



Säkerhetspolisens behandling av personuppgifter inom ramen för NCT-samarbetet

1. SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat Säkerhetspolisens behandling av personuppgifter inom ramen för samarbetet i Nationellt centrum för terrorhotbedömning, som är en permanent arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt och Militära underrättelse- och säkerhetstjänsten. Nationellt centrum för terrorhotbedömning har till uppgift att göra strategiska bedömningar av terrorhot mot Sverige och svenska intressen i utlandet. Bedömningarna görs i rapporter som skrivs gemensamt av analytiker från de tre myndigheterna.

Nämndens granskning har framför allt fokuserat på frågan om Säkerhetspolisens personuppgiftsansvar vid upprättandet av rapporter inom ramen för samarbetet. Nämnden anser att Säkerhetspolisen är personuppgiftsansvarig för all behandling som sker vid upprättandet av rapporter, således även i rapportutkastet.

Vid en översiktlig granskning av ett antal rapporter har nämnden inte påträffat några uppgifter som bedöms falla utanför de för Säkerhetspolisen tillåtna ändamålen. Nämnden har inte heller påträffat några känsliga personuppgifter som behandlas utan stöd i polisdatalagen. Slutligen bedömer nämnden att det elektroniska utlämnande av uppgifter som sker vid upprättandet av rapporter är förenligt med polisdatalagen.

Innehåll

1. SAMMANFATTNING.....	1
2. BAKGRUND OCH AVGRÄNSNING	3
2.1. Tre myndigheter arbetar gemensamt i NCT	3
2.2. Samarbetet inom NCT försvåras av regelverkets utformning	3
2.3. Avgränsning.....	4
3. RÄTTSLIGA UTGÅNGSPUNKTER.....	4
3.1. Säkerhetspolisen ansvarar för sin personuppgiftsbehandling	4
3.2. Uppgifter får behandlas bara om det behövs för vissa ändamål	5
3.3. Bara enstaka uppgifter får lämnas ut elektroniskt.....	6
4. UTREDNINGEN	7
4.1. Granskningens genomförande	7
4.2. Vilken behandling i rapporterna ansvarar Säkerhetspolisen för?	7
4.3. Får Säkerhetspolisen behandla uppgifterna i rapporterna?.....	8
4.4. Lämnar Säkerhetspolisen ut uppgifter på ett otillåtet sätt?.....	9
4.5. Personuppgifter i de granskade rapporterna	9
5. NÄMNDENS BEDÖMNING	9
5.1. Vilken behandling ansvarar Säkerhetspolisen för?.....	9
<i>Är Säkerhetspolisen personuppgiftsbiträde?</i>	<i>9</i>
<i>Är Säkerhetspolisen personuppgiftsansvarig för samtliga uppgifter i rapportutkasten?</i>	<i>10</i>
<i>Övriga NCT-myndigheters personuppgiftsansvar</i>	<i>11</i>
5.2. Får Säkerhetspolisen behandla uppgifterna i rapporterna enligt PDL? 11	
5.3. Lämnar Säkerhetspolisen ut uppgifter elektroniskt på ett otillåtet sätt?12	
5.4 Avslutande synpunkter.....	13

2. BAKGRUND OCH AVGRÄNSNING

2.1. Tre myndigheter arbetar gemensamt i NCT

Nationellt centrum för terrorhotbedömning (NCT) är en permanent arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten (Must). Gruppen tillhörde ursprungligen Samverkansrådet mot terrorism, där fjorton myndigheter samarbetar för att stärka Sveriges förmåga att motverka och hantera terrorism. Sedan år 2009 är gruppen dock direkt underställd Säkerhetspolisen, FRA och Försvarsmakten genom Must (NCT-myndigheterna). Samarbetet regleras i en skriftlig överenskommelse mellan NCT-myndigheterna.

NCT har till uppgift att göra strategiska bedömningar av terrorhot mot Sverige och svenska intressen i utlandet på kort och på lång sikt. Inom NCT arbetar analytiker från de tre NCT-myndigheterna i gemensamma lokaler hos Säkerhetspolisen. Genom att de tillsammans analyserar underrättelseinformation från alla tre myndigheterna ska myndigheternas samlade förmåga att göra strategiska bedömningar stärkas.

NCT:s rapporter med bedömningar delges alltid de tre NCT-myndigheterna. Vid behov delges rapporterna även delar av Regeringskansliet och övriga myndigheter inom Samverkansrådet mot terrorism. Till andra än NCT-myndigheterna skickas ofta bearbetade versioner av rapporterna, som har kortats ned för att inte röja känslig underrättelseinformation.

2.2. Samarbetet inom NCT försvåras av regelverkets utformning

I en gemensam skrivelse till regeringen daterad den 25 oktober 2011 framförde NCT-myndigheterna att det finns ett behov av att se över regleringen för samarbetet. I skrivelsen beskrivs problemen med regleringen på följande sätt.

NCT är en samarbetsform som inte förutsågs när de tre olika regelverk som gäller för NCT-myndigheternas personuppgiftsbehandling kom till. De tre myndigheternas olika regelverk fungerar bra för deras egen verksamhet men medför praktiska problem i det dagliga NCT-samarbetet. Frågor uppstår om vem som är personuppgiftsansvarig för viss behandling och hur långt man kan gå när det gäller att samarbeta i t.ex. en gemensam databas. Regleringens utformning förhindrar därmed en effektivare samverkan inom NCT.

I sin nationella strategi mot terrorism från år 2012¹ noterar regeringen att NCT-myndigheterna har framfört ett behov av förbättrade möjligheter att utbyta information och konstaterar att det finns anledning att följa frågan vidare. Regeringen påpekar också att NCT har en central funktion för

¹ Regeringens skrivelse 2011/12:73 Ansvar och engagemang – en nationell strategi mot terrorism.

hotbedömningar mot Sverige och svenska intressen. Någon översyn av tillämpliga regler för NCT-samarbetet har dock inte gjorts.

2.3. Avgränsning

Nämnden har tillsyn över Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (2010:361) och den äldre polisdatalagen (1998:622). Granskningen har därför inte omfattat frågan hur de två andra NCT-myndigheterna behandlar personuppgifter inom samarbetet.

Under ärendets handläggning har granskningen avgränsats och inriktats särskilt på vissa grundläggande frågor som har central betydelse för behandlingen av personuppgifter i NCT:s verksamhet.

- Vilken behandling av personuppgifter ansvarar Säkerhetspolisen för inom ramen för NCT-samarbetet?
- Får Säkerhetspolisen behandla uppgifterna?
- Lämnar Säkerhetspolisen ut uppgifter elektroniskt på ett otillåtet sätt?

Syftet med granskningen har således inte varit att göra en heltäckande genomgång av om Säkerhetspolisens behandling av personuppgifter inom NCT-samarbetet uppfyller kraven i PDL. Granskningen har inte heller omfattat frågan om utlämnande av uppgifter mellan myndigheterna inom NCT-samarbetet är förenligt bestämmelserna i offentlighets- och sekretesslagen (2009:400).

3. RÄTTSLIGA UTGÅNGSPUNKTER

3.1. Säkerhetspolisen ansvarar för sin personuppgiftsbehandling

När Säkerhetspolisen behandlar personuppgifter i sin brottsbekämpande verksamhet gäller PDL. När FRA och Must behandlar personuppgifter gäller däremot andra regler.²

Enligt PDL är Säkerhetspolisen personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.³ Med behandling av personuppgifter avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, användning, utlämnande genom översändande,

² Bland annat lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet och lagen (2007:258) om behandling av personuppgifter i Försvarmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

³ 5 kap. 5 § PDL.

spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring.⁴

Personuppgiftsansvaret innebär ett ansvar för att behandlingen sker i enlighet med PDL:s regler. Ansvaret innebär också bland annat en skyldighet att på begäran av en registrerad rätta, blockera eller utplåna personuppgifter som behandlas i strid med PDL⁵ och att i vissa fall utge skadestånd till den registrerade om uppgifter behandlats på ett olagligt sätt⁶.

Enligt definitionen i personuppgiftslagen (1998:204), som gäller för Säkerhetspolisens behandling av personuppgifter enligt PDL, är den personuppgiftsansvarig som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.⁷ Vem som bestämmer över ändamålen och medlen avgörs genom en bedömning av de faktiska omständigheterna i det enskilda fallet.⁸ För en och samma behandling kan det finnas två eller flera personuppgiftsansvariga.⁹

Ett personuppgiftsbiträde kan behandla personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde och den eller de personer som arbetar under bitrådets eller den personuppgiftsansvariges ledning får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Det ska finnas ett skriftligt avtal om personuppgiftsbitrådets behandling av personuppgifter för den personuppgiftsansvariges räkning. I det avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktioner från den personuppgiftsansvarige.¹⁰

3.2. Uppgifter får behandlas bara om det behövs för vissa ändamål

Säkerhetspolisen får behandla personuppgifter i sin brottsbekämpande verksamhet bara om det *behövs* för något av de ändamål som anges i PDL. Bland annat får uppgifter behandlas om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar terroristbrott eller finansiering av vissa typer av särskilt allvarlig brottslighet.¹¹

Så kallade känsliga personuppgifter får behandlas endast om det är *absolut nödvändigt* för ändamålet med behandlingen.¹² Ett exempel på känsliga

⁴ 2 kap. 2 § första stycket 1 och 5 kap. 4 § 1 PDL samt 3 § personuppgiftslagen (1998:204).

⁵ 2 kap. 2 § första stycket 6 och 5 kap. 4 § 1 PDL samt 28 § personuppgiftslagen.

⁶ 2 kap. 2 § första stycket 12 och 5 kap. 4 § 1 PDL samt 48 § personuppgiftslagen.

⁷ 2 kap. 2 § första stycket 1 och 5 kap. 4 § 1 PDL samt 3 § personuppgiftslagen.

⁸ Datainspektionens beslut 2010-07-02, dnr 686-2010.

⁹ Öman & Lindblom, Personuppgiftslagen – En kommentar, fjärde upplagan, 2011, s. 99.

¹⁰ 3 och 30 §§ personuppgiftslagen.

¹¹ 5 kap. 1 § 1 b och 1 c PDL.

¹² 2 kap. 10 § och 5 kap. 4 § 4 PDL.

personuppgifter är uppgifter om en persons religiösa övertygelse. Att det ska vara absolut nödvändigt att behandla uppgifterna innebär att behovet måste prövas noga i det enskilda fallet.¹³

När uppgifter har samlats in för ett tillåtet ändamål får de också vidarebehandlas för vissa andra ändamål. Bland annat får uppgifterna vidarebehandlas för att tillhandahålla information som en annan myndighet behöver inom ramen för myndighetsöverskridande samverkan mot brott.¹⁴ Samverkansrådet mot terrorism nämns i PDL:s förarbeten som ett sammanhang där Säkerhetspolisen behöver ha möjlighet att tillhandahålla information till andra myndigheter.¹⁵

3.3. Bara enstaka uppgifter får lämnas ut elektroniskt

Personuppgifter får enligt PDL lämnas ut på *medium för automatiserad behandling*. Det får dock bara röra sig om enstaka uppgifter.¹⁶ Bestämmelsen är tillämplig så snart det rör sig om någon form av elektroniskt utlämnande. Som exempel nämns i PDL:s förarbeten 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.¹⁷

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 telefonnummer. Även utlämnande av t.ex. ett ärende eller delar av ett ärende där personuppgifter förekommer är förenligt med bestämmelsen.¹⁸

En särskild typ av elektroniskt utlämnande är så kallad *direktåtkomst*. Säkerhetspolisen får inte lämna ut uppgifter genom direktåtkomst.¹⁹

Begreppet direktåtkomst har inte definierats i lag. Enligt förarbetena till PDL är den grundläggande innebörden av begreppet att någon har direkt tillgång till någon annans register, databaser eller andra samlingar av uppgifter och på

¹³ Prop. 2009/10:85 s. 325.

¹⁴ 5 kap. 2 § första stycket 2 PDL.

¹⁵ Prop. 2009/10:85 s. 262.

¹⁶ 2 kap. 20 § och 5 kap. 4 § 7 PDL.

¹⁷ Prop. 2009/10:85 s. 185 och s. 333.

¹⁸ Prop. 2009/10:85 s. 333.

¹⁹ 5 kap. 4 § 4 och 2 kap. 21 § PDL samt prop. 2009/10:85 s. 178 f.

egen hand kan söka efter information, dock utan att kunna påverka innehållet i uppgiftssamlingen.²⁰

4. UTREDNINGEN

4.1. Granskningens genomförande

Säkerhetspolisen har besvarat frågor om personuppgiftsbehandlingen inom ramen för NCT. Nämnden har också tagit del av NCT:s skriftliga rutinbeskrivningar och NCT-myndigheternas överenskommelser avseende samarbetet.

Nämnden har genomfört en inspektion hos NCT den 10 mars 2015. Vid inspektionen har tio rapporter från de senaste åren granskats översiktligt. Sju av dessa rapporter färdigställdes under år 2013 och 2014. Tre av rapporterna var utkast under bearbetning.

4.2. Vilken behandling i rapporterna ansvarar Säkerhetspolisen för?

Säkerhetspolisen har uppgett följande.

Analytikerna vid NCT använder sina egna myndigheters it-system och har inte tillgång till varandras system. De tre NCT-myndigheterna har också varsin avskild NCT-mapp på Säkerhetspolisens server som bara den egna myndighetens personal har tillgång till. Varje myndighet är ansvarig för den behandling av personuppgifter som förekommer i den egna NCT-mappen.

Utöver myndigheternas egna NCT-mappar finns även en gemensam NCT-mapp, som analytikerna från alla tre myndigheterna har tillgång till. Den gemensamma mappen innehåller utkastet till de NCT-rapporter som ännu inte har färdigställts.

En rapport skrivs alltid av flera analytiker tillsammans. Det ska normalt sett finnas minst en analytiker från varje NCT-myndighet med i den grupp som skriver rapporten. En av analytikerna brukar vara huvudredaktör för rapporten och skriva det mesta av texten. Därmed brukar det också vara den personen som lägger in de flesta av personuppgifterna i rapporten, om sådana förekommer. Detta gäller oavsett vilken NCT-myndighet personuppgifterna ursprungligen kommer ifrån eftersom analytikerna från de olika myndigheterna diskuterar och planerar innehållet i rapporten tillsammans. De få personuppgifter som finns i rapporterna brukar dock röra personer som alla tre NCT-myndigheter redan känner till och behandlar uppgifter om.

²⁰ Prop. 2009/10:85 s. 168 och s. 333 f.

När en analytiker lägger in en personuppgift i ett utkast till en rapport ska analytikern märka uppgifterna med en fotnot där han eller hon lägger in sin signatur. Personuppgifter kan också läggas in i en fotnot, och ska även då åtföljas av en signatur.

NCT-myndigheterna är bara personuppgiftsansvariga för de uppgifter som respektive myndighets egna analytiker har lagt in i utkastet till rapporter. Det finns enligt Säkerhetspolisens bedömning inte några uppgifter som två eller tre av myndigheterna har gemensamt personuppgiftsansvar för.

Eftersom Säkerhetspolisen ansvarar för administration och teknisk support av alla NCT-mappar kan myndigheten rent tekniskt komma att behandla de personuppgifter som de andra myndigheterna ansvarar för. Denna behandling utför Säkerhetspolisen dock som personuppgiftsbiträde för den aktuella myndigheten enligt de överenskommelser om personuppgiftsbiträde som upprättats mellan Säkerhetspolisen och FRA respektive Must. PDL är därför inte tillämplig på den behandlingen.

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 tagits bort. De upprättade versionerna av rapporten flyttas i samband med expediering över till Säkerhetspolisens NCT-mapp tillsammans med den slutliga versionen av rapporten som innehåller fotnoter. Samtliga versioner av rapporterna raderas från den gemensamma NCT-mappen. I samband med detta blir Säkerhetspolisen ansvarig för behandlingen av alla personuppgifter i rapporten. Uppgifterna sparas hos Säkerhetspolisen i syfte att kunna garantera spårbarhet avseende underlaget till de bedömningar som NCT gör i sina rapporter. Uppgifterna gallras i enlighet med PDL:s regler.

4.3. Får Säkerhetspolisen behandla uppgifterna i rapporterna?

Säkerhetspolisen har uppgett följande.

Säkerhetspolisens eget analysarbete inom NCT sker främst med stöd av bestämmelserna i 5 kap. 1 § punkt 1 b och c PDL om terroristbrott och finansiering av särskilt allvarlig brottslighet. Informationsutbytet med FRA och Must sker med stöd av bestämmelsen i 5 kap. 2 § första stycket 2 PDL om myndighetssamverkan mot brott.

4.4. Lämnar Säkerhetspolisen ut uppgifter på ett otillåtet sätt?

Säkerhetspolisen har uppgett följande.

Den specifika situation som den gemensamma rapportskrivningen inom NCT utgör har ingen motsvarighet i de exempel som finns i förarbetena till PDL. Det rör sig dock inte om åtkomst till ett register eller en databas på ett sådant sätt att det kan anses utgöra direktåtkomst i PDL:s mening.

Det gemensamma rapportskrivandet får däremot anses vara en form av utlämnande av uppgifter på medium för automatiserad behandling. Det innebär att bara enstaka personuppgifter får lämnas ut. Eftersom det behandlas förhållandevis få personuppgifter i rapporterna får det anses röra sig om enstaka uppgifter i PDL:s mening.

4.5. Personuppgifter i de granskade rapporterna

De flesta av de vid inspektionen granskade rapporterna – såväl färdigställda som utkast – innehöll bara personuppgifter om en eller ett fåtal personer, som inte sällan var ledare för större internationella terrorgrupper med religiös inriktning. En av de granskade rapporterna innehöll emellertid uppgifter om ett trettiotal personer. De flesta av personuppgifterna i den rapporten förekom i fotnoterna.

5. NÄMNDENS BEDÖMNING

5.1. Vilken behandling ansvarar Säkerhetspolisen för?

För att PDL:s integritetsskydd ska upprätthållas är det viktigt att det står klart vilken behandling Säkerhetspolisen är personuppgiftsansvarig för. Även ur ett tillsynsperspektiv är det viktigt att det är klarlagt vilken myndighet som har personuppgiftsansvar för viss behandling.

Säkerhetspolisen är enligt 5 kap. 5 § PDL personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför. Även själva lagringen av uppgifter utgör personuppgiftsbehandling. All personuppgiftsbehandling i NCT-samarbetet sker på Säkerhetspolisens server. Fråga uppkommer därför vilket personuppgiftsansvar Säkerhetspolisen har för denna behandling.

Är Säkerhetspolisen personuppgiftsbiträde?

Säkerhetspolisen har uppgett att den genom överenskommelser är personuppgiftsbiträde i förhållande till övriga myndigheter i fråga om viss personuppgiftsbehandling i NCT-samarbetet. Det gäller *dels* sådana uppgifter som endast personal från FRA och Must har tillgång till i sina respektive mappar, *dels* sådana uppgifter som personal från FRA och Must lägger in i

utkasterna till rapporterna i den gemensamma mappen och som dessa myndigheter enligt Säkerhetspolisen ensamma är personuppgiftsansvariga för.

Den behandling av personuppgifter som Säkerhetspolisen utför i form av ren it-administration i de mappar som endast FRA respektive Must har tillgång till får enligt nämndens bedömning anses ske i rollen som personuppgiftsbiträde. För dessa uppgifter har Säkerhetspolisen alltså inte personuppgiftsansvar.

Rapportutkasterna finns i en gemensam mapp som samtliga NCT-myndigheters personal har tillgång till. Endast de för FRA och Must avskilda mapparna och en NCT-gemensam mapp för administrativa dokument omfattas av de överenskommelser om personuppgiftsbiträde som Säkerhetspolisen ingått med FRA respektive Must. Rapportutkasterna kan inte anses vara administrativa dokument och omfattas således inte av överenskommelserna. Redan på denna grund saknas förutsättningar för Säkerhetspolisen att i egenskap av personuppgiftsbiträde behandla uppgifterna i rapportutkasterna.

Utformningen av rapporterna sker gemensamt av de samarbetande myndigheternas personal. Enligt Säkerhetspolisen skrivs rapporterna alltid av flera analytiker tillsammans, och det framstår närmast som en slump vilken av analytikerna som lägger in och märker respektive personuppgift. Uppgifterna i rapportutkasterna behandlas således inte endast i enlighet med instruktioner från Must och FRA, vilket innebär att Säkerhetspolisen inte kan anses behandla uppgifterna i egenskap av personuppgiftsbiträde för Must och FRA. Vidare ifrågasätter nämnden om det överhuvudtaget är möjligt att vara personuppgiftsbiträde avseende enskilda uppgifter i ett dokument där personal från flera olika myndigheter samarbetar och har lika stora möjligheter att lägga till, ta bort och ändra personuppgifter.

Av ovan angivna skäl kan Säkerhetspolisen inte anses behandla uppgifter i rapportutkasterna i egenskap av personuppgiftsbiträde.

Är Säkerhetspolisen personuppgiftsansvarig för samtliga uppgifter i rapportutkasterna?

Som framgått ovan lagras uppgifterna i rapportutkasterna på Säkerhetspolisens server och lagringen sker inte i Säkerhetspolisens egenskap av personuppgiftsbiträde för Must och FRA. Mycket talar därför för att Säkerhetspolisen har personuppgiftsansvar för behandlingen av samtliga uppgifter i rapportutkasterna. När flera behandlar personuppgifter tillsammans måste dock personuppgiftsansvaret bedömas utifrån vem som kan bestämma ändamålen och medlen för behandlingen. Frågan är då om det finns sådana omständigheter som medför att Säkerhetspolisen trots allt inte är personuppgiftsansvarig för sådana uppgifter som personal från FRA eller Must lagt in i rapportutkasterna.

Upprättandet av ett utkast till rapport sker gemensamt av personal från alla tre NCT-myndigheterna i ett dokument. I fotnoter anges vem som fört in en viss personuppgift. Personal från alla tre myndigheterna har möjlighet att lägga till, ändra och ta bort samtliga personuppgifter i utkasten. Behandlingen av personuppgifter sker således i ett mycket nära samarbete mellan personal från samtliga tre myndigheter. Vem som faktiskt för in en personuppgift i ett rapportutkast framstår, som nämnts ovan, närmast som en slump.

Nämnden konstaterar dessutom att systemet med fotnoter, för att peka ut en av NCT-myndigheterna som ensam ansvarig för en personuppgift, inte är konsekvent genomfört i praktiken. Nämnden har endast granskat ett mindre antal NCT-rapporter. Trots detta har nämnden påträffat flera personuppgifter som inte har märkts med någon fotnot. I flera fall har också två myndigheter pekats ut som ansvariga för en och samma personuppgift.

Den märkning av personuppgifter som sker i fotnoterna motsvaras därför inte av någon faktisk begränsning i respektive myndighets möjligheter att bestämma ändamål och medel 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.

Enligt nämndens uppfattning medför inte ordningen med fotnoter att Säkerhetspolisens undgår personuppgiftsansvar för de uppgifter där det anges att personal från någon av de övriga NCT-myndigheterna har lagt in uppgiften. Säkerhetspolisens är således personuppgiftsansvarig för samtliga personuppgifter i de gemensamma rapportutkasten.

Övriga NCT-myndigheters personuppgiftsansvar

Det kan inte uteslutas att även övriga NCT-myndigheter har personuppgiftsansvar för uppgifter i rapportutkasten. Denna fråga ligger dock utanför nämndens tillsynsområde.

5.2. Får Säkerhetspolisen behandla uppgifterna i rapporterna enligt PDL?

Som nämnden konstaterat ovan är Säkerhetspolisen ansvarig även för behandling av sådana personuppgifter som personal från de andra NCT-myndigheterna lagt in vid utarbetandet av rapporterna. För Säkerhetspolisens behandling gäller alltså bestämmelserna i PDL.

Eftersom olika registerförfattningar gäller för de samarbetande myndigheterna, finns det enligt nämnden en risk för att Säkerhetspolisen kan komma att behandla personuppgifter i strid med PDL. Vid sin översiktliga granskning av

ett antal NCT-rapporter och utkast till sådana har nämnden emellertid inte påträffat några uppgifter som bedöms falla utanför de för Säkerhetspolisen tillåtna ändamålen. I de fall som känsliga personuppgifter har behandlats har detta framstått som absolut nödvändigt för syftet med behandlingen.

5.3. Lämnar Säkerhetspolisen ut uppgifter elektroniskt på ett otillåtet sätt?

Säkerhetspolisen får endast lämna ut enstaka uppgifter elektroniskt. Direktåtkomst är inte tillåten till personuppgifter som Säkerhetspolisen behandlar. När Säkerhetspolisen för in personuppgifter i de gemensamma rapporterna innebär det att uppgifterna på elektronisk väg görs tillgängliga för de andra NCT-myndigheterna. Det innebär således en form av elektroniskt utlämnande av personuppgifter. Frågan är om det rör sig om direktåtkomst eller utlämnande på medium för automatiserad behandling.

Med direktåtkomst avses vanligtvis 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.²¹ Det gemensamma rapportförfattandet innebär i och för sig att Säkerhetspolisen regelbundet och i inte obetydlig omfattning ger FRA och Must tillgång till personuppgifter som behandlas i utkasten. Mot bakgrund av att antalet personuppgifter som behandlas i respektive rapport normalt sett är få, att behandlingen inte genererar någon så kallad överskottsinformation²² – vilket normalt sett är fallet vid direktåtkomst – och att alla de tre samarbetande myndigheterna har faktisk möjlighet att påverka innehållet i rapporterna, framstår det som främmande att karakterisera utlämnandet som direktåtkomst. Nämnden bedömer därför att Säkerhetspolisen inte ger direktåtkomst åt de övriga NCT-myndigheterna.

Enstaka personuppgifter får lämnas ut på medium för automatiserad behandling enligt PDL. I takt med att tekniken utvecklats har begreppet utlämnande på medium för automatiserad behandling getts en vidare innebörd än att avse ett överlämnande av elektroniskt lagrade uppgifter via något slags medium för lagring eller överföring.²³ Begreppet får numera anses omfatta i princip all elektronisk överföring av uppgifter.

När Säkerhetspolisen för in personuppgifter i de gemensamma rapporterna får det i det här sammanhanget anses att uppgifterna lämnas ut till de andra NCT-myndigheterna på medium för automatiserad behandling. I de rapporter nämnden granskat rör det sig vanligtvis om få personuppgifter i handlingar som består av löpande text och inte någon sammanställning av

²¹ Prop. 2009/10:85 s. 168.

²² SOU 2012:90 s. 118 f.

²³ SOU 2015:39 s. 128.

personuppgifter. Utlämnandet är snarast att jämföras med utlämnande av ett ärende där personuppgifter förekommer, vilket i förarbetena till PDL nämns som ett exempel på tillåtet utlämnande på medium för automatiserad behandling.

Det kan enligt nämndens uppfattning därför inte anses röra sig om mer än enstaka uppgifter i lagens mening. Utlämnandet är därmed förenligt med PDL i detta avseende.

5.4 Avslutande synpunkter

Nämnden kan konstatera att regleringen i PDL inte är anpassad för sådant samarbete mellan myndigheter som förekommer inom ramen för NCT. Det finns således en risk för att den enskildes integritet åsidosätts. Till exempel är frågan om myndigheternas personuppgiftsansvar otydlig. Utöver frågor som rör behandlingen av personuppgifter finns sekretessrelaterade problem i samarbeten av nu aktuellt slag. Just denna problemställning har nämnden dock inte granskat i detta ärende.

Enligt nämndens uppfattning finns det anledning att närmare analysera de rättsliga förutsättningar som gäller vid samarbete av det slag som förekommer inom NCT. Särskilt bör uppmärksammas om det finns behov av författningsändringar som garanterar att enskildas integritet inte kränks då personuppgifter behandlas i samarbetet.

Sändlista:

Säkerhetspolisen (dnr 2014-22743-3)

För kännedom:

Justitiedepartementet

Datainspektionen

Nationellt centrum för terrorhotbedömning

Statens inspektion för försvarsunderrättelseverksamheten