SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

2013-02-21
Dnr 35-2013

Redovisning av ett uppdrag angående Säkerhets- och integritetsskyddsnämndens tillsynsverksamhet avseende polisens personuppgiftsbehandling

Postadress	Telefon	E-post	Organisationsnummer
Box 22523, 104 22 Stockholm	08-617 98 00	sakint@sakint.se	202100-5703
Besöksadress	**Telefax**	**Webbplats**	**Bankgiro**
Norr Mälarstrand 6, Stockholm	08-617 98 88	www.sakint.se	782-4329

Redovisningens innehåll

1. Sammanfattning

Säkerhets- och integritetsskyddsnämndens tillsynsverksamhet vad gäller personuppgiftsbehandling har sedan den 1 mars 2012 riktats särskilt mot den öppna polisens behandling av personuppgifter. Nämnden har inlett åtta tillsynsärenden på eget initiativ och gjort sex uttalanden om olika uppgiftssamlingar eller företeelser som rör den öppna polisens personuppgifts-behandling. Tillsynen har omfattat såväl inspektioner som andra undersökningar. Den har inneburit att rutiner kartlagts samt att enskilda ärenden och interna föreskrifter kontrollerats.

Nämnden har uppmärksammat brister i några avseenden. Bristerna kan sammanfattas på följande sätt. RPS och granskade polismyndigheter saknar rutiner och tillräcklig intern kontroll för att regleringen om känsliga personuppgifter i polisdatalagen (2010:361) (PDL) och lagen (2010:362) om polisens allmänna spaningsregister (spaningsregisterlagen) ska få tillräckligt genomslag. Några fall av behandling av känsliga personuppgifter som strider mot PDL har kunnat konstateras och i ett par fall har nämnden ifrågasatt om reglerna har följts. När det gäller polisens interna kontroll har nämndens tillsyn visat att den centrala säkerhetsloggen (CSL) ännu några månader efter ikraftträdandet av PDL och spaningsregisterlagen var mycket sparsamt använd av polismyndigheterna. Logguppföljning har vidare inte använts alls i syfte att kontrollera efterlevnaden av förbudet att söka på känsliga personuppgifter i PDL i granskade uppgiftssamlingar.

Nämndens kontroller av den öppna polisens personuppgiftsbehandling på begäran av enskilda har inneburit stora utmaningar för kansliet, och handläggningen har försenats bl.a. på grund av att kontroller i vissa lokala register med teknisk åtkomst hos RPS ännu inte kan göras centralt.

2. Uppdraget

Regeringen har i nämndens regleringsbrev för budgetår 2012 gett nämnden i uppdrag att senast den 15 mars 2013 redovisa hur myndigheten har bedrivit sina nya tillsynsuppgifter med anledning av ikraftträdandet av PDL och spaningsregisterlagen. Redovisningen ska innehålla en sammanhållen beskrivning av den tillsynsverksamhet som bedrivits på området samt en redogörelse för resursanvändningen.

Nämnden har sedan tidigare tillsyn över Säkerhetspolisens person-uppgiftsbehandling enligt bl.a. PDL. Redovisningen omfattar därför endast nämndens tillsyn över den öppna polisens personuppgiftsbehandling.

3. Nämndens uppgifter

Sedan nämnden inrättades har dess tillsyn, enligt lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (tillsynslagen), omfattat brottsbekämpande myndigheters användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet, samt Säkerhetspolisens personuppgiftsbehandling enligt den äldre polisdatalagen (1998:622).

Den 1 mars 2012 trädde vissa ändringar i tillsynslagen i kraft, som innebar att nämndens tillsynsområde utökades till att omfatta hela polisens behandling av personuppgifter enligt PDL och spaningsregisterlagen. Tillsynen ska enligt lagen särskilt avse sådan behandling som avses i 2 kap. 10 § PDL och 12 § spaningsregisterlagen, dvs. behandling av känsliga personuppgifter. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning (1 § tillsynslagen).

I sin tillsyn får nämnden uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten. Nämnden ska vidare verka för att brister i lag eller annan författning avhjälps (2 § tillsynslagen).

Nämnden är även skyldig att på begäran av en enskild kontrollera bl.a. om han eller hon har varit föremål för polisens behandling av personuppgifter enligt PDL och spaningsregisterlagen och om behandlingen har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen utförts (3 § tillsynslagen).

Om nämnden i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska nämnden anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Uppmärksammar nämnden felaktigheter som kan medföra skadeståndsansvar för staten gentemot fysisk eller juridisk person, ska nämnden anmäla det till Justitiekanslern. Finner nämnden omständigheter som Datainspektionen bör uppmärksammas på, ska nämnden anmäla det till inspektionen (20 § förordning [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden).

4. Redovisning av uppdraget

4.1 Resursanvändning

4.1.1 Förberedelser

Inför ikraftträdandet av PDL och spaningsregisterlagen samt ändringarna i nämndens tillsynslag den 1 mars 2012 rekryterade nämnden en projektledare, vars huvudsakliga uppgift var att förbereda de nya tillsynuppgifterna genom bl.a. kartläggning av befintliga uppgiftssamlingar hos den öppna polisen,

analys av tillsynsområdets omfattning samt externa kontakter med företrädare för såväl polisen som andra aktörer, t.ex. Datainspektionen, Justitiekanslern och Riksdagens ombudsmän (JO). Projektledaren anställdes i oktober 2011. Från detta datum fram till ikraftträdandet den 1 mars 2012 var även två föredragande sysselsatta till ca 75 procent av nämnda förberedelser. Även nämndledamöterna, kanslichefen och övriga medarbetare var i viss omfattning involverade i förberedelsearbetet. All kanslipersonal har genomgått en för myndigheten framtagen utbildning om PDL och flera föredragande har deltagit i utbildningar om personuppgiftsbehandling. En stor del av förberedelsearbetet gick åt till att förbereda hanteringen av enskildas begäran om kontroll av polisens personuppgiftsbehandling, framför allt frågan om hur nämndens kontroller skulle avgränsas mot bakgrund av det mycket stora antal uppgiftssamlingar hos den öppna polisen som omfattas av PDL:s tillämpnings-område.

4.1.2. Arbetet efter den 1 mars 2012

Nämndens tillsyn såvitt gäller personuppgiftsbehandling har utökats markant sedan den 1 mars 2012. Tillsynen på detta område omfattade tidigare endast Säkerhetspolisens behandling av personuppgifter. Inom den öppna polisen finns en betydligt större mängd register och andra uppgiftssamlingar än inom Säkerhetspolisen. Behandling av personuppgifter enligt de angivna lagarna sker också i väsentligt större utsträckning vid landets samtliga polismyndigheter än vid Säkerhetspolisen.

Under tiden 1 mars 2012 till och med september 2012 utgjordes en arbetsledande tjänst och två föredragandetjänster till ca 75 procent av arbetet med tillsyn över öppna polisens personuppgiftsbehandling. Även de övriga fyra föredragandena vid nämnden arbetade med granskning av öppna polisens personuppgiftsbehandling i samband med handläggning av ärenden om enskildas begäran om kontroll.

Den 1 oktober 2012 genomfördes en omorganisation av kansliet som resulterade i att två sakenheter bildades vilka leds av var sin enhetschef. Den ena enheten arbetar företrädelsevis med polisens (inklusive Säkerhetspolisens) personuppgiftsbehandling och den andra med hemliga tvångsmedel och kvalificerade skyddsidentiteter. På personuppgiftsbehandlingsenheten arbetar sedan dess en enhetschef och tre föredragande. Kansliets arbete med tillsyn på eget initiativ har under år 2012 till ca 40 procent rört den öppna polisens personuppgiftsbehandling. Förutom arbete med direkt tillsyn går en inte obetydlig del av arbetet på enheten till annat arbete såsom utarbetande av rutiner, externa kontakter, hantering av remisser och beredning av ärenden om samråd enligt 2 § polisdataförordningen (2010:1155). Liksom tidigare utförs granskning av öppna polisens personuppgiftsbehandling även av övriga föredragande i samband med handläggning av ärenden om enskildas begäran

om kontroll. Det nya sakområdet har också inneburit merarbete för kanslichefen och den administrativa personalen.

Även för nämnden som sådan har det nya tillsynsområdet inneburit merarbete. Antalet sammanträden har däremot inte påverkats av de nya tillsynsuppgifterna. Relevant utbildning har anordnats för nämndledamöterna.

Nämndens samlade bedömning är att tillsynen avseende polisens (inklusive Säkerhetspolisens) personuppgiftsbehandling tar uppskattningsvis fem årsarbetskrafter i anspråk. Det gångna året har dessa resurser, som nämnts ovan, framför allt lagts på den öppna polisens personuppgiftsbehandling.

4.2 Tillsyn på nämndens eget initiativ

4.2.1 Urval

När nämnden beslutar att inleda tillsynsärenden på eget initiativ görs detta främst utifrån bedömningen av var risken för en felaktig rättstillämpning hos de granskade myndigheterna är som störst. Bedömningen baseras på nämndens egna erfarenheter men även andra myndigheters (t.ex. Datainspektionens) iakttagelser kan vägas in. Nämnden kan även inleda tillsynsärenden på eget initiativ efter att någon företeelse inom nämndens tillsynsområde har uppmärksammats i media. Som hjälp i sin omvärldsbevakning använder myndigheten en nyhetsbevakningstjänst. Inriktningen av nämndens tillsyn på eget initiativ sker med beaktande av de uppdrag som myndigheten får från regeringen. Med utgångspunkt från ovanstående beslutar nämnden om fokusområden för sin tillsyn. Nämndens ambition är att sprida sina tillsynsinsatser såväl geografiskt som verksamhetsmässigt.

4.2.2 Metodik

Nämndens initiativärenden bedrivs huvudsakligen *tematiskt*, dvs. att tillsynen tar sin utgångspunkt i frågeställningar som utreds och granskas. Vid den tematiska tillsynen analyseras gällande författningar och vanligtvis hämtas interna föreskrifter och riktlinjer in från berörda myndigheter. Därefter undersöks rutiner och praktisk tillämpning, t.ex. genom frågeformulär som ställs till ansvariga tjänstemän eller genom en granskning av ett urval av myndigheternas ärenden. De fortsatta undersökningarna kan även innefatta samtal med enskilda tjänstemän eller frågor till andra myndigheter eller organisationer.

Nämnden genomför även *inspektioner* och *stickprovskontroller*. Båda dessa granskningsmetoder kan användas inom ramen för ett tematiskt tillsynsprojekt men kan också användas separat för att granska exempelvis rutiner eller enskilda ärenden.

Med utgångspunkt från vad som framkommer vid granskningen redovisar nämnden sina iakttagelser och bedömningar i uttalanden till berörda myndigheter. Uttalandena finns även tillgängliga på nämndens hemsida, www.sakint.se.

4.2.3 Tillsynens inriktning

Under år 2012 har nämndens tillsyn av den öppna polisen omfattat i huvudsak områdena behandling av känsliga personuppgifter och intern kontroll.

Nämnden har beslutat om att inleda följande tillsynsärenden på eget initiativ som rör den öppna polisens personuppgiftsbehandling under året:

- Polismyndigheternas behandling av känsliga personuppgifter
- Rikspolisstyrelsens (RPS) rutiner för och kontroll av behandling av känsliga personuppgifter
- Rikspolisstyrelsens (RPS) rutiner för och kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättelseregistret, KUR (avskilt från huvudärendet ovan)
- Polismyndigheternas användning av centrala säkerhetsloggen
- Tilldelning och användning av behörigheter i DurTvå
- Behandlingen av personuppgifter i Ekobrottsmyndighetens underrättelseverksamhet
- Behandlingen av personuppgifter i Rikskriminalpolisens register över spaningsfilmer
- Polismyndigheternas behandling av känsliga personuppgifter i KUT-info

Samtliga utom ärendet rörande tilldelning och användning av behörigheter i DurTvå har avslutats då denna redovisning avges. Ärendet om behandling av personuppgifter i Ekobrottsmyndighetens underrättelseverksamhet har avslutats utan närmare granskning eftersom de initiala kontrollerna visat att behandlingen där i sin helhet fortfarande tycks ske enligt den äldre polisdatalagen (1998:622) och således faller utanför nämndens tillsynsområde. Nämndens beslut i det ärendet har delgetts Datainspektionen. Sammanlagt sex uttalanden har gjorts i ovannämnda ärenden.

4.3 Tillsyn på begäran av enskilda

Under år 2012 har 27 personer begärt lagenlighetskontroller avseende den öppna polisens personuppgiftsbehandling. Endast ett av dessa ärenden har avslutats. Nämndens utökade tillsynsområde har föranlett mer än en fördubbling av antalet kontroller i varje ärende, och en väsentligt utökad arbetsbörda i varje ärende vad gäller granskning och analys av den behandling som har utförts. Handläggningen av enskildas begäran om kontroll avseende den öppna polisen har inneburit stora utmaningar för kansliet, som

kontinuerligt har fått omvärdera och omarbeta sina rutiner i takt med att ny information har förvärvats i samband med kontroller. Det faktum att kontroller i vissa lokala register med nationell spridning och teknisk åtkomst hos RPS (PUST och DurTvå) ännu inte kan göras centralt via RPS har försenat handläggningen av enskilda ärenden väsentligt, eftersom träff i dessa register är vanligt förekommande och kontroller ofta måste göras hos flera olika polismyndigheter i respektive register.

5. Iakttagelser och analys

5.1 Inledning

Nedan följer en redogörelse för de mer övergripande iakttagelser nämnden har gjort i sin tillsyn av den öppna polisens personuppgiftsbehandling.

5.2 Behandling av känsliga personuppgifter - rutiner i samband med registrering

5.2.1 Iakttagelser

Fem av de sex uttalanden som nämnden har gjort rörande polisens personuppgiftsbehandling avser helt eller delvis behandlingen av känsliga personuppgifter. Uttalandena har rört en kartläggning av polisens användning av känsliga personuppgifter, RPS behandling av känsliga personuppgifter i KUR respektive ASP, polismyndigheternas behandling av känsliga personuppgifter i KUT-info och RPS behandling av personuppgifter i registret över spaningsfilmer.

Nämnden har i sin granskning av alla de ovannämnda uppgiftssamlingarna kunnat konstatera att RPS och polismyndigheterna saknar särskilda rutiner för den prövning som enligt PDL och spaningsregisterlagen ska göras i samband med varje registrering av känsliga personuppgifter. Ansvaret för att denna ur integritetsperspektiv centrala – och svårtillämpade – del av regleringen följs har i stort sett helt lagts på den enskilde användaren med behörighet att registrera uppgifter.

5.2.2 Analys

Nämndens iakttagelser ovan tyder på att avsaknaden av särskilda rutiner för registreringen av känsliga personuppgifter är ett utbrett problem inom polisen. Den noggranna prövning som förutsätts i förarbetena kan knappast genomföras utan att det finns rutiner som innebär att frågan stäms av med annan, lämpligen närmaste chef, och att sådana rutiner finns väl dokumenterade och spridda bland användarna. Nämnden har i de ovannämnda uttalandena påpekat bl.a. att rutiner bör införas och dokumenteras samt att användarna kontinuerligt bör få utbildning i identifiering och registrering av känsliga personuppgifter. Detta ligger också i linje med Datainspektionens förelägganden i beslut av den 20

november 2012 efter granskning av polismyndigheterna i Jämtlands och Västmanlands län (dnr 604-2012 och 605-2012).

5.3 Behandling av känsliga personuppgifter – tillämpningen av rekvisitet ”absolut nödvändigt”

5.3.1 Iakttagelser

Enligt 2 kap. 10 § PDL och 12 § spaningsregisterlagen får uppgifter om en person inte behandlas 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 (känsliga personuppgifter). Uppgifter om en person som behandlas på annan grund, får dock kompletteras med sådana uppgifter när det är absolut nödvändigt för syftet med behandlingen.

Vid granskningen av det centrala kriminalunderrättelseregistret, KUR, konstaterade nämnden att behandling av känsliga personuppgifter hade skett utan att det framstod som absolut nödvändigt för syftet med behandlingen i tre av de ärenden som utvalts för granskning i samband med nämndens inspektion. De aktuella ärendena rörde registreringar av etnicitet (rom, kurd) och religion (shiamuslim). Även vid granskningen av polisens behandling av känsliga personuppgifter i elektroniska informationsblad från underrättelseverksamheten, s.k. KUT-info, kunde nämnden iaktta exempel på registreringar där misstänkta personer omnämndes som romer där det, på det underlag nämnden hade tillgång till, kunde ifrågasättas om det var absolut nödvändigt för syftet med behandlingen att registrera uppgiften.

5.3.2 Analys

Registrering av känsliga personuppgifter utan grund är allvarligt ur ett integritetsperspektiv. Nämnden har i sina uttalanden betonat att rekvisitet ”absolut nödvändigt” är ett mycket högt ställt krav och att det inte är tillräckligt att en känslig personuppgift har betydelse för ett ärende för att den ska få behandlas. Nämnden vill dock understryka att det, med det underlag som nämnden haft, inte har rört sig om något stort antal iakttagna felaktigheter. Nämnden menar att en ökad medvetenhet kring definitionen av och förutsättningarna för registrering av känsliga personuppgifter hos polisen generellt är nödvändig och har som nämnts ovan uppmanat till bl.a. förbättrade rutiner och mer utbildning.

5.4 Behandling av känsliga personuppgifter – sökförbudet

5.4.1 Iakttagelser

Enligt 3 kap. 5 § PDL och 14 § spaningsregisterlagen får uppgifter som avslöjar känsliga personuppgifter inte användas som sökbegrepp vid sökning i personuppgifter som gjorts gemensamt tillgängliga. Trots sökförbudet har det i

alla de uppgiftssamlingar nämnden har granskat sedan 1 mars 2012, dvs. KUR, ASP, KUT-info och spaningsfilmsregistret varit möjligt att söka på känsliga personuppgifter i någon omfattning. Varken RPS eller de granskade polismyndigheterna hade enligt egen uppgift någon intern kontroll av efterlevnaden av förbudet i form av regelbundna stickprovskontroller eller logguppföljning. Vid kontakter med IT-tekniker hos polisen, bl.a. i samband med ett samrådsförfarande, har åsikten framförts att det inte ens i nybyggda system finns möjligheter att helt eliminera möjligheten till fritextsökning.

Inom ramen för granskningen av KUR framkom vidare att RPS menar att sökförbudet i 3 kap. 5 § PDL omöjliggör en effektiv registervård när det gäller känsliga personuppgifter, såsom radering av känsliga personuppgifter som behandlas utan stöd i PDL.

5.4.2 Analys

Förbudet att söka på känsliga personuppgifter har införts för att förhindra kartläggning av individer baserat på exempelvis deras etnicitet eller politiska åsikter. Från integritetssynpunkt är denna reglering av fundamental betydelse. Liksom när det gäller registrering av känsliga personuppgifter har granskade delar av polisen lagt ett stort ansvar på den enskilde användaren för att sökförbudet efterlevs. Nämnden har påpekat att det inte är tillräckligt och att detta ansvar måste kompletteras med återkommande utbildning och en effektiv internkontroll. Intern kontroll är en förutsättning för att reglerna om sökbegränsningar ska kunna uppfyllas, framför allt när det gäller behandling i större system som KUR och ASP. Nämnden återkommer till frågor om intern kontroll nedan.

Nämnden instämmer i RPS synpunkt att regleringen är otydlig när det gäller frågan om sökningar får göras i registervårdande syfte. Nämnden har uttalat att en konsekvens som den RPS nämner är olycklig ur ett integritetsperspektiv och att ett förtydligande av regleringen i polisdatalagen och spaningsregisterlagen bör övervägas (uttalande om RPS rutiner för och kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättelseregistret, KUR, dnr 231-2012). Uttalandet har delgetts Regeringskansliet.

5.5 Logguppföljning och stickprovskontroller

5.5.1 Iakttagelser

Syftet med PDL är bl.a. att möjliggöra att personuppgifter kan behandlas hos polisen i större system i stället för i flera separata register. Det är också polisens ambition att successivt samla de uppgifter som behandlas i polisens verksamhet i större, centrala IT-system. Vid personuppgiftsbehandling i stora uppgiftssamlingar blir begränsningar av tillgängligheten för användarna ett viktigt integritetsskydd, vilket avspeglas i den nya lagstiftningen. Tilldelning

av behörigheter och olika typer av uppföljning, såsom loggning, blir därmed centrala verktyg för att upprätthålla integritetsskyddet vid behandling av personuppgifter enligt PDL (prop. 2009/10:85 s. 94 f. och 270 f.).

För att förbättra den tekniska kontrollen över IT-användningen har polisen utvecklat ett centralt system för att samla in och analysera loggar från polisens IT-system; CSL. Systemet drivs och underhålls av RPS. Syftet med CSL är dels att skydda enskildas integritet, dels att skydda den information som polisen behandlar mot otillåten behandling och angrepp.

Av nämndens granskning av polismyndigheternas beställningar till CSL under tiden 1 mars – 30 juni 2012 framgår att flertalet polismyndigheter inte hade gjort någon logguppföljning alls för de CSL-anslutna IT-systemen under perioden, och att logguppföljningen har varit av mycket begränsad omfattning även hos vissa av de större polismyndigheterna. Nämnden kunde också konstatera att de flesta beställningarna avsåg reaktioner på misstänkt otillåtna slagningar i förfluten tid.

Även vid granskningen av behandling av känsliga personuppgifter i olika uppgiftssamlingar har framkommit att någon logguppföljning av otillåtna sökningar på sådana uppgifter inte har gjorts sedan PDL och spaningsregisterlagen trädde ikraft. Inte heller finns enligt uppgift några rutiner för regelbundna stickprovskontroller av gjorda registreringar i syfte att kontrollera efterlevnaden av sökförbudet.

5.5.2 Analys

Nämnden har i sina uttalanden framhållit att för att loggning ska bli det centrala verktyg för att upprätthålla integritetsskyddet som förutsätts i förarbetena till PDL, måste loggutvärdering ske frekvent och såväl förebyggande som reaktivt. Nämnden har betonat att sådana kontroller är ett viktigt sätt att säkerställa att användare endast tar del av information de behöver för att kunna fullgöra sina arbetsuppgifter och på så sätt skydda de registrerades integritet.

Avsaknaden av tydliga rutiner för logguppföljning och stickprovskontroller är en allvarlig brist, inte minst med beaktande av att flera av polisens system innehåller sökbara känsliga personuppgifter. Med tanke på att utvecklingen går mot större gemensamma system är det av största vikt ur integritetssynpunkt att det finns en effektiv intern kontroll.

6. Avslutning

Nämnden har sedan den 1 mars 2012 fått en bild av hur regelverket kring känsliga personuppgifter i PDL och spaningsregisterlagen tillämpas hos den

öppna polisen och av hur den interna kontrollen i form av logguppföljning och stickprovstagning har fungerat under den nya lagstiftningens första månader. Nämndens sammanfattande bedömning är att rutiner för och intern kontroll av tillämpningen av regelverket kring känsliga personuppgifter i stort sett saknas och att logguppföljning och stickprovskontroller ännu inte tycks användas i en utsträckning som säkerställer ett effektivt integritetsskydd. Nämnden har dock endast i ett fåtal fall påträffat förhållanden som strider mot lag eller annan författning. Nämnden planerar flera uppföljningsärenden under innevarande år, för att kontrollera om de iakttagna bristerna har åtgärdats.

Denna redovisning har beslutats av nämnden. I beslutet har ledamöterna Sigurd Heuman, ordförande, Susanne Nylund, Linnéa Darell, Susanne Eberstein, Ulf Grape, Leif Hallberg, Alf Karlsson och Eric Myrin deltagit. Föredragande har varit Ulrika Söderqvist.

Sigurd Heuman

Ulrika Söderqvist