuppgifter och att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna ska iaktta i sin nationella lagstiftning. Personuppgifter som är föremål för automatiserad behandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Vidare ska uppgifterna vara relevanta för ändamålen och får inte senare användas på ett sätt som är oförenligt med dessa. Uppgifterna måste också vara riktiga och aktuella och de får inte bevaras längre än vad som är nödvändigt för ändamålen.

Vissa typer av personuppgifter får behandlas endast om den nationella lagstiftningen ger ett ändamålsenligt skydd. Till sådana personuppgifter hör uppgifter som avslöjar ras, politisk tillhörighet, religiös tro eller övertygelse i övrigt, hälsa och sexualliv samt uppgifter om brott.

För att skydda personuppgifter mot bl.a. oavsiktlig eller otillåten förstörelse föreskriver konventionen att lämpliga skyddsåtgärder ska vidtas. Vidare föreskrivs att den registrerade ska ha möjlighet till insyn i register och till att få uppgifter rättade. I vissa fall får undantag göras från bestämmelserna om uppgifternas beskaffenhet och rätten till insyn. Sådana inskränkningar förutsätter enligt konventionen stöd i den nationella lagstiftningen och att inskränkningen är nödvändig i ett demokratiskt samhälle för vissa angivna

ändamål, t.ex. statens ekonomiska intressen och brottsbekämpning, samt för att skydda enskildas fri- och rättigheter.

Konventionens roll som grundläggande dokument för automatiserad behandling av personuppgifter inom EU har i princip övertagits av dataskyddsdirektivet, se avsnitt 5.3.2. Direktivet omfattar dock inte behandling av personuppgifter inom områden som allmän säkerhet, försvar och statens säkerhet. På dessa områden är dataskyddskonventionen därför fortfarande av betydelse.

Det har inletts ett arbete med att modernisera dataskyddskonventionen, bl.a. mot bakgrund av den tekniska utvecklingen och globaliseringen. På uppdrag av Europarådet har en forskargrupp tagit fram en rapport om behovet av ändringar i konventionen. Förhandlingar om moderniseringen pågår.

5.2.4 Riktlinjer från OECD

Inom Organisationen för ekonomiskt samarbete och utveckling, OECD, har en expertgrupp utarbetat vissa riktlinjer i fråga om integritetsskyddet och persondataflödet över gränserna. Riktlinjerna antogs år 1980 av OECD:s råd tillsammans med en rekommendation till medlemsländernas regeringar om att beakta riktlinjerna i nationell lagstiftning. Samtliga medlemsländer, däribland Sverige, har godtagit rekommendationen och åtagit sig att följa denna. Riktlinjerna är tillämpliga på personuppgifter inom både den offentliga och privata sektorn. De gäller dels för uppgifter som lagras automatiskt, dels för uppgifter som förs manuellt. Syftet med riktlinjerna är att undvika de risker för intrång i den personliga integriteten och i individens frihet som behandling av personuppgifter kan medföra på grund av det sätt på vilket de behandlas, på grund av uppgifternas natur eller på grund av de sammanhang i vilka de används. År 2013 reviderades riktlinjerna genom införandet av vissa nyheter och förändringar.

5.3 EU:s dataskyddsreglering

5.3.1 Europeiska unionens stadga om de grundläggande rättigheterna

Europeiska unionens stadga om de grundläggande rättigheterna beskriver de fri- och rättigheter som EU erkänner att varje människa har. Stadgan är till stor del en sammanfattning av de rättigheter som tidigare var spridda i olika rättsakter, exempelvis i nationella lagar och internationella förpliktelser, Europakonventionen, Europeiska unionens och Europarådets sociala stadgor samt rättspraxis vid Europeiska unionens domstol och Europadomstolen för mänskliga rättigheter. Det handlar t.ex. om tanke-, religions-, yttrande- och mötesfrihet, rätt till ett skyddat privatliv och barns rätt till skydd och omvårdnad. Stadgan är från och med den 1 december 2009, när Lissabonfördraget trädde i kraft, rättsligt bindande för EU:s medlemsstater. En referens till stadgan har införts i artikel 6.1 i det ändrade EU-fördraget (prop. 2007/08:168 s. 58).

I artikel 7 i stadgan föreskrivs att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. I artikel 8 föreskrivs vidare att var och en har rätt till skydd för de personuppgifter som rör honom eller henne. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade.

Stadgan riktar sig till den verksamhet som utförs av EU:s egna organ och institutioner och blir tillämplig för medlemsstaterna endast i de fall där de tillämpar EU-rätten (artikel 51).

När det gäller de garanterade rättigheternas räckvidd följer av artikel 52 i stadgan att varje begränsning i utövningen av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och vara förenlig med proportionalitetsprincipen och det väsentliga innehållet i fri- och rättigheterna. I den mån rättigheterna i stadgan motsvarar rättigheter som skyddas av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Stadgans artiklar får inte tolkas så att de inskränker eller inkräktar på rättigheter enligt andra konventioner eller överenskommelser om fri- och rättigheter (artikel 53).

5.3.2 Dataskyddsdirektivet m.m.

Dataskyddsdirektivet

Den 24 oktober 1995 antogs Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Direktivet syftar till att garantera en hög och i alla medlemsstater likvärdig skyddsnivå när det gäller enskilda personers fri- och rättigheter med avseende på behandling av personuppgifter och att främja ett fritt flöde av personuppgifter mellan medlemsstaterna. Medlemsstaterna får inom den ram som anges i direktivet närmare precisera villkoren för när behandling av personuppgifter får förekomma. Sådana preciseringar får dock inte hindra det fria flödet av personuppgifter inom unionen.

Dataskyddsdirektivet gäller inte för sådan behandling av personuppgifter som faller utanför unionsrätten, t.ex. allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område. Behandling av personuppgifter i Förvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst samt i FRA:s försvarsunderrättelseverksamhet omfattas således inte av direktivet. Inte heller den behandling av personuppgifter som Säkerhetspolisen utför i sin brottsbekämpande verksamhet omfattas av direktivet.

Dataskyddsdirektivet har genomförts i svensk rätt genom personuppgiftslagen (1998:204), se avsnitt 5.4.2, och ett antal särregleringar i förhållande till denna lag (särskilda registerförfattningar). Personuppgiftslagen har gjorts generellt tillämplig och omfattar således även sådan verksamhet som faller utanför direktivets tillämpningsområde (prop. 1997/98:44 s. 40 f.).

Dataskyddsrambeslutet

Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (dataskyddsrambeslutet) reglerar dataskyddet inom angivna områden. Dataskyddsrambeslutet är endast tillämpligt på uppgifter som överförs eller görs tillgängliga mellan medlemsstaterna. Rambeslutet förpliktar medlemsstaterna att behandla personuppgifter som utbyts mellan medlemsstaterna

inom ramen för det angivna samarbetet på ett sådant sätt att skyddet för den personliga integriteten värnas. Det innehåller bl.a. bestämmelser om allmänna utgångspunkter för behandlingen av personuppgifter och känsliga personuppgifter, rättelse, radering och gallring av personuppgifter, information till den registrerade samt skadestånd och sanktioner. Till stora delar motsvarar innehållet dataskyddsdirektivet.

Vid genomförandet av dataskyddsrambeslutet bedömdes merparten av rambeslutets artiklar motsvaras av bestämmelser i svensk rätt, dels i personuppgiftslagen, dels i berörda myndigheters registerförfattningar. De kompletterande bestämmelser som krävdes genomfördes i en särskild lag, lagen (2013:329) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

EU:s dataskyddsreform

EU-kommissionen presenterade i januari 2012 ett förslag till en genomgripande reform av EU:s regler om skydd för personuppgifter. Detta resulterade i att Europaparlamentet och EU:s ministerråd i april 2016 antog dels en ny förordning om dataskydd, dels ett nytt direktiv med särregler för den brottsbekämpande sektorn.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) utgör en ny generell reglering för personuppgiftsbehandling inom EU och kommer att ersätta det nuvarande dataskyddsdirektivet. Det huvudsakliga syftet med förordningen är att ytterligare harmonisera och effektivisera skyddet för personuppgifter för att förbättra den inre marknadens funktion och öka enskildas kontroll över sina personuppgifter. Förordningen baseras till stor del på dataskyddsdirektivets struktur och innehåll men innebär även en rad nyheter såsom en utökad informationsskyldighet, administrativa sanktionsavgifter och inrättandet av Europeiska dataskyddsstyrelsen. Förordningen är direkt tillämplig i medlemsstaterna vilket innebär att den kommer att ersätta personuppgiftslagen. Förordningen förutsätter och möjliggör dock kompletterande nationella

bestämmelser av olika slag. Det finns t.ex. ett förhållandevis stort utrymme att behålla eller införa särregleringar för sådan personuppgiftsbehandling som är nödvändig för att den personuppgiftsansvarige ska kunna uppfylla en rättslig skyldighet, utföra en arbetsuppgift av allmänt intresse eller behandla uppgifter i samband med myndighetsutövning.

Från förordningens tillämpningsområde undantas behandling av personuppgifter som utgör ett led i en verksamhet som a) inte omfattas av unionsrätten, b) utförs av medlemsstaterna när de utför aktiviteter som omfattas av den gemensamma utrikes- och säkerhetspolitiken, c) utförs av en fysisk person som ett led i verksamhet av privat natur eller som har samband med dennes hushåll eller d) utförs av behöriga myndigheter för ändamålen att förebygga, utreda, upptäcka eller lagföra brott eller verkställa straffrättsliga påföljder, inkluderande skydd mot samt förebyggande av hot mot allmän säkerhet. Förordningen gäller inte heller för behandling av personuppgifter som utförs av EU:s institutioner, organ och byråer. Sådan behandling regleras i stället i Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter.

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, innehåller särregler för den personuppgiftsbehandling som behöriga myndigheter utför i ovan nämnda syften samt för att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten. Direktivet ska dels skydda fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till skydd av personuppgifter, dels underlätta det informationsutbyte mellan behöriga myndigheter som är nödvändigt enligt unionsrätt eller nationell rätt. Direktivet ska ersätta det gällande dataskyddsrambeslutet (2008/977/RIF) som reglerar utbyte av personuppgifter mellan medlemsstaterna inom denna sektor. Direktivets tillämpningsområde omfattar till skillnad från rambeslutet emellertid även rent nationell personuppgiftsbehandling på

området för brottsbekämpning, brottmålshantering och straffverkställighet.

Den 25 maj 2018 kommer den allmänna dataskyddsförordningen att ersätta den svenska personuppgiftslagen. Det nya direktivet blir emellertid inte direkt tillämpligt i svensk rätt, utan ska i stället införas i den nationella lagstiftningen inom två år efter att det formellt antagits.

5.4 Grundläggande nationella bestämmelser om behandling av personuppgifter

5.4.1 Regeringsformen

I regeringsformen (RF) finns grundläggande bestämmelser till skydd för den personliga integriteten. I målsättningsstadgandet i 1 kap. 2 § RF slås det fast att den offentliga makten ska utövas med respekt bl.a. för den enskilda människans frihet och att det allmänna ska värna om den enskildes privatliv och familjeliv.

Av 2 kap. 6 § andra stycket RF följer sedan den 1 januari 2011 att var och en gentemot det allmänna även är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. En begränsning av det skydd som bestämmelsen föreskriver får endast göras i lag och under de förutsättningar som anges i 2 kap. 21–22 §§ RF. Bestämmelsen omfattar bara vissa kvalificerade intrång i den personliga integriteten. Vid bedömningen av vad som kan anses utgöra ett betydande intrång ska man enligt förarbetsuttalandena väga in bl.a. uppgifternas karaktär och omfattning samt ändamålet med behandlingen och omfattningen av utlämnandet av uppgifter till andra (prop. 2009/10:80 s. 178 f.).

Bakgrunden till bestämmelsen är att det ansågs finnas vissa brister i lagstiftning som innefattade intrång i den enskildes personliga integritet. Dessa brister bestod i att de avvägningar mellan olika motstående intressen som normalt ska göras i lagstiftningsärenden i vissa fall var bristfälligt redovisade och att det i första hand var de negativa effekterna av olika integritetsbegränsande åtgärder som var knapphändigt belysta (prop. 2009/10:80 s. 175 f.). Av bl.a. dessa skäl ansågs det därför finnas ett behov av att stärka skyddet för den personliga integriteten i grundlag. I en övergångsbestäm-

melse till bestämmelsen i 2 kap. 6 § andra stycket RF anges att äldre föreskrifter som innebär betydande intrång i den personliga integriteten behåller sin giltighet, dock längst t.o.m. den 31 december 2015. Grundlagsändringen medför bl.a. att viss personuppgiftsbehandling som har reglerats i förordning måste regleras i lag.

5.4.2 Personuppgiftslagen

Personuppgiftslagen (1998:204), PuL, innehåller generella regler om behandling av personuppgifter och ska tillämpas i hela samhället av både myndigheter och enskilda. Lagen har till syfte att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Genom personuppgiftslagen har dataskyddsdirektivet genomförts i svensk rätt.

Personuppgiftslagen är subsidiär i förhållande till annan lagstiftning. Detta innebär att om det i en annan lag eller i en förordning finns bestämmelser som avviker från personuppgiftslagen, ska de bestämmelserna gälla (2 § PuL). Vid lagens införande anfördes att det traditionella svenska systemet med särregler isärskilda författningar var att föredra framför generella undantag från den nya lagen (prop. 1997/98:44 s. 41).

Personuppgiftslagen omfattar all helt eller delvis automatiserad behandling av personuppgifter (5 § första stycket PuL). Lagen är teknikoberoende i den meningen att den i fråga om automatiserad behandling inte begränsas till dataregister. All automatiserad behandling omfattas, alltså även personuppgifter som framgår av bilder och ljud. Avgörande är om personuppgifterna är föremål för automatiserad behandling, inte om de är ordnade i ett register eller inte. Det är vidare tillräckligt att behandlingen av personuppgifter endast delvis är automatiserad för att den ska falla under lagens bestämmelser. Om uppgifter samlas in manuellt och sedan behandlas automatiserat är även insamlandet en sorts behandling som omfattas av lagen. På samma sätt faller ett utlämnande genom manuella utskrifter från ett automatiserat register under lagens bestämmelser. Personuppgiftslagen gäller även för manuella register med personuppgifter som är strukturerade eller ordnade så att de är sökbara enligt särskilda kriterier (5 § andra stycket PuL). Det görs dock undantag för behandling av personuppgifter i ostrukturerat material

(5 a § PuL). Vid sådan behandling av uppgifter i exempelvis löpande text behöver merparten av lagens hanteringsregler inte tillämpas. Behandlingen får dock inte utföras om den innebär en kränkning av den registrerades personliga integritet.

Med personuppgifter avses enligt lagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet (3 § PuL). Begreppet behandling av personuppgift omfattar varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte. Exempel på behandling av personuppgifter är insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring (3 § PuL).

Det finns några viktiga undantag från personuppgiftslagens tillämpningsområde. Lagen gäller t.ex. inte vid behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur (6 § PuL). Bestämmelserna i lagen tillämpas inte heller i den utsträckning det skulle strida mot grundlagsbestämmelserna om tryck- och yttrandefrihet (7 § första stycket PuL). I princip ska personuppgiftslagens bestämmelser inte heller tillämpas för journalistisk, konstnärlig eller litterär verksamhet (7 § andra stycket PuL). Vidare anges i personuppgiftslagen att lagen inte gäller i den mån det skulle inskränka offentlighetsprincipen (8 § första stycket PuL).

I 9 § PuL uppställs vissa grundläggande krav på all behandling av personuppgifter som omfattas av lagen. Den personuppgiftsansvarige ska se till att personuppgifter bara behandlas om det är lagligt samt att personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed. Vidare ska personuppgifter endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålet måste bestämmas redan när uppgifterna samlas in. Att ändamålet ska vara särskilt innebär att en alltför allmänt hållen ändamålsangivelse inte kan godtas. Den personuppgiftsansvarige ska definiera avsikten med insamlingen och användningen av personuppgifterna på ett så precist sätt som möjligt. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in (den s.k. finalitetsprincipen). Det sistnämnda kan bli aktuellt att pröva när

personuppgifter lämnas ut till tredje man. Ett sådant utlämnande får alltså inte vara oförenligt med det ändamål för vilket uppgifterna ursprungligen samlades in. Om personuppgifter lämnas ut i form av allmänna handlingar med stöd av bestämmelserna i 2 kap. tryckfrihetsförordningen, TF, blir en sådan prövning dock inte aktuell.

Av 9 § PuL framgår också att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen. Inte heller får fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Därutöver ska de uppgifter som behandlas vara riktiga och, om det är nödvändigt, aktuella. Alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen. Personuppgifter får inte heller bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Varje behandling av personuppgifter måste kunna hänföras till någon av de situationer som anges i personuppgiftslagens regler om när behandling av personuppgifter är tillåten. Av 10 § PuL följer att personuppgifter endast får behandlas om den registrerade har lämnat sitt samtycke till behandlingen eller om behandlingen är nödvändig för att:

a) ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas,

b) den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet,

c) vitala intressen för den registrerade ska kunna skyddas,

d) en arbetsuppgift av allmänt intresse ska kunna utföras,

e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut ska kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller

f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut ska kunna tillgodoses, om detta

intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Enligt 13 § PuL är det som huvudregel förbjudet att behandla känsliga personuppgifter. Med känsliga personuppgifter avses sådana personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening eller som rör hälsa eller sexualliv. Från förbudet att behandla känsliga personuppgifter finns dock vissa undantag (se 15–20 §§ PuL). Särskilda bestämmelser om uppgifter om lagöverträdelser och behandling av personnummer finns vidare i 21 och 22 §§ PuL. Av 21 § framgår att det är förbjudet för andra än myndigheter att behandla uppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Regeringen, eller den myndighet regeringen bestämmer, får dock meddela föreskrifter om undantag från förbudet. Datainspektionen har meddelat sådana föreskrifter i DIFS 1998:3.

Bestämmelser om i vilka fall information om behandling av personuppgifter ska lämnas till den enskilde finns i 23–27 §§ PuL och bestämmelser om den registrerades rätt att begära rättelse och omprövning av automatiserade beslut finns i 28 och 29 §§ PuL. Föreskrifter om säkerheten vid behandling av personuppgifter finns i 30–32 §§ PuL.

Enligt 33 § PuL är det förbjudet att till tredje land, dvs. ett land utanför EU eller EES, föra över personuppgifter som är under behandling, om landet inte har en adekvat nivå för skydd av personuppgifter. Trots förbudet är det dock enligt 34 § PuL tillåtet att under vissa förutsättningar föra över uppgifter till tredje land. En sådan överföring förutsätter antingen att den registrerade gett sitt samtycke till överföringen eller att överföringen är nödvändig bl.a. för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras eller att vitala intressen för den registrerade ska kunna skyddas. Vidare är det tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen. Regeringen får dessutom meddela föreskrifter om ytterligare undantag från förbudet mot överföring (35 § PuL).

I personuppgiftslagen finns det även bestämmelser om bl.a. anmälan till tillsynsmyndigheten, skadestånd och straff.

5.4.3 Registerförfattningar

Utöver personuppgiftslagen har det utarbetats en stor mängd specialförfattningar, s.k. registerförfattningar, som reglerar framför allt myndigheters behandling av personuppgifter. Syftet med sådana specialförfattningar är att anpassa lagstiftningen till de behov som finns inom olika verksamhetsområden och samtidigt göra avvägningar mellan behovet av effektivitet i berörd verksamhet och behovet av skydd för enskildas integritet. Detta särskilt då det finns behov av att avvika från eller komplettera det integritetsskydd som personuppgiftslagen annars ger. Den bakomliggande tanken är att myndighetsregister med ett stort antal registrerade och med ett känsligt innehåll ska regleras särskilt i lag (prop. 1990/91:60 s. 58 och bet. KU 1990/91:11 s. 11). En utgångspunkt vid utarbetandet av registerförfattningar är att regleringen så långt som möjligt ska vara i överensstämmelse med personuppgiftslagen och därmed även dataskyddsdirektivets materiella bestämmelser samt att behovet av särregler i förhållande till personuppgiftslagen bör övervägas noga (prop. 1997/98:44 s. 41).

En registerförfattning kan under vissa förutsättningar anses innebära ett stärkt integritetsskydd för särskilt känsliga register eller andra personuppgiftssamlingar. Andra exempel på när en särskild författningsreglering i form av en registerförfattning kan anses motiverad är när:

– en nödvändig behandling av personuppgifter över huvud taget inte är tillåten enligt personuppgiftslagen,
– personuppgiftslagen visserligen reglerar ett visst förhållande men det finns anledning att avvika från eller precisera den regleringen,
– personuppgiftslagens bestämmelser kan ge upphov till tolkningsproblem och det finns anledning att ha tydliga bestämmelser,
– det finns anledning att begränsa möjligheterna till behandling av uppgifter av integritetsskäl i fråga om myndigheters registrering och åtkomst till stora och känsliga uppgiftsmängder, eller

– det finns anledning att vara särskilt tydlig gentemot allmänheten, t.ex. i fråga om vilka uppgifter om enskilda som en myndighet registrerar.

Behandlingen av personuppgifter hos de tre NCT-myndigheterna regleras i tre olika registerförfattningar. En närmare redogörelse för dessa regelverk följer i nästa avsnitt.

5.5 NCT-myndigheternas behandling av personuppgifter

5.5.1 Säkerhetspolisen

Allmänt

I 6 kap. PDL finns särskilda bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. PDL gäller i stället för personuppgiftslagen men hänvisar till vissa bestämmelser i den lagen som gäller även i Polismyndighetens och Säkerhetspolisens brottsbekämpande verksamhet. PDL kompletteras av polisdataförordningen (2010:1155). I denna förordning finns kompletterande bestämmelser om bl.a. behörigheter, ändamål, elektroniskt utlämnande, bevarande och gallring.

Ändamål m.m.

Säkerhetspolisen får behandla personuppgifter i sin brottsbekämpande verksamhet bara om det behövs för något av de ändamål som anges i PDL. Av 6 kap. 1 § 1 b PDL framgår att personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott. När uppgifter har samlats in för ett tillåtet ändamål får de också vidarebehandlas för vissa andra ändamål, s.k. sekundära ändamål. Av 6 kap. 2 § PDL framgår att uppgifter får vidarebehandlas bl.a. för att tillhandahålla information som en annan myndighet behöver inom ramen för myndighetsöverskridande samverkan mot brott. I förarbetena till lagen nämns Samverkansrådet mot terrorism som ett sammanhang där Säkerhetspolisen behöver ha möjlighet att

tillhandahålla information till andra myndigheter (prop. 2009/10:85 s. 262). I fråga om personuppgiftsbehandling för andra sekundära ändamål än de i lagen angivna gäller finalitetsprincipen i 9 § första stycket d) PuL.

Säkerhetspolisen får behandla känsliga personuppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen (2 kap. 10 § och 6 kap. 4 § 4 PDL). Att det ska vara absolut nödvändigt att behandla uppgifterna innebär att behovet måste prövas noga i det enskilda fallet (prop. 2009/10:85 s. 325). Tillgången till personuppgifter ska vidare begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (2 kap. 11 § och 6 kap. 4 § 5 PDL). I 6 kap. 5 § PDL anges att Säkerhetspolisen är personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför.

Elektroniskt utlämnande

När det gäller utlämnande av uppgifter framgår det av PDL att Säkerhetspolisen får lämna ut enstaka personuppgifter på medium för automatiserad behandling (2 kap. 20 § och 6 kap. 4 § 7 PDL). Regeringen har dock getts en möjlighet att meddela föreskrifter om att uppgifter får lämnas ut på sådant medium även i andra fall. Sådana föreskrifter finns i polisdataförordningen. Som exempel på denna form av utlämnande nämns i förarbetena att uppgifter lämnas ut i ett e-postmeddelande, på ett USB-minne eller genom direkt överföring från ett datasystem till ett annat via allmänna kommunikationsnät (prop. 2009/10:85 s. 185 och s. 333). Att endast enstaka uppgifter får lämnas ut elektroniskt innebär enligt förarbetena att det inte är tillåtet att lämna ut en större mängd personuppgifter, t.ex. ett helt register eller delar av ett register. Ordet enstaka har dock en annan innebörd i bestämmelsen än i vanligt språkbruk. När personuppgifter förekommer i en eller ett fåtal handlingar är bestämmelsen inte avsedd att utgöra ett hinder mot att handlingarna lämnas ut. Detta gäller även om en handling innehåller ett större antal personuppgifter, t.ex. en lista över personnummer. Även utlämnande av t.ex. ett ärende eller delar av ett ärende där personuppgifter förekommer är förenligt med bestämmelsen (prop. 2009/10:85 s. 333).

Enligt 2 kap. 21 § PDL är utlämnande genom direktåtkomst tillåtet bara i den utsträckning som följer av lagen. Eftersom Säkerhetspolisen behandlar särskilt känsliga uppgifter har myndigheten i PDL inte getts någon möjlighet att lämna ut uppgifter genom direktåtkomst (prop. 2009/10:85 s. 178–179).

Gemensamt tillgängliga uppgifter

I 6 kap. 8–14 §§ PDL regleras Säkerhetspolisens behandling av gemensamt tillgängliga uppgifter. Gemensamt tillgängliga uppgifter infördes som ett nytt begrepp i PDL i stället för de mer traditionella begreppen register och databas. I förarbetena anges att registerbegreppet och begreppet databas har en stark teknisk anknytning och att detta inte är ett helt relevant sätt att se på samlingar av uppgifter i elektronisk form. Det konstaterades att det väsentliga i sammanhanget inte är på vilket sätt uppgifterna tekniskt lagras utan den faktiskt åsyftade tillgängligheten, dvs. om ett flertal personer har möjlighet att ta del av uppgiften (prop. 2009/10:85, s. 126). Genom att använda uttrycket gemensamt tillgängliga uppgifter i stället för exempelvis register eller databas har lagstiftningen gjorts teknikneutral.

En grundläggande förutsättning för att personuppgifter ska anses vara gemensamt tillgängliga bör enligt motiven vara att de kan användas gemensamt av flera, dvs. att fler än en person har åtkomst till uppgifterna. Personuppgifter blir att anse som gemensamt tillgängliga om dessa exempelvis behandlas för att en obestämd krets ska kunna ta del av uppgifterna, t.ex. hela polisorganisationen eller en viss enhet inom organisationen. Så är fallet med t.ex. det allmänna spaningsregistret och det centrala kriminalunderrättelseregistret. Uppgifter bör dock anses vara gemensamt tillgängliga även i vissa fall när den personkrets som har tillgång till uppgifterna är bestämd och avgränsad om det då rör sig om ett relativt stort antal personer. Uppgifter som endast ett fåtal personer har rätt att ta del av bör emellertid inte anses som gemensamt tillgängliga. I förarbetena anges som tumregel att uppgifter normalt bör anses som gemensamt tillgängliga när fler än ett tiotal personer har tillgång till dem (se prop. 2009/10:85, s. 127 f.).

Av bestämmelsen i 6 kap. 8 § PDL framgår att personuppgifter får göras gemensamt tillgängliga i Säkerhetspolisens verksamhet om det behövs för något av de ändamål för vilka Säkerhetspolisen får behandla personuppgifter. När det gäller uppgifter som har gjorts gemensamt tillgängliga ska det genom en särskild upplysning eller på något annat sätt framgå för vilket närmare ändamål uppgifterna behandlas (6 kap. 9 § PDL). Om uppgifterna direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller komma att utöva brottslig verksamhet ska det framgå att personen inte är misstänkt (6 kap. 10 § första stycket PDL). Uppgifter om en person som kan antas ha samband med misstänkt brottslig verksamhet ska vidare förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Detta behövs dock inte om uppgifterna ingår i en uppgiftssamling som har skapats för att bearbeta och analysera information så länge bearbetningen och analysen befinner sig i ett inledande skede (6 kap. 10 § andra stycket PDL). Vid sökning i gemensamt tillgängliga uppgifter får Säkerhetspolisen använda känsliga personuppgifter som sökbegrepp endast om det är absolut nödvändigt (6 kap. 11 § PDL).

5.5.2 Försvarets radioanstalt

Allmänt

FRA:s personuppgiftsbehandling regleras i FRA-PuL med tillhörande förordning. Lagen innehåller en heltäckande reglering på området och ersätter personuppgiftslagen fullt ut (1 kap. 1 § andra stycket).

Ändamål m.m.

Av 1 kap. 8 § FRA-PuL framgår att personuppgifter får behandlas i FRA:s försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. I den lagen anges att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets-, och försvarspolitik samt i övrigt för kartläggning av yttre hot

mot landet samt att försvarsunderrättelseverksamhet endast får avse utländska förhållanden. Det anges att regeringen ska bestämma försvarsunderrättelseverksamhetens inriktning (1 §). Verksamheten ska vidare fullgöras genom inhämtning, bearbetning och analys av information (2 §). Genom hänvisningen till lagen om försvarsunderrättelseverksamhet framgår att såväl de direkt i lagen angivna ändamålen som de ändamål som återfinns i regeringens inriktning utgör avgränsningar för behandlingen av personuppgifter (prop. 2006/07:46 s. 65).

I ändamålsbestämmelsen i 1 kap. 8 § FRA-PuL anges vidare att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Med preciserad inriktning avses de interna inriktningar som FRA fastställer för närmare avgränsning av verksamheten (prop. 2006/07:46 s. 67). Vilken grad av anknytning en person ska ha till en preciserad inriktning måste med hänsyn till verksamhetens speciella karaktär avgöras från fall till fall. Av förarbetena framgår dock att det alltid måste finnas en sådan koppling mellan en person och den företeelse som verksamheten syftar till att kartlägga att man i efterhand kan kontrollera att personuppgiftsbehandlingen är motiverad av verksamhetsskäl och kan hänföras till en viss preciserad inriktning (prop. 2006/07:46 s. 65).

När det gäller vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga, s.k. sekundära ändamål, får detta göras med stöd av 1 kap. 6 § 4 FRA-PuL. Där anges att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Sådan vidarebehandling görs således med stöd av den s.k. finalitetsprincipen.

FRA får behandla känsliga personuppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen (1 kap. 11 §). Tillgången till personuppgifter ska vidare begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter (1 kap. 16 §). Av 1 kap. 5 § FRA-PuL framgår att FRA är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Uppgiftssamlingar

I 1 kap. 7 § FRA-PuL anges att FRA får behandla personuppgifter i uppgiftssamlingar. Av förordningen framgår vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling. I 4 § i förordningen anges exempelvis att det vid FRA får finnas uppgiftssamlingar för underrättelser och att dessa samlingar endast får innehålla färdiga underrättelserapporter.

När det gäller begreppet uppgiftssamling konstateras i förarbetena att lagstiftningen bör vara teknikneutral och att det allmänt vedertagna begreppet databas kan medföra att myndigheterna finner sig bundna till vissa tekniska system. Av den anledningen föreslogs att den helt neutrala beteckningen uppgiftssamling i stället skulle användas (prop. 2006/07:46 s. 59). För att en uppgift ska anses ingå i en uppgiftssamling ska den, enligt förarbetena, användas gemensamt i en viss verksamhet för de ändamål som styr behandlingen av uppgifter inom verksamheten. En uppgift används gemensamt om den behandlas på ett sätt som medför att den är allmänt tillgänglig i verksamheten. Uppgifter i t.ex. e-post, ordbehandlingsdokument, och tillfällig behandling av uppgifter som lagras på en hårddisk eller i en server faller utanför uppgiftssamlingarna (prop. 2006/07:46 s. 59 och s. 120).

Elektroniskt utlämnande m.m.

I 1 kap. 14 och 15 §§ FRA-PuL regleras elektroniskt utlämnande. Av dessa bestämmelser framgår att FRA som huvdregel endast får lämna ut enstaka personuppgifter på medium för automatiserad behandling. Regeringen kan dock besluta att myndigheten får lämna ut uppgifter på sådant medium även i andra fall. Av förordning framgår att utlämnande på sådant medium får omfatta fler än enstaka uppgifter om uppgifterna lämnas ut till en annan statlig myndighet. När det gäller direktåtkomst framgår av lagen att regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. I förordningen räknas ett antal myndigheter upp, bl.a. Säkerhetspolisen och Försvarsmakten, som får ha direktåtkomst till uppgifter i en uppgiftssamling för underrättelser i den omfattning som FRA beslutar.

I lagens övriga kapitel finns bestämmelser om bl.a. information till den enskilde, rättelse, skadestånd, tillsynsmyndighet och gallring.

5.5.3 Militära underrättelse- och säkerhetstjänsten

Allmänt

Försvarsmaktens/Musts personuppgiftsbehandling inom ramen för försvarsunderrättelseverksamheten och den militära säkerhetstjänsten regleras i PuL UNDSÄK med tillhörande förordning. Lagen är uppbyggd på samma sätt som den lag som reglerar FRA:s behandling av personuppgifter, se avsnitt 5.5.2, och merparten av bestämmelserna ser likadana ut. Det som anges i förarbetena och som hänvisas till ovan gäller således även denna reglering. Även denna lag är en heltäckande reglering som ersätter personuppgiftslagen fullt ut (1 kap. 1 § andra stycket).

Ändamål m.m.

Precis som när det gäller FRA anges det i 1 kap. 8 § PuL UNDSÄK att personuppgifter får behandlas i Försvarsmaktens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. I bestämmelsen anges också att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Den ändamålsbestämmelsen ser således exakt likadan ut som ändamålsbestämmelsen i den lag som gäller för FRA. Enligt 1 kap. 9 § PuL UNDSÄK får personuppgifter dessutom behandlas i Försvarsmaktens militära säkerhetstjänst för att upptäcka, förebygga och avvärja säkerhetshotande verksamhet som riktas mot Försvarsmakten och dess säkerhetsintressen om det är nödvändigt för att (1) klarlägga verksamhet som innefattar hot mot rikets säkerhet eller (2) vidta åtgärder som hindrar eller försvårar säkerhetshotande verksamhet. För dessa ändamål får uppgifter om en person behandlas endast om uppgifterna t.ex. ger grundad anledning att anta att personen har utövat eller kan komma att utöva verksamhet som innefattar brott som kan

hota rikets säkerhet eller terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller motsvarande brottslighet enligt tidigare lagstiftning. När det gäller vidarebehandling av personuppgifter för vissa andra ändamål än de ursprungliga, s.k. sekundära ändamål, får detta även här göras med stöd av 1 kap. 6 § 4 PuL UNDSÄK, dvs. den s.k. finalitetsprincipen.

Försvarsmakten får behandla känsliga personuppgifter endast om det är absolut nödvändigt för ändamålet med behandlingen (1 kap. 12 §) och tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter (1 kap. 16 §). Av 1 kap. 5 § PuL UNDSÄK framgår att Försvarsmakten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.

Uppgiftssamlingar

Precis som FRA får Försvarsmakten behandla personuppgifter i uppgiftssamlingar (1 kap. 7 §). Av förordningen framgår vilka uppgiftssamlingar som får finnas och vilka uppgifter som får behandlas i respektive samling. I 2 § i förordningen anges exempelvis att det vid Försvarsmakten får finnas uppgiftssamlingar för försvarsunderrättelseverksamhet. Dessa uppgiftssamlingar får endast innehålla identitetsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamhet samt upplysningar om varifrån den registrerade uppgiften kommer och om en uppgiftslämnares trovärdighet. Det framgår vidare att uppgiftssamlingarna endast får innehålla uppgifter som behövs för att Försvarsmakten ska kunna fullgöra uppgifter enligt lagen (2000:130) om försvarsunderrättelseverksamhet.

Elektroniskt utlämnande m.m.

Reglerna om elektroniskt utlämnande ser likadana ut för Försvarsmakten som för FRA. Myndigheten får således endast lämna ut enstaka personuppgifter på medium för automatiserad behandling (1 kap. 14 §). Av förordning framgår dock att utlämnande på sådant medium får omfatta fler än enstaka uppgifter om uppgifterna lämnas

ut till en annan statlig myndighet. När det gäller direktåtkomst framgår det av lagen att regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar (1 kap. 15 §). I förordningen anges bl.a. att FRA får ha direktåtkomst till uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet i den omfattning som Försvarsmakten beslutar.

I lagens övriga kapitel finns bestämmelser om bl.a. information till den enskilde, rättelse, skadestånd, tillsynsmyndighet och gallring.

5.6 Offentlighet och sekretess

5.6.1 Offentlighetsprincipen

Offentlighetsprincipen är en av de grundläggande principerna för vårt statsskick. Den innebär att allmänheten och massmedierna ska ha insyn i statens och kommunernas verksamhet. Offentlighetsprincipen kommer till uttryck på olika sätt, exempelvis genom yttrande- och meddelarfrihet för tjänstemän, genom domstolsoffentlighet och genom offentlighet vid beslutande församlingars sammanträden. När det mer allmänt talas om offentlighetsprincipen åsyftas dock i första hand reglerna om allmänna handlingars offentlighet. Denna princip infördes genom 1766 års tryckfrihetsförordning och regleras numera i 1949 års tryckfrihetsförordning (TF).

Enligt 2 kap. 1 § TF har varje svensk medborgare rätt att ta del av allmänna handlingar. Av 2 kap. 3 § TF följer att en handling är allmän om den förvaras hos en myndighet och anses inkommen till myndigheten eller upprättad där. Handlingsoffentlighet gäller framför allt i det allmännas verksamhet, men även i vissa privaträttsliga organ som räknas upp i en bilaga till OSL.

Enligt 2 kap. 2 § första stycket TF får rätten att ta del av allmänna handlingar begränsas endast om det är påkallat med hänsyn till vissa angivna intressen, t.ex. skyddet för enskilds personliga eller ekonomiska förhållanden eller intresset att förebygga eller beivra brott. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag (OSL) eller, om det i visst fall är lämpligare, i en annan lag vartill den särskilda lagen hänvisar.

5.6.2 Allmänt om sekretess

Sekretess innebär ett förbud att röja en uppgift, oavsett om det sker genom utlämnande av en handling eller genom att röja uppgiften muntligen eller på något annat sätt (3 kap. 1 § OSL). Sekretessen innebär således dels handlingssekretess, dels tystnadsplikt. Till den del sekretessen innebär tystnadsplikt innebär sekretessen en begränsning av yttrandefriheten enligt regeringsformen.

Sekretessbestämmelsernas uppbyggnad

En sekretessbestämmelse består i regel av tre huvudsakliga rekvisit, dvs. förutsättningar för bestämmelsens tillämplighet. Dessa tre rekvisit anger sekretessens föremål, sekretessens räckvidd och sekretessens styrka.

Sekretessens föremål är den information som kan hemlighållas och anges i lagen genom ordet ”uppgift” tillsammans med en mer eller mindre långtgående precisering av uppgiftens art, t.ex. uppgift om enskilds personliga förhållanden.

En sekretessbestämmelses räckvidd bestäms normalt genom att det i bestämmelsen preciseras att sekretessen för de angivna uppgifterna bara gäller i en viss typ av ärende, i en viss typ av verksamhet eller hos en viss myndighet. Några få sekretessbestämmelser gäller utan att räckvidden är begränsad. En uppgift kan då hemlighållas oavsett i vilket ärende, i vilken verksamhet eller hos vilken myndighet den förekommer.

Sekretessens styrka bestäms i regel med hjälp av s.k. skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att viss skada eller men uppkommer om uppgiften röjs. Det omvända skaderekvisitet har den omvända utgångspunkten, dvs. det uppställer sekretess som huvudregel. Vid ett omvänt skaderekvisit gäller således sekretess om det inte står klart att uppgiften kan röjas utan att viss skada eller men uppstår. En del bestämmelser innehåller ett kvalificerat rakt skaderekvisit, dvs. det krävs särskilt mycket för att sekretessen ska gälla. Sekretessen kan också vara absolut. I ett sådant fall ska de uppgifter som omfattas av bestämmelsen hemlighållas utan någon skadeprövning om uppgifterna begärs ut.

Sekretess mellan myndigheter och sekretessbrytande bestämmelser

Sekretess gäller såväl mot enskilda som mot andra myndigheter. Sekretess kan gälla även mellan olika verksamhetsgrenar inom en myndighet om de är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL).

Syftet med sekretess mellan myndigheter är i första hand att värna om den enskildes integritet. I förarbetena till sekretesslagen (1980:100) som föregick OSL framhålls att ett fullgott integritetsskydd för information om en enskild hos en myndighet i princip ställer krav på att informationen inte vidarebefordras utanför den verksamhet i vilken den har inhämtats. Det anges att uppgifter hos en annan myndighet kan läggas till grund för åtgärder som, även om de är helt lagenliga, har en negativ innebörd för den enskilde. Även den omständigheten att ett större antal tjänstemän kan få kunskap om ett känsligt förhållande kan enligt förarbetena upplevas som menligt av den som uppgiften rör. Risken för obehörig vidarespridning anses också öka även om de funktionärer hos den myndighet som får del av informationen i sin tur har tystnadsplikt (prop. 1979/80:2 Del A s. 90).

Samtidigt har myndigheter behov av att utbyta information med varandra. Sedan länge har det också ansetts vara en självklar princip att myndigheter är skyldiga att samarbeta och bistå varandra i den utsträckning som det kan ske. Principen kommer till uttryck i bl.a. 6 § förvaltningslagen (1986:223) där det stadgas att varje myndighet ska lämna andra myndigheter hjälp inom ramen för den egna verksamheten. Vidare föreskrivs i 6 kap. 5 § OSL att en myndighet på begäran av en annan myndighet ska lämna uppgifter som den förfogar över, i den mån hinder inte möter på grund av bestämmelser om sekretess eller av hänsyn till arbetets behöriga gång. Denna bestämmelse kan ses som en precisering av 6 § förvaltningslagen.

I många fall måste myndigheter kunna utbyta information för att kunna utföra sina uppgifter. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser. Dessa har utformats efter en intresseavvägning mellan myndigheternas behov av att utbyta uppgifter och det intresse som den aktuella sekretessbestämmelsen avser att skydda, se avsnitt 5.6.5.

Överföring av sekretess

En grundläggande princip i OSL är att sekretess som huvudregel inte följer med en uppgift när den lämnas till en annan myndighet. Det beror bl.a. på att behovet av och styrkan i sekretessen inte kan bestämmas enbart med hänsyn till sekretessintresset. Detta måste i varje sammanhang vägas mot intresset av insyn i myndighetens verksamhet. Offentlighetsintresset kan således kräva att de uppgifter som behandlas som hemliga hos en myndighet är offentliga hos en annan myndighet som har inhämtat dem hos den förstnämnda (prop. 1979/80:2 Del A s. 75 f.). Lagstiftaren har alltså tagit ställning mot en allmän bestämmelse om överföring av sekretess. Vissa bestämmelser om överföring av sekretess med begränsade och överblickbara tillämpningsområden har dock införts. Sådana bestämmelser innebär att en sekretessbestämmelse som är tillämplig hos den utlämnande myndigheten även ska tillämpas hos den mottagande myndigheten.

Vid överföring av sekretess skiljer man mellan *primära* och *sekundära* sekretessbestämmelser. Dessa begrepp definieras i 3 kap. 1 § OSL. En sekretessbestämmelse som är direkt tillämplig hos en myndighet kallas primär sekretessbestämmelse. En bestämmelse kan vara direkt tillämplig hos en myndighet antingen därför att det anges i bestämmelsens ordalydelse att sekretessen i fråga gäller hos den aktuella myndigheten eller därför att bestämmelsen reglerar sekretessen för en viss verksamhetstyp eller en viss ärendetyp som hanteras hos myndigheten eller därför att bestämmelsen reglerar sekretessen för vissa uppgifter som råkar finnas hos myndigheten. Vid överföring av sekretess ska en sekretessbestämmelse, som utgör en primär sekretessbestämmelse hos en utlämnande myndighet och som enligt sin ordalydelse inte är direkt tillämplig hos den mottagande myndigheten, ändå tillämpas hos den sistnämnda myndigheten. En sekretessbestämmelse som på grund av en bestämmelse om överföring av sekretess ska tillämpas hos en mottagande myndighet kallas sekundär sekretessbestämmelse när den tillämpas hos den mottagande myndigheten. Den mottagande myndigheten kan bara tillämpa en sekundär sekretessbestämmelse på uppgifter som den får från den överlämnande myndigheten.

Konsekvenser av att en uppgift lämnas över till en annan myndighet

Om en sekretessreglerad uppgift lämnas från en myndighet till en annan gäller sekretess för uppgiften hos den mottagande myndigheten antingen om sekretess följer av en primär sekretessbestämmelse, som är tillämplig hos den myndigheten, eller om sekretess följer av en bestämmelse om överföring av sekretess. Om ingen av dessa förutsättningar är uppfyllda blir uppgiften offentlig hos den mottagande myndigheten. Motsvarande gäller om en myndighet har direktåtkomst till sekretessreglerade uppgifter hos en annan myndighet (7 kap. 2 § OSL). I det fallet gäller dock en generell bestämmelse om överföring av sekretess (11 kap. 4 § OSL).

Konkurrens mellan sekretessbestämmelser

Vid konkurrens mellan flera tillämpliga sekretessbestämmelser i ett enskilt fall är huvudregeln att den eller de bestämmelser enligt vilka uppgiften är sekretessbelagd har företräde framför bestämmelser enligt vilka uppgiften ska lämnas ut (7 kap. 3 § OSL). Det spelar härvidlag ingen roll om det är fråga om konkurrens mellan primära sekretessbestämmelser, mellan sekundära sekretessbestämmelser eller mellan primära och sekundära sekretessbestämmelser. I samtliga fall är huvudregeln att det är den eller de sekretessbestämmelser enligt vilken uppgiften är sekretessbelagd som har företräde (prop. 2008/09:150 s. 367).

Undantag från huvudregeln finns bl.a. i 11 kap. 8 § OSL. Där anges att de bestämmelser om överföring av sekretess som räknas upp i kapitlet inte ska tillämpas på en uppgift när det finns en annan primär sekretessbestämmelse än 21 kap. 1, 3, 5 och 7 §§ till skydd för samma intresse som är tillämplig på uppgiften hos den mottagande myndigheten. Detta gäller även om den primära sekretessbestämmelsen ger ett svagare skydd för uppgiften.

5.6.3 Sekretess till skydd för enskilda hos NCT-myndigheterna

I 21 kap. OSL finns generella regler om sekretess till skydd för uppgift om enskilds personliga förhållanden oavsett i vilket sammanhang uppgiften förekommer. Därutöver gäller olika regler för sekretess, dels till skydd för enskild, dels till skydd för verksamheten inom respektive myndighets ansvarsområde och verksamhet. Nedan redogörs för de mest centrala sekretessreglerna till skydd för enskild som aktualiseras hos de myndigheter som samarbetar inom NCT.

Säkerhetspolisen

För Säkerhetspolisen är sekretessbestämmelsen till skydd för enskild i 35 kap. 1 § OSL tillämplig. Där regleras sekretessen för bl.a. Polismyndighetens och Säkerhetspolisens förundersöknings- och underrättelseverksamhet, register m.m. Bestämmelsen reglerar uppgifter som rör en enskilds personliga och ekonomiska förhållanden och som förekommer i verksamhet för att t.ex. förebygga brott. Sådana uppgifter omfattas av sekretess om det inte står klart att uppgiften kan röjas utan att den enskilde lider skada eller men.

Vidare kan uppgifter om enskilda hos Säkerhetspolisen omfattas av sekretess enligt 37 kap. 1 OSL. Enligt 37 kap. 1 § OSL gäller sekretess i verksamhet för kontroll över utlänningar och i ärenden om svenskt medborgarskap för uppgift om en enskilds personliga förhållanden. Bestämmelsen har ett omvänt skaderekvisit.

Därutöver är bestämmelsen i 21 kap. 5 § OSL tillämplig hos Säkerhetspolisen. Bestämmelsen reglerar sekretess till skydd för utlännings säkerhet i vissa fall. 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 utlänningar. Bestämmelsen har ett rakt skaderekvisit och är tillämplig oavsett i vilket sammanhang uppgifterna förekommer. Bestämmelsen gäller således i hela den offentliga förvaltningen.

Försvarsmakten och FRA

Hos Försvarsmakten och FRA regleras sekretessen till skydd för enskild i 38 kap. 4 § OSL. Där anges att sekretess gäller hos Försvarsmakten i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten samt hos FRA i underrättelse- och säkerhetsverksamheten för uppgift om en enskilds personliga eller ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till denne lider skada eller men. Som framgår innehåller paragrafen ett omvänt skaderekvisit, dvs. det råder presumtion för sekretess.

Därutöver är bestämmelsen i 21 kap. 5 § OSL om sekretess till skydd för utlännings säkerhet tillämplig även hos Försvarsmakten och FRA.

5.6.4 Sekretess till skydd för verksamheten och Sveriges intressen

När det gäller de tre NCT-myndigheterna aktualiseras också vissa generella sekretessbestämmelser till skydd för verksamheten. 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. Härutöver är också 18 kap. 2 § OSL tillämplig. Denna bestämmelse reglerar sekretess till skydd för intresset av att förebygga, förhindra eller upptäcka brott hänförligt till underrättelseverksamhet m.m.

15 kap. 1 och 2 §§ OSL – Utrikes- och försvarssekretess

I 15 kap. 1 och 2 §§ OSL regleras utrikes- och försvarssekretessen. Där finns regler om sekretess till skydd för Sveriges säkerhet och Sveriges förhållande till andra stater eller mellanfolkliga organisationer.

Enligt 15 kap. 1 § OSL gäller sekretess för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet

om uppgiften röjs. Bestämmelsen är en primär sekretessbestämmelse, vars räckvidd inte har begränsats. Bestämmelsen är således tillämplig inom all offentlig verksamhet som omfattas av lagen.

Av 15 kap. 2 § OSL framgår att sekretess gäller för uppgift som rör verksamhet för att försvara landet eller planläggning eller annan förberedelse av sådan verksamhet eller som i övrigt rör totalförsvaret, om det kan antas att det skadar landets försvar eller på annat sätt vållar fara för rikets säkerhet om uppgiften röjs. Det sekretessreglerade området omfattar inte bara rent militära företeelser utan också åtgärder med avseende på totalförsvaret i övrigt. Även denna bestämmelse är en primär sekretessbestämmelse, vars räckvidd inte har begränsats. Bestämmelsen kan således tillämpas av alla myndigheter och andra organ som ska tillämpa OSL, men den har förstås sin största betydelse hos Försvarsmakten och andra myndigheter som handhar militär verksamhet, t.ex. Försvarets materielverk och FRA (Lenberg m.fl., kommentaren till 15 kap. 2 §).

Båda bestämmelserna innehåller, som framgår ovan, raka skaderekvisit och presumtionen är således offentlighet. Bestämmelserna är tillämpliga på uppgifter som rör en viss verksamhet och gäller generellt i hela statsförvaltningen där det behandlas sådana uppgifter. Detta innebär att bestämmelserna är primära hos de tre NCT-myndigheterna.

18 kap. 2 § OSL – Underrättelseverksamhet m.m.

Bestämmelsen i 18 kap. 2 § OSL föreskriver att sekretess till skydd för det allmännas arbete med att förebygga, förhindra eller upptäcka brottslig verksamhet gäller för uppgift som hänför sig till underrättelseverksamhet. Sekretessen gäller med ett omvänt skaderekvisit vilket innebär att uppgifterna i regel omfattas av sekretess om det inte står klart att uppgifterna kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Underrättelseverksamhet innebär i detta sammanhang verksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning. Sekretessen gäller bl.a. i Polismyndighetens, Säkerhetspolisens och Ekobrottsmyndighetens verksamhet.

Sekretess enligt 18 kap. 2 § OSL kan emellertid också gälla hos myndigheter som inte bedriver brottsbekämpande verksamhet. Sekretessen gäller nämligen för uppgift som hänför sig till förundersökning eller underrättelseverksamhet hos de i bestämmelserna angivna myndigheterna. Detta innebär att sekretessen följer med uppgiften när den lämnas vidare till en annan myndighet. Uppgifter som skyddas av sekretess på grund av att de hänför sig till underrättelseverksamhet hos en brottsbekämpande myndighet skyddas av samma sekretess, oavsett om de lämnats till en annan brottsbekämpande myndighet eller till en icke brottsbekämpande myndighet (prop. 2015/16:167 s. 38).

Bestämmelsen är en primär sekretessbestämmelse hos de myndigheter som tillämpar den.

5.6.5 Sekretessbrytande bestämmelser

För att tillgodose myndigheternas informationsbehov finns i OSL flera undantag från sekretessen mellan myndigheter. Sekretessbrytande bestämmelser finns även i andra författningar som OSL hänvisar till eller som en uppgiftsskyldighet varvid 10 kap. 28 § OSL blir tillämplig. Nedan anges de huvudsakliga sekretessbrytande bestämmelser i OSL som aktualiseras vid sådan myndighetssamverkan som NCT utgör.

10 kap. 27 § OSL – Generalklausulen

Den bestämmelse som framför allt tillämpas vid uppgiftsutbytet inom ramen för NCT är den s.k. 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.

Generalklausulen var en del av sekretesslagen (1980:100) redan när lagen tillkom och innebar en kodifiering av vad som redan gällde i praktiken (prop. 1979/80:2 Del A s. 91 och 326 f.). I förarbetena framfördes att sekretesslagstiftningen inte bör hindra myndigheterna från att utväxla uppgifter i situationer där intresset

av att uppgifterna lämnas ut bör ha företräde framför det intresse som sekretessen ska skydda.

Vissa sekretessbestämmelser har ansetts särskilt angelägna att upprätthålla gentemot andra myndigheter, t.ex. hälso- och sjukvårdssekretess och socialtjänstsekretess. Dessa områden är undantagna från generalklausulens tillämpningsområde. En förutsättning för att generalklausulen ska vara tillämplig är vidare att utlämnandet inte strider mot en sådan specialreglering av uppgiftslämnandet i fråga som finns i lag eller förordning. Har det t.ex. i lag föreskrivits att en viss myndighet för sin verksamhet på angivna villkor kan få ta del av även hemliga uppgifter hos en annan myndighet, kommer det givetvis inte i fråga att, när de angivna villkoren inte är uppfyllda, lämna ut uppgifterna med stöd av generalklausulen i stället. Anges i en lag eller förordning uttömmande i vilka fall uppgifter får lämnas mellan myndigheter eller verksamhetsgrenar inom en myndighet kan generalklausulen inte heller tillämpas (Lenberg m.fl., kommentaren till 10 kap. 27 §).

När det gäller den intresseavvägning som ska göras enligt klausulen har det ansetts att möjligheterna att utväxla uppgifter mellan myndigheter får utnyttjas mer sparsamt och med större försiktighet om informationen inte är sekretesskyddad hos den mottagande myndigheten. Detta gäller särskilt i fråga om uppgifter som är hemliga med hänsyn till enskilds intressen. Om en uppgift inte skyddas av sekretess hos den mottagande myndigheten kan vid en intresseavvägning enligt generalklausulen, risken för att skada ska uppkomma vara så stor att uppgiften inte bör lämnas ut. Uppgifter som en enskild person har lämnat i förtroende kan det finnas särskild anledning att inte lämna ut. Däremot har det i förarbetena ansetts att det förhållandet att sekretessen hos den mottagande myndigheten är något svagare än hos den utlämnande myndigheten, inte spelar så stor roll i praktiken (prop. 1979/80:2 Del A s. 76 f. och s. 91).

Generalklausulen hindrar inte att utbyte av uppgifter mellan myndigheter eller mellan verksamhetsgrenar inom en myndighet sker rutinmässigt även utan en särskild författningsreglering. Det framgår dock av förarbetena att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. I de undantagsfall när rutinmässigt uppgiftslämnande inte är författningsreglerat men likväl kan anses tillräckligt motiverat måste den intresseavvägning, som ska göras

enligt generalklausulen, ske på förhand. I den situationen behöver det således inte ske en prövning av individuella fall (nämnda prop. s. 327). Bedömningen kan enligt uttalanden i förarbetena i dessa fall göras på ett sätt som liknar det som ska ske i fråga om massuttag. I situationer med massuttag kan den tjänsteman som ska lämna ut handlingarna av naturliga skäl inte bilda sig en uppfattning om den särskilda skaderisk som kan vara förbunden med en enskild uppgift. Å andra sidan har tjänstemannen alltid kännedom om beställarens identitet och oftast också om dennes avsikt med uppgifterna. Dessa kunskaper i förening med en bedömning av den skaderisk som typiskt sett är förbunden med uppgifter av det slag som avses med beställningen bör enligt förarbetsuttalanden i de allra flesta fall ge fullt tillräckligt underlag för bedömningen av om sekretessregleringen ska anses hindra ett utlämnande eller inte (nämnda prop. s. 81). Man ska vid prövningen av en utlämnandefråga enligt generalklausulen väga den mottagande myndighetens behov av uppgifterna mot det intresse som sekretesskyddet typiskt sett tillgodoser (nämnda prop. s. 327).

Generalklausulen är subsidiär i förhållande till andra sekretessbrytande bestämmelser och ska alltså inte tillämpas i ett fall där någon annan sekretessbrytande bestämmelse kan tillämpas.

10 kap. 28 § OSL

Enligt 10 kap. 28 § OSL hindrar sekretess inte att en uppgift lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning. Paragrafen är tillämplig när det gäller att lämna uppgifter såväl mellan två myndigheter som mellan två olika verksamhetsgrenar inom en och samma myndighet när de är att anse som självständiga i förhållande till varandra (jfr 8 kap. 2 § OSL). En verksamhetsgren inom en myndighet kan vara skyldig att lämna uppgifter till en annan.

Enligt paragrafen får uppgifter lämnas utan hinder av sekretess när det följer av annan lag än OSL eller av förordning att uppgiften ska lämnas till en annan myndighet eller verksamhetsgren. Det är alltså fråga om en generell regel om att en bestämmelse i en lag eller förordning om uppgiftsskyldighet ska tillämpas också när det gäller sekretess för de uppgifter som omfattas av skyldigheten (se dock

27 kap. 5 §, 30 kap. 7 och 11 §§, 35 kap. 3 §, 37 kap. 2 § och 30 kap. 24 § OSL).

Det är inte nödvändigt att bestämmelsen om uppgiftslämnande har utformats med tanke på att uppgifterna kan vara hemliga. Däremot krävs för att bestämmelsen ska beaktas att den uppfyller vissa krav på konkretion. Den kan a) ta sikte på utlämnande av uppgifter av ett speciellt slag, b) gälla en viss myndighets rätt att få del av uppgifter i allmänhet eller c) avse en skyldighet för en viss myndighet att lämna andra myndigheter information (Lenberg m.fl., kommentaren till 10 kap. 28 §).

6 kap. 5 § OSL

I detta sammanhang finns det skäl att även framhålla bestämmelsen om uppgiftsskyldighet i 6 kap. 5 § OSL. Som framgår ovan ska en myndighet, enligt denna bestämmelse, på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Bestämmelsen är inte en sekretessbrytande regel utan en föreskrift om informationsskyldighet mellan myndigheter. Den kan ses som en precisering av den allmänna samverkansskyldighet som gäller enligt 6 § förvaltningslagen (1986:223). Bestämmelsen är tillämplig på såväl statliga som kommunala myndigheter samt på sådana med myndigheter jämställda organ som avses i 2 kap. 2–5 §§ OSL.

Informationsskyldigheten enligt paragrafen är inte undantagslös. Bestämmelserna i OSL reglerar i princip också sekretessen mellan myndigheter och reservation har därför gjorts för vad som följer av en bestämmelse om sekretess eller arbetets behöriga gång.

Skyldigheten att lämna information till andra myndigheter är mera vidsträckt än skyldigheten gentemot allmänheten. Enligt denna paragraf omfattar skyldigheten varje uppgift som myndigheten förfogar över, alltså inte bara uppgifter ur allmänna handlingar. Anmärkas bör också att en ännu längre gående uppgiftsskyldighet gentemot andra myndigheter i vissa fall kan följa av särskilda föreskrifter i lag eller förordning (jfr 10 kap. 15 § och 28 § första stycket OSL).

Om en sekretessbrytande bestämmelse är tillämplig på en uppgift, så innebär denna bestämmelse att en myndighet är skyldig att

lämna uppgiften till den myndighet som begär det. Den sekretessbrytande bestämmelsen innebär att uppgiften i just den situationen inte är sekretessbelagd. Detta gäller även den s.k. generalklausulen i 10 kap. 27 § OSL (Lenberg m.fl., kommentaren till 6 kap. 5 §).

6 Myndigheternas personuppgiftsbehandling inom ramen för NCT-samarbetet

6.1 Inledning

En del av vårt uppdrag är att beskriva den verksamhet som bedrivs inom ramen för NCT-samarbetet och analysera de rättsliga förutsättningarna för Säkerhetspolisens, Försvarsmaktens och FRA:s personuppgiftsbehandling inom ramen för samarbetet. Syftet med denna analys är att klarlägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling som sker. För att kunna analysera de rättsliga förutsättningarna för personuppgiftsbehandlingen är det nödvändigt att först gå igenom och fastställa vad det är för sådan behandling som faktiskt sker inom ramen för samarbetet. I detta kapitel lämnas därför en redogörelse för det praktiska arbete som bedrivs inom NCT och den personuppgiftsbehandling som utförs i samband med detta. Redogörelsen bygger på uppgifter hämtade från interna arbetsdokument, från företrädare för NCT och de tre myndigheterna samt från våra egna iakttagelser vid besök hos NCT. Vi har även tagit del av underrättelserapporter producerade av NCT under 2015 och 2016 för att få en bild av arbetsmetodiken och hanteringen av uppgifter.

Vi har valt att beskriva verksamheten inom NCT dels med utgångspunkt i de olika system och mappar som analytikerna har tillgång till och arbetar i, dels utifrån NCT:s huvudsakliga arbetsuppgifter, dvs. författande av rapporter och utbyte av information. I avsnittet behandlas således den personuppgiftsbehandling som sker i myndigheternas egna system och i de myndighetsspecifika NCT-mapparna, den behandling som sker genom användande av e-post och personliga mappar samt den behandling som sker i den

gemensamma NCT-mappen som alla tre myndigheterna har tillgång till. Därutöver beskriver vi det informationsutbyte som sker mellan myndigheterna samt hur rapportskrivandet går till. I anslutning till varje beskrivning kommenterar vi den aktuella personuppgiftsbehandlingen något samt lyfter de eventuella frågor som har uppkommit.

6.2 Allmänna utgångspunkter

NCT är ett samarbete mellan tre myndigheter och utgör inte ett eget rättssubjekt. De tre NCT-myndigheterna deltar i samarbetet utifrån sitt respektive uppdrag och den verksamhet som bedrivs inom ramen för NCT-samarbetet grundas därmed på den rättsliga reglering som gäller för var och en av de samarbetande myndigheterna. Det betyder bl.a. att respektive myndighet gör en sekretessprövning innan uppgifter lämnas ut till övriga myndigheter och att respektive myndighet i princip är ansvarig för den egna behandlingen av personuppgifter. Regler om utlämnande av uppgifter från en myndighet till en annan finns dels i OSL, dels i de författningar som reglerar myndigheternas personuppgiftsbehandling. När det gäller Säkerhetspolisen är det PDL med tillhörande förordning som är tillämplig på myndighetens behandling av personuppgifter. För Försvarsmaktens/Musts och FRA:s del är det i stället FRA-PuL respektive PuL UNDSÄK med tillhörande förordningar som är tillämpliga. NCT är samlokaliserade i Säkerhetspolisens lokaler och all den personuppgiftsbehandling som förekommer inom NCT-samarbetet, förutom den behandling som analytikerna företar i myndigheternas egna system, utförs därför rent faktiskt på Säkerhetspolisens server.

Analytikerna vid NCT är, vid sin placering där, fortfarande anställda vid respektive myndighet och företräder också den myndigheten i arbetet vid NCT. Utgångspunkten i den fortsatta framställningen är således att den behandling av personuppgifter som respektive analytiker utför inom ramen för NCT-samarbetet, utför denne som företrädare för den egna myndigheten.

Vi har inte för avsikt att i denna framställning gå igenom och beskriva alla de uppgiftsamlingar och ärendehanteringssystem som tjänstemännen vid NCT har tillgång till i sina respektive myndig-

heters egna system. Detta eftersom vår uppgift inte är att se över myndigheternas behandling av personuppgifter i de egna systemen inom ramen för den egna myndighetens verksamhet, utan enbart den behandling som myndigheterna utför inom ramen för själva samarbetet.

6.3 Personuppgiftsbehandlingen inom ramen för NCT-samarbetet

6.3.1 Myndigheternas egna system

Beskrivning

Myndigheternas IT-system

En stor del av arbetet vid NCT handlar om att ta del av och analysera information. Informationen hämtas in av analytikerna vid NCT från deras respektive hemmamyndigheter. Analytikerna använder sina egna myndigheters IT-system och har inte tillgång till varandras system. Några gemensamma databaser finns inte. I myndigheternas egna system söker, läser, hämtar och sparar analytikerna olika sorters uppgifter från olika typer av källor. Från systemen skriver analytikerna också ut handlingar som sparas i pappersformat samt lämnar ut uppgifter muntligen.

Den information som analytikerna tar del av i sina egna myndigheters system innehåller en varierande mängd personuppgifter och det kan röra sig om både känsliga och icke känsliga personuppgifter. I försvarsunderrättelseverksamheten behandlas t.ex. uppgifter om personer som förekommer i underrättelserapporter eller kan komma att få ett underrättelsevärde (prop. 2006/07:46 s. 27). Hos Säkerhetspolisen kan det röra sig om uppgifter om personer mot vilka det föreligger misstankar om brottslig verksamhet eller uppgifter om personer som har samband med någon som har antecknats på grund av en misstanke (prop. 2009/10:85. s. 473).

Som nämnts ovan är analytikerna vid NCT anställda vid respektive hemmamyndighet. Vid sin placering på NCT har de i princip tillgång till samma information som de har på hemmamyndigheten beroende på vilken behörighet de har där. Det finns dock vissa användarbegränsningar kopplade till analytikernas placering vid

NCT. Detta innebär att tillgången till information har begränsats genom olika behörigheter och att analytikerna endast kommer åt sådan information från hemmamyndigheterna som anses vara relevant för det uppdrag de har vid NCT.

När det gäller FRA har de anställda generellt tillgång till uppgifter och system i den omfattning som varje anställd utifrån arbetsuppgifter har behov av. FRA:s medarbetare placerade vid NCT har i sin tur ännu mer begränsad tillgång till FRA:s system. FRA-tjänstemännen vid NCT har tillgång till tre olika typer av uppgiftssamlingar i FRA:s system; uppgiftssamlingar för analys, uppgiftssamlingar för underrättelser och uppgiftssamlingar för information om företeelser mot vilka signalspaning inriktas. Inom dessa uppgiftssamlingar har tjänstemännen endast tillgång till information som rör terrorism. FRA-tjänstemännen vid NCT har dock inte tillgång till all information som rör detta ämne, utan mängden uppgifter begränsas ytterligare genom olika kriterier. Begränsningen och tillgången för varje medarbetare beror på vilka arbetsuppgifter, och därmed vilket behov, den enskilde medarbetaren har inom NCT-samarbetet.

Must-tjänstemännen vid NCT kan enligt gällande behörigheter ta del av information med bäring på terrorism inkommen till Försvarsmakten/Must. Tjänstemännen har tillgång till sådan information som Försvarsmakten/Must bedömer är av nytta för NCT med hänsyn till verksamhetens ändamål och uppgift. NCT-tjänstemännen har således inte tillgång till all information som rör terrorområdet, utan enbart den information som Försvarsmakten/Must bedömer att de behöver. Behörigheten är tekniskt reglerad i Försvarsmaktens system. Inom dessa ramar delger Försvarsmakten/Must sina tjänstemän vid NCT utgående underrättelserapportering innehållande strategiska terrorbedömningar samt för kännedom vilka bedömningar som Must gör av inkommande hotvarningar. Informationen utgörs främst av rapporter. Must-tjänstemännen vid NCT använder sedan de delar av informationen som bedöms vara relevant för aktuell bearbetning vid NCT.

För Säkerhetspolisens del ser behörighetsstyrningen lite olika ut beroende på var informationen lagras. Ett ärende i Säkerhetspolisens ärende- och dokumenthanteringssystem kan innehålla underrättelseinformation från inkomna eller upprättade handlingar. För varje ärende finns en utpekad befattningshavare som är ärendeansvarig. Han eller hon tilldelar manuellt behörighet till ärendet till

andra medarbetare eller grupper av medarbetare. Enbart de som har behov av informationen för att kunna utföra sina arbetsuppgifter får behörighet. Inkomna handlingar med underrättelseinformation fördelas i ett första led av registrator till berörd mottagningsfunktion. Befattningshavarna vid mottagningsfunktionen har bland annat i uppgift att avgöra om den inkomna handlingen tillhör ett pågående ärende eller om ett nytt ärende ska skapas. Behörighetsstyrningen tillämpas på sådant sätt att Säkerhetspolisens tjänstemän vid NCT, liksom övriga medarbetare som arbetar med kontraterrorism, inte har tillgång till all inkommen och upprättad information som har bäring på terrorområdet.

Underrättelseinformation finns också tillgänglig i Säkerhetspolisens bearbetnings- och analysdatabaser. Myndighetens centrala bearbetnings- och analysdatabas innehåller två delar; en uppgiftssamling med uppgifter under bearbetning och en uppgiftssamling med bedömd information. En uppgiftssamling med uppgifter under bearbetning har inrättats för att till exempel underlätta identifieringen av en person eller för att bedöma om en uppgift har relevans för Säkerhetspolisens verksamhet. I den centrala bearbetnings- och analysdatabasen har NCT-tjänstemännen anställda hos Säkerhetspolisen generellt sett tillgång till uppgifter under bearbetning som rör kontraterrorism samt i princip all information rörande övriga verksamhetsområden, om informationen finns i uppgiftssamlingen med bedömd information. Behörigheten bestäms av systemägaren efter att ansvarig chef intygat medarbetarens behov av tillgång till uppgifterna för att kunna fullgöra sina arbetsuppgifter och att medarbetaren genomfört relevant utbildning. NCT-tjänstemännens åtkomst till underrättelseinformation som rör kontraterrorism i bearbetnings- och analysdatabasen sker automatiskt genom kontroll av användarens behörighet mot informationen som efterfrågas. Oavsett vilken underrättelseinformation det gäller så är det analytikerna anställda av Säkerhetspolisen vid NCT som sedan bedömer vilken av den information som de har getts behörighet till som är relevant för arbetet inom NCT.

Myndigheternas säkerhetsskåp

Varje myndighet har ett eget säkerhetsskåp i NCT:s lokaler som endast myndighetens personal har tillgång till. I dessa säkerhetsskåp förvaras pärmar med olika typer av dokument, exempelvis underrättelserapporter, som analytikerna har skrivit ut från den egna myndighetens IT-system. Enligt de interna arbetsrutinerna ska information som NCT-medarbetarna får kännedom om och som är relevant för bedömningen av hotet mot Sverige och svenska intressen skrivas ut ur respektive myndighets system och sättas in i dessa förevisningspärmar. Det finns inget datoriserat och sökbart index över de handlingar som förvaras i säkerhetsskåpen. Handlingarna är emellertid diarieförda i respektive myndighets diariehanteringssystem och genom loggfunktioner är det spårbart när och av vem handlingarna har skrivits ut. De handlingar som förvaras i säkerhetsskåpen lämnas inte ut till övriga myndigheter inom samarbetet utan informationen delges övriga medarbetare vid NCT genom att handlingarna visas för dem, s.k. förevisning. Enligt de interna arbetsrutinerna ansvarar respektive myndighet för att materialet i pärmarna gallras efter ett år.

Kommentarer

Som framgår ovan vidtar analytikerna vid NCT en mängd olika åtgärder i sina hemmamyndigheters IT-system. Analytikerna söker, sparar, bearbetar, skriver ut och lämnar ut uppgifter ur systemen. I princip utgör alla dessa åtgärder olika typer av automatiserade behandlingar av personuppgifter. Även åtgärden att skriva ut personuppgifter i pappersformat eller lämna ut dem muntligen är att bedöma som en delvis automatiserad personuppgiftsbehandling trots att åtgärden i sig inte kan anses ske automatiserat. Anledningen är att uppgifterna som skrivs ut eller lämnas ut finns i datorformat (se Öman/Lindblom, s. 122, se vidare avsnitt 6.3.5 om informationsutbyte). Vår utgångspunkt är att den personuppgiftsbehandling som myndigheterna inom ramen för samarbetet vidtar i de egna systemen är förenlig med respektive registerförfattning samt gällande rätt i övrigt. Vi återkommer till detta när vi redovisar våra överväganden gällande personuppgiftsbehandlingen i kapitel 7 nedan.

När det gäller förvaringen av olika typer av handlingar i myndigheternas säkerhetsskåp torde denna åtgärd emellertid vara att bedöma som en rent manuell behandling av de personuppgifter som finns där. Personuppgifterna förekommer i de flesta fall endast i löpande text och dokumenten är inte sorterade på så sätt att det är möjligt att söka på personuppgifterna. Det rör sig således inte om något manuellt register i personuppgiftslagens mening. Dokumenten är visserligen diarieförda i något av myndigheternas system, men det finns inte något datoriserat index knutet specifikt till handlingarna i skåpen. Det är således inte möjligt att på det sättet söka fram uppgifter om individer i dokumenten (jfr Öman/Lindblom, s. 12 f.). Eftersom det endast är myndighetens personal som har tillgång till myndighetens säkerhetsskåp sker det inte heller något utlämnande av uppgifter till övriga myndigheter när handlingar skrivs ut och sätts in i förevisningspärmarna i skåpen. Hanteringen av handlingar i myndigheternas säkerhetsskåp kommer därför inte att beröras närmare i detta arbete.

6.3.2 Myndigheternas NCT-mapp

Beskrivning

Säkerhetspolisen, Försvarsmakten/Must och FRA har varsin logiskt avskild NCT-mapp på Säkerhetspolisens server som bara den egna myndighetens personal placerad vid NCT har tillgång till. I dessa mappar lagras bl.a. de slutliga versioner av de färdiga rapporterna som innehåller alla fotnoter om personuppgiftsbehandling, men endast fotnoter kopplade till respektive myndighets källor (se avsnitt 6.3.6 om författande av rapporter). Vilken typ av information eller dokument som i övrigt lagras i mapparna varierar från myndighet till myndighet och beror troligtvis också på de tjänstemän som är placerade vid NCT vid tillfället. Detta innebär också att det kan förekomma personuppgifter i varierande omfattning och av varierande art i dessa mappar.

Eftersom Försvarsmaktens/Musts och FRA:s NCT-mappar ligger på Säkerhetspolisens server och Säkerhetspolisen ansvarar för administration och teknisk support av dessa mappar kan Säkerhetspolisen rent tekniskt komma att behandla personuppgifter som Försvarsmakten/Must och FRA är ansvariga för. Säkerhetspolisen

har därför ingått personuppgiftsbiträdesöverenskommelser med Försvarsmakten/Must och FRA där det framgår att Säkerhetspolisen agerar som personuppgiftsbiträde åt myndigheterna när de utför denna behandling. I detta sammanhang kan nämnas att SIN i sin rapport har konstaterat att den behandling av personuppgifter som Säkerhetspolisen utför i form av ren it-administration i de mappar som endast FRA respektive Försvarsmakten/Must har tillgång får anses ske i rollen som personuppgiftsbiträde och att Säkerhetspolisen alltså inte har något personuppgiftsansvar för dessa uppgifter (se SIN dnr 324-2014, s. 10).

Kommentarer

När det gäller myndigheternas egna NCT-mappar är varje myndighet själv ansvarig för innehållet i sin mapp och, som framgår ovan, är det endast myndighetens egen personal vid NCT som har tillgång till mappen även om mappen rent tekniskt är placerad på Säkerhetspolisens server. Vi har därför utgått från att det är myndigheternas respektive registerförfattningar som är tillämpliga på den personuppgiftsbehandling som förekommer i dessa mappar och att behandlingen där utförs i enlighet med dessa bestämmelser. Vi återkommer till detta resonemang i kapitel 7.2.2 nedan.

6.3.3 Personliga mappar m.m.

Beskrivning

All personal placerad vid NCT har tillgång till en personlig mapp i Säkerhetspolisens interna system. Denna mapp ska endast användas för personlig administration. Ingen underrättelsebearbetning får således ske där. Vad som lagras i de personliga mapparna är i princip upp till varje medarbetare att bestämma och det är endast medarbetaren själv som har tillgång till den personliga mappen. Säkerhetspolisen står för support och datatekniskt underhåll.

Personalen placerad vid NCT har också tillgång till Säkerhetspolisens öppna nät för bl.a. användande av e-post, internet samt tillgång till Säkerhetspolisens OSI-portal (Open source intelligence). OSI-portalen är en slags hemsida med länkar till bl.a. nyheter och

öppna databaser. Medarbetarna vid NCT har också en e-postadress i Säkerhetspolisens slutna nät som endast används för intern kommunikation.

Kommentarer

När tjänstemännen vid NCT använder sina personliga mappar så agerar de, precis som vid allt annat arbete inom NCT, som företrädare för sin egen myndighet. Det är endast medarbetaren själv som har tillgång till den personliga mappen och varje myndighet är i regel ansvarig för den eventuella behandling av personuppgifter som medarbetaren utför där. Här kan dock för tydlighets skull nämnas att om personuppgiftsbehandlingen i den personliga mappen överhuvudtaget inte är relaterad till den anställning som medarbetaren har vid myndigheten torde den anställde själv vara personuppgiftsansvarig för den behandling som denne utför där (se Öman/Lindblom, s. 101). Samma sak gäller vid medarbetarnas användande av e-post.

Som framgår ovan ska de personliga mapparna endast användas för personlig administration. Detta användande kan inte anses ske inom ramen för Säkerhetspolisens brottsbekämpande verksamhet eller den försvarsunderrättelseverksamhet som FRA och Försvarsmakten bedriver. I den utsträckning det behandlas personuppgifter i de personliga mapparna blir därför PuL tillämplig på den behandlingen i stället för myndigheternas registerförfattningar. Vår bedömning i denna del framgår av kapitel 7.2.2 nedan.

6.3.4 Myndigheternas gemensamma NCT-mapp

Beskrivning

Utöver de olika mappar som beskrivits ovan finns det också en gemensam NCT-mapp som alla medarbetare vid NCT har tillgång till. Denna mapp har skapats för lagring av administrativa dokument, metoddokument och pågående rapportproduktion. Den gemensamma NCT-mappen är uppdelad i flera olika undermappar och all personal har tillgång till alla undermappar. Det finns således inga mappar i den gemensamma NCT-mappen som endast används av

en myndighet. I princip kan det förekomma personuppgifter i alla undermappar i den gemensamma mappen även om det förekommer fler i vissa undermappar än i andra. Eftersom alla medarbetare vid NCT har tillgång till den gemensamma mappen kan alla medarbetare i princip lägga in, bearbeta och radera uppgifter i mappen. Det är också så det är tänkt att fungera, dvs. alla medarbetare ska kunna arbeta i den gemensamma mappen oberoende av varandra.

I den gemensamma NCT-mappen lagras olika typer av dokument och uppgifter. Här finns exempelvis rent administrativa dokument. Det kan röra sig om interna arbetsrutiner och överenskommelser, olika metoddokument och mallar samt semesterlistor, löneuppgifter och budget. I dessa dokument förekommer det relativt få personuppgifter som dessutom främst utgörs av uppgifter om anställd personal. I mappen sparas även mötesprotokoll och minnesanteckningar från interna möten. I sådana dokument kan det enligt uppgift förekomma personuppgifter. Vem som lägger in uppgifterna i mappen varierar och beror exempelvis på vilka analytiker som har deltagit vid det aktuella mötet och vem som har fört protokollet eller skrivit anteckningarna. En del undermappar innehåller återkommande underlag och rapporter, t.ex. underlag och talepunkter till generaldirektören, samt presentationer och arbetsmaterial som används vid möten med Regeringskansliet eller någon annan myndighet eller utländsk partner. I den gemensamma NCT-mappen sparas också öppen och offentligt tillgänglig information som kan vara av intresse för NCT-samarbetet. Det kan handla om rapporter och artiklar från exempelvis Utrikespolitiska institutet eller något annat organ.

I den gemensamma NCT-mappen ligger också den gemensamma produktionsmapp där analytikerna vid NCT arbetar med att ta fram rapporter. Här lagras och bearbetas utkasten till rapporter samt information och arbetsmaterial som gemensamt används vid rapportskrivandet (se avsnitt 6.3.6 nedan för en närmare beskrivning av själva rapportskrivandet). Arbetsmaterialet kan bestå av olika typer av sammanställningar, bakgrundsdokument, listor samt uppgifter och utdrag hämtade ur olika underrättelserapporter. Det lagras inga kompletta underrättelserapporter eller liknande dokument i mappen utan endast uppgifter hämtade ur sådana dokument. Mängden och arten av personuppgifter som förekommer i rapport-

utkasten och i arbetsmaterialet varierar beroende på vilken typ av ärende det rör sig om. Det kan i vissa fall röra sig om känsliga personuppgifter. Enligt de interna arbetsrutinerna ska personuppgiftsbehandling loggas manuellt i både arbetsdokument och rapportutkast i mappen. Det ska således framgå vem som har lagt in eller ändrat en viss personuppgift i ett arbetsdokument eller i ett rapportutkast. Loggningen sker genom fotnoter där det anges datum samt behandlande handläggare (se vidare avsnitt 6.3.6 nedan).

Personuppgifterna i den gemensamma mappen gallras inte utifrån enhetliga kriterier, utan beroende på vilken typ av uppgift det rör sig om. Som huvudregel gallras uppgifterna dock när de inte längre behövs för arbetet inom NCT. Hur länge det kan finnas behov av att spara en uppgift varierar dock från fall till fall. Uppgifter som är aktuella i ett specifikt ärende kan exempelvis även bli aktuella i ett annat ärende längre fram. De uppgifter som lagras i den s.k. produktionsmappen och som i huvudsak förekommer i underlag och utkast till rapporter och annan produktion, gallras då en skriftlig rapport är färdigställd om underlagen och utkasten inte behövs i annan planerad produktion.

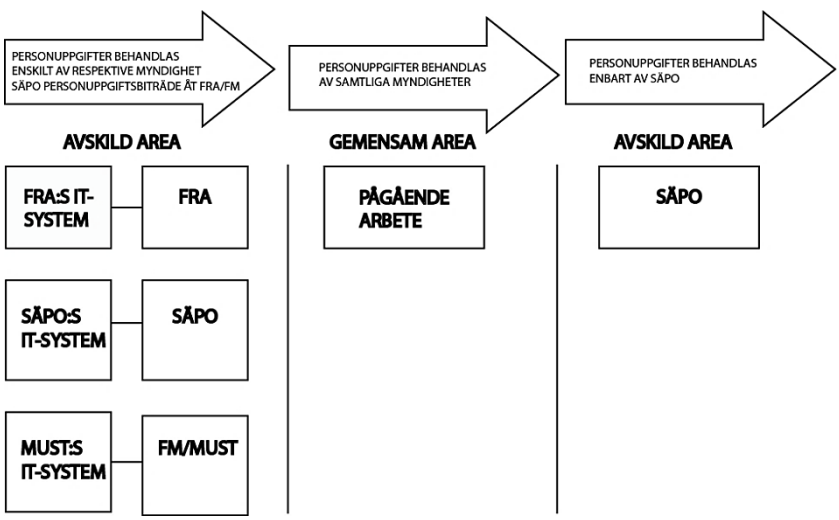
Kommentarer

Det som skiljer den gemensamma NCT-mappen från övriga mappar och system som myndigheterna använder, är att alla medarbetare vid NCT, oavsett vid vilken myndighet de är anställda, har tillgång till mappen och kan lägga in och bearbeta information där. De personuppgifter som förekommer i mappen behandlas således av alla tre NCT-myndigheterna när de har lagts in i mappen. Även om personuppgifterna är märkta med en analytikers signatur så har alla analytiker vid NCT tillgång till mappen och kan således rent teoretiskt ändra, radera eller på annat sätt bearbeta alla uppgifter som finns där. Det finns enligt vår bedömning skäl att närmare överväga vad detta innebär för personuppgiftsansvaret och myndigheternas ändamålsbestämmelser samt vilken registerförfattning som ska tillämpas. Ska myndigheterna exempelvis anses vara gemensamt personuppgiftsansvariga för alla personuppgifter i den gemensamma mappen och vad innebär det i så fall i praktiken? Är det i stället

möjligt att se det som ett delat personuppgiftsansvar där varje myndighet ansvarar för den behandling som myndigheten faktiskt utför?

Säkerhetspolisen, Försvarsmakten och FRA är vidare tre olika myndigheter med olika arbetsuppgifter och syften. Framför allt skiljer sig Säkerhetspolisens verksamhet och uppgift från den verksamhet som Försvarsmakten och FRA bedriver. Detta innebär i sin tur att myndigheternas personuppgiftsbehandling styrs av olika regelverk och därmed också olika ändamålsbestämmelser. När de tre myndigheterna arbetar tillsammans i den gemensamma NCT-mappen behandlar de inte bara uppgifter från sina egna system utan även uppgifter från varandra. Kan det till följd av detta finnas en risk att den behandling som myndigheterna utför i den gemensamma mappen faller utanför myndigheternas respektive ändamålsbestämmelser?

Det finns således en del frågor gällande NCT-myndigheternas användning av den gemensamma mappen som behöver analyseras närmare. Liknande frågor gör sig också gällande vid myndigheternas författande av rapporter som sker där. Vår avsikt är att återkomma till dessa frågeställningar i kapitel 7 där vi presenterar våra överväganden gällande personuppgiftsbehandlingen inom samarbetet.



Förenklad skiss över de mappar och system som används inom NCT.

6.3.5 Informationsutbyte

Beskrivning

Inom NCT-samarbetet utbyter myndigheterna kontinuerligt information med varandra. Detta sker genom att analytikerna vid NCT lämnar ut uppgifter till varandra på olika sätt. Inom samarbetet sker informationsutbytet främst muntligen eller på papper. Det är exempelvis vanligt att uppgifter lämnas ut genom att de visas för berörd person på en datorskärm eller i ett dokument, s.k. förevisning. Information utbyts också muntligen genom att myndigheterna gör källjämförelser. När det gäller uppgifter som lämnas ut muntligen eller genom förevisning ska utlämnandet vid särskilda händelser eller i känsliga ärenden redovisas i respektive myndighets system, t.ex. i form av tjänsteanteckningar eller ärendeloggar.

Inom NCT-samarbetet förekommer också ett visst elektroniskt informationsutbyte. Detta sker genom att uppgifter förs över från myndigheternas system eller de myndighetsspecifika NCT-mapparna till den gemensamma NCT-mappen. Eftersom alla medarbetare vid NCT har tillgång till den gemensamma NCT-mappen, där också rapportutkasten lagras och bearbetas, ses det som ett elektroniskt utlämnande när en handläggare lägger in uppgifter i ett rapportutkast eller i mappen i övrigt och på så sätt gör uppgifterna tillgängliga för handläggarna vid de två andra myndigheterna. SIN har vidare konstaterat att detta elektroniska utlämnande är att bedöma som ett utlämnande på medium för automatiserad behandling (SIN dnr 324-2014, s. 12). Någon annan typ av elektroniskt utlämnande förekommer enligt uppgift inte inom NCT-samarbetet.

Respektive myndighet ansvarar för att det görs en sekretessprövning av den information som lämnas ut till övriga myndigheter inom samarbetet. I praktiken är det tjänstemännen vid NCT som ska göra denna bedömning inför varje utlämnande.

Kommentarer

Som framgår ovan sker utlämnande av uppgifter inom samarbetet antingen elektroniskt, genom att uppgifter förs över från myndigheternas egna system eller mappar till den gemensamma NCT-

mappen, eller manuellt genom överlämnande på papper eller muntligen. Ett manuellt utlämnande på papper eller muntligen är i det här fallet att bedöma som en delvis automatiserad personuppgiftsbehandling eftersom uppgifterna som lämnas ut finns i datorformat (se Öman/Lindblom, s. 122). Oavsett om utlämnandet sker elektroniskt eller manuellt är det den utlämnande myndigheten som är ansvarig för den behandling som utlämnandet innebär och det är den utlämnande myndighetens registerförfattning som är tillämplig på behandlingen.

Ett utlämnande av personuppgifter innebär alltså att en behandling av personuppgifter utförs. Denna behandling styrs, precis som övriga behandlingar, av ändamålsbestämmelserna i myndigheternas registerförfattningar. Som framgår i avsnitt 6.3.1 har vår utgångspunkt varit att den personuppgiftsbehandling som myndigheterna inom ramen för samarbetet vidtar för egen räkning i sina egna system är förenlig med respektive registerförfattnings ändamålsbestämmelser. Frågan är dock om även den behandling som utlämnandet av uppgifter till övriga myndigheter inom samarbetet innebär, har stöd i myndigheternas ändamålsbestämmelser. Som framgår ovan är vidare det elektroniska utlämnande som sker genom att myndigheterna överför uppgifter till den gemensamma NCT-mappen att se som ett utlämnande på medium för automatiserad behandling (se SIN dnr 324-2014, s. 12). Sådant elektroniskt utlämnande regleras specifikt i myndigheternas registerförfattningar. Frågan om detta utlämnande är förenligt med bestämmelserna i registerförfattningarna kan därför behöva analyseras närmare. Vi behandlar dessa frågor i kapitel 7.2.3.

Utlämnande av information mellan myndigheter styrs också av reglerna i OSL. Som framgår ovan gör handläggarna vid NCT-myndigheterna en sekretessprövning inför varje utlämnande av uppgifter till övriga myndigheter inom samarbetet. Myndigheterna har uppgett att sekretessbelagda uppgifter lämnas ut med stöd av generalklausulen i 10 kap. 27 § OSL. Eftersom uppgifter endast lämnas ut manuellt eller elektroniskt på medium för automatiserad behandling finns det utrymme för myndigheterna att i varje enskilt fall göra en sekretessprövning. Vår uppfattning är att detta förfarande fungerar bra inom samarbetet. Myndigheterna har inte heller påtalat några svårigheter eller problem när det gäller att göra dessa bedömningar. Vi ser därför ingen anledning att beröra sekre-

tessregleringens betydelse för uppgiftsutbytet inom samarbetet närmare i detta sammanhang.

Myndigheterna har däremot lyft fram behovet av att effektivisera det informationsutbyte som sker inom samarbetet. Att utbyta information muntligen eller på papper, vilket är det tillvägagångssätt som i dag används inom samarbetet, är enligt myndigheterna ineffektivt och tidskrävande. De tre myndigheterna har därför framfört att det finns ett behov av att kunna medge övriga myndigheter inom samarbetet direktåtkomst till vissa avgränsade uppgifter hos den egna myndigheten. I vårt uppdrag ingår att analysera hur informationsutbytet inom samarbetet kan effektiviseras och vi återkommer därför till frågor om olika former för elektroniskt utlämnande samt sekretess när vi i kapitel 8 redovisar våra överväganden och förslag i den delen.

6.3.6 Författande av rapporter

Beskrivning

Författandet av rapporter sker som nämnts ovan i produktionsmappen i den gemensamma NCT-mappen. Inför författandet av en rapport skapas en undermapp i den gemensamma produktionsmappen där dokument som används gemensamt under produktionen samlas tillsammans med själva rapportutkastet.

Rapporterna skrivs tillsammans av en grupp analytiker. Det ska normalt sett finnas minst en analytiker från varje NCT-myndighet med i den grupp som skriver rapporten. En av analytikerna brukar som regel 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 rapportutkasten, men det förekommer också att en analytiker arbetar ensam i ett dokument. När en analytiker lägger in en personuppgift i ett utkast till en rapport ska analytikern märka uppgiften med en fotnot där han eller hon lägger in sin signatur samt aktuellt datum. Om någon ytterligare behandling av personuppgiften sedan sker, t.ex. att den ändras, ska även denna behandling loggas på samma sätt. Rapportutkasten innehåller också fotnoter med hänvisning till de källor som ligger till grund för bedömningen. Informationen i rapporterna ska nämligen i så stor ut-

sträckning som möjligt följas av referenser till ursprungsdokument. Det kan här röra sig om både offentliga källor och källor som av olika anledningar är hemliga eller känsliga. Alla analytiker som arbetar med en rapport har möjlighet att lägga till, ändra eller ta bort samtliga personuppgifter i rapportutkasten. Det brukar dock enligt uppgift vara den analytiker som är huvudredaktör för den aktuella rapporten som lägger in de flesta av personuppgifterna oavsett vilken NCT-myndighet uppgifterna ursprungligen kommer ifrån. De personuppgifter som förekommer i rapporterna brukar också röra personer som alla tre NCT-myndigheterna redan känner till och behandlar uppgifter om, t.ex. ledare för större internationella terrornätverk.

Analytikerna från FRA och Must deltar inte alltid fullt ut i rapportskrivandet. Detta beror på att FRA och Försvarsmakten, i enlighet med sina registerförfattningar, endast får behandla personuppgifter som rör utländska förhållanden och som har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten. Skulle en rapport eller en del av en rapport behandla företeelser som endast rör inhemska förhållanden, deltar således inte medarbetarna från FRA och Must i rapportskrivandet i den delen. Det är dock sällsynt att uppgifterna i rapporterna inte på något sätt har kopplingar till utländska förhållanden.

I rapportutkasten behandlas en varierande mängd personuppgifter i löpande text. En del rapporter innehåller inga personuppgifter alls medan andra kan innehålla ett flertal sådana uppgifter. Det kan förekomma känsliga personuppgifter i rapporterna, t.ex. namn på personer kopplade till en viss religiös inriktning. En del rapporter kan också innehålla indirekta personuppgifter, dvs. uppgifter som inte direkt kan hänföras till en viss person men som indirekt med hjälp av annan tillgänglig information kan kopplas till en individ. Eftersom NCT gör strategiska bedömningar innehåller rapporterna emellertid generellt relativt få personuppgifter.

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 personuppgifter och hemliga och känsliga källor tagits bort. De upprättade rapporterna sparas och diarieförs hos respektive hemmamyndighet. Enligt de interna arbetsrutinerna ska av NCT upprättade handlingar diarieföras hos

Säkerhetspolisen som upprättade och hos de övriga myndigheterna som inkomna.

Den slutliga versionen av rapporten som innehåller samtliga fotnoter, dvs. både hänvisningar till personuppgifter och till offentliga och hemliga källor, flyttas i samband med expediering över till Säkerhetspolisens NCT-mapp och raderas då från den gemensamma NCT-mappen. Detta exemplar av rapporten kallas masterexemplaret. Som framgår ovan är det bara NCT-personal anställd vid Säkerhetspolisen som har tillgång till Säkerhetspolisens NCT-mapp. Uppgifterna i masterexemplaret sparas hos Säkerhetspolisen i syfte att kunna garantera spårbarhet avseende underlaget till de bedömningar som NCT gör i sina rapporter.

Som framgår ovan i avsnitt 6.3.2. sparas också en slutlig version av rapporten i FRA:s och Försvarsmaktens/Must NCT-mapp. Denna version innehåller samtliga fotnoter om personuppgiftsbehandling, men endast de fotnoter som är hänförliga till respektive myndighets källor. Fotnoter som innehåller känslig information rörande exempelvis källor och individer får, enligt interna arbetsrutiner, endast delges den myndighet som äger informationen. I FRA:s NCT-mapp sparas således en version av rapporterna som innehåller samtliga fotnoter om personuppgiftsbehandling men endast hänvisningar till FRA-källor och i Försvarsmaktens/Musts NCT-mapp sparas en version som innehåller samtliga fotnoter om personuppgiftsbehandling men endast hänvisningar till Must-källor.

Kommentarer

Vid rapportskrivandet behandlas personuppgifter genom att dessa skrivs in i rapportutkasten och sedan bearbetas och lagras där under den tid som rapporten färdigställs. Det som utmärker det gemensamma rapportskrivandet är att medarbetare från tre olika myndigheter arbetar tillsammans i ett dokument och att dessa medarbetare var för sig kan lägga in, bearbeta och radera information i dokumentet. Den behandling av personuppgifter som förekommer vid rapportskrivandet utförs således, precis som i den gemensamma NCT-mappen i övrigt, av alla tre NCT-myndigheterna. SIN har också i sin rapport konstaterat att behandlingen av personuppgifter vid framtagandet av rapporter sker i ett mycket nära samarbete

mellan personal från samtliga tre myndigheter (SIN dnr 324-2014, s. 11).

Den behandling av personuppgifter som utförs av myndigheterna vid framtagandet av en rapport är emellertid tidsbegränsad, eftersom den enbart pågår under den tid som rapporten skrivs och sedan upphör när rapporten har färdigställts. När rapporten är färdigställd är alla uppgifter färdigbehandlade och får, enligt myndigheternas interna rutiner, varken ändras, blockeras eller utplånas, eftersom bevarandet av dem är nödvändigt för spårbarheten. Den färdigställda rapporten flyttas då från den gemensamma produktionsmappen och sparas sedan i olika versioner i myndigheternas egna NCT-mappar. Den behandling av personuppgifter som sker där, dvs. lagring av uppgifter, ansvarar respektive myndighet för och det är respektive myndighets regelverk som är tillämpligt på den behandlingen. Som framgår ovan sparas också den upprättade och expedierade versionen av rapporten, som i princip inte innehåller några fotnoter, hos varje myndighet.

Precis som när det gäller myndigheternas överföring av uppgifter till den gemensamma NCT-mappen i övrigt, innebär rapportskrivandet att uppgifter lämnas ut från respektive myndighet till de övriga myndigheterna inom NCT. När analytikerna för in personuppgifter i rapportutkasten innebär det nämligen att uppgifterna på elektronisk väg görs tillgängliga för de andra myndigheterna. Precis som vid utlämnande av uppgifter mellan myndigheterna i övrigt regleras detta elektroniska utlämnande av den utlämnande myndighetens registerlag (se avsnitt 6.3.5 om informationsutbytet mellan myndigheterna). Om en personuppgift som skrivs in i ett rapportutkast däremot hämtas från arbetsmaterialet som lagras i den aktuella rapportmappen, har denna uppgift redan lämnats ut och införandet av uppgiften i rapportutkastet torde inte innebära ett ytterligare utlämnande, utan i stället vara att se som en behandling som utförs i den gemensamma mappen.

Som framgår ovan använder myndigheterna ett fotnotssystem för att märka personuppgifterna i rapporterna. Detta för att på så sätt kunna härleda en viss personuppgift och en viss personuppgiftsbehandling till en viss myndighet. SIN har dock konstaterat att systemet med fotnoter inte är konsekvent genomfört i praktiken eftersom vissa personuppgifter helt saknat märkning och två myndigheter ibland pekats ut som ansvariga för samma person-

uppgift. Personal från alla tre myndigheterna har dessutom, oavsett märkningen, möjlighet att lägga till, ändra och ta bort samtliga personuppgifter i utkasten. Enligt SIN motsvaras därför inte den märkning av personuppgifter som sker i fotnoterna av någon faktisk begränsning i respektive myndighets möjlighet att bestämma ändamål och medel för behandlingen. Det går exempelvis inte av märkningen att utläsa vilken myndighet som är initiativtagare till en viss behandling eller vilken myndighet som har rätt att besluta om radering av en viss uppgift (SIN dnr 324-2014, s. 11). Efter att ha tagit del av sammanlagt 15 rapporter producerade av NCT under främst 2015 kan vi, i likhet med SIN, konstatera att fotnotssystemet inte är helt konsekvent genomfört i praktiken. Även vi noterade att det i flera rapporter exempelvis fanns personuppgifter som inte var märkta med någon fotnot. Eftersom systemet med fotnoter innebär att en manuell åtgärd rent faktiskt måste vidtas av en handläggare i varje enskilt fall är risken att en personuppgift av misstag inte markeras naturligtvis större än om märkningen i stället hade skett genom automatisk loggning i systemet. Att fotnotssystemet inte är helt konsekvent genomfört innebär att det inte i alla situationer går att utläsa vem som har lagt in eller på annat sätt behandlat en viss personuppgift i ett rapportutkast och vilken myndighet som således har tagit initiativ till behandlingen. Även om en personuppgift är märkt med en fotnot som pekar ut handläggare och myndighet, är det dessutom svårt att enbart av märkningen dra några säkra slutsatser om vilka behandlingar som har utförts och av vem. Frågan är vad detta får för betydelse för bedömningen av exempelvis personuppgiftsansvaret.

Precis som vid användandet av den gemensamma NCT-mappen, behandlar myndigheterna vid det gemensamma rapportskrivandet inte bara uppgifter från sina egna system utan även uppgifter från varandra. Som konstaterats i avsnitt 6.3.4 kan det därför finnas anledning att överväga hur detta förhåller sig till de ändamålsbestämmelser som myndigheten har att följa.

Frågor om personuppgiftsansvar och ändamål för personuppgiftsbehandlingen aktualiseras således även vid det gemensamma rapportskrivandet. Precis som när det gäller användandet av den gemensamma mappen i övrigt avser vi att återkomma till dessa frågeställningar i kapitel 7 nedan.

7 Överväganden gällande personuppgiftsbehandlingen inom NCT-samarbetet

7.1 Inledning

Vi har fått i uppdrag att beskriva den verksamhet som bedrivs inom ramen för NCT-samarbetet och analysera de rättsliga förutsättningarna för Säkerhetspolisens, Försvarsmaktens och FRA:s personuppgiftsbehandling inom samarbetet i syfte att klarlägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling som sker. I kapitel 4 har vi översiktligt beskrivit NCT-samarbetet och den verksamhet som myndigheterna bedriver där. Därefter har vi i det föregående kapitlet mer detaljerat redogjort för det praktiska arbete som bedrivs inom samarbetet och den personuppgiftsbehandling som handläggarna vid NCT utför i samband med detta. Syftet har varit att tydliggöra vilken personuppgiftsbehandling som faktiskt utförs och mot bakgrund av detta överväga om det är något som är oklart ur rättslig synvinkel. Som framgår ovan har vi gått igenom de system och de olika situationer där personuppgifter behandlas inom samarbetet och i samband med detta analyserat hur personuppgiftsbehandlingen förhåller sig till den rättsliga regleringen.

I detta sammanhang bör återigen nämnas att NCT är ett samarbete mellan tre myndigheter och alltså inte utgör ett eget rättssubjekt. Samarbetet är frivilligt mellan de tre berörda myndigheterna och inte beslutat av regeringen. De tre NCT-myndigheterna deltar i samarbetet utifrån sitt respektive uppdrag och den verksamhet som bedrivs vid NCT grundas därmed på den rättsliga reglering som gäller för var och en av de samarbetande myndigheterna.

Som framgår ovan ingår det i vårt uppdrag att klarlägga om det finns behov av ett tydligare lagstöd för personuppgiftsbehandlingen inom samarbetet. Vi har därför i vår analys fokuserat på myndigheternas behandling av personuppgifter och de regler som styr detta. Även andra regelverk och därtill hörande frågeställningar aktualiseras dock vid samarbetet inom NCT. Här kan exempelvis nämnas reglerna i TF och OSL. När Säkerhetspolisen, FRA och Försvarsmakten samarbetar inom ramen för NCT måste de självfallet förhålla sig till regleringen även i dessa författningar. Det innebär bl.a. att myndigheterna har fått överväga hur eventuella allmänna handlingar och begäran att få ta del av sådana handlingar ska hanteras inom samarbetet samt vad sekretessregleringen innebär för möjligheter till informationsutbyte. I den överenskommelse som tecknats mellan myndigheterna finns därför rutiner för hur allmänna handlingar ska diarieföras inom samarbetet. Myndigheterna har uppgett att det även finns rutiner för hur en begäran om att få ta del av allmänna handlingar hanteras. Vi har inte kunnat se annat än att myndigheterna i den här delen uppfyller de krav som ställs på dem och kommer därför inte att ytterligare beröra förhållandet till TF. Vi kommer dock att behandla frågan om gallring av personuppgifter varvid dessa frågor till viss del berörs. Vi återkommer till sekretessregleringen när vi i nästa kapitel redovisar våra överväganden och förslag gällande uppgiftsutbytet inom samarbetet.

Vid den genomgång av personuppgiftsbehandlingen inom NCT-samarbetet som vi har gjort har vi identifierat några områden där vi ser att det finns behov av vissa förtydliganden och andra områden där vi gör bedömningen att befintlig reglering är tillräcklig och att tillämpningen fungerar väl utan sådana förtydliganden. Det område där vi gör bedömningen att det finns behov av förtydliganden är behandlingen av personuppgifter i den gemensamma NCT-mappen. Som framgår av genomgången i föregående kapitel är det framför allt frågan om personuppgiftsansvarets fördelning som behöver analyseras närmare. Även frågan om hur myndigheternas ändamålsbestämmelser förhåller sig till den behandling av personuppgifter som förekommer i den gemensamma mappen behöver belysas. Däremot har vi inte sett att den behandling av personuppgifter som myndigheterna inom ramen för samarbetet utför i sina egna system och mappar medför några oklarheter eller ger

upphov till frågor. Vi har dock ansett att det finns ett behov av att analysera huruvida utlämnandet av uppgifter från myndigheternas egna system till övriga myndigheter inom samarbetet har stöd i de befintliga registerförfattningarna.

I detta kapitel redovisar vi vår bedömning när det gäller personuppgiftsbehandlingen inom NCT och de överväganden och slutsatser som ligger bakom dessa. Framställningen har fokuserats på den behandling av personuppgifter som sker i den gemensamma mappen. Vi har valt att redovisa våra ställningstaganden i den delen i tre avsnitt. Först behandlas frågan om personuppgiftsansvaret i den gemensamma mappen. Därefter redogör vi något för tillämpningen av övriga dataskyddsbestämmelser vid behandling av personuppgifter i den gemensamma mappen. Slutligen behandlas frågan om ändamålen för personuppgiftsbehandlingen i den gemensamma mappen. Kapitlet inleds dock med våra överväganden gällande den behandling av personuppgifter som myndigheterna utför sina egna system och mappar.

7.2 Behandlingen av personuppgifter i myndigheternas egna system och mappar

7.2.1 Myndigheternas egna system

Som framgår av genomgången i kapitel 6 behandlar NCT-myndigheterna personuppgifter i sina egna system och uppgiftssamlingar samt i specifika mappar avsedda för NCT-samarbetet. Inledningsvis kan konstateras att de behandlingar som myndigheterna utför i sina egna system styrs av respektive myndighets registerförfattning. Varje myndighet är i enlighet med tillämplig registerförfattning ansvarig för de behandlingar som utförs i systemen och handläggarna har att hålla sig till de ändamålsbestämmelser och övriga regler som anges i respektive registerförfattning. Det arbete som bedrivs inom NCT faller inom ramen för de tre myndigheternas respektive verksamhet och uppdrag. Samarbetet ligger inom ramen för Säkerhetspolisens uppdrag att bekämpa terrorism. Det ligger också inom Försvarsmaktens och FRA:s respektive uppdrag att bedriva försvarsunderrättelseverksamhet. Vår utgångspunkt har därför varit att den personuppgiftsbehandling som myndigheterna vidtar i de egna systemen är förenlig med respektive registerförfatt-

nings ändamålsbestämmelser och sker i enlighet med tillämpliga regler i övrigt. Som framgår av vår genomgång av personuppgiftsbehandlingen i föregående kapitel har vi under utredningens gång inte stött på något som gett oss anledning att utgå från något annat. Som vi tidigare redogjort för är exempelvis tillgången till information i myndigheternas system tekniskt reglerad genom olika typer av behörigheter. På så sätt kan myndigheterna begränsa tillgången till personuppgifter för analytikerna vid NCT, så att de endast får åtkomst till sådan information som de behöver för att kunna fullgöra sina arbetsuppgifter inom NCT-samarbetet. Sådana tekniska åtgärder är ett exempel på hur man kan säkerställa att den personuppgiftsbehandling som utförs vid myndigheten sker i enlighet med gällande rätt. Vi har således inte uppfattat att myndigheternas verksamhet inom NCT-samarbetet medför något problem eller några oklarheter när det gäller behandlingen av personuppgifter i de egna systemen (se dock nedan angående utlämnande av personuppgifter) och vi avser därför inte att i det här kapitlet gå närmare in på den personuppgiftsbehandling som sker där.

7.2.2 De myndighetsspecifika NCT-mapparna samt handläggarnas personliga mappar

Som tidigare redogjorts för har myndigheterna tilldelats myndighetsspecifika NCT-mappar på Säkerhetspolisens server. Det är endast handläggarna från den berörda myndigheten som har tillgång till och som använder myndighetens NCT-mapp. Överförandet av uppgifter till den egna NCT-mappen innebär därför inte något utlämnande av uppgifter till övriga myndigheter inom samarbetet. På samma sätt har varje medarbetare vid NCT en personlig mapp på Säkerhetspolisens server, vilken endast medarbetaren själv har tillgång till. Den personuppgiftsbehandling som handläggarna vidtar i dessa mappar utför de, precis som vid all annan personuppgiftsbehandling inom samarbetet, som företrädare för den egna myndigheten. Precis som när det gäller myndigheternas egna system styrs behandlingen av personuppgifter i de myndighetsspecifika mapparna av reglerna i respektive registerförfattning. Varje myndighet är således i enlighet med tillämplig registerförfattning ansvarig för de behandlingar som utförs i mapparna och handläggarna har även här att hålla sig till de ändamålsbestämmelser och övriga regler

som anges i respektive registerförfattning. De personliga mapparna ska däremot endast användas för personlig administration. Detta användande kan inte anses ske inom ramen för Säkerhetspolisens brottsbekämpande verksamhet eller den försvarsunderrättelseverksamhet som FRA och Försvarsmakten bedriver. I den utsträckning det behandlas personuppgifter i de personliga mapparna blir således PuL tillämplig på den behandlingen i stället för myndigheternas registerförfattningar. Varje myndighet är ansvarig för den personuppgiftsbehandling som medarbetaren utför i den personliga mappen, så länge medarbetaren utför behandlingen i sin roll som anställd.

Till skillnad mot myndigheternas egna system, ligger de myndighetsspecifika och personliga mapparna på Säkerhetspolisens server och behandlingen av personuppgifter i dessa mappar sker således rent faktiskt i Säkerhetspolisens system. Eftersom Säkerhetspolisen, genom att ombesörja administration och teknisk support av dessa mappar kan komma att behandla personuppgifter som finns i mapparna, har myndigheten tecknat personuppgiftsbiträdesavtal med Försvarsmakten och FRA. I dessa fall agerar Säkerhetspolisen i enlighet med avtalen som personuppgiftsbiträde åt Försvarsmakten respektive FRA. Av avtalen framgår bl.a. att Säkerhetspolisen åtar sig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas samt att se till att personuppgifter under vissa förutsättningar inte kommer annan till del. Personuppgiftsbiträdesavtalen har några år på nacken och myndigheterna har uppgett att avtalen inom kort ska ses över. Vi utgår från att eventuella oklarheter som kan finnas i avtalen rättas till inom ramen för det arbetet. Mot denna bakgrund gör vi bedömningen att personuppgiftsbehandlingen i myndigheternas myndighetsspecifika NCT-mappar samt i handläggarnas personliga mappar fungerar väl inom samarbetet och att några åtgärder med anledning av detta inte behöver vidtas. Vi går därför inte närmare in på denna personuppgiftsbehandling i de följande avsnitten.

7.2.3 Myndigheternas utlämnande av personuppgifter inom samarbetet

Bedömning: Det utlämnande av personuppgifter som sker mellan myndigheterna inom ramen för samarbetet har stöd i respektive myndighets registerförfattning. Det behöver inte införas något förtydligande författningsstöd med anledning av den behandlingen.

Skälen för bedömningen

Ändamålsbestämmelsernas betydelse för utlämnandet av uppgifter

Bestämmelser om för vilka ändamål uppgifter får behandlas har en viktig roll i de s.k. registerförfattningarna. Genom ändamålen sätts ramen för vilken behandling som är tillåten. I registerförfattningar delar man ofta upp ändamålen i primära och sekundära sådana. De primära ändamålen tillgodoser den behandling som behövs i den berörda myndighetens egen verksamhet, medan de sekundära ändamålen tillgodoser den behandling som behövs för att den berörda myndigheten ska kunna lämna information till andra som behöver informationen i sin verksamhet. De primära och sekundära ändamålen kompletteras som regel av en möjlighet att behandla uppgifter även för ändamål som inte är oförenliga med insamlingsändamålet, den s.k. finalitetsprincipen. Detta kommer ofta till uttryck genom en särskild bestämmelse eller genom en hänvisning till personuppgiftslagens bestämmelser, men det förekommer även att det endast går att utläsa i förarbetsuttalanden och utifrån praxis att så är fallet. I doktrinen har det hävdats att relationen mellan de primära och sekundära ändamålen får förstås så att behandlingen för att lämna ut personuppgifter till annan enligt de sekundära ändamålen bara får avse personuppgifter som myndigheten samlat in och i övrigt behandlat för sina egna primära ändamål (Öman, Festskrift till Peter Seipel, 2006, s. 699 f.). I vissa registerförfattningar görs inte någon uppdelning mellan primära och sekundära ändamål. Som utgångspunkt gäller dock samma principer för behandlingen av personuppgifter, dvs. att de angivna ändamålen kompletteras av en möjlighet att behandla uppgifter för ändamål som inte är oförenliga med insamlingsändamålet.

När det gäller myndigheters utlämnande av personuppgifter har finalitetsprincipen varit föremål för diskussion eftersom det inte sällan uppstått osäkerhet kring frågan om förhållandet mellan denna princip, ändamålsbestämmelser i registerförfattningar och bestämmelser i bl.a. OSL. Enligt 6 kap. 5 § OSL ska en myndighet på begäran av en annan myndighet lämna uppgift som den förfogar över, om inte uppgiften är sekretessbelagd eller det skulle hindra arbetets behöriga gång. Bestämmelsen omfattar såväl uppgifter som inte är sekretessreglerade, som uppgifter som kan lämnas ut med tillämpning av en sekretessbrytande bestämmelse. Det har ifrågasatts om denna skyldighet står i strid med finalitetsprincipen och det nu gällande dataskyddsdirektivet.

Offentlighets- och sekretesskommittén (OSEK) behandlade frågan i sitt huvudbetänkande Ny sekretesslag (SOU 2003:99) och uttalade att regering och riksdag redan vid personuppgiftslagens tillkomst fick anses ha tagit ställning för att bestämmelsen i dåvarande 15 kap. 5 § sekretesslagen (nuvarande 6 kap. 5 § OSL) inte strider mot dataskyddsdirektivet. Enligt kommittén ska således ett utlämnande av uppgifter till en annan myndighet anses vara förenligt med finalitetsprincipen om utlämnandet är tillåtet enligt sekretesslagen (SOU 2003:99 s. 231 och prop. 1997/98:44 s. 116). OSEK anförde vidare att finalitetsprincipen har utformats i en politisk miljö där majoriteten av medlemsstaterna inte har någon offentlighetsprincip och därmed inte heller någon sekretessreglering. Kommittén ansåg att den svenska sekretessregleringen, vilken även gäller mellan myndigheter, fyller samma syfte som finalitetsprincipen eftersom den hindrar myndigheter från att lämna ut integritetskänsliga uppgifter till andra myndigheter för ändamål som av lagstiftaren bedömts vara oförenliga med de ändamål för vilka uppgifterna samlats in (SOU 2003:99 s. 232).

Utlämnandet av uppgifter inom samarbetet

Från myndigheternas egna system och myndighetsspecifika mappar lämnar handläggarna ut uppgifter muntligen, på papper eller elektroniskt genom överföring till den gemensamma NCT-mappen. Som vi har konstaterat i kapitel 6 är myndigheternas elektroniska utlämnande genom överföring av uppgifter till den gemensamma

NCT-mappen att se som ett utlämnande på medium för automatiserad behandling. I myndigheternas registerförfattningar anges förutsättningarna för när personuppgifter får lämnas ut på detta sätt. Säkerhetspolisen får således enlig 6 kap. 4 § och 2 kap. 20 § PDL endast lämna ut enstaka uppgifter på medium för automatiserad behandling, medan FRA och Försvarsmakten, enligt 8 § FRA-PuF respektive 7 § PuF UNDSÄK, får lämna ut fler än enstaka personuppgifter på detta sätt om det sker till en annan statlig myndighet. Som vi har redogjort för i kapitel 6 har SIN konstaterat att det utlämnande av personuppgifter som Säkerhetspolisen företar vid författandet av rapporterna inte kan anses avse mer än vad som i lagens mening kan anses utgöra enstaka uppgifter och att utlämnandet därmed är förenligt med PDL (se SIN dnr 324-2014, s. 13). Mot bakgrund av detta, och då begränsningen till enstaka uppgifter inte gäller för FRA och Försvarsmakten, har vi gjort bedömningen att även FRA:s och Försvarsmaktens utlämnande av uppgifter i motsvarande situation är förenligt med respektive registerförfattning. Vi anser därmed att det inte finns behov av några förtydliganden vad gäller dessa bestämmelser. Som framgår av kapitel 8 nedan anser vi dock att en ändring bör göras i polisdataförordningen (2010:1155) för att möjliggöra för Säkerhetspolisen att lämna ut fler än enstaka personuppgifter på medium för automatiserad behandling till FRA och Försvarsmakten inom ramen för NCT-samarbetet. Detta förslag föranleds dock av de åtgärder vi föreslår för ett effektivare informationsutbyte och grundar sig således inte på att det inte skulle finnas rättsligt stöd för det utlämnandet av personuppgifter som sker i dag (se kapitel 8.5 nedan).

För att myndigheter ska kunna utbyta information som innefattar personuppgifter krävs det också att ändamålsbestämmelserna i myndigheternas registerförfattningar ger stöd för detta. Ett utlämnande av personuppgifter innebär nämligen en behandling av personuppgifter och styrs, precis som övriga behandlingar, av myndigheternas ändamålsbestämmelser.

Inom NCT lämnar Säkerhetspolisen ut personuppgifter till FRA och Försvarsmakten med stöd av bestämmelsen i 6 kap. 2 § 2 PDL. Där anges att personuppgifter som behandlas i Säkerhetspolisens brottsbekämpande verksamhet får behandlas även när det är nödvändigt för att tillhandahålla information som behövs i en

myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott. Av förarbetena framgår att bestämmelsen i första hand ska tillgodose behovet av informationsutbyte med andra myndigheter än de brottsbekämpande och Samverkansrådet mot terrorism nämns som ett exempel på sådan samverkan (prop. 2009/10:85 s. 262 och 365). Syftet med NCT:s verksamhet är att stärka den samlade förmågan hos Säkerhetspolisen, Försvarsmakten och FRA att genomföra strategiska bedömningar till stöd för Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorism. Syftet är således i vart fall indirekt att förebygga och förhindra terrorbrott. Även om FRA och Försvarsmakten inte är brottsbekämpande myndigheter och NCT-samarbetet inte syftar till att utreda brott, är det vår bedömning att samarbetet utgör en sådan samverkan som i lagen avses med uttrycket myndighetsöverskridande samverkan mot brott. Säkerhetspolisen har således stöd i PDL för det utlämnande av personuppgifter som inom ramen för samarbetet sker till FRA och Försvarsmakten och något förtydligande är inte nödvändigt i den delen.

Enligt 1 kap. 6 § 4 FRA-PuL och 1 kap. 6 § 4 PuL UNDSÄK får FRA och Försvarsmakten inte behandla personuppgifter för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Dessa bestämmelser ger uttryck för den s.k. finalitetsprincipen. FRA och Försvarsmakten får således behandla personuppgifter genom att lämna ut dem endast om ändamålet med utlämnandet inte är oförenligt med de ursprungliga ändamål som gäller för deras respektive verksamheter, dvs. i det här fallet att bedriva försvarsunderrättelseverksamhet i enlighet med reglerna i lagen (2000:130) om försvarsunderrättelseverksamhet och de för varje myndighet mer preciserade inriktningarna. Det kan enligt vår bedömning inte anses vara oförenligt med detta ändamål att FRA och Försvarsmakten lämnar ut uppgifter till Säkerhetspolisen och till varandra, för att inom ramen för NCT-samarbetet indirekt förebygga och förhindra terrorism. Vi anser därför att även FRA och Försvarsmakten har stöd i sina respektive registerförfattningar för det utlämnande av personuppgifter som sker inom ramen för samarbetet. Det finns inte heller något behov av förtydligande författningsstöd för denna behandling.

7.3 Personuppgiftsansvaret för behandlingen av personuppgifter i den gemensamma NCT-mappen

7.3.1 Allmänt om personuppgiftsansvar

Personuppgiftslagen och de särskilda registerförfattningarna innehåller ett stort antal hanteringsregler som innebär olika skyldigheter för den som är ansvarig för den personuppgiftsbehandling som sker i en viss verksamhet. Den som är personuppgiftsansvarig är skyldig att se till att de grundläggande kraven på behandling av personuppgifter iakttas. Det innebär bl.a. ett ansvar för att personuppgifterna är korrekta, att de behandlas på ett sätt som inte strider mot tillämpliga bestämmelser samt att de gallras i rätt tid. Vidare innebär personuppgiftsansvaret en skyldighet att självmant och på särskild begäran lämna information till den registrerade, att på den registrerades begäran rätta, blockera eller utplåna personuppgifter som inte behandlats i enlighet med gällande lagstiftning, att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas samt att ersätta den registrerade för den skada en lagstridig behandling av personuppgifter för med sig.

Enligt 3 § PuL är den personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. Vem som rent faktiskt gör detta kan dock ibland vara svårt att avgöra. Personuppgiftsansvarig är normalt den juridiska person eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. DI har uttryckt sig enligt följande (beslut 2010-07-02, dnr 686-2010):

> Vem som bestämmer över ändamålen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet. Avgörande för denna bedömning är bl.a. varför behandlingen utförs och vem som är initiativtagare till behandlingen. Att bestämma över medlen för behandlingen avser främst att bestämma över de tekniska och organisatoriska medlen för behandlingen, dvs. ”hur” behandlingen ska gå till, t.ex. vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifter och när uppgifter ska raderas.

Olika avtalskonstruktioner där personuppgiftsansvaret preciseras kan beaktas i denna bedömning men avgörande är alltid vem eller vilka som faktiskt har bestämt över personuppgiftsbehandlingen (Öman/Lindblom, s. 93).

Det kan också genom lag eller förordning bestämmas vem som är personuppgiftsansvarig för en viss behandling. Så har ofta skett i de särskilda registerförfattningar som finns för den offentliga sektorn, särskilt när ändamålen med de aktuella behandlingarna eller registren bestäms i författningen och således inte av den aktuella myndigheten. Det har nämligen befarats att tveksamhet annars kan uppstå om huruvida myndigheten verkligen har ett sådant inflytande över ändamålen med behandlingen att den blir att anse som personuppgiftsansvarig vid en tillämpning av personuppgiftslagens regler (se t.ex. Lagrådets synpunkter i prop. 1997/98:80 s. 117 och prop. 1997/98:108 s. 125). Från integritetsskyddssynpunkt har det vidare ofta ansetts lämpligt att på ett tydligt sätt peka ut vem som är personuppgiftsansvarig för den behandling som regleras i en registerförfattning (se t.ex. prop. 2000/01:126 s. 33). När ändamålen med en viss behandling anges i en registerförfattning, innebär det i princip att den som utför behandlingen inte är den som bestämmer ändamålen. I sådana fall går det därmed inte att utifrån personuppgiftslagens definition dra några egentliga slutsatser om vem som är personuppgiftsansvarig.

7.3.2 Närmare om gemensamt personuppgiftsansvar

För en och samma behandling av personuppgifter kan det finnas två eller flera personuppgiftsansvariga. För att någon ska anses som personuppgiftsansvarig räcker det nämligen att han eller hon tillsammans med andra kan bestämma ändamålen med och medlen för behandlingen. Det torde räcka att flera gemensamt och i samråd faktiskt har bestämt att genomföra en viss behandling även om var och en rättsligt eller faktiskt har haft möjlighet att ensam bestämma. Om flera gemensamt har samlat in och lagrat en viss mängd personuppgifter är de tillsammans personuppgiftsansvariga för lagringen av dessa uppgifter och därmed var och en skyldig att se till att uppgifterna t.ex. inte används på ett sätt som är oförenligt med de ändamål som de har bestämt för behandlingen. Om någon av

dem skulle använda uppgifterna för andra ändamål är således alla ansvariga för att uppgifterna behandlats olagligt (Öman/Lindblom, s. 99 f.).

När flera aktörer är involverade i processer eller informationssystem där personuppgifter behandlas, t.ex. vid interaktiva tjänster på nätet eller i myndighetsövergripande samarbeten, kan det uppkomma frågor kring vem eller vilka som är personuppgiftsansvariga för de olika momenten i hanteringen samt hur personuppgiftsansvaret ska fördelas vid olika typer av gemensam behandling eller gemensam användning av system. Personuppgiftslagen innehåller inte några bestämmelser till ledning för hur dessa frågor ska bedömas (SOU 2015:39 s. 342). Det saknas också praxis i form av vägledande domstolsavgöranden när det gäller just gemensamt eller delat personuppgiftsansvar.

Vissa uttalanden angående gemensamt personuppgiftsansvar har dock gjorts i förarbetena. Så är t.ex. fallet när det gäller personuppgiftsbehandlingen i verksamhet inom socialförsäkringens administration, dvs. hos Försäkringskassan och Pensionsmyndigheten. Enligt 114 kap. 6 § socialförsäkringsbalken är en myndighet inom socialförsäkringens administration personuppgiftsansvarig för ”den behandling av personuppgifter som den utför”. I förarbetena till bestämmelsen diskuterades frågan om lämpligheten i myndighetsgemensamt personuppgiftsansvar. Regeringen anförde att det inte var ändamålsenligt att i lag i detalj specificera vem som skulle vara personuppgiftsansvarig för alla de olika typer av behandlingar som kunde tänkas förekomma inom socialförsäkringens administration. Särskilt gällde detta de mer komplexa förhållanden som rådde vid myndighetsgemensam användning av de stora register som ingår i socialförsäkringsdatabasen. I stället borde personuppgiftsansvaret fördelas genom en regel av mer övergripande karaktär som tog sikte på den myndighet som utför en viss behandling. Enligt regeringen var det den enskilda behandlingen som skulle utgöra grunden för fördelningen av personuppgiftsansvaret. Regeringen fortsatte enligt följande (prop. 2002/03:135 s. 52 f.).

> Har en uppgift lagrats i databasen är det den myndighet som i och för sin verksamhet utför lagringsåtgärden som är ansvarig för att den lagrade uppgiften är korrekt. Ansvaret för uppgiften bör rimligtvis sedan sträcka sig så långt som fram till den tidpunkt då gallring aktualiseras, dock inte längre än fram till den tidpunkt då den myndigheten av olika skäl inte längre besitter möjligheter att förfoga

över uppgiften genom rättning, blockering, borttagning etc. Om en personuppgift lämnas ut av en annan myndighet än den som registrerade uppgiften svarar naturligtvis den utlämnande myndigheten för den behandling som utgörs av själva utlämnandet.

För den fortsatta behandlingen av uppgiften efter en registrering kan även andra myndigheter vara ansvariga, allt efter vilka faktiska behandlingar som utförs. Förslaget om fördelning av personuppgiftsansvar förutsätter naturligtvis att det går att genom loggning spåra vilken myndighet som företagit en viss behandling.

I övergripande frågor, såsom ansvar för att tekniska eller organisatoriska säkerhetsåtgärder vidtas, måste personuppgiftsansvaret fördelas efter vilka myndigheter som har befogenhet och skyldighet att utföra dessa åtgärder. I regel torde det följa av åläggandet för Riksförsäkringsverket i verksinstruktionen att vara ansvarig systemägare för Riksförsäkringsverkets och försäkringskassornas gemensamma It-system att det är verket som har personuppgiftsansvaret vad avser sådana frågor. Enligt regeringens uppfattning innebär det lämnade förslaget i princip ett sådant "gemensamt" personuppgiftsansvar som ett flertal försäkringskassor efterlyst. Att införa en bestämmelse som innefattar begreppet "gemensamt personuppgiftsansvar" är dock inte i sig ägnat att bringa större klarhet rörande fördelningen av personuppgiftsansvaret eftersom det i enlighet med vad som anförts ovan i själva verket är så att personuppgiftsansvaret splittras upp på de olika myndigheterna. Enligt regeringens uppfattning bör personuppgiftsansvaret i stället fördelas utifrån en bestämmelse som tar sikte på vilken myndighet som utför en behandling av personuppgifter.

I förarbetena till patientdatalagen (2008:355) har regeringen bl.a. uttalat sig om personuppgiftsansvaret vid sammanhållen journalföring. Sammanhållen journalföring innebär att vårdgivare genom direktåtkomst kan dela med sig av sin vårddokumentation till varandra. Enligt 2 kap. 6 § patientdatalagen ansvarar varje hälso- och sjukvårdsmyndighet för den personuppgiftsbehandling som myndigheten utför. I paragrafen förtydligas att detta även omfattar den behandling av personuppgifter som en myndighet utför när myndigheten genom direktåtkomst i ett enskilt fall bereder sig tillgång till personuppgifter om en patient hos en annan vårdgivare eller hälso- och sjukvårdsmyndighet. Detta gäller även vid sammanhållen journalföring. I 6 kap. 6 § patientdatalagen stadgas dock att regeringen eller den myndighet regeringen bestämmer, vid sammanhållen journalföring med direktåtkomst mellan vårdgivare eller över myndighetsgränser, får meddela föreskrifter om vem som ska ha personuppgiftsansvar för övergripande frågor om tekniska och organisatoriska säkerhetsåtgärder. I motiven framhöll regeringen

att beroende på organisation och samarbetsformer vid olika system för sammanhållen journalföring torde regeln i 2 kap. 6 § ofta innebära ett solidariskt personuppgiftsansvar för övergripande frågor om tekniska och organisatoriska säkerhetsåtgärder. En sådan ordning framstår dock inte alltid som naturlig. Om exempelvis allas vårddokumentation lagras och behandlas i en gemensam databas som administreras av bara en av vårdgivarna, t.ex. ett landsting – som också i praktiken dikterar villkoren för de andra vårdgivarnas deltagande i systemet – kan det tala för att det aktuella landstinget bör anses ha ett personuppgiftsansvar för övergripande frågor. Regeringen menade vidare att eftersom det inte alltid är helt klart hur det förhåller sig med personuppgiftsansvaret i övergripande frågor vid gränsöverskridande personuppgiftsbehandling, kan det finnas ett behov av en tydlig reglering i dessa frågor. Därför fanns det ett behov av det aktuella bemyndigandet för regeringen (prop. 2007/08:126. s. 255). Några sådana föreskrifter som avses i 6 kap. 6 § patientdatalagen har emellertid hittills inte meddelats.

Den s.k. Artikel 29-gruppen har behandlat frågor om personuppgiftsansvarets räckvidd och fördelning mellan olika aktörer m.m. i en rapport från 2010 (opinion 1/2010 on the concept of ”controller” and ”processor”, 00264/10/EN WP 169). Artikel 29-gruppen är en arbetsgrupp som består av en företrädare för varje nationell tillsynsmyndighet i EU-medlemsstaterna, en företrädare för EU-kommissionen samt den europeiska datatillsynsmannen. Gruppen är rådgivande och oberoende och ska bl.a. se till att det nu gällande dataskyddsdirektivet tillämpas enhetligt i medlemsstaterna.

När det gäller personuppgiftsansvarets fördelning i komplexa situationer med flera inblandade aktörer har gruppen intagit ett ganska flexibelt betraktelsesätt på frågan om personuppgiftsansvaret är gemensamt eller uppdelat. I rapporten framhålls att personuppgiftsansvaret är ett funktionellt begrepp som är avsett att lägga ansvaret där det faktiska inflytandet ligger och att det är de faktiska omständigheterna som ska vara avgörande vid bedömningen. Detta gäller även vid gemensamt personuppgiftsansvar. Vid gemensamma infrastrukturer där flera aktörer tillsammans bestämmer medlen för behandling av personuppgifter kan aktörerna vara gemensamt ansvariga för infrastrukturen även om de inte har samma ändamål för sina respektive personuppgiftsbehandlingar för vilka de är separat personuppgiftsansvariga. I rapporten nämns flera

exempel på fall där personuppgiftsansvaret vid olika samarbeten m.m. kan vara delvis gemensamt, delvis uppdelat. Vidare betonas att ansvaret mycket väl kan vara differentierat mellan aktörerna och att olika grader av kontroll kan ge upphov till olika grader av ansvar. I komplexa system kan t.ex. enskilda registrerades rätt till information och andra rättigheter tillgodoses på olika nivåer av de olika aktörerna. Avtalsmässiga villkor och förhållanden mellan aktörerna kan vara användbara vid bedömningen av ansvarets förläggande eller fördelning, särskilt om det inte finns någon anledning att ifrågasätta att avtalet korrekt speglar verkligheten.

I rapporten ställs frågan om gemensamt personuppgiftsansvar också innebär ett gemensamt solidariskt ansvar. Arbetsgruppen konstaterar här att det i praktiken finns en mängd olika sätt att samarbeta och agera tillsammans och att detta ibland kan medföra att det i en viss situation föreligger ett gemensamt solidariskt personuppgiftsansvar. I regel är dock de inblandade aktörerna ansvariga för behandlingen av personuppgifter i olika skeden och i olika grad. Enligt gruppen bör ett gemensamt och solidariskt ansvar för samtliga inblandade parter övervägas främst för att undvika eventuella oklarheter och därför användas endast om parterna inte har kommit överens om en annan, tydlig och lika effektiv fördelning av skyldigheter och ansvar eller om dessa inte tydligt framgår av de faktiska omständigheterna.

Artikel 29-gruppen betonar slutligen i sin rapport att det är särskilt viktigt att efterlevnaden av dataskyddsbestämmelserna och ansvaret för eventuella brott mot bestämmelserna är tydligt fördelade i komplexa behandlingsmiljöer så att inga situationer uppstår där skyldigheter och rättigheter som följer av bestämmelserna inte följs av någon av aktörerna. Så länge som fullständig efterlevnad garanteras, har dock de inblandade aktörerna utrymme för en viss flexibilitet vid fördelningen av skyldigheter och ansvar. Regler för hur det gemensamma ansvaret ska utövas bör i princip fastställas av de personuppgiftsansvariga aktörerna, även om de faktiska omständigheterna bör beaktas. Den enskilde registrerade måste dock i dessa situationer få utförlig information om de olika aktörerna och personuppgiftsbehandlingens olika moment samt om hur ansvaret för att tillgodose den enskildes rättigheter fördelas mellan aktörerna.

SIN har i ett ärende om personuppgiftsansvar vid behandling av personuppgifter i det centrala kriminalunderrättelseregistret (KUR) uttalat sig om ett gemensamt personuppgiftsansvar (SIN dnr 37-2013). Registret fördes vid den tiden gemensamt av polismyndigheterna och Rikspolisstyrelsen (RPS). Granskningen gällde ärenden i KUR som initierats av en länspolismyndighet och därefter registrerats som inkomna hos Rikskriminalpolisen (RKP) som var en del av RPS. I den här situationen skapades inte ett nytt ärende i KUR utan ärendet fick bara ett ytterligare ärendenummer. I KUR fanns det således ett enda underliggande gemensamt ärende som båda myndigheterna hade tillgång till och där såväl länspolismyndigheten som RKP kunde göra ändringar. SIN konstaterade att denna gemensamma behandling av uppgifter talade för att personuppgiftsansvaret måste vara delat efter att ärendet delgetts RKP. Enligt SIN var dock den närmare innebörden av ett delat personuppgiftsansvar i en situation som denna inte helt klar. I avsaknad av tydlig reglering av personuppgiftsansvarets närmare fördelning vid en sådan gemensam behandling som avsågs talade mycket enligt nämnden för att personuppgiftsansvaret för all behandling i det gemensamma ärendet skulle anses vara solidariskt. Nämnden menade dock att den närmare fördelningen av personuppgiftsansvaret i det enskilda fallet var en fråga som måste avgöras av rättstillämpningen. Slutligen uppmanade nämnden RPS att tillsammans med länspolismyndigheterna analysera hur man såg på fördelningen av ansvaret och att dokumentera och sprida denna analys i organisationen. Detta bl.a. för att säkerställa att anspråk från enskilda skulle kunna tas om hand på ett lagenligt sätt.

Även DI har i några ärenden diskuterat ett gemensamt personuppgiftsansvar. Så gjorde myndigheten exempelvis vid sin tillsyn över personuppgiftsbehandlingen i de politiska partiernas centrala medlemsregiser (dnr 1669 – 1676-2011). DI konstaterade att personuppgiftsansvaret i dessa medlemsregister var gemensamt för riksorganisationerna och de lokala avdelningarna och att de alla således hade ansvar för att behandlingen skedde i enlighet med gällande rätt. Eftersom tillsynen enbart gällde riksorganisationerna uttalade sig emellertid inte DI närmare om innebörden av detta gemensamma ansvar. I två av ärendena påpekade DI dock vikten av att klarlägga vem som gör vad inom ramen för det gemensamma personuppgiftsansvaret och att de registrerade får korrekt information.

Liknande uttalanden gjordes även vid DI:s tillsyn av Riksidrottsförbundets behandling av personuppgifter i systemet IdrottOnline (se dnr 1499-2009).

I detta sammanhang kan också nämnas att det i det nya dataskyddsdirektivet för den brottsbekämpande sektorn (direktiv [EU] 2016/680) har tagits in en bestämmelse som rör gemensamt personuppgiftsansvar. Där anges att två eller flera personuppgiftsansvariga har gemensamt ansvar för ett register, om de gemensamt fastställer behandlingens ändamål och medel. Det anges vidare att de personuppgiftsansvariga under öppna former ska fastställa sitt respektive ansvar för efterlevnaden av direktivet, särskilt vad gäller utövandet av den registrerades rättigheter och sina respektive skyldigheter att tillhandahålla den information som avses i artikel 13, genom ett inbördes arrangemang, såvida inte och i den mån som de personuppgiftsansvarigas respektive skyldigheter fastställs i unionsrätt eller medlemsstaternas nationella rätt som de personuppgiftsansvariga omfattas av. Inom ramen för arrangemanget ska även en kontaktpunkt för de registrerade utses. En bestämmelse med liknande innebörd har även tagits in i den allmänna dataskyddsförordningen (förordning [EU] 2016/679).

7.3.3 Personuppgiftsansvaret i den gemensamma NCT-mappen i dag

Bedömning: Varje myndighet inom NCT-samarbetet är som huvudregel ansvarig för den behandling av personuppgifter som myndigheten utför inom samarbetet. För det fall det inte går att urskilja vilken myndighet som har utfört en specifik behandling och det inte heller på annat sätt går att urskilja någon tydlig fördelning av ansvaret får det anses föreligga ett gemensamt solidariskt personuppgiftsansvar för den behandlingen.

Skälen för bedömningen

Samarbetet inom NCT bedrivs inom ramen för den rättsliga reglering som gäller för var och en av myndigheterna. Myndigheternas personuppgiftsbehandling styrs i dag av PDL, FRA-PuL, PuL

UNDSÄK och PuL med tillhörande förordningar. Av respektive registerförfattning följer att myndigheterna är ansvariga för den behandling av personuppgifter som myndigheterna utför. Den rättsliga regleringen innebär således att varje myndighet inom NCT-samarbetet är ansvarig för den behandling av personuppgifter som myndigheten utför inom samarbetet. Av den överenskommelse daterad den 5 maj 2014 som tecknats mellan myndigheterna med anledning av samarbetet framgår att myndigheterna har bedömt att var och en av dem är personuppgiftsansvarig för den behandling som en myndighet utför i sin myndighetsspecifika mapp. Däremot anges inte i överenskommelsen något närmare om personuppgiftsansvaret vid myndigheternas användning av den gemensamma mappen. SIN har vid sin granskning emellertid konstaterat att Säkerhetspolisen är personuppgiftsansvarig för samtliga personuppgifter i de gemensamma rapportutkasten. Nämnden har dock påpekat att det inte kan uteslutas att även övriga NCT-myndigheter har personuppgiftsansvar för uppgifter i rapportutkasten, men att denna fråga ligger utanför nämndes tillsynsområde (SIN dnr 324-2014, s. 11).

När det gäller behandlingen av personuppgifter i de myndighetsspecifika NCT-mapparna samt i de personliga mapparna är det, som konstaterats ovan, tydligt vilken myndighet som utför dessa behandlingar och vilken myndighet som är ansvarig för behandlingarna. I den gemensamma NCT-mappen är emellertid förhållandena annorlunda. Som framgår av genomgången i föregående kapitel har både Säkerhetspolisen, Försvarsmakten och FRA tillgång till den gemensamma mappen och alla tre myndigheterna behandlar också personuppgifter på olika sätt där, t.ex. genom att skriva in, ändra eller radera uppgifter. Behandlingarna utförs i praktiken i ett ordbehandlingsprogram. Det finns inget system för loggning av de åtgärder som vidtas. Som vi har konstaterat är det därför svårt att i den gemensamma mappen urskilja vilken myndighet som utför vilken behandling. Ofta behandlar myndigheterna samma personuppgifter i mappen samtidigt. Om endast en myndighet under en viss tid utför en viss behandling, t.ex. om en handläggare arbetar ensam i ett rapportutkast, är det svårt att urskilja den behandlingen från övriga behandlingar. Den enda uppdelning som relativt tydligt går att urskilja är att FRA och Försvarmakten, i enlighet med de regler som gäller för försvarsunderrättelseverksamheten,

i den gemensamma mappen endast behandlar uppgifter som rör utländska förhållanden, medan Säkerhetspolisen behandlar både sådana uppgifter och uppgifter som rör inhemska förhållanden, i enlighet med de begränsningar som gäller för myndighetens personuppgiftsbehandling i övrigt. FRA och Försvarsmakten behandlar således en något mer begränsad del av de uppgifter som finns i den gemensamma mappen. Därutöver har myndigheterna försökt dela upp personuppgiftsansvaret genom att med fotnoter märka personuppgifterna och på så sätt peka ut vilken myndighet som är ansvarig för de behandlingar som vidtas i mappen. Även om märkningen genomförs konsekvent visar den dock huvudsakligen bara från vilken myndighet uppgiften härstammar. Tanken är visserligen att varje behandling av en personuppgift som utförs i den gemensamma mappen ska märkas och på så sätt loggas, således även ändringar av redan införda uppgifter eller borttagande av uppgifter. Det är emellertid inte möjligt att med hjälp av märkningen avgöra vilken behandling som har förekommit, dvs. om en uppgift har lagts in eller ändrats på något sätt. Som framgår i kapitel 6 ovan har SIN också konstaterat att märkningen inte motsvaras av någon faktisk begränsning i respektive myndighets möjlighet att bestämma ändamålen och medlen för behandlingen. Det går exempelvis inte av märkningen att utläsa vilken myndighet som är egentlig initiativtagare till en viss behandling eller vilken myndighet som har rätt att besluta om radering av en viss uppgift (SIN dnr 324-2014, s. 11). Myndigheternas märkning av personuppgiftsbehandlingar i den gemensamma mappen medför således inte att det härigenom på ett tydligt sätt går att urskilja vilken myndighet som har utfört vilken behandling.

Mot bakgrund av detta är det vår bedömning att varje myndighet inom samarbetet som huvudregel är ansvarig för den personuppgiftsbehandling som den myndigheten utför i den gemensamma mappen. För det fall det inte går att urskilja vem som har utfört en specifik behandling och det inte heller på annat sätt går att urskilja någon tydlig fördelning av ansvaret, får det i stället anses föreligga ett gemensamt personuppgiftsansvar för den behandlingen. Detta gemensamma personuppgiftsansvar torde i realiteten bli ett solidariskt ansvar mellan myndigheterna, eftersom det i princip inte går att urskilja vem som har utfört en viss behandling i den gemensamma mappen. Det innebär att Säkerhetspolisen, Försvarsmakten

och FRA i de flesta fall är solidariskt ansvariga för de personuppgiftsbehandlingar som myndigheterna utför i den gemensamma mappen om personuppgifterna har en utländsk koppling, vilket torde vara fallet i nästan alla situationer. Om uppgifterna i något enstaka fall enbart rör inhemska förhållanden behandlas de som tidigare nämnts endast av Säkerhetspolisen och det är således Säkerhetspolisen som då är personuppgiftsansvarig för dessa behandlingar. Denna slutsats ligger i linje med vad SIN har kommit fram till beträffande Säkerhetspolisens personuppgiftsansvar.

För ett gemensamt personuppgiftsansvar talar även den omständigheten att myndigheterna tillsammans har tagit initiativ till samarbetet dem emellan och således också till den personuppgiftsbehandling som utförs i den gemensamma mappen. Myndigheterna behandlar uppgifterna i den gemensamma mappen för samma ändamål, dvs. för att göra analyser och hotbedömningar och presentera dessa i rapporter. Även i ett större sammanhang är det övergripande ändamålet med personuppgiftsbehandlingen för alla tre myndigheterna detsamma, nämligen att motverka och förhindra terrorism (se avsnitt 7.5 gällande ändamålsbestämmelser). Myndigheterna har vidare tillsammans bestämt hur behandlingen ska gå till i den gemensamma mappen och vid rapportskrivandet, t.ex. vilka personuppgifter som ska behandlas, vilka tredje män som ska få tillgång till de behandlade personuppgifterna och när uppgifter ska raderas, även om detta inte har formaliserats på något sätt. Myndigheterna har således bestämt medlen för behandlingen tillsammans. De tre NCT-myndigheterna torde därmed ha bestämt både ändamålen med och medlen för behandlingen tillsammans. I vart fall är det svårt att urskilja en av myndigheterna som den som ensam har bestämt ändamålen med och medlen för behandlingen.

I detta sammanhang vill vi framhålla att slutsatserna ovan endast är ett resultat av våra överväganden inom ramen för uppdraget att avgöra 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.

7.3.4 Innebörden av det gemensamma personuppgiftsansvaret bör förtydligas

Bedömning: NCT-myndigheterna styrs av tre olika regelverk och är gemensamt och solidariskt ansvariga för merparten av de behandlingar av personuppgifter som utförs i den gemensamma mappen. Ett sådant gemensamt och solidariskt ansvar kan riskera att medföra vissa otydligheter, både inom myndigheterna och utåt mot allmänheten. Den närmare innebörden av ett sådant personuppgiftsansvar bör därför förtydligas. Detta kan exempelvis ske genom att myndigheterna i en överenskommelse tydliggör den praktiska innebörden av det gemensamma personuppgiftsansvaret.

Skälen för bedömningen

Innebörden av ett gemensamt personuppgiftsansvar för NCT-myndigheterna

Det finns inget som säger att personuppgiftsansvar inte kan vara gemensamt och delas solidariskt mellan flera aktörer. Ett gemensamt personuppgiftsansvar som delas mellan flera aktörer kan dock medföra vissa otydligheter både för den enskilde registrerade och för aktörerna själva. Det kan exempelvis vara svårt för den enskilde att veta vem denne ska vända sig till för att få information om personuppgiftsbehandlingen eller för att göra eventuella anspråk gällande. Det kan vidare vara svårt för de personuppgiftsansvariga aktörerna att på ett effektivt och ändamålsensligt sätt utöva sitt personuppgiftsansvar om det är oklart vad deras ansvar och skyldigheter egentligen innefattar.

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 kan bevaka sina rättigheter. De få personuppgifter som förekommer i den gemensamma mappen, och då främst i produktionsmappen 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. De problem som

ett otydligt personuppgiftsansvar innebär för den enskilde registrerade i den här situationen torde därför främst vara ett teoretiskt problem och sällan realiseras i praktiken. Detta innebär dock inte att frågor om personuppgiftsansvarets närmare innebörd och fördelning kan lämnas olösta i situationer som denna. Vid förhållanden som dessa blir det i stället upp till tillsynsmyndigheterna att granska och kontrollera den personuppgiftsbehandling som sker. För att tillsynsmyndigheterna ska kunna göra detta och på så sätt bevaka den enskildes rättigheter är det viktigt att personuppgiftsansvaret är tydligt och att det framgår vem som är ansvarig för vad.

Som konstaterats ovan kan det vara svårt för de personuppgiftsansvariga aktörerna att på ett effektivt och ändamålsensligt sätt utöva sitt personuppgiftsansvar om det finns oklarheter kring detta. Det kan exempelvis framstå som oklart för de enskilda medarbetarna vad som i praktiken gäller i en specifik situation och hur man ska agera korrekt vid behandlingen av personuppgifter. Detta kan i sin tur få negativa konsekvenser för integritetsskyddet. Eventuella oklarheter gällande personuppgiftsansvaret kan också medföra att arbetet i övrigt blir ineffektivt, då tid kanske måste läggas på att i olika situationer utreda vad som gäller. Inom NCT-samarbetet har myndigheterna exempelvis utarbetat ett system för märkning av personuppgifter och personuppgiftsbehandling i den gemensamma mappen i syfte att försöka förtydliga ansvarets fördelning. Att på detta sätt manuellt logga olika personuppgiftbehandlingar tar värdefull tid i anspråk från den huvudsakliga verksamheten och är också svårt att genomföra på ett korrekt sätt.

En ytterligare fråga som aktualiseras vid gemensamt solidariskt personuppgiftsansvar är vilka regler som ska tillämpas på de behandlingar som utförs av de inblandade aktörerna. När aktörerna styrs av samma regelverk, t.ex. personuppgiftslagen, torde detta inte innebära några större problem. Inom NCT samarbetar emellertid tre olika myndigheter som styrs av tre olika registerförfattningar. Om det inte går att urskilja vem som har företagit en viss behandling och ansvaret till följd av detta får anses vara gemensamt och solidariskt mellan myndigheterna innebär det således i princip att tre olika regelverk blir tillämpliga på samma behandling. I stora delar ser dock NCT-myndigheternas registerförfattningar relativt lika ut och de följer också i många delar personuppgiftslagen. Det är dess-

utom relativt få bestämmelser som aktualiseras vid den begränsade behandling av personuppgifter som förekommer i den gemensamma mappen. Man skulle därför kunna argumentera för att det egentligen inte innebär något problem att tre olika regelverk är tillämpliga på samma behandlingar.

Ett gemensamt och solidariskt personuppgiftsansvar kan alltså medföra vissa otydligheter, både inom myndigheterna och utåt mot allmänheten. Som konstaterats ovan finns det dock inget som säger att ett sådant ansvar inte kan eller bör förekomma. Gemensamt personuppgiftsansvar har tvärtom lyfts fram och reglerats specifikt i EU:s nya regelverk för dataskydd (se avsnitt 7.3.2). Detta talar för att olika typer av gemensamt personuppgiftsansvar blir allt vanligare. Trots de omständigheter som påtalats ovan har vi inte sett annat än att personuppgiftsbehandlingen inom samarbetet fungerar väl och att myndigheterna är medvetna om vad som innefattas i deras respektive personuppgiftsansvar och hur detta ansvar i praktiken ska utövas. Som framgår av avsnitt 7.4 nedan ser vi inte heller att tillämpningen av tre olika registerförfattningar medför några större problem i praktiken eftersom de bestämmelser som aktualiseras i princip ser likadana ut i alla tre författningarna. Mot bakgrund av detta anser vi att det inte finns ett sådant nödvändigt behov av förtydliganden vad gäller personuppgiftsansvaret att lagstiftningsåtgärder behöver vidtas för att åstadkomma en förändring.

Ett gemensamt personuppgiftsansvar kan emellertid, framför allt utåt sett, framstå som otydligt. Den omständigheten att tre olika regelverk är tillämpliga i den aktuella situationen kan, även om bestämmelserna ser likadana ut, innebära en viss otydlighet i sig. Det kan därför, ur ett integritetsperspektiv, vara bra om den praktiska innebörden av det gemensamma personuppgiftsansvaret inom samarbetet på något sätt tydliggörs.

Hur kan ett förtydligande uppnås?

Vi har under arbetets gång övervägt flera alternativa lösningar när det gäller förtydligandet av personuppgiftsansvaret i den gemensamma mappen och noga analyserat eventuella för- och nackdelar med de olika förslagen. Eftersom vårt uppdrag har varit att klar-

lägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling som sker inom samarbetet har vi inledningsvis övervägt om det är möjligt att författningsreglera personuppgiftsansvaret och vad det i så fall skulle få för konsekvenser för myndigheternas personuppgiftsbehandling dels i den egna verksamheten, dels inom samarbetet. Vi har också övervägt möjligheten att på olika sätt förtydliga personuppgiftsansvaret mellan myndigheterna utan författningsreglering och vad det skulle innebära i praktiken samt om det skulle vara möjligt att uppnå en tydligare fördelning genom olika tekniska lösningar.

Vi har i vårt arbete även studerat hur man har löst motsvarande problem i andra typer av myndighetssamarbeten, t.ex. den nationella satsningen mot den grova organiserade brottsligheten. NCT-samarbetet skiljer sig dock från andra myndighetssamarbeten på det sättet att det är ett relativt formaliserat och långtgående samarbete som både till sin form och till sitt arbetssätt påminner mycket om en egen myndighet. Till skillnad från många andra myndighetssamarbeten arbetar exempelvis handläggarna från myndigheterna enbart vid NCT under sin placering där och inte dessutom vid den egna myndigheten. Samarbetet inom NCT handlar vidare inte bara om att utbyta information och erfarenheter, utan handläggarna vid NCT-myndigheterna arbetar tätt tillsammans och utför också arbetsuppgifter gemensamt. Det har mot bakgrund av detta varit svårt att hämta vägledning från andra liknande samarbeten när det gäller frågor om personuppgiftsbehandling.

Organisatoriska åtgärder

Inledningsvis vill vi något beröra frågan om det går att åstadkomma större tydlighet i fråga om personuppgiftsansvaret genom organisatoriska förändringar. Om NCT exempelvis skulle organisera sig under en myndighet eller ombildas till en egen myndighet är det möjligt att regleringen av personuppgiftsbehandlingen skulle kunna lösas på ett enklare sätt, även om en sådan åtgärd i sin tur skulle generera ett flertal andra frågor som måste lösas. Som konstaterats redan i det inledande kapitlet har det dock inte ingått i vårt uppdrag att föreslå organisatoriska förändringar för NCT-samarbetet.

Sådana lösningar kräver också en större och mer genomgripande översyn av verksamheten och de samarbetande myndigheterna än vad som har varit möjligt att genomföra inom ramen för vårt begränsade uppdrag. Vi har således inte närmare övervägt organisatoriska förändringar som ett alternativ för att åstadkomma en tydligare struktur när det gäller personuppgiftsbehandlingen inom NCT-samarbetet.

Författningsreglering

Ett sätt att åstadkomma en större tydlighet i fråga om personuppgiftsansvaret inom samarbetet är självfallet att man i en författning anger vem eller vilka som är personuppgiftsansvariga. Man skulle exempelvis kunna föreskriva att en myndighet är ansvarig för all behandling som sker i den gemensamma mappen. Ett annat alternativ är att man anger att varje myndighet är ansvarig för den behandling som myndigheten utför eller att det mer konkret anges vilka behandlingar i den gemensamma mappen som respektive myndighet är ansvarig för.

Det är således möjligt att en författningsreglering av personuppgiftsansvaret skulle kunna åstadkomma en större tydlighet vad gäller ansvar för personuppgiftsbehandling inom samarbetet. Som vi har konstaterat ovan anser vi dock inte att behovet av förtydliganden vad gäller personuppgiftsansvaret är av sådan art att lagstiftningsåtgärder behöver vidtas för att åstadkomma en förändring. Vi har därför inte närmare övervägt alternativet att författningsreglera personuppgiftsansvaret inom samarbetet.

I detta sammanhang kan det emellertid finnas skäl att peka på några av de svårigheter som en författningsreglering torde vara förenad med. Det skulle enligt vår bedömning behöva skapas en mer eller mindre heltäckande reglering för all personuppgiftsbehandling i den gemensamma mappen, eftersom en reglering av personuppgiftsansvaret medför att även andra frågor om personuppgiftsbehandlingen skulle behöva regleras. En sådan författning skulle vidare tillämpas av tre olika myndigheter som bedriver skilda verksamheter och utöver den aktuella författningen styrs av tre olika regelverk. Detta väcker bl.a. frågor om hur eventuella ändamålsbestämmelser bör utformas och hur tillsynen av den behand-

ling som sker enligt författningen ska utövas och av vem. En sådan författning skulle också behöva gälla utöver myndigheternas befintliga registerförfattningar och för en begränsad del av NCT-samarbetet. Det skulle innebära att myndigheterna skulle behöva förhålla sig till två olika författningar när de behandlar personuppgifter inom NCT-samarbetet. En sådan ordning riskerar att skapa nya tillämpningsproblem och oklarheter. En författning som ska reglera tre olika myndigheters personuppgiftsbehandling inom ett så pass känsligt område som det här är fråga om kräver därför noggranna överväganden. Till detta kommer att Försvarsmakten och FRA är försvarsunderrättelsemyndigheter, vars verksamheter är relativt strängt reglerade i flera författningar på området. En ytterligare författning som reglerar dessa myndigheters personuppgiftsbehandling skulle eventuellt kunna få effekter för den befintliga regleringen och kräver även av det skälet en djupgående analys av hela det rättsliga område som berörs. Som vi nyss har anfört har vi inte gått vidare med våra överväganden kring en eventuell författningsreglering, eftersom det enligt vår bedömning inte finns något egentligt behov av så genomgripande åtgärder och innebörden av det gemensamma, solidariska ansvar som nu gäller kan tydliggöras på annat sätt.

En överenskommelse som förtydligar den praktiska innebörden av personuppgiftsansvaret

Vår bedömning är alltså att det inte finns något behov av att förtydliga personuppgiftsansvaret genom lagstiftningsåtgärder, men att den praktiska innebörden av det befintliga ansvaret bör tydliggöras inom samarbetet. En fördel med en sådan lösning är att myndigheterna inte begränsas till en viss ansvarsfördelning eller ett visst arbetssätt. De tre myndigheterna får härigenom större möjligheter att framöver själva reglera hur samarbetet ska se ut och det ger därmed en större flexibilitet. Detta kan också vara att föredra mot bakgrund av att samarbetet inom NCT är frivilligt mellan de tre myndigheterna och således varken formellt sanktionerat eller reglerat av regeringen. Frågan är hur ett sådant tydliggörande av det befintliga personuppgiftsansvaret bör åstadkommas.

Som angetts ovan har vi övervägt möjligheten att uppnå en tydligare fördelning av personuppgiftsansvaret genom olika tekniska

lösningar. Här kan konstateras att om det på ett tydligt sätt skulle gå att urskilja vilken myndighet som har utfört en viss personuppgiftsbehandling i den gemensamma mappen skulle oklarheterna kring personuppgiftsansvarets fördelning till viss del kunna lösas. Ett sätt att uppnå detta skulle eventuellt kunna vara att personuppgiftsbehandlingarna loggades automatiserat i det aktuella systemet. Sådan automatiserad loggning skulle i vart fall till viss del kunna ge den spårbarhet som behövs och även ge möjlighet till uppföljning och kontroll av vilken medarbetare som skapat, ändrat eller tagit bort information i den gemensamma mappen samt tidpunkten för åtgärden. Det kan dock ifrågasättas om en sådan lösning egentligen skulle ge en tillfredsställande tydlighet. Handläggarna från de tre myndigheterna arbetar ofta tillsammans i ett dokument och behandlar då eventuella personuppgifter samtidigt, även om det endast är en av dem som är inloggad i systemet och som således skulle loggas automatiserat. Ett sådant system skulle därmed visserligen visa vem som vid en viss tid varit inloggad och utfört en viss behandling, men det skulle kanske inte vara helt överensstämmande med verkligheten. Det skulle också i det fallet innebära att det är slumpen som blir avgörande för vem som blir personuppgiftsansvarig för en viss behandling och vilka regler som därmed blir tillämpliga på behandlingen. Enligt uppgift från Säkerhetspolisen är det dessutom i dag rent tekniskt inte möjligt att i det system som den gemensamma mappen utgör, logga specifika personuppgiftsbehandlingar på det sätt som avses. Att förtydliga personuppgiftsansvaret genom en sådan åtgärd är därmed inte en möjlig lösning och vi har därför inte övervägt detta alternativ närmare. Vi har inte heller sett att någon annan teknisk lösning skulle medföra det förtydligande av personuppgiftsansvaret som önskas.

Det alternativ som kvarstår och som enligt vår bedömning framstår som det mest lämpliga är att myndigheterna sinsemellan kommer överens om en närmare fördelning av de uppgifter som personuppgiftsansvaret innefattar vid behandling av personuppgifter i den gemensamma mappen. Detta skulle kunna göras i den överenskommelse som har tecknats mellan de samarbetande myndigheterna med anledning av samarbetet och som reglerar andra närliggande frågor. Det skulle även kunna göras i en separat överenskommelse mellan myndigheterna.

En överenskommelse om personuppgiftsansvarets fördelning skulle framför allt syfta till att myndigheterna klargör vem eller vilka som åtar sig att i första hand svara för olika tekniska eller organisatoriska säkerhetsåtgärder eller andra uppgifter med anledning av personuppgiftsbehandlingen. Överenskommelsen skulle däremot inte ha någon formell rättsverkan och skulle inte heller innebära något avsteg från principen om att det är de faktiska förhållandena som i slutändan avgör på vilket sätt personuppgiftsansvaret är fördelat. Myndigheterna kan inte heller genom en sådan överenskommelse avtala bort gällande författningsbestämmelser. En överenskommelse av detta slag kan således inte befria någon från ett ansvar som följer av gällande rätt, utan bara reglera hur bestämmelserna ska tillämpas i praktiken. Myndigheterna skulle exempelvis kunna bestämma att en myndighet ska ansvara för att gallring av personuppgifter sker i rätt tid, men inte att en viss bestämmelse om gallring på grund av detta inte ska gälla. Det viktiga med en överenskommelse är dock att innebörden av personuppgiftsansvaret inom samarbetet blir tydligt dels internt för de samarbetande myndigheterna, dels externt för den enskilde och för tillsynsorganen, samt att efterlevnaden av dataskyddsbestämmelserna härigenom kan garanteras. Genom en överenskommelse som förtydligar den praktiska tillämpningen av personuppgiftsansvaret inom samarbetet skulle myndigheterna enligt vår bedömning kunna uppnå den tydlighet vad gäller personuppgiftsbehandlingen som behövs inom NCT.

Exempel på fördelning av de uppgifter som personuppgiftsansvaret innefattar

En sådan överenskommelse som vi förordar kan utformas på olika sätt. Ett alternativ skulle kunna vara att göra en uppdelning efter vilken typ av behandling det rör sig om, t.ex. lagring, bearbetning eller utlämnande, och var denna behandling utförs, t.ex. i rapportutkasten eller någon annanstans i den gemensamma mappen. Ett annat alternativ kan vara att göra en fördelning utifrån vad ansvaret faktiskt innebär, t.ex. en skyldighet att se till att personuppgifterna gallras i rätt tid och att lämpliga tekniska och organisatoriska åtgärder vidtas för att skydda de personuppgifter som behandlas. Som vi ser det finns det inget som hindrar att en fördelning mellan

myndigheterna skulle kunna göras på båda dessa sätt. I enlighet med vad Artikel 29-gruppen uttryckt i sin tidigare nämnda rapport torde myndigheterna nämligen kunna vara relativt flexibla vid fördelningen av skyldigheter och ansvar så länge som fullständig efterlevnad garanteras. Mot bakgrund av hur svårt det är att urskilja och separera de olika behandlingar som utförs i den gemensamma mappen tror vi dock att en uppdelning utifrån ansvarets innebörd främst är att föredra.

Personuppgiftsansvaret innebär en skyldighet att se till att de grundläggande kraven på behandling av personuppgifter iakttas. Detta innebär bl.a. ett ansvar för att personuppgifterna är korrekta, att behandlingen är tillåten, dvs. att ändamålen följs och att uppgifterna är relevanta och nödvändiga i förhållande till ändamålen, samt att uppgifterna gallras i rätt tid. Det innebär också en skyldighet att självmant och på särskild begäran lämna information till den registrerade, att på den registrerades begäran rätta, blockera eller utplåna personuppgifter som inte behandlats i enlighet med gällande bestämmelser, att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas samt att ersätta den registrerade för den skada en lagstridig behandling av personuppgifter för med sig. En fördelning utifrån ansvarets innebörd bör så långt som möjligt ta sin utgångspunkt i dessa skyldigheter.

En reglering myndigheterna emellan skulle inledningsvis kunna ange en myndighet som primärt ansvarig för övergripande tekniska och organisatoriska säkerhetsåtgärder. Denna myndighet skulle då få ansvaret för att inom samarbetet vidta lämpliga åtgärder för att skydda de personuppgifter som behandlas. Eftersom all personuppgiftsbehandling i den gemensamma mappen sker på Säkerhetspolisens server och det är Säkerhetspolisen som tillhandahåller de tekniska systemen skulle detta ansvar förslagsvis kunna ges till den myndigheten.

När det gäller skyldigheten att på begäran lämna information till den registrerade skulle det i överenskommelsen kunna anges att en myndighet ska vara ansvarig för att i första hand ta emot en sådan begäran från en enskild. Denna myndighet skulle sannolikt behöva vidarebefordra denna begäran till övriga myndigheter för bedömning av om och i så fall vilken information om den registrerade i den gemensamma mappen som kan lämnas ut. Det viktiga är dock

att det tydligt framgår för allmänheten att det finns en myndighet som, oavsett om även de andra myndigheterna berörs, är beredd att ta emot och behandla en sådan förfrågan. Som vi tidigare framhållit fråntar en överenskommelse inte de övriga myndigheterna deras ansvar, varför en registrerad alltid kan välja att vända sig till vilken som helst av de tre NCT-myndigheterna.

När det gäller de grundläggande kraven på behandling, dvs. att ändamålen följs och att de uppgifter som behandlas är relevanta, nödvändiga och korrekta, är det svårare att åstadkomma ökad tydlighet genom en överenskommelse mellan myndigheterna. Som regel bör dock den myndighet som uppgiften ursprungligen kommer ifrån ha bäst möjlighet att garantera uppgiftens riktighet. Överenskommelsen skulle i denna del kunna ange att varje myndighet är ansvarig för att de personuppgifter de överför till den gemensamma mappen är korrekta. En sådan ordning har t.ex. använts i belastningsregistret och i misstankeregistret. Polismyndigheten är ansvarig för behandlingen av personuppgifter i dessa register. Det anges dock i respektive förordning att den myndighet som har lämnat uppgifter till Polismyndigheten enligt förordningen, ansvarar för att uppgifterna är riktiga (36 § förordning [1999:1134] om belastningsregister samt 14 § förordning [1999:1135] om misstankeregister). Det skulle även för tydlighets skull kunna anges att varje myndighet ansvarar för att behandlingen sker i enlighet med tillämpliga ändamålsbestämmelser även om detta följer av gällande rätt. I anslutning till detta skulle det också kunna förtydligas att FRA och Försvarsmakten behandlar personuppgifter i den gemensamma mappen med vissa begränsningar.

I en överenskommelse skulle myndigheterna vidare kunna ange vilken myndighet som har det praktiska ansvaret för att personuppgifterna i den gemensamma mappen gallras i rätt tid och i enlighet med tillämpliga bestämmelser. I denna del förenklas saken av att myndigheternas gallringsbestämmelser i princip ser likadana ut. Eftersom den gemensamma mappen ligger på Säkerhetspolisens server ligger det nära till hands att ge Säkerhetspolisen ansvar för gallringen av uppgifterna där. Därutöver skulle myndigheterna även kunna komma överens om vem som ska ansvara för att åtgärder vidtas när personuppgifter är oriktiga eller behandlas på ett otillåtet sätt, dvs. vem som ska rätta, blockera eller utplåna sådana uppgifter. Även här tror vi att ansvaret för att vidta sådana åtgärder i

den gemensamma mappen skulle kunna åläggas en myndighet när det väl har konstaterats att uppgifterna är felaktiga eller har behandlats felaktigt. Precis som när det gäller gallringen skulle Säkerhetspolisen troligtvis vara den myndighet som är bäst lämpad att svara för detta.

Konsekvenser av bedömningen

Ett gemensamt och solidariskt personuppgiftsansvar innebär att de tre myndigheterna inom NCT är solidariskt ansvariga för merparten av de behandlingar som utförs i den gemensamma mappen. Detta solidariska ansvar gäller för alla personuppgifter i den gemensamma mappen oavsett varifrån de ursprungligen kommer, dock med undantag för de uppgifter som FRA och Försvarsmakten inte behandlar med hänsyn till sina preciserade inriktningar. Den märkning av personuppgifter och behandlingar som myndigheterna vidtar i den gemensamma mappen har varit ett sätt att försöka urskilja vilka uppgifter som behandlas av vilken myndighet, för att på så sätt fördela personuppgiftsansvaret. Som tidigare redogjorts för har SIN dock konstaterat att denna märkning inte motsvaras av någon faktiskt begränsning i respektive myndighets möjligheter att bestämma ändamål och medel för behandlingen och att myndigheterna därför inte kan undgå ansvar för de uppgifter där det anges att personal från en annan myndighet har lagt in uppgiften (SIN dnr 324-2014, s. 11). Även vi har gjort bedömningen att den aktuella märkningen inte medför att det tillräckligt tydligt går att urskilja vilken myndighet som har företagit en viss behandling och att personuppgiftsansvaret därför trots märkningen måste anses vara gemensamt och solidariskt.

Vid denna bedömning av personuppgiftsansvaret tappar märkningen av personuppgifter i den gemensamma mappen sitt egentliga syfte. Även om exempelvis en handläggare från Säkerhetspolisen har lagt in en viss personuppgift i den gemensamma mappen är alla tre myndigheterna solidariskt ansvariga för de behandlingar av uppgiften som därefter sker och en eventuell märkning av uppgifterna fyller därmed egentligen inte någon funktion. Om myndigheterna dessutom förtydligar och så långt som möjligt fördelar de uppgifter som följer av det gemensamma ansvaret torde det eventuella behovet av

märkningen bli ännu mindre. Det är dock möjligt att det kan finnas en viss fördel med att veta från vilken myndighet en personuppgift härstammar, bl.a. av det skälet att den myndigheten har bäst möjlighet att se till att uppgiften är korrekt. Vi tror dock att myndigheterna kan avgöra detta utan en speciell märkning av personuppgiften. Merparten av uppgifterna i rapporterna, även personuppgifterna, åtföljs t.ex. av referenser till källor där det går att utläsa vilken myndighet som uppgiften kommer ifrån. Även i det arbetsmaterial som ligger i den gemensamma mappen torde det vara möjligt för myndigheterna att utläsa varifrån en viss uppgift kommer. Vi ser därför inte att det är nödvändigt att fortsätta med märkningen av personuppgifterna enbart för att ange varifrån uppgifterna kommer.

Vi gör således bedömningen att en märkning av personuppgifterna i den gemensamma mappen inte fyller något egentligt syfte. Som vi ser det finns det därför inte någon anledning för myndigheterna att i den rådande situationen fortsätta med denna rutin. Att manuellt logga personuppgifter på detta sätt och försäkra sig om att loggningen i varje situation blir korrekt utförd är svårt och tar tid i anspråk från den huvudsakliga verksamheten. Om myndigheterna skulle kunna upphöra med märkningen skulle det således innebära en förenkling och effektivisering av verksamheten.

7.3.5 Sammanfattning

När det gäller personuppgiftsansvaret i den gemensamma mappen är det vår bedömning att varje myndighet inom NCT-samarbetet som huvudregel är ansvarig för den behandling av personuppgifter som myndigheten utför inom samarbetet. För det fall det inte går att urskilja vilken myndighet som har utfört en specifik behandling och det inte heller på annat sätt går att urskilja någon tydlig fördelning av ansvaret får det anses föreligga ett gemensamt solidariskt personuppgiftsansvar för den behandlingen.

Mot bakgrund av vad som framkommit om NCT-myndigheternas personuppgiftsbehandling i den gemensamma mappen, anser vi att det inte finns ett sådant behov av förtydliganden vad gäller personuppgiftsansvaret att lagstiftningsåtgärder behöver vidtas för att åstadkomma en förändring. Ett gemensamt och solida-

riskt personuppgiftsansvar kan dock i vissa fall framstå som otydligt, både inom myndigheterna och utåt mot allmänheten. Vi anser därför att den närmare innebörden av ett sådant personuppgiftsansvar bör förtydligas. Detta kan exempelvis ske genom att myndigheterna i en överenskommelse tydliggör den praktiska innebörden av det gemensamma personuppgiftsansvaret och fördelar de uppgifter som ansvaret innefattar.

7.4 Regleringen i övrigt när det gäller behandlingen av personuppgifter i den gemensamma mappen

Bedömning: Merparten av de bestämmelser som aktualiseras vid behandlingen av personuppgifter i den gemensamma mappen ser likadana ut i NCT-myndigheternas registerförfattningar, däribland bestämmelserna om gallring. De få avvikelser som förekommer är inte av sådan karaktär att det medför några större problem vid myndigheternas behandling av personuppgifter i den gemensamma mappen. Det finns därför inget behov av att i dessa delar införa något förtydligande författningsstöd i myndigheternas registerförfattningar.

Skälen för bedömningen

Inledning

Inom NCT samarbetar tre olika myndigheter som styrs av tre olika registerförfattningar. Enligt vår bedömning får det anses föreligga ett gemensamt och solidariskt personuppgiftsansvar för den behandling som förekommer i den s.k. gemensamma mappen om det inte går att urskilja vem som har företagit en viss behandling och det inte heller på annat sätt går att urskilja någon tydlig fördelning av ansvaret. Detta får till följd att tre olika regelverk blir tillämpliga på samma behandling. Även om myndigheterna har möjlighet att komma överens om en fördelning av de uppgifter som följer med ansvaret är det ändå de tre registerförfattningarna som reglerar behandlingen av personuppgifter i den gemensamma mappen. Det finns därför anledning att i detta sammanhang överväga om de

bestämmelser som aktualiseras vid personuppgiftsbehandlingen i den gemensamma mappen ser likadana ut i de olika registerförfattningarna eller inte och vad detta i så fall får för konsekvenser för samarbetet.

Grundläggande bestämmelser

I stora delar är NCT-myndigheternas registerförfattningar relativt lika. Det som främst skiljer dem åt är av naturliga skäl ändamålsbestämmelserna. Vi återkommer till detta i avsnitt 7.5. De grundläggande kraven på behandling av personuppgifter regleras på samma sätt i myndigheternas registerförfattningar som i personuppgiftslagen, med undantag för bestämmelserna om bevarande och gallring (se nedan). De grundläggande bestämmelserna är alltså likartade i alla tre författningarna. Säkerhetspolisen, FRA och Försvarsmakten är således alla skyldiga att bl.a. se till att personuppgifter behandlas på ett korrekt sätt och i enlighet med god sed, att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål, att de personuppgifter som behandlas är riktiga samt adekvata och relevanta i förhållande till ändamålen med behandlingen samt att inte fler personuppgifter behandlas än som är nödvändigt.

Känsliga personuppgifter m.m.

Även behandlingen av känsliga personuppgifter och personnummer samt sökbegränsningar regleras på samma sätt i de tre registerförfattningarna. Ingen av myndigheterna får behandla personuppgifter enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Om uppgifter om en person behandlas på annan grund får de dock kompletteras med sådana uppgifter när det är absolut nödvändigt för syftet med behandlingen. Vid sökning får sådana känsliga personuppgifter användas som sökbegrepp endast om det är absolut nödvändigt för syftet med behandlingen. Vidare får uppgifter om personnummer eller samordningsnummer hos de tre myndigheterna bara behandlas när det är klart motiverat med hänsyn till ändamålet med behand-

lingen, vikten av en säker identifiering eller något annat beaktansvärt ändamål. I alla tre författningarna anges vidare att tillgången till personuppgifter ska begränsas till vad var och en behöver för att kunna fullgöra sina arbetsuppgifter.

Information, rättelse och skadestånd m.m.

När det gäller information till den registrerade samt rättelse och skadestånd hänvisar PDL till motsvarande bestämmelser i PuL. I PuL UNDSÄK och FRA-PuL har lagstiftaren i stället valt att skriva ut dessa bestämmelser. Bestämmelserna i dessa författningar motsvarar dock bestämmelserna i PuL, vilket innebär att regleringen är densamma för alla tre myndigheterna. Detsamma gäller bestämmelserna om säkerhet vid behandlingen. Alla tre myndigheterna är således skyldiga att till var och en som ansöker om det en gång per kalenderår gratis lämna besked om huruvida personuppgifter som rör den sökande behandlas eller inte. Detta gäller dock inte i den utsträckning sekretess hindrar att uppgifterna lämnas ut till den registrerade. För FRA:s del har det emellertid i författningen inte tagits in någon bestämmelse som reglerar informationsskyldighet då uppgifter samlas in från den registrerade personen själv. För Försvarsmaktens del finns en sådan bestämmelse, men denna gäller bara inom den militära säkerhetstjänsten. Anledningen till detta är att det i princip aldrig samlas in några uppgifter från de registrerade personerna själva i FRA:s försvarsunderrättelse- och utvecklingsverksamhet verksamhet eller i Försvarsmaktens försvarsunderrättelseverksamhet. Om inhämtning från enskilda någon gång sker i Försvarsmaktens försvarsunderrättelseverksamhet bedrivs denna verksamhet under sådana förhållanden att undantag från informationsskyldigheten pga. sekretess alltid gäller (prop. 2006/07:46 s. 87). Alla tre myndigheterna är dock skyldiga att på begäran av den registrerade snarast rätta, blockera eller utplåna sådana personuppgifter som inte har behandlats i enlighet med lagen eller föreskrifter som meddelats med stöd av lagen samt att ersätta den registrerade för skada och kränkning av den personliga integriteten som en behandling i strid med lagen eller föreskrifter som meddelats med stöd av lagen har orsakat. Myndigheterna är också skyldiga att vidta lämpliga tekniska och

organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Gallring

När det gäller gallring av personuppgifter är huvudregeln i alla tre registerförfattningarna att personuppgifter ska gallras så snart uppgifterna inte längre behövs för det ändamål för vilket de behandlas. Detta framgår av 6 kap. 6 § PDL, 6 kap. 1 § PuL UNDSÄK och 6 kap. 1 § FRA-PuL. I myndigheternas registerförfattningar finns det dock mer preciserade gallringsbestämmelser beroende på vilken typ av uppgifter det rör sig om. För att kunna avgöra vilka regler om gallring hos myndigheterna som gäller för uppgifterna i den gemensamma mappen måste man därför först ta ställning till hur uppgifterna i den gemensamma mappen ska bedömas utifrån varje myndighets perspektiv.

Inledningsvis kan konstateras att de delar av den gemensamma mappen som enbart innehåller administrativa dokument och metoddokument torde falla utanför de tre registerförfattningarnas tillämpningsområde, dvs. den behandling som sker där kan inte anses ske i Säkerhetspolisens brottsbekämpande verksamhet eller i Försvarsmaktens eller FRA:s försvarsunderrättelseverksamhet. I förarbetena till PuL UNDSÄK och FRA-PuL anges uttryckligen att författningsregleringen inte ska omfatta behandling av personuppgifter i samband med de interna och administrativa åtgärder som kan förekomma i myndigheternas verksamhet (prop. 2006/07:46, s. 47). PDL tar sin utgångspunkt i Säkerhetspolisens uppgifter enligt polislagen (1984:387) och myndighetens administrativa arbete regleras inte där. Behandlingen, och därmed också gallringen, av eventuella personuppgifter i denna del av den gemensamma mappen torde därmed för alla tre myndigheterna styras av PuL.

Säkerhetspolisen har förklarat att uppgifterna i den gemensamma produktionsmappen, dvs. den mapp där rapportutkasten med tillhörande arbetsmaterial lagras, enligt myndighetens bedömning är att anse som gemensamt tillgängliga i PDL:s mening och att mappen är att bedöma som en uppgiftssamling för bearbetning och analys. Personuppgifter som behandlas i en sådan uppgiftssamling ska enligt 6 kap. 12 § andra stycket PDL gallras senast tre år efter

utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Enligt 6 kap. 14 § PDL får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om att personuppgifter, med avvikelse från 12 §, får bevaras för historiska, statistiska och vetenskapliga ändamål. I 27 § polisdataförordningen (2010:1155) anges att Riksarkivet får meddela föreskrifter om att uppgifter som ska gallras enligt 6 kap. 12 § PDL får bevaras för historiska, statistiska eller vetenskapliga ändamål. Riksarkivet har också meddelat föreskrifter om detta.

När det gäller FRA och Försvarsmakten definieras en uppgiftssamling i deras respektive registerförfattningar som en samling uppgifter som med hjälp av automatiserad behandling används gemensamt. De delar av den gemensamma mappen som omfattas av respektive registerförfattning måste således vara att se som en uppgiftssamling även i dessa myndigheters respektive verksamheter. För FRA:s del gör vi bedömningen att den del av den gemensamma mappen som utgörs av produktionsmappen är att se som en uppgiftssamling för analyser och för Försvarsmaktens del gör vi bedömningen att motsvarande del av den gemensamma mappen är att se som en uppgiftssamling för försvarsunderrättelseverksamhet.

För Försvarsmaktens del finns det i 3–5 §§ PuF UNDSÄK preciserade gallringsbestämmelser för uppgifter som behandlas i olika uppgiftssamlingar. Några sådana preciserade gallringsbestämmelser finns dock inte när det gäller uppgifter som behandlas i en uppgiftssamling för försvarsunderrättelseverksamhet. Det är således huvudregeln i 6 kap. 1 § PuL UNDSÄK som är tillämplig på dessa uppgifter. Enligt 12 § PuF UNDSÄK får Riksarkivet meddela föreskrifter om att uppgifter och handlingar som ska gallras enligt 6 kap. 1 § PuL UNDSÄK ska bevaras. Detta har Riksarkivet gjort.

För FRA:s del finns det i 2 § och i 5 och 6 §§ FRA-PuF preciserade gallringsbestämmelser för uppgifter som behandlas i vissa uppgiftssamlingar. Några sådana preciserade gallringsbestämmelser finns dock inte när det gäller uppgifter som behandlas i en uppgiftssamling för analyser. Enligt 12 § FRA-PuF får Riksarkivet meddela föreskrifter om att uppgifter och handlingar som ska gallras enligt 6 kap. 1 § FRA-PuL ska bevaras. Riksarkivet har inte meddelat några föreskrifter om bevarande av uppgifter i uppgiftssamlingar för analyser.

Huvudregeln för alla tre myndigheterna är således, enligt vår bedömning, att personuppgifterna i den gemensamma produktionsmappen ska gallras när de inte längre behövs för något av de ändamål som de behandlas för. Som framgår ovan finns det dock i PDL en tidsgräns för när uppgifterna i den gemensamma mappen senast måste gallras, vilket inte finns i övriga registerförfattningar. Säkerhetspolisen har uppgett att uppgifterna i produktionsmappen i praktiken inte sparas så länge som tre år. Den preciserade gallringsbestämmelsen i PDL utgör därför inte något problem i praktiken. Vår bedömning är således att det är likartade regler som gäller för gallringen av personuppgifterna i den gemensamma produktionsmappen hos alla tre myndigheterna. Som framgår av redogörelsen i kapitel 6 gallras också personuppgifterna i mappen i enlighet med dessa bestämmelser.

I den mån det i den gemensamma mappen i övrigt, dvs. utanför produktionsmappen, lagras material eller uppgifter som skulle kunna omfattas av myndigheternas registerförfattningar, torde huvudregeln att eventuella personuppgifter ska gallras när de inte längre behövs för något av de ändamål som de behandlas för, gälla även för en sådan samling av uppgifter. Den preciserade gallringsbestämmelsen i 6 kap. 12 § första stycket PDL, vilken anger att personuppgifter som har gjorts gemensamt tillgängliga i Säkerhetspolisens verksamhet ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes, borde inte heller här utgöra något hinder för gallringen av personuppgifter i mappen.

För Försvarsmaktens och Säkerhetspolisens del har Riksarkivet emellertid meddelat föreskrifter som anger att vissa uppgifter som ska gallras enligt ovan ska bevaras för historiska, statistiska och vetenskapliga ändamål (se Riksarkivets föreskrifter RA-MS 2014:38 och RA-MS 2015:61). Dessa uppgifter får således inte gallras i Försvarsmaktens och Säkerhetspolisens verksamhet. När det gäller skyldigheten att bevara uppgifter på detta sätt borde det dock vara tillräckligt att ursprungsmaterialet bevaras. De uppgifter som ligger i den gemensamma mappen har hämtats från myndigheternas egna system och det är där som ursprungsuppgifterna förvaras. Vår bedömning är således att det borde vara tillräckligt att Säkerhetspolisen och Försvarsmakten tillämpar Riksarkivets föreskrifter på uppgifterna i sina egna system och ser till att uppgifterna bevaras

där. Vid sådana förhållanden påverkas inte gallringen i den gemensamma mappen närmare. Det skulle dock kunna vara så att några av de uppgifter eller sammanställningar som finns i den gemensamma mappen har den karaktären att de även om ursprungsmaterialet finns någon annanstans bör bevaras enligt Riksarkivets föreskrifter. Om dessa uppgifter omfattas av de aktuella föreskrifterna från Riksarkivet måste Säkerhetspolisen och Försvarsmakten i sådana fall, innan uppgifterna i den gemensamma mappen gallras, ta om hand och bevara dessa uppgifter i sin verksamhet. Uppgifterna behöver således inte bevaras i den gemensamma mappen, utan kan arkiveras någon annanstans. Vi bedömer att de föreskrifter som har meddelats av Riksarkivet inte påverkar frågan om gallring i den gemensamma mappen närmare, utan främst blir en fråga för de berörda myndigheterna att hantera. För att helt säkerställa att uppgifter som eventuellt omfattas av Riksarkivets föreskrifter inte gallras bör rimligtvis en dialog föras mellan myndigheterna inför förestående gallring.

Behandling av personuppgifter i uppgiftssamlingar

I myndigheternas registerförfattningar finns också vissa bestämmelser som närmare reglerar behandlingen av personuppgifter i uppgiftssamlingar. Dessa bestämmelser kan aktualiseras vid behandlingen av personuppgifter i den gemensamma mappen. I 6 kap. 9 § PDL anges exempelvis att det vid behandling av personuppgifter som har gjorts gemensamt tillgängliga genom en särskild upplysning eller på annat sätt ska framgå för vilket närmare ändamål personuppgifterna behandlas. Av 6 kap. 10 § PDL framgår att om sådana uppgifter direkt kan hänföras till en person som inte är misstänkt för brott eller för att ha utövat eller kan komma att utöva brottslig verksamhet ska det genom en särskild upplysning eller på något annat sätt framgå att personen inte är misstänkt. Uppgifter om en person som kan antas ha samband med brottslig verksamhet ska förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak. Sådan upplysning behöver dock inte lämnas om det på grund av särskilda omständigheter är onödigt eller om uppgifterna ingår i en samling som har skaptas för att bearbeta och analysera information och som enbart särskilt

angivna tjänstemän har åtkomst till och bearbetningen och analysen befinner sig i ett inledande skede.

En bestämmelse av liknande innebörd finns för Försvarsmaktens del i 2 § PuF UNDSÄK när det gäller uppgiftssamlingar för försvarsunderrättelseverksamhet. Där anges nämligen att en sådan uppgiftssamling endast får innehålla identifieringsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamheten och upplysningar om varifrån den registrerade uppgiften kommer och uppgiftslämnares trovärdighet. Någon liknande reglering finns inte när det gäller FRA:s behandling av personuppgifter i myndighetens uppgiftssamlingar. I 3 § FRA-PuF, som reglerar uppgiftssamlingar för analyser, anges att dessa uppgiftssamlingar enbart får innehålla analysresultat samt bearbetnings- och rapportunderlag.

Inledningsvis kan konstateras att det är upp till respektive myndighet att se till att uppgifterna i den gemensamma mappen behandlas i enlighet med de regler som gäller för gemensamt tillgängliga uppgifter eller uppgiftssamlingar. I det här fallet är det främst Säkerhetspolisen som måste tillämpa vissa specifika bestämmelser på de uppgifter som finns i den gemensamma mappen. Dessa bestämmelser anger att Säkerhetspolisen ska förse vissa uppgifter med en särskild upplysning. Som framgår av ordalydelsen behöver dock informationen inte anges genom en särskild upplysning om denna i stället framgår på något annat sätt. För det fall det exempelvis framgår av omständigheterna för vilket ändamål en uppgift behandlas krävs således inte någon särskild upplysning om detta (prop. 2009/10:85 s. 369 f.). När det gäller uppgifter i den gemensamma mappen torde det i de allra flesta fall framgå av sammanhanget och omständigheterna i övrigt varför uppgifterna behandlas och om den aktuella personen är misstänkt för brott eller inte. En särskild upplysning om detta torde därför sällan behöva införas i den gemensamma mappen. Säkerhetspolisen behöver dock se till att uppgifter i den gemensamma mappen om en person som kan antas ha samband med misstänkt brottslig verksamhet förses med en upplysning om uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak, om detta inte på grund av särskilda omständigheter är onödigt. Vi ser emellertid inte att denna uppgift

för Säkerhetspolisen medför några problem för myndigheternas användning av den gemensamma mappen.

7.5 Ändamålsbestämmelser gällande behandlingen av personuppgifter i den gemensamma mappen

Bedömning: Säkerhetspolisens, FRA:s och Försvarsmaktens verksamhet inom NCT-samarbetet styrs av ändamålsbestämmelser med samma övergripande innebörd. Det finns därmed inte någon risk att myndigheterna i den gemensamma mappen behandlar personuppgifter i strid med sina respektive ändamålsbestämmelser. Till följd av detta finns det för närvarande inte något behov av att i de befintliga registerförfattningarna införa förtydligande ändamålsbestämmelser för Säkerhetspolisens, FRA:s och Försvarsmaktens verksamhet inom NCT-samarbetet.

Skälen för bedömningen

Ändamålsbestämmelsernas betydelse vid gemensam behandling av personuppgifter

Som konstaterats ovan deltar myndigheterna i NCT-samarbetet utifrån sitt respektive uppdrag. Utgångspunkten har därför varit att de ändamålsregleringar som styr behandlingen av personuppgifter i den egna verksamheten är tillräckliga och ändamålsenliga även för den verksamhet som myndigheterna bedriver inom NCT-samarbetet. I enlighet med detta har vi också gjort bedömningen att den behandling av personuppgifter som myndigheterna utför i de egna systemen och de myndighetsspecifika och personliga mapparna är förenlig med respektive registerförfattnings ändamålsbestämmelser och även sker i enlighet med dessa regler i övrigt. Vi har vidare gjort bedömningen att det utlämnande av uppgifter som sker mellan myndigheterna har stöd i respektive registerförfattnings bestämmelser. Till skillnad från många andra samarbeten handlar NCT-samarbetet emellertid inte enbart om att utbyta information. Handläggarna vid NCT-myndigheterna arbetar också

tillsammans i en gemensam area där de gemensamt tar fram rapporter med bedömningar av terrorhotet mot Sverige och svenska intressen med hjälp av underlag från de tre myndigheterna. Frågan är vad denna gemensamma behandling får för betydelse för tillämpningen av ändamålsbestämmelserna.

När handläggarna från myndigheterna arbetar i sin egen myndighets system eller i de NCT-mappar som bara de själva eller myndighetens personal har tillgång till, behandlar handläggarna i princip bara uppgifter från den egna myndigheten. I dessa situationer styrs de också av olika typer av behörigheter vilket innebär att de bara har tillgång till och kan behandla personuppgifter som behövs för att de ska kunna utföra sina arbetsuppgifter inom NCT. I den gemensamma NCT-mappen lägger myndigheterna in uppgifter från de egna systemen som används vid framtagandet av rapporter. Detta innebär att handläggarna när de därefter arbetar i den gemensamma mappen kan komma att behandla även uppgifter som handläggare från de andra myndigheterna har lagt in i mappen. Eftersom olika registerförfattningar med olika ändamålsbestämmelser gäller för de samarbetande myndigheterna kan man fråga sig om det finns en risk för att myndigheterna då behandlar personuppgifter i strid med sin egen registerförfattning. Personuppgifter som FRA eller Försvarsmakten har fört över till den gemensamma mappen från myndighetens eget system skulle i vart fall teoretiskt kunna vara av den karaktären att de inte behövs i Säkerhetspolisens verksamhet för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terrorbrott. På samma sätt skulle uppgifter som Säkerhetspolisen fört över till mappen kunna vara av sådan karaktär att de inte behövs för att bedriva försvarsunderrättelseverksamhet på det sätt som FRA och Försvarsmakten enligt sin inriktning ska göra. SIN har vid sin granskning av Säkerhetspolisens personuppgiftsbehandling inom NCT påtalat denna risk. Nämnden har vid granskningen dock inte sett att Säkerhetspolisen till följd av detta behandlat några personuppgifter i strid med PDL (SIN dnr 324-2014, s. 11 f.). Frågan är om det ändå finns anledning att på något sätt förtydliga myndigheternas ändamålsbestämmelser så att det tydligt framgår att myndigheterna får behandla personuppgifter i den gemensamma mappen om det behövs för att bedriva verksamheten inom NCT-samarbetet.

NCT-myndigheternas ändamålsbestämmelser

Av 6 kap. 1 § 1 b PDL följer att personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar bl.a. brott mot rikets säkerhet och terrorbrott. I förarbetena betonas att Säkerhetspolisen behöver kunna samla in, sammanställa och analysera uppgifter inom exempelvis kontraterrorismverksamheten även om uppgifterna inte kan hänföras vare sig till något visst konkret brott eller till någon mer konkret definierad brottslig verksamhet. Säkerhetspolisen behöver exempelvis, med utgångspunkt i svenska intressen, följa den politiska utvecklingen i andra länder och verksamheter inom vissa grupper, som kan utgör ett hot mot det svenska samhället eller som kan komma att göra sig skyldiga till terroristbrott. Under ändamålet förebygga, förhindra eller upptäcka brottslig verksamhet faller, enligt förarbetena, bl.a. Säkerhetspolisens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag (prop. 2009/10:85 s. 256 och 362).

FRA och Försvarsmakten får enligt 1 kap. 8 § FRA-PuL och 1 kap. 8 § PuL UNDSÄK behandla personuppgifter i sin försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Detta innebär att det tillåtna ändamålet för myndigheternas behandling av personuppgifter i försvarsunderrättelseverksamheten, är att myndigheterna ska kunna utföra de uppgifter som åligger dem enligt lagen om försvarsunderrättelseverksamhet och den därtill hörande förordningen (prop. 2006/07:46 s. 64). Av lagen om försvarsunderrättelseverksamhet framgår att försvarsunderrättelseverksamhet ska bedrivas till stöd för svensk utrikes-, säkerhets- och försvarspolitik samt i övrigt för kartläggning av yttre hot mot landet. Det anges vidare att försvarsunderrättelseverksamhet endast får avse utländska förhållanden. FRA bedriver sin försvarsunderrättelseverksamhet genom signalspaning och styrs således också av lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet. Där anges att signalspaning i försvarsunderrättelseverksamhet får ske bl.a. i syfte att kartlägga strategiska förhållanden avseende internationell terrorism och annan grov

gränsöverskridande brottslighet som kan hota väsentliga nationella intressen.

Utöver bestämmelserna i de ovan angivna lagarna styrs FRA:s och Försvarsmaktens verksamhet av regeringens årliga inriktning, vilken ytterligare avgränsar de ändamål för vilka verksamheten får bedrivas. För FRA:s del anges vidare i lagen om signalspaning i försvarsunderrättelseverksamhet att inriktning av signalspaning får anges förutom av regeringen, av Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen i Polismyndigheten. Dessa myndigheter lämnar således närmare inriktning till FRA inom ramen för regeringens inriktning. Inom Försvarsmakten inriktar överbefälhavaren Must ytterligare vad gäller Försvarsmaktens underrättelsebehov. Därutöver producerar både FRA och Försvarsmakten/Must interna styrdokument där en ytterligare precisering i förhållande till övriga inriktningar görs. För FRA:s del beslutas denna preciserade inriktning årligen av FRA:s generaldirektör. Inriktningen anger prioriterade och konkretiserade underrättelseuppgifter som underrättelseavdelningarna ska utföra under året. För Musts del preciseras regeringens inriktning närmare i en inhämtandeplan. Både de i lagen om försvarsunderrättelseverksamhet angivna ändamålen samt de ändamål som återfinns i regeringens inriktning utgör avgränsningar – inte bara för själva försvarsunderrättelseverksamheten – utan också för behandlingen av personuppgifter hos FRA och Försvarsmakten. Därutöver har det i ändamålsbestämmelserna i FRA-PuL och PuL UNDSÄK gjorts ytterligare en avgränsning genom att det där anges att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen. Med preciserad inriktning avses de interna inriktningar som FRA och Försvarsmakten/Must fastställer för närmare avgränsning av verksamheten. Vilken grad av anknytning en person ska ha till en preciserad inriktning får avgöras från fall till fall. Av motiven framgår dock att det i vart fall måste finnas en sådan koppling mellan personen och den företeelse som verksamheten syftar till att kartlägga, exempelvis internationell terrorism, att man i efterhand kan kontrollera att personuppgiftsbehandlingen är motiverad av verksamhetsskäl och kan hänföras till en viss preciserad inriktning (prop. 2006/07:46 s. 65 f.).

Innebörden av ändamålsbestämmelserna

När flera myndigheter samarbetar och behandlar personuppgifter i en gemensam area som alla myndigheterna både har tillgång till och överför uppgifter till är det en fördel om myndigheterna styrs av liknande ändamålsbestämmelser. På så sätt riskerar myndigheterna inte att behandla personuppgifter i strid med de egna ändamålsbestämmelserna. Som framgår ovan styrs NCT-myndigheterna av olika ändamålsbestämmelser, dvs. ändamålsbestämmelserna är utformade på olika sätt och placerade i olika regelverk. De bestämmelser som reglerar FRA:s och Försvarsmaktens personuppgiftsbehandling inom försvarsunderrättelseverksamheten är dock likalydande. Frågan är om det till följd av detta finns en risk att NCT-myndigheterna när de behandlar personuppgifter i den gemensamma mappen gör detta i strid med de egna ändamålsbestämmelserna.

Som tidigare har redovistas är NCT:s uppgift att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt. Detta inkluderar strategiska analyser av händelser, trender, fenomen och omvärldsutveckling med koppling till terrorism. NCT:s bedömningar syftar till att ge tidig förvarning om utvecklingen inom terrorism som berör, eller kan komma att beröra, Sverige och svenska intressen. Syftet med NCT:s verksamhet är att stärka den samlade förmågan hos Säkerhetspolisen, Försvarsmakten och FRA att genomföra dessa strategiska bedömningar till stöd för Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorism. Det övergripande syftet med NCT:s verksamhet är således att förebygga och förhindra terrorism.

Som framgår ovan får Säkerhetspolisen behandla personuppgifter i sin brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar bl.a. brott mot rikets säkerhet och terrorbrott. Av förarbetena framgår att det som bl.a. avses är Säkerhetspolisens kartläggning och kontroll av personer, företeelser och annat som kan belysa riskerna för brott av nu aktuellt slag.

FRA och Försvarsmakten får behandla personuppgifter om det behövs för att bedriva försvarsunderrättelseverksamhet. Denna verksamhet begränsas som framgår ovan av regeringens inriktning

samt de mer preciserade inriktningar som beslutas internt av FRA och Försvarsmakten.

Inom Försvarsmakten har Must till uppgift att identifiera, bevaka och bedöma yttre hot mot Sverige och svenska intressen i utlandet. Ett av de yttre hot som Must bevakar och rapporterar om är terrorism. På uppdrag från regeringen inhämtar och bearbetar Must information om internationella terroristgrupper och deras nätverk i syfte att dels förse regeringen och Regeringskansliet med underrättelser om och bedömningar av den internationella terrorismens utveckling, dels stödja de samverkande nationella myndigheterna i sitt arbete att motverka terrorism. Försvarsmakten/Must får således behandla personuppgifter för dessa ändamål.

FRA får bedriva signalspaning endast i de fall regeringen eller annan utpekad myndighet har bestämt inriktningen av signalspaningen. Signalspaning får därtill ske endast för vissa i lag angivna ändamål, bl.a. för att kartlägga strategiska förhållanden avseende internationell terrorism som kan hota väsentliga nationella intressen. Enligt uppgift från företrädare för FRA sammanfaller det i författningen angivna ändamålet och de ändamål som återfinns i regeringens inriktning. FRA får således behandla personuppgifter om det behövs för att kartlägga strategiska förhållanden avseende internationell terrorism som kan hota väsentliga nationella intressen. Som framgår ovan inriktas FRA närmare även av Försvarsmakten och Säkerhetspolisen. Dessa myndigheter har inte möjlighet att inrikta FRA utanför regeringens inriktning, utan har att hålla sig inom ramen för de ändamål som regeringen bestämmer. Den ytterligare begränsning av ändamålen som dessa inriktningar innebär torde därför inte påverka FRA:s möjligheter att behandla personuppgifter i syfte att kartlägga strategiska förhållanden avseende internationell terrorism närmare. Det torde vidare ligga i både Säkerhetspolisens och Försvarsmaktens intresse att inom ramen för regeringens inriktning styra FRA:s verksamhet på sådant sätt att myndigheten kan bistå dem i arbetet med att motverka terrorism.

Även om ändamålsbestämmelserna i myndigheternas registerförfattningar är utformade på olika sätt och FRA och Förvarsmakten måste hålla sig inom försvarsunderrättelseverksamhetens ramar och därtill hörande regler, styrs myndigheterna indirekt av likalydande ändamålsbestämmelser. När det gäller FRA:s och För-

svarsmaktens bestämmelser har dessa utformats med beaktande av att det inte ansetts möjligt att detaljreglera denna verksamhet i lag. I förarbetena anges att ändamålsbestämmelserna därför oundvikligen lämnar ett visst mått av utrymme för myndigheterna att bedöma om en behandling ryms inom det angivna ändamålet eller inte (se prop. 2006/07:46 s. 64). För FRA:s och Försvarsmaktens del måste man således, med tanke på hur ändamålsbestämmelserna är utformade, beakta vad som i praktiken innefattas i deras respektive verksamheter. Mot bakgrund av detta anser vi att Säkerhetspolisens, FRA:s och Försvarsmaktens verksamhet inom ramen för NCT-samarbetet i praktiken styrs av ändamålsbestämmelser med samma innebörd. Vår bedömning är därmed att det inte finns någon risk att myndigheterna i den gemensamma mappen behandlar personuppgifter i strid med sina respektive ändamålsbestämmelser. Det finns därför inte heller skäl att i de befintliga registerförfattningarna införa förtydligande ändamålsbestämmelser för myndigheternas verksamhet inom NCT-samarbetet.

Även om vi inte ser någon risk för att myndigheternas personuppgiftsbehandling kommer i konflikt med de respektive ändamålsbestämmelserna, är det möjligt att man i och för sig skulle kunna uppnå en något större tydlighet om det fanns enhetliga ändamålsbestämmelser utformade specifikt för NCT-samarbetet. Att införa sådana ändamålsbestämmelser skulle emellertid kunna få den följden att FRA och Försvarsmakten, inom NCT-samarbetet, skulle få behandla personuppgifter som de inte får behandla inom sina respektive verksamheter i övrigt. Enhetligt utformade ändamålsbestämmelser för samarbete skulle nämligen, som vi ser det, inte kunna knytas till regleringen av försvarsunderrättelseverksamheten på det sätt som nu har gjorts i FRA:s och Försvarsmaktens registerförfattningar. Sådana förändringar kräver noggranna överväganden av principiell karaktär, ett arbete som inte ryms inom detta uppdrag. Här bör också beaktas att en översikt av de aktuella registerförfattningarna för närvarande pågår eller inom kort ska påbörjas. Mot bakgrund av detta, och då vi inte anser att de befintliga ändamålsbestämmelserna utgör något hinder för verksamheten, har vi inte närmare övervägt några sådana förändringar.

8 Ett effektivare informationsutbyte

8.1 Inledning

Vårt uppdrag har innefattat två delar. Förutom att analysera de rättsliga förutsättningarna för myndigheternas personuppgiftsbehandling inom ramen för NCT-samarbetet, har vi också fått i uppdrag att undersöka hur informationsutbytet inom samarbetet kan effektiviseras. Frågan om ett effektivare informationsutbyte inom NCT-samarbetet utgör således den andra delen av uppdraget. Vårt arbete i den här delen har gått ut på att analysera och överväga olika sätt att effektivisera informationsutbytet för att slutligen föreslå det vi anser mest lämpligt med beaktande av både effektivitetsskäl och integritetsskäl.

I denna del av arbetet har vi tagit vår utgångspunkt i den beskrivning av verksamheten vid NCT och de samarbetande myndigheterna som framgår av tidigare avsnitt. Vi har också tagit del av skriftliga och muntliga synpunkter från företrädare för NCT och de tre myndigheterna. En fråga som lyfts särskilt i den här delen av uppdraget är frågan om direktåtkomst. Av uppdraget framgår att vi särskilt ska undersöka i vilken utsträckning Säkerhetspolisen ska kunna medge övriga myndigheter inom NCT direktåtkomst till uppgifter som är gemensamt tillgängliga för NCT-samarbetet i Säkerhetspolisens verksamhet. Under arbetets gång har även fråga uppkommit om behovet för FRA och Försvarsmakten att på samma sätt kunna medge övriga myndigheter inom samarbetet direktåtkomst till uppgifter i sina respektive verksamheter. Så som uppdraget har formulerats har det således varit inriktat mot en effektivisering av uppgiftsutbytet genom direktåtkomst. Vi har dock varit oförhindrade att inom ramen för uppdraget föreslå även andra åtgärder för att öka effektiviteten inom samarbetet. I detta avsnitt

redovisar vi våra förslag samt de överväganden och bedömningar som ligger bakom förslagen.

8.2 Behovet av ett effektivt informationsutbyte mellan myndigheterna inom NCT-samarbetet

Bedömning: Det finns behov av att effektivisera det informationsutbyte som förekommer inom NCT-samarbetet i dag.

Skälen för bedömningen

Regeringens strategi mot terrorism

Arbetet med att motverka terrorism följer inte traditionella gränsdragningar mellan svenska myndigheter och kräver därför ett nära myndighetssamarbete. I regeringens strategi mot terrorism (skr. 2014/15:146 Förebygga, förhindra och försvåra – den svenska strategin mot terrorism, s. 3) har regeringen påtalat att det behöver göras mer för att bekämpa terrorism och att myndigheter som länge arbetat för att motverka terrorism måste bli ännu mer effektiva i sitt arbete. I takt med att fler aktörer deltar i arbetet med att bekämpa terrorism blir samverkan enligt regeringen än viktigare. Regeringen har i strategin betonat behovet av ökad samverkan och samordning mellan alla berörda aktörer och det anges att regeringen ska verka för att myndigheterna har de verktyg de behöver för att kunna utföra sina respektive uppdrag och samverka med berörda myndigheter eller aktörer (nämnda skrivelse, s. 6). Enligt regeringen är tillgången till information en grundläggande förutsättning för myndigheternas möjligheter att förhindra terroristbrottslighet. Myndigheterna måste vidare ha tillgång till adekvat information i rätt tid och de måste också ha möjlighet att bearbeta och analysera denna information. Möjlighet till samverkan och informationsutbyte, såväl på strategisk nivå som i den operativa verksamheten, är enligt regeringens uppfattning därför av stor vikt (nämnda skrivelse, s. 15).

Utvecklingen av den internationella terrorismen

I regeringens skrivelse 2015/16:74, 2015 års redogörelse för tillämpningen av lagen om särskild utlänningskontroll, redogörs för utvecklingen av den internationella terrorismen. Där framgår att terrorhotet, sedan början av 2000-talet, internationellt sett främst utgörs av aktörer motiverade av våldsbejakande islamistisk extremism. Under 1990-talet och i början av 2000-talet var våldsbejakande islamistiska nätverk i Sverige huvudsakligen inriktade på att ge finansiellt och logistiskt stöd till våldsfrämjande islamistiska internationella terroristnätverk och stridande grupperingar utomlands med antingen lokal, regional eller, en under senare tid alltmer framväxande och därtill dominerande, global agenda. Med start i början av 2000-talet började dock individer i den våldsfrämjande islamistiska miljön i Sverige i allt större utsträckning ta aktiv del i terrorrelaterade våldshandlingar, i huvudsak genom resor till konfliktområden där internationella terrornätverk är närvarande, t.ex. Afghanistan, Somalia och Jemen. I skrivelsen anges att Syrien och Irak sedan 2012 har kommit att bli de konfliktområden som individer från Sverige främst reser till för att ansluta sig till våldsbejakande islamistiska grupper. Resandet från Sverige till Syrien och Irak för att delta i terrorrelaterad träning och strid har varit exceptionellt omfattande i förhållande till tidigare trender och det finns, enligt regeringen, inga indikationer på att denna typ av resande kommer att avta i närtid (skr. 2015/16:74, s. 5 f.).

Av ovan nämnda redogörelse framgår att Sverige sedan 2008 har fått en ökad negativ uppmärksamhet bland förespråkare av global våldsbejakande islamism, framför allt p.g.a. upplevda kränkningar av islam. Detta har sedan dess präglat motivbilden vid attentatsplanering och attentatsförsök. Hotbilden mot Danmark och övriga Skandinavien anses också vara relevant i detta avseende då Skandinavien ibland betraktas som en enhet i våldsbejakande islamistiska miljöer. Man menar också att upplevda militära aggressioner mot muslimska länder sannolikt även hör till motivbilden. Sveriges internationella militära engagemang, exempelvis insatsen i Afghanistan, har medfört att Sverige uppfattas som ett legitimt mål i den våldsbejakande islamistiska kontexten (nämnda skrivelse, s. 6).

Sommaren 2014 inledde den USA-ledda koalitionen ett militärt ingripande mot våldsbejakande islamistiska mål i Irak och därefter

Syrien. Ledande personer inom dessa nätverk och grupper uppmanade då enskilda individer i västvärlden att genomföra attentat mot mål i västerländska länder. Båda dessa omständigheter har lett till att det nu bedöms kunna skönjas ett ökat stöd för den globala våldsfrämjande islamismen samt en ökad attentatsavsikt hos enskilda individer och grupper världen över. Denna utveckling kan, enligt regeringen, också komma att påverka attentatsavsikten hos individer i Sverige mot svenska mål (nämnda skrivelse, s. 6). Enligt uppgift från företrädare för Säkerhetspolisen har antalet attentat mot västerländska mål, bl.a. i Europa, också ökat påtagligt sedan sommaren 2014.

Sedan 2010 har antalet attentat och attentatshot med koppling till Sverige, samt svenska individers inblandning i attentat och attentatsplanering i andra länder, ökat. Under samma tid har Sverige i större utsträckning kommit att omnämnas som ett legitimt attentatsmål. Hösten 2010 höjdes därför hotnivån avseende terrorhotet mot Sverige för första gången till förhöjt hot, nivå tre på en femgradig skala. Hotet låg sedan kvar på den nivån fram till den 18 november 2015 då hotnivån höjdes från förhöjt till högt hot, dvs. från tre till fyra på den femgradiga skalan (nämnda skrivelse, s. 7). Den 2 mars 2016 beslutades emellertid att terrorhotnivån skulle återgå till den förhöjda hotnivå som rått i Sverige sedan hösten 2010.

Enligt Säkerhetspolisen har utvecklingen på terrorområdet internationellt, den våldsbejakande islamismens alltmer globala karaktär och ambitioner, samt utvecklingen relaterat till miljöer och individer i Sverige, sammantaget medfört ett ökat behov av nära samverkan på både strategisk, taktisk och operativ nivå. En viktig del i detta är möjligheten för de ansvariga myndigheterna att kunna utbyta relevant information i syfte att bedöma hoten både sammantaget och från enskilda individer och nätverk, för att i förlängningen kunna förhindra terrorverksamhet.

Andra myndighetsöverskridande samarbeten

Olika former av samverkan mellan myndigheter har blivit allt vanligare. Bakgrunden till detta är bl.a. att regeringen genom regleringsbrev och separata regeringsuppdrag uppmanat myndigheterna att samverka och att effektivisera den samverkan som redan finns

etablerad. Det är sedan länge en självklar princip att alla myndigheter är skyldiga att samarbeta och bistå varandra i den utsträckning det kan ske. Principen kommer bl.a. till uttryck i 6 § förvaltningslagen (1986:223) där det anges att varje myndighet ska lämna andra myndigheter hjälp inom ramen för den egna verksamheten. Samarbete mellan myndigheter kan ske mer eller mindre formaliserat. Det förekommer samarbeten i allt från tydliga och långsiktiga samverkansstrukturer till tillfälliga bilaterala kontakter mellan olika myndigheter.

Inom den brottsbekämpande och brottsförebyggande sektorn förekommer myndighetsövergripande samarbeten på många olika håll. Det är naturligt och nödvändigt att de brottsbekämpande myndigheterna samarbetar på olika sätt för att bekämpa brottslighet. För att på ett effektivt sätt angripa och begränsa brottsligheten krävs dock ett utvecklat samarbete även med andra aktörer. Ett exempel på sådan samverkan är den nationella satsningen mot den grova organiserade brottsligheten. Inom ramen för denna satsning samarbetar ett antal brottsbekämpande och icke brottsbekämpande myndigheter för att förebygga, förhindra eller upptäcka viss organiserad brottslighet. Myndigheterna samverkar inom de områden som respektive myndighets uppdrag och regelverk medger. En stor del av samarbetet handlar om att utbyta information och för att underlätta detta har det i en särskild lag införts en sekretessbrytande uppgiftsskyldighet för myndigheterna inom samarbetet (lag [2016:774] om uppgiftsskyldighet vid samverkan mot viss organiserad brottslighet). Lagen kom till mot bakgrund av de svårigheter som, vid myndighetssamverkan av detta slag, ibland kan föreligga när det gäller att bedöma om sekretessbelagda uppgifter kan utbytas mellan myndigheterna (prop. 2015/16:167 s. 1).

Ytterligare exempel på myndighetsöverskridande samverkan är arbetet i sociala insatsgrupper för att förebygga att unga fastnar i kriminalitet. Inom dessa grupper samarbetar socialtjänsten med Polismyndigheten och andra berörda myndigheter på kommunal nivå för att hjälpa unga som riskerar att bli kriminella. Syftet är att på individnivå möjliggöra att hjälp och stöd från berörda myndigheter och övriga aktörer kan samordnas under ledning av socialtjänsten. Informationsutbytet mellan aktörerna möjliggörs till stor del genom samtycke från den enskilde (Polismyndigheten, Nationella riktlinjer. Polisens arbete i sociala insatsgrupper, 2014, s. 4 f.).

I detta sammanhang bör också Samverkansrådet mot terrorism nämnas. Samverkansrådet mot terrorism är ett nätverk som syftar till att på nationell nivå förbättra samordningen och effektivisera arbetet före, under och efter ett terroristattentat. Rådet har inte någon egen juridisk status eller formellt uppdrag, men har ett uttalat stöd från regeringen. Rådet består av fjorton myndigheter som alla, på olika sätt, har en funktion i arbetet med att motverka eller hantera terrorism. Säkerhetpolisen är sammankallande i rådet. Samverkansrådet mot terrorism bedriver ett strategiskt arbete för att långsiktigt stärka förmågan att motverka och hantera terrorism. Rådet tar årligen fram handlingsplaner med projekt för att utveckla metoder och arbetssätt. Rådet utbildar och övar löpande rådets myndigheter i samverkansfrågor och samverkar kontinuerligt kring kommunikation med allmänhet och medier rörande terrorismfrågor. Arbetet kan dessutom bestå av att identifiera ansvarförhållanden de deltagande myndigheterna emellan, och utbyta erfarenheter med aktörer som inte deltar i Samverkansrådet (http://www.sakerhetspolisen.se/kontraterrorism/samverkansradet-mot-terrorism. Hämtat 2016-07-10).

Verksamheten vid NCT

För att bedöma terrorhotet mot Sverige och svenska intressen, och tillgodose Sveriges strategiska underrättelsebehov, krävs samarbete mellan flera myndigheter. En effektiv terrorbekämpning är resurskrävande, teknikintensiv och kräver hög kompetens hos alla berörda myndigheter. Som tidigare nämnts är syftet med verksamheten inom NCT att stärka den samlade förmågan hos Säkerhetspolisen, Försvarsmakten och FRA att genomföra strategiska bedömningar till stöd för Sveriges förmåga att förebygga, avvärja, hindra och hantera konsekvenserna av terrorism. Samarbetet möjliggör ett tillvaratagande av de tre myndigheternas samlade kompetens. NCT har sedan starten 2005 utvecklats till att bli en nationellt och internationellt erkänd auktoritet på området och NCT:s analyser utgör i dag beslutsunderlag för myndigheter inom Samverkansrådet mot terrorism samt för Regeringskansliet. Regeringen har i sin strategi mot terrorism betonat att NCT fyller en viktig funktion (skr. 2014/15:146 s. 20). Det är därför angeläget att samarbetet

fortsätter och att myndigheterna ges så bra förutsättningar som möjligt att utföra sitt arbete. För att NCT ska kunna leverera relevanta och aktuella strategiska bedömningar krävs att medarbetarnas kompetens tas tillvara fullt ut. Det krävs också att medarbetarna snabbt har tillgång till relevant underrättelseinformation från de tre myndigheterna. Det inkluderar även uppgifter på individnivå, dvs. personuppgifter, vilket är nödvändigt för att medarbetarna vid NCT ska kunna bedöma olika aktörers avsikt och förmåga. Det finns således ett behov hos samtliga medarbetare vid NCT att på ett effektivt sätt kunna ta del av och använda uppgifter från de samarbetande myndigheterna. Detta är viktigt inte minst vid brådskande ärenden kopplade till en ökad risk för attentat mot Sverige eller svenska intressen (Säkerhetspolisens skrivelse Ju2015/05096/L4, s. 8 f.).

Inom NCT-samarbetet utbyter myndigheterna kontinuerligt information med varandra och, som framgår ovan, kan informationen innehålla personuppgifter. Som framgår av kapitel 6.3.6 sker utbytet främst genom att handlingar lämnas ut till respektive myndighet eller genom att handlingar, utan att de lämnas ut, visas för medarbetarna från de andra myndigheterna, dvs. ett slags muntligt utlämnande. Det förekommer i princip inte något elektroniskt utlämnande av information mellan myndigheterna i dag, med undantag för det elektroniska utlämnande som sker mellan myndigheterna genom användandet av den gemensamma NCT-mappen. Varje myndighet ansvarar för att det görs en sekretessprövning av den information som ska lämnas ut till övriga myndigheter. Detta innebär att handläggarna i princip måste göra en sekretessprövning inför varje utlämnande.

Det ovan beskrivna arbetssättet är på många sätt tidskrävande och ineffektivt. De handlingar som kan bli aktuella att visa för övriga myndigheter inom samarbetet förvaras i respektive myndighets säkerhetsskåp. Om en uppgift som finns i en sådan handling behöver delges en medarbetare från en annan myndighet måste således handläggaren från den aktuella myndigheten låsa upp säkerhetsskåpet, ta fram den aktuella handlingen, visa den för den andra medarbetaren och därefter återigen placera handlingen i skåpet och låsa detta. Om medarbetaren från den andra myndigheten av någon anledning exempelvis skulle behöva kontrollera uppgifterna i handlingen igen måste samma procedur genomföras en gång till. Även

om myndigheterna genom väl inarbetade rutiner och kompetent personal har uppnått ett väl fungerade arbetssätt, tar detta förfarande för utbyte av information naturligtvis viktig tid i anspråk för medarbetarna och riskerar således att hämma effektiviten inom samarbetet. Detta innebär i sin tur att kompetensen och kapaciteten inom samarbete kanske inte kan tas tillvara fullt ut.

Den verksamhet som bedrivs inom NCT-samarbetet kräver att medarbetarna i rätt tid har tillgång till relevant och korrekt information. Den information som medarbetarna lägger till grund för sina bedömningar måste således vara aktuell och uppdaterad. Det händer mycket på terrorområdet runt om i världen och information som är aktuell den ena dagen kan vara inaktuell dagen efter. Information i underrättelserapporter och andra handlingar som skrivs ut och sparas i pappersform kan inte uppdateras och blir således fort inaktuell. Den pappershantering 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 kan i sin tur påverka NCT:s förmåga att göra korrekta bedömningar.

Det manuella informationsutbytet mellan myndigheterna inom NCT-samarbetet bygger i dag på att handläggarna antingen vet vilken information de bör efterfråga från någon av de andra samarbetsparterna eller inser att viss, specifik information som de förfogar över skulle kunna vara till nytta för någon av de andra handläggarna. Det säger sig självt att det i en sådan verksamhet som den som NCT bedriver, är svårt att på förhand veta exakt vilken information en annan handläggare skulle kunna ha nytta av. På motsvarande sätt är det givetvis svårt för en handläggare som arbetar med en viss fråga, att veta vilken information som kan finnas hos någon av de andra myndigheterna och som skulle kunna vara relevant i sammanhanget. I båda fallen finns det en risk för att betydelsefull information inte kommer en handläggare till del i rätt tid. Även detta kan därför 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.

Även på detta sätt finns det en risk för att NCT:s förmåga att ge tidig förvarning om förändringar av terrorhotet mot Sverige och svenska intressen påverkas på ett negativt sätt. Detta blir särskilt tydligt i brådskande ärenden och i ärenden som grundar sig på mycket tidskritisk information. Det arbetssätt som används för utbyte av information inom NCT i dag medför således att produktiviteten inom samarbetet inte är helt optimal (Säkerhetspolisens skrivelse Ju2015/05096/L4, s. 9).

Ett förbättrat informationsutbyte inom samarbetet gör det möjligt att utnyttja de samlade resurserna effektivare. 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 innebär 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 står det klart att det finns ett behov av ett effektiviserat informationsutbyte mellan de samarbetande myndigheterna inom NCT. Ett förbättrat och effektiviserat informationsutbyte innebär dock, oavsett på vilket sätt det sker, med största sannolikhet ett ökat flöde av uppgifter mellan myndigheterna. Detta kan i och för sig skapa större risker för intrång i den personliga integriteten. Även insamling och utbyte av förhållandevis harmlösa uppgifter kan, om de skapar en totalbild av en enskild persons förhållanden, riskera att leda till intrång i den personliga integriteten (prop. 2009/10:85 s. 167). De uppgifter som behandlas inom NCT-samarbetet omfattas dock i princip av samma sekretesskydd hos alla berörda myndigheter (se vidare avsnitt 8.6). Därutöver är också skyddet vid personuppgiftsbehandling i stora delar likartat. Även om det kan finnas nackdelar med ett ökat informationsflöde mellan myndigheterna inom NCT-samarbetet får sammantaget fördelarna anses väga över. De eventuella integritetsrisker som kan identifieras bör dock vägas in både vid bedömningen av på vilket sätt informationsutbytet lämpligen bör effektiviseras och vid utformningen av den rättsliga regleringen.

8.3 Hur kan informationsutbytet inom NCT-samarbetet effektiviseras?

8.3.1 Alternativa lösningar

Som vi har konstaterat ovan finns det ett behov av ett effektiviserat informationsutbyte inom NCT-samarbetet, så att mer tid och arbete kan läggas på det viktiga analysarbete som handläggarna vid NCT har till uppgift att utföra. Som framgår ovan bör eventuella integritetsrisker vägas in vid bedömningen av vilka effektiviseringsåtgärder som bör vidtas. Det är härvid inte självklart att den åtgärd som framstår som den mest effektiva är den åtgärd som alltid bör väljas. En avvägning måste alltid göras mellan risken för intrång i den personliga integriteten och den förväntade effektivitetsvinsten.

En effektivisering kan givetvis åstadkommas på flera olika sätt. Det är exempelvis möjligt att man genom organisatoriska förändringar skulle kunna möjliggöra ett effektivare informationsutbyte. Vi har emellertid, vid våra bedömningar, att utgå från den organisatoriska form som myndigheterna har valt – tre självständiga myndigheter som samverkar på lika villkor under tre olika regelverk. Vi har därför inte närmare övervägt vilka effekter för informationsutbytet en annan organisationsform skulle kunna få.

Man skulle också kunna tänka sig att utökade resurser i form av fler medarbetare vid NCT till viss del skulle kunna effektivisera det informationsutbyte som sker i dag. Det skulle innebära större möjligheter för var och en av myndigheterna att alltid ha någon medarbetare på plats. På så sätt skulle risken minska för att informationsutbytet mellan myndigheterna fördröjs. Fler medarbetare skulle också innebära att den tid som går åt till att administrera det manuella utlämnandet av uppgifter inte skulle påverka verksamheten i övrigt i samma utsträckning som i dag. Utökade personalresurser skulle dock inte lösa de grundläggande problem som ett manuellt informationsutbyte muntligen eller via papper medför, dvs. att uppgifterna inte uppdateras samt att viktig information kan falla mellan stolarna. En sådan åtgärd skulle därför inte medföra den förbättring och effektivisering av verksamheten som eftersträvas.

Det alternativ som kvarstår och som vi bedömer vara det mest lämpliga är att ge myndigheterna möjlighet att på något sätt utbyta information elektroniskt. Som framgår ovan har vi också fått i

uppdrag att särskilt analysera förutsättningarna för ett elektroniskt informationsutbyte genom s.k. direktåtkomst. Vi kommer därför i den fortsatta framställningen särskilt fokusera på förutsättningarna att inom samarbetet utbyta information på detta sätt.

8.3.2 Elektroniskt informationsutbyte

Allmänt

I takt med att tekniken för att dels hantera information automatiserat inom den egna myndigheten, dels elektroniskt överföra information mellan myndigheter, har blivit mer avancerad och förfinad har den automatiserade informationshanteringen blivit mer regel än undantag. Utvecklingen har gått från manuella utlämnanden av information mellan myndigheter, t.ex. genom brev- eller telefonförfrågningar, till elektroniska former av informationsutbyten, t.ex. via e-post, elektronisk åtkomst till varandras informationssamlingar m.m. Att en myndighet har elektronisk åtkomst till en annan myndighets register, databas eller informationssamlingar är numera en naturlig del i en myndighets verksamhet. Formerna eller sätten för elektroniskt informationsutbyte mellan myndigheter kan dock se olika ut (SOU 2012:90 s. 53 f.).

Olika former av elektroniskt utlämnande

Att myndigheter ges möjlighet att lämna ut och hämta in information elektroniskt, i stället för att exempelvis göra detta i pappersform, innebär ofta en effektivisering av verksamheten. Personuppgiftslagen innehåller inte några särskilda bestämmelser om sättet för att lämna ut personuppgifter. Lagen innehåller däremot bestämmelser som anses innebära begränsningar i möjligheten att lämna ut uppgifter. Dessa begränsningar finns särskilt i 9 § första stycket d, e och f PuL som anger att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in, att de personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen samt att inte fler personuppgifter får behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen. I

lagen ställs det också krav på att behandlingen ska vara tillräckligt säker i förhållande till hur integritetskänsliga uppgifterna som ska lämnas ut är. Av 31 § PuL följer bl.a. att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

I de s.k. registerförfattningarna föreskrivs ofta begränsningar för olika typer av elektroniskt utlämnande. Anledningen är att utlämnande av personuppgifter elektroniskt anses kunna medföra risker för otillbörliga integritetsintrång eftersom mottagaren efter utlämnandet har större möjligheter att bearbeta och sprida informationen än om utlämnandet hade skett i pappersform. Som anges nedan finns det flera olika varianter av elektroniskt utlämnande. De termer som ofta används i lagstiftningssammanhang för sådant utlämnande är direktåtkomst och utlämnande på medium för automatiserad behandling.

Utlämnande på medium för automatiserad behandling

Utlämnande på medium för automatiserad behandling kan innebära att elektronisk information överförs t.ex. via e-post, genom utlämnande av uppgifter på cd-rom, DVD, USB-minne eller genom direkt överföring från ett datorsystem till ett annat via allmänna kommunikationsnät. Begreppet utlämnande på medium för automatiserad behandling har dock i takt med att tekniken utvecklats ibland getts en vidare innebörd (se SOU 2012:90 s. 198). I förarbetsuttalanden har som exempel på sådant utlämnande exempelvis framhållits s.k. batchkörningar, dvs. ett automatiskt utlämnande efter sökningar och sammanställningar där svar lämnas med viss tidsfördröjning (se prop. 2000/01:129 s. 76 och prop. 2007/08:160 s. 60). I princip anses allt elektroniskt utlämnande som inte sker genom direktåtkomst ske genom utlämnande på ett medium för automatiserad behandling. Gemensamt för alla dessa former av elektroniskt utlämnande är att den utlämnande myndigheten i varje enskilt fall mer eller mindre automatiserat tar ställning till om uppgifter kan lämnas ut och vilka uppgifter som i så fall ska lämnas. En eventuell sekretessprövning kan därmed ske i samband med utlämnandet i det enskilda fallet.

Begreppet utlämnande på medium för automatiserad behandling torde emellertid numera anses som omodernt (se SOU 2015:73 s. 301). Informationshanteringsutredningen har i sitt betänkande Myndighetsdatalag (SOU 2015:39 s. 442 f.) föreslagit att man i stället bör använda begreppet utlämnande i elektronisk form, varmed avses alla andra elektroniska utlämnanden än direktåtkomst. Utlämnande på medium för automatiserad behandling är dock det begrepp som alltjämt används i NCT-myndigheternas registerförfattningar.

Direktåtkomst

Det finns inte någon legaldefinition av begreppet direktåtkomst. Det som vanligtvis avses med direktåtkomst är dock att någon har direkt tillgång till någon annans register eller databas och på egen hand kan söka efter information, dock utan att kunna påverka innehållet i registret eller databasen. Enligt Informationshanteringsutredningen bör begreppet definieras på så sätt att en direktåtkomst föreligger om en myndighet hos en annan myndighet har en sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF, dvs. om upptagningen är tillgänglig för myndigheten med tekniskt hjälpmedel som myndigheten själv utnyttjar för överföring i sådan form att den kan läsas, avlyssnas eller på annat sätt uppfattas (se SOU 2015:39 s. 390 f.). I begreppet direktåtkomst ligger också att den som är personuppgiftsansvarig för registret eller databasen inte har någon kontroll över vilka uppgifter som mottagaren vid ett visst söktillfälle tar del av. Från integritetssynpunkt har det därför ansetts angeläget att frågor om tillgång till uppgifter genom direktåtkomst särskilt regleras i registerlagstiftningen (prop. 2000/01:129 s. 74, prop. 2001/02:144 s. 35 f. och prop. 2005/06:52 s. 8).

Högsta förvaltningsdomstolen (HFD) har i rättsfallet HFD 2015 ref. 61 uttalat sig om begreppet direktåtkomst. Frågan i målet gällde om socialnämndernas åtkomst till socialförsäkringsdatabasen genom datasystemet LEFI Online var att anse som direktåtkomst i socialförsäkringsbalkens mening. HFD hänvisade till 2 kap. 3 § andra stycket TF och konstaterade att allmänna handlingar hos en myndighet som en annan myndighet genom direktåtkomst får

tillgång till utgör allmänna handlingar även hos denna myndighet. Den avgränsning som på detta sätt görs av begreppet direktåtkomst genom tillämpning av tryckfrihetsförordningens bestämmelser om allmänna handlingars offentlighet kunde, enligt domstolen, användas även för att bestämma innehållet i detta begrepp i socialförsäkringsbalken. Det avgörande var således om upptagningen kunde anses förvarad hos socialnämnderna i tryckfrihetsförordningens mening. I det aktuella fallet ansågs socialnämnderna inte ha sådan teknisk tillgång till upptagningar som avses i 2 kap. 3 § andra stycket TF och förfarandet var därför inte att betrakta som direktåtkomst.

Vid direktåtkomst fattas beslutet om överföring i varje enskilt fall av mottagaren. En sekretessprövning måste därför göras redan då uppgifterna görs tillgängliga för direktåtkomst, oavsett om någon mottagare vid den tidpunkten faktiskt tar del av dem. En sådan prövning innefattar alla de uppgifter som mottagaren har möjlighet att ta del av genom sin direktåtkomst. Den faktiska begränsningen av direktåtkomsten görs sedan med hjälp av olika tekniska lösningar, beroende på hur omfattningen av direktåtkomsten har begränsats i det enskilda fallet, exempelvis genom olika behörighetsnivåer. Direktåtkomst anses således föreligga inte bara när tillgång ges utan begränsning, utan även vid mer eller mindre förfinade avgränsningar av åtkomst till enstaka eller ett flertal uppgifter (E-delegationens rapport ”Direktåtkomst och utlämnande på medium för automatiserad behandling”, s. 8). Det är den personuppgiftsansvariga myndigheten som ska se till att åtkomsten rent faktiskt begränsas på det sätt som föreskrivs.

När det gäller elektroniskt utlämnande brukar utlämnande genom direktåtkomst förknippas med särskilda risker. Ett skäl till detta är att de upptagningar som direktåtkomsten avser blir allmänna handlingar hos en mottagande myndighet (se SOU 2012:90 s. 64 f. och 123 f. samt SOU 2015:39 s. 134 f.). Som framgår ovan anses sammanställningar av uppgifter som i samband med direktåtkomst görs tekniskt tillgängliga för den mottagande myndigheten, enligt 2 kap. 3 § andra stycket TF, förvarade hos myndigheten och utgör således en allmän handling hos den myndigheten. Allmänna handlingar är som huvudregel offentliga och ju fler myndigheter som har direktåtkomst till uppgifter i ett datasystem, desto större blir således allmänhetens möjlighet att få tillgång till

dessa uppgifter (se SOU 2003:40 s. 201 och SOU 2015:73 s. 304). Generellt kan sägas att möjligheten till direktåtkomst ökar riskerna för intrång i den personliga integriteten, eftersom det typiskt sett innebär att uppgifter blir tillgängliga för fler personer och att den utlämnande myndighetens möjligheter att kontrollera användningen av uppgifterna minskar (se prop. 2015/16:65 s. 89 f.).

Den tekniska utvecklingen har lett till att skillnaderna mellan direktåtkomst och utlämnande på medium för automatiserad behandling blivit så liten att det ibland kan vara svårt att dra en gräns mellan dessa former av utlämnande. Man kan därför fråga sig om det finns skäl att i registerförfattningarna upprätthålla en skillnad mellan direktåtkomst och andra former av elektroniskt utlämnande eller om denna åtskillnad bör utmönstras. Enligt Informationshanteringsutredningen medför dock principiella och rättsliga skäl samt konkreta krav på förberedande analyser och åtgärder, att det finns starkt vägande skäl för att behålla en begreppsmässig skillnad mellan å ena sidan direktåtkomst och å andra sidan annat utlämnande i elektronisk form (SOU 2015:39 s. 149 f.).

Myndigheternas möjligheter att utbyta information elektroniskt inom samarbetet i dag

Säkerhetspolisen kan, enligt 2 kap. 20 § och 6 kap. 4 § 7 PDL, lämna ut enstaka personuppgifter på medium för automatiserad behandling till övriga myndigheter inom NCT-samarbetet. FRA och Försvarsmakten har getts möjlighet att lämna ut fler än enstaka personuppgifter på detta sätt om uppgifterna lämnas ut till en annan statlig myndighet, vilket är fallet inom samarbetet. Detta följer av 8 § FRA-PuF och 7 § PuF UNDSÄK. Alla tre myndigheterna inom NCT-samarbetet har således möjlighet att lämna ut personuppgifter till varandra på medium för automatiserad behandling, även om Säkerhetspolisens möjlighet till detta är något mer begränsad än övriga myndigheters.

När det gäller utlämnande genom direktåtkomst framgår det av 2 kap. 21 § PDL att sådant utlämnande är tillåtet endast i den utsträckning det följer av den lagen. Säkerhetspolisen har i lagen inte getts någon möjlighet att lämna ut uppgifter på detta sätt och kan därför i dag varken ge FRA eller Försvarsmakten direktåtkomst till myndighetens uppgiftssamlingar. FRA och Försvars-

makten har däremot getts vissa möjligheter att medge andra myndigheter direktåtkomst till uppgifter i sina respektive verksamheter. Enligt 9 § FRA-PuF får bl.a. Säkerhetspolisen och Försvarsmakten ha direktåtkomst till uppgifter i en uppgiftssamling för underrättelser i den omfattning som FRA beslutar. En sådan uppgiftssamling får, enligt 4 § samma förordning, endast innehålla färdiga underrättelserapporter. Enligt 8 § PuF UNDSÄK får FRA ha direktåtkomst till uppgifter i en uppgiftssamling för försvarsunderrättelseverksamhet i den omfattning som Försvarsmakten beslutar. En sådan uppgiftssamling får, enligt 2 § samma förordning, endast innehålla identitetsuppgifter, uppgifter om de omständigheter och händelser som ger anledning att anta att den registrerade har betydelse för försvarsunderrättelseverksamhet samt upplysningar om varifrån den registrerade uppgiften kommer och om en uppgiftslämnares trovärdighet.

8.4 Direktåtkomst

Bedömning: Samtliga myndigheter inom NCT-samarbetet har behov av att kunna få direktåtkomst till uppgifter hos övriga myndigheter inom samarbetet. Informationsutbytet inom NCT-samarbetet bör därför effektiviseras på så sätt att de samarbetande myndigheterna ges möjlighet att medge varandra direktåtkomst.

Förslag: 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 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 närmare 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 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 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 ramen för samverkan behöver ha tillgång till uppgifterna.

Direktåtkomst till uppgifter ska inte få medges innan respektive myndighet har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet.

Skälen för bedömningen och förslagen

Behovet av direktåtkomst

Utgångspunkten är att verksamheten inom NCT-samarbetet måste kunna bedrivas effektivt. Modern teknik ökar möjligheterna för myndigheterna att skapa överblick och samordning i arbetet och att utnyttja tillgänglig information på ett effektivt sätt. Det är angeläget att dessa möjligheter kan utnyttjas på bästa sätt.

Som framgår ovan behöver medarbetarna vid NCT snabbt ha 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. Som tidigare påpekats kan sådan information även inkludera person-

uppgifter. 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.

Som framgår ovan är den manuella pappershantering och det muntliga utlämnande av information som används inom samarbetet i dag ineffektivt och tidskrävande. Enligt vår bedömning skulle dessa problem i princip kvarstå om myndigheterna i stället skulle utbyta information via e-post eller genom annan elektronisk överföring. Ett sådant utlämnande skulle visserligen medföra en viss tidsvinst i förhållande till pappershanteringen men denna tidsvinst skulle vara marginell i jämförelse med vad man uppnår vid direktåtkomst. Ett sådant elektroniskt utlämnande förutsätter också, precis som vid utlämnande muntligen eller på papper, att det finns personal på plats från varje myndighet för att administrera utlämnandet. Ur den aspekten innebär således inte ett sådant elektroniskt utlämnade någon större skillnad i jämförelse med det sätt som används inom samarbetet i dag. I jämförelse med annat elektroniskt utlämnande innebär direktåtkomst ofta effektivitetsvinster 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 krävs i den utlämnande myndighetens personuppgiftssamling. 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. En möjlighet till direktåtkomst för de samarbetande myndigheterna skulle innebära effektivitetsvinster både för myndigheternas egna verksamheter och för samarbetet i sig.

Vid annat elektroniskt utlämnande än direktåtkomst måste den handläggare som begär ut informationen veta vad det är för information han eller hon behöver och specificera det för den utlämnande myndigheten. Handläggaren måste då också i princip veta vilken typ av relevant information som finns tillgänglig hos den utlämnande myndigheten. När handläggarna vid NCT arbetar med framtagandet av de strategiska rapporterna är det långt ifrån självklart vilken typ av information de behöver ta del av. Det är inte heller självklart var denna information kommer ifrån och var den

finns tillgänglig. Det är således inte så att handläggarna vid en av myndigheterna vid rapportskrivandet rutinartat kan begära in den information de behöver från någon av de andra två myndigheterna inom samarbetet, så som exempelvis kan vara fallet när handläggare från andra förvaltningsmyndigheter, t.ex. Försäkringskassan eller Skatteverket, handlägger ärenden. 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. Så som arbetssättet inom NCT fungerar i dag förutsätter det att varje analytiker, när denne tar del av information i den egna myndighetens system, också överväger om den informationen eller eventuell annan information som finns tillgänglig kan vara av intresse för någon annan inom samarbetet. Mot bakgrund av den mängd information som handläggarna tar del av kan detta vara mycket svårt att avgöra och det finns då en risk att information inte kommer rätt handläggare till del. Information kan således gå förlorad då den som vid det aktuella tillfället bäst behöver informationen inte alltid är den som kan få tag på informationen. Om handläggarna vid NCT ges möjlighet att självmant söka efter information i övriga myndigheters uppgiftsamlingar skulle detta kunna undvikas.

Ett utlämnande genom direktåtkomst kan även innebära fördelar ur informationssäkerhetssynpunkt, eftersom överföring av information vid direktåtkomst kan ske på ett säkrare sätt än till exempel genom e-post. Vid elektronisk överföring av information via e-post kan obehöriga lättare få tillgång till informationen (prop. 2009/10:85 s. 174). Direktåtkomst ger också möjlighet till loggning av alla händelser och aktiviteter som företas i det aktuella systemet, t.ex. inloggning, läsande, tillförande, förändring och radering av uppgifter. Någon motsvarande möjlighet finns inte vid pappershantering eller annat elektroniskt utlämnande. Vid sådan elektronisk åtkomst till information som direktåtkomst innebär, kan det således vara lättare att kontrollera och i efterhand utreda om information exempelvis har använts felaktigt eller obehörigt.

Som vi har konstaterat ovan finns det 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 själv-

mant 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 informationen med annan tillgänglig information för att på så sätt göra korrekta bedömningar. Att i stället få del av information genom annan elektronisk överföring ger inte samma möjligheter. Precis som vid pappershanteringen kan uppgifter som lämnas ut på detta sätt fort bli inaktuella då de inte uppdateras efter att de har lämnat systemet.

Sammanfattningsvis är det vår 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.

Bör direktåtkomst medges?

Möjlighet till direktåtkomst skulle generellt kunna medföra en ökad risk för intrång i den personliga integriteten. Som framgår ovan innebär direktåtkomst typiskt sätt att uppgifter blir tillgängliga för fler personer och att den ursprungliga myndighetens möjligheter att kontrollera användningen av uppgifterna minskar. Även om det är möjligt att genom särskilda åtgärder motverka dessa eventuella risker är det ändå viktigt att myndigheternas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna. Mot NCT-myndigheternas verksamhetsbehov måste således hänsynen till den enskildes integritet vägas.

Vid polisdatalagens 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. Några skäl till varför en sådan möjlighet skulle ges hade inte heller framkommit under remissbehandlingen (prop. 2009/10:85 s. 178 f.). Det är naturligtvis fortfarande så att de uppgifter som Säkerhetspolisen behandlar är av känslig natur. De flesta känsliga uppgifter hos Säkerhetspolisen torde dock behandlas i myndighetens operativa verksamhet. Myndigheterna inom NCT-samarbetet arbetar med att göra strategiska bedömningar av terrorhotet och bedriver således ingen operativ verksam-

het. Myndigheterna har därmed inte heller något behov av att ta del av uppgifter som enbart har betydelse för Säkerhetspolisens operativa verksamhet. Även om de uppgifter som Säkerhetspolisen behandlar är särskilt känsliga, torde ett elektroniskt utlämnande inom NCT-samarbetet omfatta en begränsad mängd sådana uppgifter. Vi återkommer till den närmare avgränsningen av direktåtkomsten i nästa avsnitt. 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 och som beskrivs i avsnitt 8.2. Som konstaterats ovan har det blivit allt tydligare att ett utökat och förbättrat samarbete på alla nivåer är en förutsättning för att effektivt kunna bekämpa terrorismen. Denna utveckling har också medfört att NCT har fått en allt viktigare roll. Mot bakgrund av detta anser vi att det numera finns starka skäl som, trots uttalandena i förarbetena till PDL, talar för att direktåtkomst till uppgifter hos Säkerhetspolisen i vissa fall bör kunna medges.

Enligt uppgift från myndigheterna kommer en övervägande del av den information som används inom samarbete från Säkerhetspolisen. Man skulle därför kunna tänka sig att behovet av ett effektiviserat uppgiftsutbyte i tillräcklig utsträckning skulle kunna tillfredsställas genom att FRA och Försvarsmakten ges direktåtkomst till Säkerhetpolisens uppgifter. En viktig princip inom NCT-samarbetet är dock att de tre myndigheterna deltar på lika villkor. Myndigheterna har också själva påtalat att det finns ett behov för samtliga handläggare vid NCT att kunna ta del av uppgifter från alla tre myndigheterna. Att enbart ge en myndighet möjlighet att ge övriga myndigheter direktåtkomst, innebär att den pappershantering som förekommer i dag i princip skulle få fortsätta vad gäller övriga myndigheters utlämnande. Även om utlämnande av uppgifter från dessa myndigheter i dagsläget inte förekommer i lika stort utsträckning som från Säkerhetspolisen, är det minst lika viktigt att information från FRA och Försvarsmakten när den väl behövs, är uppdaterad och korrekt. Det är vidare möjligt att fördelningen av informationsbehovet inom samarbetet kan förändras med tiden. För att arbetet ska fungera så bra och effektivt som möjligt är det alltså viktigt att handläggarna från alla tre myndigheterna ges samma möjlighet till elektronisk åtkomst. Vår bedömning är således att alla tre myndigheterna har lika stort behov av att

få direktåtkomst till övriga myndigheters uppgifter. Att ge alla tre myndigheterna möjlighet att lämna ut uppgifter genom direktåtkomst innebär, i jämförelse med att t.ex. endast ge Säkerhetspolisen den möjligheten, inte heller en så mycket större risk för integritetsintrång att det av den anledningen är olämpligt. Vår utgångspunkt är därför att alla tre NCT-myndigheterna ska ges möjlighet att lämna ut uppgifter genom direktåtkomst till övriga myndigheter inom samarbetet.

För att intrånget i den personliga integriteten vid direktåtkomst ska bli acceptabelt måste emellertid vissa krav ställas (se prop. 2007/08:160 s. 46 f. och s. 56 f., SOU 2012:90 s. 123 f. samt SOU 2015:39 s. 138 f. och s. 387 f.). Vad det i princip handlar om är att skyddet för personuppgifterna vid direktåtkomst ska säkerställas på olika sätt. Om det skyddet kan garanteras behöver direktåtkomst inte vara så mycket känsligare än andra former av informationsutbyten (SOU 2015:73 s. 310).

En viktig aspekt som bör beaktas då direktåtkomst övervägs är, i de fall direktåtkomsten avser sekretessbelagda uppgifter, vilka sekretessbestämmelser som blir tillämpliga hos de mottagande myndigheterna. Om sekretesskyddet hos den mottagande myndigheten är lika långtgående som sekretesskyddet hos den utlämnande myndigheten behöver ett utlämnande av uppgifter genom direktåtkomst inte innebära en ökning av integritetsriskerna i förhållande till allmänheten.

En annan viktig fråga är hur uppgifterna sprids och används hos den mottagande myndigheten. Om kretsen av personer som har tillgång till uppgifterna kan begränsas är risken för integritetsintrång generellt sett mindre. Den mottagande myndigheten måste därför begränsa åtkomstmöjligheterna så mycket som möjligt med hänsyn till den aktuella verksamheten och känsligheten hos personuppgifterna. Det leder till att anställda inom en myndighet får elektronisk tillgång endast till de personuppgifter som de behöver i sitt arbete.

En tredje betydelsefull aspekt är vilka bestämmelser om informationssäkerhet som gäller hos den mottagande myndigheten. Om informationssäkerheten hos den mottagande myndigheten är hög, så att det kan garanteras att informationen endast når dem som har rätt till den, inger möjlighet till direktåtkomst mindre

betänkligheter från integritetssynpunkt än vad som annars hade varit fallet (prop. 2009/10:85 s. 176).

När det gäller sekretessregleringen kan det konstateras att denna i princip ger samma skydd hos alla tre myndigheterna (se avsnitt 8.6.1 och 8.6.3 nedan). De uppgifter som ska lämnas ut genom direktåtkomst omfattas som regel av sekretess enligt 15 kap. 1 och 2 §§ och 18 kap. 2 § OSL. Dessa bestämmelser är primära sekretessbestämmelser hos alla tre NCT-myndigheterna och gäller till skydd för nationen och dess förbindelser, försvaret samt underrättelseverksamhet. Även bestämmelsen i 21 kap. 5 § OSL om s.k. utlänningssekretess är en primär sekretessbestämmelse hos alla tre myndigheterna. När det gäller skyddet för enskildas personliga och ekonomiska förhållanden regleras detta i olika bestämmelser för Säkerhetspolisen respektive FRA och Försvarsmakten. I Säkerhetspolisens verksamhet finns reglerna i 35 kap. 1 § och 37 kap. 1 § OSL, medan det för FRA:s och Försvarsmaktens del finns regler i 38 kap. 4 § OSL. Samtliga dessa bestämmelser är dock försedda med ett omvänt skaderekvisit, vilket innebär att uppgifterna i princip har samma sekretesskydd hos alla tre myndigheterna.

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. Vi föreslår dessutom att detta ska förtydligas i bestämmelserna om direktåtkomst. Därutöver kan kon stateras att tillgången till de uppgifter som ska lämnas ut genom direktåtkomst, hos alla tre myndigheterna kommer att vara begränsad till den personal som deltar i NCT-samarbetet. Detta säkerställs dels genom utformningen av de aktuella författningsbestämmelserna, dels genom de tekniska behörighetsstyrningar som enligt myndigheterna kommer att användas. Det är således en mycket snäv krets som kommer att ha tillgång till de uppgifter som görs tillgängliga via direktåtkomst.

Vad slutligen gäller informationssäkerheten kan det konstateras att det i det här sammanhanget rör sig om tre myndigheter som generellt har en mycket hög säkerhet när det gäller hantering av information. Den personuppgiftsbehandling som kommer att förekomma genom att uppgifter lämnas ut genom direktåtkomst, kommer att loggas och följas upp av respektive myndighet. Inför ett

utlämnande genom direktåtkomst bör emellertid den myndighet som beslutar om sådan åtkomst försäkra sig om att den mottagande myndigheten har en acceptabel säkerhetsnivå, exempelvis vad gäller system för utlämnande av behörighet och loggning av transaktioner samt tillsyn (se prop. 2009/10:85 s. 177). Var och en av myndigheterna inom NCT bör därför, innan systemet med direktåtkomst genomförs göra en risk- och sårbarhetsanalys och komma överens med övriga myndigheter om hur skyddet för personuppgifterna ska säkerställas. Myndigheterna har själva uppgett att de har för avsikt att inom ramen för en sådan analys reglera och komma överens om sådana frågor. Bestämmelser om att så ska ske skulle dessutom kunna föras in i den överenskommelse som reglerar samarbetet mellan myndigheterna.

När det gäller informationssäkerhet i samband med direktåtkomst har regeringen i polisdataförordningen (2010:1155) gett Polismyndigheten möjlighet att meddela närmare föreskrifter om vad som krävs i fråga om behörighet och säkerhet, för att myndigheten ska kunna medge direktåtkomst till uppgifter för de myndigheter som anges i PDL (14 §). I samma bestämmelse anges att direktåtkomst till uppgifterna inte får medges innan Polismyndigheten har försäkrat sig om att den mottagande myndigheten uppfyller kraven på behörighet och säkerhet. Mot bakgrund av att vi nu föreslår att även Säkerhetspolisen ska få lämna ut uppgifter genom direktåtkomst bör en liknande bestämmelse införas i förordningen även för Säkerhetspolisen. När det gäller FRA och Försvarsmakten har någon uttrycklig bestämmelse om krav på behörighet och säkerhet vid direktåtkomst inte tagits in i respektive registerförfattning. Vi anser att det finns lika stor anledning att kräva att FRA och Försvarsmakten försäkrar sig om att de mottagande myndigheterna uppfyller kraven på behörighet och säkerhet innan de medger direktåtkomst till sina system. En bestämmelse som föreskriver detta bör därför införas på förordningsnivå även för deras del. Myndigheterna bör även uttryckligen ges möjlighet att meddela närmare föreskrifter om behörighet och säkerhet vad gäller direktåtkomsten.

De ökade integritetsrisker som en möjlighet till direktåtkomst skulle kunna medföra kan således motverkas genom bestämmelser av annat slag, t.ex. bestämmelser om sekretess, om tillgång till uppgifter och om informationssäkerhet. Genomgången ovan ger vid

handen att risken för integritetsintrång i förevarande fall måste bedömas som relativt liten. Som framgår nedan kommer dessutom de uppgifter som ska få lämnas ut genom direktåtkomst att vara avgränsade på flera sätt. Med hänsyn till Sveriges behov av ett fullgott antiterrorarbete anser vi att övervägande skäl talar för att det ökade utbyte av information som direktåtkomst medför inte innebär sådana risker att fördelarna inte överväger nackdelarna. Vår bedömning är därför 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.

Hur bör direktåtkomsten avgränsas?

De uppgifter som respektive myndighet inom samarbetet ska kunna medge direktåtkomst till måste vara väl avgränsade. Direktåtkomsten ska i princip inte omfatta fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra på papper eller muntligen.

En första förutsättning för att en myndighet inom samarbetet ska kunna ges direktåtkomst till uppgifter hos en annan myndighet inom samarbetet är att uppgifterna är gemensamt tillgängliga i verksamheten eller har gjorts gemensamt tillgängliga i en uppgiftssamling hos den senare myndigheten. Vid tillkomsten av FRA:s och Försvarsmaktens registerförfattningar har man ansett att direktåtkomst inte ska få förekomma till andra uppgifter än sådana som förkommer i uppgiftssamlingar (prop. 2006/07:46 s. 79). På samma sätt gjorde man vid tillkomsten av PDL bedömningen, när det gäller den öppna polisen, att direktåtkomst endast borde medges till uppgifter som är gemensamt tillgängliga (prop. 2009/10:85 s. 177 f.). Det finns inte skäl att göra någon annan bedömning gällande de uppgifter som ska få lämnas ut inom NCT-samarbetet.

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, och ska inte på något sätt styras av myndigheternas behov i övrigt. 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. Direktåtkomst ska exempelvis inte kunna ges till uppgifter hos Säkerhetspolisen, vilka enbart har betydelse för myndighetens operativa verksamhet eller till sådana uppgifter hos Försvarsmakten som enbart rör andra militära hot mot landet. De uppgifter som görs tillgängliga ska bara användas inom ramen för NCT-samarbetet till stöd för strategiska bedömningar avseende internationell terrorism och inte i myndighetsutövning mot någon enskild. I det sammanhanget kan det framhållas att Försvarmakten och FRA är två försvarsunderrättelsemyndigheter som inte har till uppgift att bekämpa brott. Det bör dock påpekas att det i och för sig inte finns någon sekretessgräns mellan handläggarna vid NCT och deras respektive myndigheter. Uppgifter som handläggarna får del av inom samarbetet skulle därmed rent teoretiskt kunna lämnas vidare inom den egna myndigheten. Handläggarna vid de tre myndigheterna utbyter emellertid de aktuella uppgifterna redan i dag och den omständigheten att uppgifterna inte omfattas av sekretess i förhållande till den egna myndigheten har inte ansetts innebära några problem. Sammantaget menar vi alltså att direktåtkomsten bör avgränsas till uppgifter 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.

Från ett integritetsperspektiv är det en fördel om det tydligt framgår av författningstexten 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. 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 man i författningstexten pekar ut en specifik uppgiftssamling eller uppgiftstyp samt genom

att man, som krav för direktåtkomst, beskriver ändamålet med uppgiftsutlämnandet på det sätt som vi föreslagit ovan.

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. Försvarsmakten har uppgett att de uppgifter hos myndigheten 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 vi föreslår, får var och en av myndigheterna själva bedöma vilka uppgifter som är relevanta för arbetet inom NCT och som till följd härav bör göras tillgängliga för övriga myndigheter. Självfallet kan dock endast sådana uppgifter göras tillgängliga som den mottagande myndigheten får behandla i sin verksamhet. Detta är särskilt viktigt för Försvarsmakten och FRA som endast får behandla personuppgifter som har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och som härmed t.ex. endast får behandla personuppgifter som avser utländska förhållanden. Eftersom det förekommer ett relativt omfattande informationsutbyte mellan de berörda myndigheterna redan i dag, både inom NCT-samarbetet och inom ramen för annat samarbete, är myndigheterna emellertid vana vid att göra dessa avvägningar och vet vad som kan och inte kan lämnas ut. Myndigheterna har också uppgett att de är väl medvetna om vilka begränsningar som i detta avseende föreligger inom samarbetet och att de också är kapabla att självmant begränsa åtkomsten i enlighet med dessa. Vi anser dock att det ur integritetssynpunkt är viktigt att, när det gäller FRA och Försvarsmakten, denna begränsning framgår av den föreslagna bestämmelsen om direktåtkomst, som en erinran till den utlämnande myndigheten att anpassa direktåtkomsten till de rättsliga begränsningar som gäller för de mottagande myndigheterna. Även om denna begränsning

således redan följer av myndigheternas respektive ändamålsbestämmelser, kan det finnas fördelar med att i ett förtydligande syfte klargöra detta. När det gäller tillgången till uppgifter hos Säkerhetspolisen bör det därför anges att Försvarsmakten och FRA endast får ges direktåtkomst till sådana uppgifter som myndigheterna får behandla i enlighet med sina respektive registerförfattningar. En sådan begränsning av omfattningen av direktåtkomsten kan dock meddelas på förordningsnivå.

I detta sammanhang bör också betonas att de uppgifter som inom samarbetet ska göras tillgängliga genom direktåtkomst utgör en mycket begränsad del av alla de uppgifter som myndigheterna behandlar i sina respektive verksamheter. Det är således inte så att myndigheterna ges möjlighet att fullständigt öppna upp alla sina system och uppgiftssamlingar för övriga myndigheter. I detta sammanhang kan det konstateras att handläggarna vid NCT själva endast har en begränsad tillgång till uppgifter i den egna myndighetens system utifrån sin placering och sina arbetsuppgifter vid NCT. Vi har i kapitel 6 ovan beskrivit närmare hur tillgången till information hos myndigheterna begränsas med hjälp av olika behörighetstilldelningar. Som framgår där är det noggrant reglerat i de tekniska systemen vem som har rätt att ta del av vilken information. 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.

Sammanfattningsvis bör således Säkerhetspolisen, FRA och Försvarsmakten få medges direktåtkomst till gemensamt tillgängliga uppgifter, eller uppgifter som har gjorts gemensamt tillgängliga i en viss uppgiftssamling hos respektive myndighet, och som behövs för att myndigheterna, inom ramen för NCT-samarbetet, ska kunna göra bedömningar på strategisk nivå av terrorhotet mot Sverige och svenska intressen. FRA:s och Försvarsmaktens direktåtkomst bör därutöver begränsas till uppgifter som dessa myndigheter får behandla enligt ändamålsbestämmelserna i sina respektive registerförfattningar.

Var ska bestämmelserna placeras?

Vår utgångspunkt har varit att följa systematiken i de befintliga författningarna. Direktåtkomst till uppgifter hos Polismyndigheten regleras i PDL på så sätt att det där anges vilka myndigheter som får ha direktåtkomst till uppgifterna samt att det ska röra sig om gemensamt tillgängliga uppgifter. Den närmare omfattningen av direktåtkomsten regleras i polisdataförordningen. Såvitt gäller FRA och Försvarsmakten regleras direktåtkomsten i FRA-PuL och PuL UNDSÄK endast genom en upplysningsbestämmelse som anger att regeringen meddelar föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. I respektive förordning preciseras sedan närmare vilka myndigheter som får ha direktåtkomst samt omfattningen av denna.

När det gäller Säkerhetspolisen finns det inte skäl att frångå systematiken som finns i PDL. Lagstiftaren har ansett att direktåtkomst till uppgifter i Polismyndighetens brottsbekämpande verksamhet ska regleras i lag och det finns inte anledning att göra någon annan bedömning när det gäller direktåtkomst till uppgifter hos Säkerhetspolisen. Vi anser vidare att direktåtkomstens omfattning så långt som möjligt ska regleras i lag. Bestämmelsen i PDL ska därför ange vilken typ av uppgifter hos Säkerhetspolisen som avses samt vilket behov som måste föreligga för att dessa uppgifter ska få lämnas ut. På samma sätt som gäller vid direktåtkomst till Polismyndighetens uppgifter bör dock regeringen eller den myndighet som regeringen bestämmer ges möjlighet att meddela närmare föreskrifter om omfattningen av direktåtkomsten. Som framgår ovan anser vi också att en sådan ytterligare begränsning av direktåtkomsten till Säkerhetspolisens uppgifter bör införas i polisdataförordningen.

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 § 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. Sam-

mantaget 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. 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.

Personuppgifter behandlas i FRA:s och Försvarsmaktens verksamhet utan att den enskildes samtycke inhämtas och behandlingen torde ofta kunna innebära en kartläggning av den enskildes personliga förhållanden. Grundlagsbestämmelsen omfattar dock bara 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 av betydelse samt omfattningen av utlämnandet av uppgifter till andra. 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).

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 (se avsnitt 8.6 nedan). 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 Försvarsmakten inriktar exempelvis, och bestämmer härmed till viss del, FRA:s verksamhet. Mycket talar därför för att direktåtkomsten till FRA:s och Försvarsmaktens 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. Vi anser emellertid ändå att det i det här fallet kan vara lämpligt att reglera direktåtkomsten i lag. Detta 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 vårt förslag ska regleras i lag. Det utlämnande som föreslås bör ses som en helhet och både direktåtkomst och uppgiftsskyldighet bör därför regleras i lag. Vi återkommer till frågan om de sekretessbrytande bestämmelserna i avsnitt 8.6.2 nedan.

8.5 Annat elektroniskt utlämnande

Förslag: Säkerhetspolisen ska få lämna ut fler än enstaka uppgifter på medium för automatiserad behandling till Försvarsmakten och FRA om det behövs inom myndighetsöverskridande samverkan mellan FRA, Försvarsmakten och Säkerhetspolisen. En bestämmelse som föreskriver ett sådant undantag från huvudregeln i 2 kap. 20 § PDL ska tas in i polisdataförordningen (2010:1155).

Skälen för förslaget

Huvudregeln i PDL är att endast enstaka personuppgifter får lämnas ut på medium för automatiserad behandling. Detta framgår av 2 kap. 20 § PDL. I 17 § polisdataförordningen (2010:1155) har det emellertid tagits in ett undantag från huvudregeln. Där anges att begränsningen i 2 kap. 20 § PDL inte gäller för myndigheter som får ha direktåtkomst enligt 3 kap. 8 § samma lag i fråga om personuppgifter som har gjorts gemensamt tillgängliga. Polismyndigheten och

Säkerhetspolisen får således lämna ut fler än enstaka personuppgifter på medium för automatiserad behandling till de myndigheter som får ha direktåtkomst till Polismyndighetens uppgifter om personuppgifterna har gjorts gemensamt tillgängliga. Försvarsmakten och FRA nämns inte i 3 kap. 8 § PDL och omfattas således inte av undantaget i polisdataförordningen. Detta innebär att Säkerhetspolisen endast kan lämna ut enstaka personuppgifter på medium för automatiserad behandling till Försvarsmakten och FRA.

För Polismyndigheten innebär undantaget i 17 § polisdataförordningen att de personuppgifter som myndigheten får lämna ut genom direktåtkomst får myndigheten också lämna ut på medium för automatiserad behandling. Som skäl anges i förarbetena till PDL att det i förhållande till myndigheter som får medges direktåtkomst inte bör gälla några begränsningar i fråga om utlämnande på annat elektroniskt medium, eftersom lagen ska vara teknikneutral (prop. 2009/10:85 s. 186). Samma bedömning har gjorts vad gäller Kustbevakningens samt Åklagarmyndighetens och Ekobrottsmyndighetens utlämnande av personuppgifter (se prop. 2011/12:45 s. 98 och prop. 2014/15:63 s. 104).

Även när det gäller FRA och Försvarsmakten är huvudregeln att myndigheterna endast får lämna ut enstaka personuppgifter på medium för automatiserad behandling. För dessa myndigheter har det dock gjorts ett generellt undantag på förordningsnivå som innebär att myndigheterna får lämna ut fler än enstaka uppgifter på sådant sätt till andra statliga myndigheter. Detta framgår av 7 § PuF UNDSÄK samt 8 § FRA-PuF. FRA och Försvarsmakten har således möjlighet att lämna ut fler än enstaka personuppgifter till varandra och till Säkerhetspolisen.

Eftersom vi föreslår att Säkerhetspolisen ska få lämna ut uppgifter till Försvarsmakten och FRA genom direktåtkomst, är det frågan om det även finns anledning att ge Säkerhetspolisen möjlighet att lämna ut dessa uppgifter på annat elektroniskt medium. Det kan här inledningsvis konstateras att förslaget om direktåtkomst endast innebär att myndigheterna ges en möjlighet att medge varandra direktåtkomst och således inte på något sätt föreskriver att så ska ske. Det är i slutändan upp till myndigheterna själva att avgöra om de vill lämna ut uppgifter på detta sätt och i vilken omfattning. Om myndigheterna inom samarbetet i stället vill ut-

byta information på något annat lämpligare sätt står det således dem fritt att göra så inom ramen för befintlig reglering.

Som tidigare nämnts har den tekniska utvecklingen lett till att skillnaderna mellan direktåtkomst och utlämnande på medium för automatiserad behandling blivit så liten att det ibland kan vara svårt att dra en gräns mellan dessa former av utlämnande. Med anledning av detta och då utvecklingen på området fortsätter att gå framåt anser vi att det är en fördel om förslag som reglerar uppgiftsutbyte mellan myndigheter är så teknikneutrala som möjligt. I dag kan exempelvis uppgifter lämnas ut genom förfaranden som är så pass automatiserade att de utåt sett framstår som direktåtkomst, men där den tekniska lösningen innebär att den utlämnande myndigheten faktiskt reagerar på en förfrågan och gör någon slags bedömning av om uppgifterna kan lämnas ut eller inte (se t.ex. HFD 2015 ref. 61). Att låsa fast myndigheterna vid en specifik teknisk lösning för utlämnande av uppgifter kan skapa problem.

Som vi tidigare har redovisat anser vi att bestämmelser om utlämnande av uppgifter, inom NCT-samarbetet, genom direktåtkomst är godtagbart även med beaktande av kravet på skydd för den personliga integriteten. Att en myndighet som under vissa förutsättningar får lämna ut uppgifter genom direktåtkomst, också ges möjlighet att under samma förutsättningar lämna ut dessa uppgifter på annat elektroniskt medium kan inte anses innebära en ökad integritetsrisk. Särskilt inte då ett sådant elektroniskt utlämnande ofta anses mindre ingripande ur integritetssynpunkt.

Här måste även beaktas att FRA och Försvarsmakten utan begränsning har möjlighet att lämna ut uppgifter på detta sätt inom samarbetet. Att inte ge Säkerhetspolisen samma möjlighet skulle således innebära en snedfördelning inom samarbetet. Det skulle även kunna skapa problem när myndigheterna tillsammans ska hitta lämpliga tekniska lösningar för informationsutbytet. Om samarbetet ska fungera så ändamålsenligt och effektivt som möjligt bör de samarbetande myndigheterna därför ha samma möjlighet till informationsutbyte sinsemellan.

Mot denna bakgrund anser vi att Säkerhetspolisen inom ramen för NCT-samarbetet bör ges möjlighet att lämna ut fler än enstaka uppgifter på medium för automatiserad behandling till FRA och Försvarsmakten.

8.6 Sekretess och uppgiftsskyldighet

8.6.1 Allmänna utgångspunkter

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

Skälen för bedömningen

Sekretess hos NCT-myndigheterna

I kapitel 5.6.3 och 5.6.4 ovan redogör vi för de sekretessregler som gäller dels till skydd för den verksamhet som NCT-myndigheterna bedriver, dels till skydd för enskilds personliga och ekonomiska förhållanden i dessa verksamheter. Där framgår att de uppgifter som myndigheterna behandlar inom ramen för samarbetet som regel omfattas av sekretess enligt 15 kap. 1 och 2 §§ OSL, dvs. utrikes- och försvarssekretess, och 18 kap. 2 § OSL, vilken reglerar sekretess till skydd för intresset av att förebygga, förhindra eller upptäcka brott hänförligt till underrättelseverksamhet m.m. Bestämmelserna är tillämpliga på uppgifter som hänför sig till eller rör en viss verksamhet. Bestämmelserna omfattar således hela det allmännas 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 enskilds 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. Utlämnande av uppgifter mellan myndigheterna inom NCT sker i dag genom tillämpning av generalklausulen i 10 kap. 27 § OSL.

Sekretess mellan myndigheter

Enligt 8 kap. 1 § OSL får uppgifter för vilka sekretess gäller inte röjas för andra myndigheter om inte annat framgår av OSL eller lag eller förordning till vilken OSL hänvisar. Sekretess gäller således även mellan myndigheter och när uppgifter ska lämnas mellan myndigheter måste därför hänsyn tas till sekretesslagstiftningen. Som redogjorts för tidigare innehåller OSL emellertid flera bestämmelser som möjliggör utbyte av uppgifter mellan myndigheter utan hinder av sekretess, s.k. sekretessbrytande bestämmelser. Exempelvis hindrar sekretess inte att uppgifter lämnas till en annan myndighet om uppgiftsskyldighet följer av lag eller förordning (10 kap. 28 § OSL). Av den s.k. generalklausulen följer vidare att en uppgift, som huvudregel, får lämnas ut till en annan myndighet om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda (10 kap. 27 § OSL).

Förhållandet mellan direktåtkomst och sekretess

En bestämmelse om direktåtkomst reglerar endast själva formen för utlämnandet, dvs. på vilket sätt uppgifterna får lämnas ut. En sådan bestämmelse är därför inte att se som en uppgiftsskyldighet enligt 10 kap. 28 § OSL och har därför inte heller någon sekretessbrytande verkan (se t.ex. prop. 2004/05:164 s. 83 och prop. 2006/07:46 s. 80). Avser direktåtkomst uppgifter som omfattas av sekretess hos den utlämnande myndigheten krävs därför författningsstöd i någon sekretessbrytande regel.

Sekretessregleringen styr således i vilken mån uppgifter över huvud taget får lämnas ut från en myndighet till en annan myndighet, medan bestämmelser om direktåtkomst enbart tar sikte på formen för utlämnandet. Regler om direktåtkomst brukar därför ofta kompletteras med sekretessbrytande bestämmelser som är

utformade som regler om uppgiftsskyldighet på sätt som avses i 10 kap. 28 § OSL. Dessa bestämmelser formuleras ofta som en rätt för mottagande myndighet att ta del av uppgifter, se till exempel 2 kap. 16 § PDL och 4 § förordningen (2001:588) om behandling av uppgifter i Skatteverkets beskattningsverksamhet. I undantagsfall skulle även sekretessbelagda uppgifter kunna lämnas ut genom direktåtkomst med stöd av generalklausulen i 10 kap. 27 § OSL. Så har i vart fall antytts i vissa förarbeten (se t.ex. prop. 2009/10:85 s. 189 och prop. 2011/12:45 s. 143). Så skedde också fram till helt nyligen i fråga om Polismyndighetens, Säkerhetspolisens och utlandsmyndigheternas direktåtkomst till Migrationsverkets verksamhetsregister enligt 6 § i den tidigare gällande förordningen (2001:720) om behandling av personuppgifter i verksamhet enligt utlännings- och medborgarskapslagstiftningen. Förordningen har den 12 februari 2016 ersatts av utlänningsdatalagen (2016:27) och utlänningsdataförordningen (2016:30) varvid en sekretessbrytande föreskrift om uppgiftsskyldighet för Migrationsverket i stället har införts (se prop. 2015/16:65 s. 93 f.).

I detta sammanhang kan också nämnas att Informationshanteringsutredningen i sitt slutbetänkande Myndighetsdatalag, har föreslagit att det i OSL införs en generell sekretessbrytande bestämmelse som innebär att föreskrifter i lag eller förordning om direktåtkomst för myndigheter i sig får en sekretessbrytande effekt. Därigenom skulle det inte längre behöva införas särskilda sekretessbrytande bestämmelser för att möjliggöra direktåtkomst (se SOU 2015:39 s. 407 f.).

Eftersom de uppgifter som myndigheterna inom NCT-samarbetet har för avsikt att lämna ut till varandra genom direktåtkomst som regel omfattas av sekretess behöver sekretessen brytas på något sätt. 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 sekretessen kan brytas på annat sätt.

Av förarbetena till OSL framgår att rutinmässigt uppgiftsutbyte i regel ska vara författningsreglerat. Endast i undantagsfall, när rutinmässigt uppgiftslämnande inte är författningsreglerat men likväl kan anses tillräckligt motiverat, kan den intresseavvägning, som ska göras enligt generalklausulen, ske på förhand (prop. 1979/80:2 Del A s. 327). Regeringen har i förarbetena till utlänningsdatalagen (2016:27) anfört att det ofta inte är lämpligt att omfattande utlämnande av sekretessbelagda uppgifter sker enbart med stöd av den sekretessbrytande generalklausulen (se prop. 2015/16:65 s. 94).

När det gäller den öppna polisens verksamhet bedömde regeringen vid PDL:s tillkomst att det behövdes en tydlig sekretessbrytande reglering för att polisen skulle kunna medge andra brottsbekämpande myndigheter direktåtkomst. Till följd härav infördes sekretessbrytande bestämmelser i form av uppgiftsskyldigheter i PDL (prop. 2009/10:85 s. 189 f.). Samma bedömning gjordes avseende utlämnande av uppgifter från Kustbevakningen samt från Åklagarmyndigheten och Ekobrottsmyndigheten (se prop. 2011/12:45 s. 142 f. och prop. 2014/15:63 s. 107).

Vi har föreslagit att Säkerhetspolisen, Försvarsmakten och FRA ska ges möjlighet att lämna ut uppgifter till varandra genom direktåtkomst. Även om det rör sig om en relativt begränsad mängd uppgifter i varje myndighets verksamhet vilka kommer att göras tillgängliga på detta sätt, innebär det ändå ett rutinmässigt uppgiftsutbyte av relativt känsliga uppgifter mellan myndigheterna. Enligt vår bedömning är det inte lämpligt att ett sådant utlämnande sker enbart med stöd av generalklausulen. Det kan vidare ifrågasättas om det är meningen att generalklausulen ska användas i fall där lagstiftaren redan har konstaterat att det finns ett behov av ett rutinmässigt utlämnande av en större mängd uppgifter och således har en möjlighet att författningsreglera detta utlämnande. Vi anser därför att det bör införas sekretessbrytande regler i form av uppgiftsskyldigheter till stöd för det utlämnande av uppgifter genom direktåtkomst som föreslås.

8.6.2 Sekretessbrytande bestämmelser

Förslag: Trots sekretess enligt 35 kap. 1 § och 37 kap. 1 § OSL, ska Försvarsmakten och FRA ha rätt att ta del av sådana uppgifter som avses i den föreslagna regeln i 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 15 § första stycket PuL UNDSÄK.

Trots sekretess enligt 38 kap. 4 § OSL, ska Säkerhetspolisen och Försvarsmakten ha rätt att ta del av sådana uppgifter som avses i den föreslagna regeln i 15 § första stycket FRA-PuL.

Skälen för förslagen

Sekretessgenombrott mellan NCT-myndigheterna

För att myndigheterna inom NCT-samarbetet ska kunna medge varandra direktåtkomst till uppgifter i den egna myndighetens verksamhet behövs det regler som bryter sekretessen. Som konstaterats i det föregående avsnittet bör därför sådana sekretessbrytande föreskrifter om uppgiftsskyldighet som avses i 10 kap. 28 § OSL införas.

Det ligger i sakens natur att sekretessbrytande bestämmelser som ska möjliggöra direktåtkomst mellan myndigheter måste vara generellt utformade, eftersom det vid direktåtkomst saknas möjlighet att göra en sekretessprövning i varje enskilt fall. Prövningen måste i stället göras i förväg (prop. 2009/10:85 s. 192). Sådana sekretessbrytande bestämmelser måste dessutom omfatta hela det initiala tillgängliggörandet eftersom redan detta tillgängliggörande för andra myndigheter innebär ett utlämnande i TF:s och OSL:s mening (SOU 2012:90 s. 83).

Sekretessbrytande bestämmelser i form av uppgiftsskyldigheter brukar ofta formuleras som en rätt för mottagande myndighet att ta del av vissa uppgifter. Denna formulering bör, enligt vår bedömning, användas även här. I förevarande fall ska de sekretessbrytande bestämmelserna införas främst för att möjliggöra ett uppgiftsutbyte genom direktåtkomst. Frågan är hur dessa bestämmelser närmare ska utformas och vad de ska omfatta.

När det gäller uppgiftsutbyten mellan andra myndigheter är omständigheterna ofta sådana att den mottagande myndigheten inte i förväg kan veta vilka personer som kan komma att bli aktuella i ärenden hos myndigheten. Vid direktåtkomst måste då den utlämnande myndigheten rent tekniskt tillgängliggöra uppgifter beträffande alla personer som är aktuella hos den utlämnande myndigheten, även om den mottagande myndigheten rent faktiskt inte kommer att ta del av dessa. Som framgår ovan måste sekretessbrytande bestämmelser som ska möjliggöra ett uppgiftsutbyte mellan två myndigheter genom direktåtkomst omfatta alla uppgifter som den utlämnande myndigheten tekniskt gör tillgängliga för den mottagande myndigheten. En sekretessbrytande regel kan således inte i dessa fall begränsas till att enbart avse sådana uppgifter som tjänstemännen hos den mottagande myndigheten i konkreta fall har rätt att ta del av enligt bestämmelsen om direktåtkomst (prop. 2007/08:160 s. 70 f.) När det gäller informationsutbytet inom NCT är de föreslagna bestämmelserna om direktåtkomst emellertid inte formulerade på så sätt att den mottagande myndigheten endast har rätt att ta del av uppgifter om vissa personer i vissa konkreta fall, t.ex. personer som förekommer i vissa ärenden hos myndigheten. Det finns således inget behov av att i det här fallet göra fler uppgifter tillgängliga än vad myndigheterna föreslås få ta del av genom direktåtkomst. De uppgifter som NCT-myndigheterna ska få rätt att ta del av hos varandra genom direktåtkomst, är också de uppgifter som myndigheterna kommer att tekniskt göra tillgängliga för varandra. Vår bedömning är därför att de sekretessbrytande bestämmelserna varken kan eller bör omfatta andra uppgifter än de som myndigheterna får ta del av hos varandra genom direktåtkomst. Myndigheterna bör således inte genom de sekretessbrytande bestämmelserna ges rätt att ta del av fler uppgifter än de kan ta del av genom direktåtkomst. Regleringen kan lämpligen utformas så att det i bestämmelserna om uppgiftsskyldighet hänvisas till de uppgifter som avses i bestämmelserna om direktåtkomst.

Tanken är inte att de sekretessbrytande reglerna om uppgiftsskyldighet generellt ska öppna upp för ett ökat informationsutbyte mellan NCT-myndigheterna. Uppgiftsskyldigheten ska enbart gälla inom ramen för NCT-samarbetet och, som framgår ovan, endast omfatta sådana uppgifter som myndigheterna får lämna ut genom direktåtkomst. De föreslagna bestämmelserna blir dock tillämpliga

även vid utlämnande av sådana uppgifter på annat sätt inom samarbetet. Eftersom direktåtkomsten i princip inte ska omfatta fler uppgifter än vad myndigheterna i dag kan lämna ut till varandra på papper eller muntligen, kommer uppgiftsskyldigheten att gälla endast sådana uppgifter som myndigheterna nu kan lämna ut till varandra med stöd av generalklausulen i 10 kap. 27 § OSL.

Eftersom de sekretessbrytande reglerna i första hand införs som ett komplement till bestämmelserna om direktåtkomst, bör bestämmelserna om uppgiftsskyldighet och bestämmelserna om direktåtkomst ses tillsammans och avvägningen i förhållande till eventuella integritetsintrång göras gentemot regleringen som helhet. Vi har ovan konstaterat 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. Vid denna bedömning har vi också beaktat att ett utlämnande genom direktåtkomst förutsätter att viss sekretess bryts mellan myndigheterna. Med hänsyn till den effektivitetsvinst och den förbättring av verksamheten som en möjlighet till utlämnande genom direktåtkomst innebär för NCT-samarbetet, anser vi därför att den ökade risk för integritetsintrång som sekretessgenombrottet i det här fallet innebär, kan godtas.

Vilka sekretessbestämmelser ska de nya bestämmelserna omfatta?

De uppgifter som Säkerhetpolisen vill kunna lämna ut till FRA och Försvarsmakten genom direktåtkomst omfattas huvudsakligen av reglerna i 15 kap. 1 och 2 §§ och 18 kap. 2 § OSL, medan de uppgifter som FRA och Försvarsmakten vill kunna lämna ut till varandra och till Säkerhetspolisen huvudsakligen omfattas av 15 kap. 1 och 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. Skaderekvisitet är då inte uppfyllt, varför uppgifterna inte är sekretessbelagda enligt dessa bestämmel-

ser. 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 utlänningar. Vår bedömning är att utlämnande av uppgifter inom NCT-samarbetet i princip inte medför någon sådan fara för enskilda eftersom den aktuella sekretessbestämmelsen är tillämplig hos alla tre myndigheterna. Det torde inte heller medföra 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 här heller och bestämmelsen torde härmed inte hindra ett utlämnande inom samarbetet.

De uppgifter som myndigheterna lämnar ut till varandra i dag och som framöver ska kunna lämnas ut genom direktåtkomst torde således inte vara sekretessbelagda enligt ovan nämnda bestämmelser, så länge det handlar om utlämnande inom NCT-samarbetet. Utgångspunkten är också att myndigheterna redan i dag kan lämna ut uppgifter som är sekretessreglerade enligt dessa bestämmelser till varandra. 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 nästa alltid anses vara till skada eller men för den enskilde. Som framgår ovan lämnar myndigheterna i dag ut sådana uppgifter till varandra med stöd av generalklausulen i 10 kap. 27 § OSL. Ett sådant utlämnande förutsätter emellertid att det görs en bedömning i varje enskilt fall av om uppgifterna trots sekretess

kan lämnas ut eller inte. Det torde således 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. Som vi har konstaterat ovan bör detta ske genom bestämmelser om uppgiftsskyldighet.

De bestämmelser om uppgiftsskyldighet som vi föreslår 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 andra sekretessbestämmelser är tillämpliga får det, 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.

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 vad 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). Vi anser att samma bedömning kan 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.

Precis som när det gäller polisverksamheten, anser vi att andra myndigheters tillgång till uppgifter som behandlas av FRA och Försvarsmakten i allmänhet bör 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 vi också föreslagit att bestämmelserna om direktåtkomst för FRA:s och Försvarsmaktens del ska införas i lag. Bestämmelserna om uppgiftsskyldighet är så tätt förknippade med bestämmelserna om direktåtkomst att de bör placeras på samma normgivningsnivå och i anslutning till varandra. Precis som när det gäller direktåtkomsten bör således de sekretessbrytande bestämmelserna om uppgiftsskyldighet införas i PuL UNDSÄK och i FRA-PuL.

8.6.3 Sekretess hos mottagande myndigheter

Bedömning: Några kompletterande sekretessbestämmelser behöver inte införas för myndigheterna inom NCT-samarbetet.

Skälen för bedömningen

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.

Som tidigare redogjorts för omfattas de uppgifter som NCT-myndigheterna vill medge direktåtkomst till 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.

Bestämmelserna till skydd för enskilds personliga och ekonomiska förhållanden är däremot inte primära hos alla tre myndigheterna. Hos Säkerhetspolisen gäller sekretess till skydd för enskild enligt 35 kap. 1 § och 37 kap. 1 § OSL. Hos FRA och Försvars-

makten skyddas uppgifter om enskilda genom sekretessbestämmelsen i 38 kap. 4 § OSL. Bestämmelserna är primära hos respektive myndighet och har således företräde framför överförd sekretess. Detta innebär att bestämmelserna inte ska tillämpas hos mottagande myndighet vid direktåtkomst. Bestämmelserna i 35 kap. 1 §, 37 kap. 1 § och 38 kap. 4 § OSL är dock alla försedda med ett omvänt skaderekvisit, vilket innebär att uppgifterna i princip 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. Vår bedömning är därför att det inte behöver införas några kompletterande sekretessbestämmelser med anledning av förslaget om direktåtkomst.

8.7 Ändamålsbestämmelser

Bedömning: Det behöver inte införas några kompletterande ändamålsbestämmelser i myndigheternas registerförfattningar med anledning av förslaget om direktåtkomst.

Skälen för bedömningen

För att myndigheter ska kunna utbyta information som innefattar personuppgifter krävs att utlämnandet inte kommer i konflikt med bestämmelser om behandling av personuppgifter i myndigheternas registerförfattningar. Det är främst ändamålsregleringen i myndigheternas registerförfattningar som är relevant i detta sammanhang.

NCT-myndigheterna lämnar redan i dag ut uppgifter till varandra inom ramen för samarbetet. Som tidigare redogjorts för sker detta dock främst på papper eller muntligen. Som vi har konstaterat i kapitel 7.2.3 har det utlämnande av personuppgifter som i dag sker mellan NCT-myndigheterna stöd i respektive myndighets registerförfattning. I PDL finns sekundära ändamålsbestämmelser som ger Säkerhetspolisen möjlighet att behandla personuppgifter

när det är nödvändigt för att tillhandahålla information som behövs i en myndighets verksamhet, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott (6 kap. 2 § 2 PDL). Säkerhetspolisen får även behandla personuppgifter i den utsträckning skyldigheten att lämna uppgifter följer av lag eller förordning (6 kap. 2 § andra stycket PDL). FRA och Försvarsmakten lämnar ut personuppgifter med stöd av den s.k. finalitetsprincipen, dvs. uppgifterna får lämnas ut om ändamålet med behandlingen inte är oförenligt med det ursprungliga ändamål för vilket uppgifterna samlades in (1 kap. 6 § FRA-PuL och 1 kap. 6 § PuL UNDSÄK).

Ändamålsbestämmelserna reglerar möjligheten att generellt behandla personuppgifter genom utlämnande oavsett i vilken form utlämnandet sker. Att NCT-myndigheterna nu ges möjlighet att lämna ut uppgifter genom direktåtkomst medför därför ingen annan bedömning av ändamålsbestämmelserna än den som gjorts i kapitel 7.2.3. Det finns således stöd i myndigheternas registerförfattningar för det utlämnande genom direktåtkomst som föreslås och några ytterligare bestämmelser behöver inte införas.

9 Konsekvenser av förslagen

Bedömning: Förslagen väntas få positiva konsekvenser för brottsbekämpningen och ger inte upphov till kostnader som inte kan täckas av myndigheternas befintliga anslag. Den eventuella risken för ökat integritetsintrång som förslagen kan medföra är godtagbar i förhållande till samhällets intresse av att terrorism bekämpas.

Skälen för bedömningen

Ekonomiska konsekvenser och konsekvenser för brottsbekämpningen

Våra förslag innebär att Säkerhetspolisen, FRA och Försvarsmakten, inom ramen för NCT-samarbetet, ges rätt att lämna ut uppgifter till varandra genom direktåtkomst. Syftet med förslagen är att uppgiftsutbytet mellan myndigheterna ska kunna underlättas så att samverkan inom NCT kan effektiviseras. 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 vår 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 datorsystem och torde således inte kräva några nya tekniska lösningar. De kostnader som kan uppkomma för att man ska kunna lösa direktåtkomsten rent tekniskt, bör rymmas inom myndigheternas anslag.

Konsekvenser för den personliga integriteten

Frågan om förslagens följder för den personliga integriteten har behandlats i avsnitten 8.4 och 8.6. Vi har där betonat vikten av att NCT-myndigheternas behov av direktåtkomst övervägs noga och att behoven vägs mot integritetsriskerna. Myndigheternas verksamhetsbehov måste således vägas mot hänsynen till den enskildes personliga integritet.

Vid en bedömning av förslagens 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.

Som vi har konstaterat tidigare kan emellertid 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. I myndigheternas registerförfattningar finns även regler som sätter gränser för behandlingen av personuppgifter, såsom 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.

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 och möjligheterna att nå de integrationspolitiska målen eller på miljön.

10 Ikraftträdande

Förslag: De föreslagna författningsändringarna ska träda i kraft den 1 januari 2018.

Skälen för förslaget

Författningsförslagen är angelägna och bör därför träda i kraft så snart som möjligt. Med hänsyn till den tid som beräknas krävas för lagstiftningsarbetet föreslås de nya bestämmelserna träda i kraft den 1 januari 2018. Några övergångsbestämmelser bedöms inte behövas.

11 Författningskommentar

11.1 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 försvarsunder rättelseverksamhet 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 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, kan med stöd av 8 kap. 7 § regeringsformen meddela

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 FRA inom ramen för samarbetet i NCT. Övervägandena finns i avsnitt 8.4.

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 normalt 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.

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 § PuF UNDSÄK.

I *andra stycket* har det gjorts en språklig ändring med anledning av att bestämmelsen i första stycket har införts. Eftersom utlämnande genom direktåtkomst till Säkerhetspolisen och FRA nu regleras i första stycket anger informationsbestämmelsen i andra stycket att regeringen, eller den myndighet som regeringen bestämmer, kan meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. Dessutom har en hänvisning till 8 kap. 7 § RF lagts till. Förändringarna innebär ingen ändring i sak.

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. Det har även införts en hänvisning till 8 kap. 7 § RF.

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 8.6.2.

I bestämmelsen anges att FRA och Säkerhetspolisen 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 den sekretess som kan gälla för uppgifterna hos Försvarsmakten.

11.2 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 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 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, kan med stöd av 8 kap. 7 § regeringsformen meddela

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 8.4.

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 normalt 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.

I *andra stycket* har det gjorts en språklig ändring med anledning av att bestämmelsen i första stycket har införts. Eftersom utlämnande genom direktåtkomst till Säkerhetspolisen och Försvarsmakten nu regleras i första stycket anger informationsbestämmelsen i andra stycket att regeringen, eller den myndighet som regeringen bestämmer, kan meddela ytterligare föreskrifter om vilka myndigheter som får ha direktåtkomst till uppgiftssamlingar. Dessutom har en hänvisning till 8 kap. 7 § RF lagts till. Förändringarna innebär ingen ändring i sak.

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. Det har även införts en hänvisning till 8 kap. 7 § RF.

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.

Paragrafen är ny och reglerar viss uppgiftsskyldighet för FRA. Övervägandena finns i avsnitt 8.6.2.

I bestämmelsen anges att Försvarsmakten och Säkerhetspolisen 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 Försvarsmakten 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, 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 Försvarsmaktens och Säkerhetspolisens rätt att ta del av uppgifterna uppkommer en sådan uppgiftsskyldighet som enligt 10 kap. 28 § första stycket OSL bryter den sekretess som kan gälla för uppgifterna hos FRA.

11.3 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 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 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 8.4.

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 Försvarsmakten 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, Försvarsmakten 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 direkt-

åtkomst får normalt 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.

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.

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.

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.

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.

Paragrafen är ny och reglerar viss uppgiftsskyldighet för Säkerhetspolisen. Övervägandena finns i avsnitt 8.6.2.

I bestämmelsen anges att FRA och Försvarsmakten 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 den sekretess som kan gälla för uppgifterna hos Säkerhetspolisen.

REGERINGSKANSLIET

Utdrag **§ 428**

Protokoll

2015-10-01 Ju/2015/07312/P

Justitiedepartementet

Uppdrag att utreda behandlingen av personuppgifter inom NCT

Bakgrund

Nationellt centrum för terrorhotbedömning – NCT

NCT bildades som en arbetsgrupp 2005 och består av personal från Säkerhetspolisen, Försvarets radioanstalt och Försvarsmakten. Samarbetet regleras sedan 2009 i en skriftlig överenskommelse mellan myndigheterna.

NCT har till uppgift att göra strategiska terrorhotbedömningar på kort och lång sikt mot Sverige och svenska intressen. NCT ska även producera strategiska analyser av händelser, trender och omvärldsutveckling med koppling till terrorism som berör, eller kan komma att beröra, Sverige och svenska intressen. Samarbetet syftar således inte till att utreda brott.

För att NCT ska kunna leverera relevanta och aktuella bedömningar krävs att medarbetarna vid NCT ges tillgång till underrättelseinformation från de tre myndigheterna, vilket kan inkludera personuppgifter. Utbytet av personuppgifter är nödvändigt för att medarbetarna ska kunna bedöma olika aktörers avsikt och förmåga.

Medarbetarna vid NCT använder sina egna myndigheters it-system och har inte tillgång till varandras system. Det finns även en gemensam NCT-mapp, som medarbetarna från alla tre myndigheterna har

tillgång till. Den gemensamma mappen innehåller utkasten till de rapporter som ännu inte färdigställts.

Behandling av personuppgifter

NCT:s bedömningar och rapporter baseras på sekretessbelagd information från de tre samarbetande myndigheterna. Informationen kan även innehålla personuppgifter.

Regler om utlämnande av uppgifter från en myndighet till en annan finns dels i offentlighets- och sekretesslagen (2009:400), dels i de författningar som reglerar myndigheternas personuppgiftsbehandling. För att myndigheter ska kunna utbyta information krävs att informationen inte omfattas av sekretess eller att sekretessen kan brytas. Vidare krävs att det finns stöd för att uppgifterna får lämnas ut.

Säkerhetspolisens behandling av personuppgifter inom ramen för NCT-samarbetet sker med stöd av 5 kap. 1 § första stycket 1 b och c polisdatalagen (2010:361). Enligt dessa bestämmelser får personuppgifter behandlas i Säkerhetspolisens brottsbekämpande verksamhet om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och brott enligt 3 § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall.

Försvarets radioanstalt behandlar personuppgifter inom ramen för samarbetet med stöd av 1 kap. 8 § lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet. Enligt bestämmelsen får personuppgifter behandlas i myndighetens försvarsunderrättelseverksamhet om det är nödvändigt för att bedriva den verksamhet som anges i lagen (2000:130) om försvarsunderrättelseverksamhet. Vidare anges att uppgifter om en person endast får behandlas om personen har anknytning till en preciserad inriktning för försvarsunderrättelseverksamheten och behandlingen är nödvändig för att fullfölja den inriktningen.

Försvarsmakten behandlar personuppgifter inom ramen för samarbetet med stöd av 1 kap. 8 § lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst. Bestämmelsens lydelse motsvarar den som finns i 1 kap. 8 § lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Tillsyns- och kontrollmyndigheter

Statens inspektion för försvarsunderrättelseverksamheten (Siun) och Säkerhets- och integritetsskyddsnämnden (SIN) har tillsyns- och kontrollansvar för den verksamhet som bedrivs vid NCT. Dessutom är Datainspektionen tillsynsmyndighet avseende personuppgiftsbehandlingen enligt lagen om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet, lagen om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och polisdatalagen.

SIN har i en rapport den 6 maj 2015 bedömt att det gemensamma rapportförfattandet som sker mellan myndigheterna är att anse som ett elektroniskt utlämnande (SIN Dnr 324-2014). SIN har vidare konstaterat att polisdatalagen inte är anpassad för sådant samarbete mellan myndigheter som förekommer inom ramen för NCT och att det finns anledning att närmare analysera de rättsliga förutsättningar som gäller vid sådant samarbete.

Behovet av en utredning

Olika former av samverkan mellan myndigheter har blivit allt vanligare. Bakgrunden till detta är bl.a. att regeringen genom regleringsbrev och separata regeringsuppdrag uppmanat myndigheterna att samverka och att effektivisera den samverkan som redan finns etablerad. När det gäller NCT har myndigheterna själva tagit initiativ till samverkan. Ett viktigt led i alla former av samverkan är möjligheten att kunna utbyta information.

Samarbetet inom NCT möjliggör ett tillvaratagande av de tre myndigheternas samlade kompetens. Det är viktigt 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 därför viktigt att samarbetet fortsätter. Samtidigt medför ökade möjligheter till utbyte av personuppgifter som behandlas automatiserat risker för den personliga integriteten. Det får heller inte råda någon tvekan om vem som är ansvarig för den personuppgiftsbehandling som sker.

Säkerhetspolisen har i en skrivelse till regeringen (Ju2015/05096/L4) pekat på ett behov av att effektivisera uppgiftsutbytet inom NCT. Säkerhetspolisen har föreslagit att myndigheten ska ges möjlighet att medge Försvarsmakten och Försvarets radioanstalt direktåtkomst till personuppgifter som gjorts gemensamt tillgängliga för NCT-samarbetet i Säkerhetspolisens verksamhet om uppgifterna behövs för att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen. Många av de uppgifter som NCT:s bedömningar och rapporter bygger på kommer från Säkerhetspolisens underrättelseinformation. Det är därför direkt avgörande för samarbetet att berörda tjänstemän från de två andra myndigheterna har direktåtkomst till relevant information från Säkerhetspolisen.

Med hänsyn till SIN:s granskning och Säkerhetspolisens skrivelse finns det anledning att närmare analysera de rättsliga förutsättningarna för det samarbete som sker inom NCT och hur samarbetet kan effektiviseras.

Uppdraget

En utredare ges i uppdrag att beskriva den verksamhet som bedrivs inom ramen för NCT-samarbetet och analysera de rättsliga förutsättningarna för Säkerhetspolisens, Försvarsmaktens och Försvarets radioanstalts personuppgiftsbehandling inom ramen för

NCT-samarbetet i syfte att klarlägga om det finns behov av ett tydligare lagstöd för den personuppgiftsbehandling som sker.

Utredaren ska 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.

Utredaren ska lämna förslag på de författningsändringar som bedöms nödvändiga. Det ska särskilt säkerställas att det blir en lämplig avvägning mellan intresset av ett effektiviserat informationsutbyte och skyddet för den personliga integriteten i de förslag som lämnas. Redovisning ska göras för hur skyddet av den personliga integriteten stärks genom en författningsreglering. Utredaren ska analysera och redovisa förslagens ekonomiska konsekvenser. Om kostnader bedöms uppkomma ska ett finansieringsförslag lämnas.

Under utförandet av uppdraget ska utredaren informera sig om annat arbete som kan vara av betydelse för uppdragets genomförande och samråda med Säkerhetspolisen, Försvarets radioanstalt, Försvarsmakten samt övriga berörda myndigheter.

Uppdraget ska redovisas senast den 31 augusti 2016.