



Rikspolisstyrelsens rutiner för och kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättsregistret, KUR

1 SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat Rikspolisstyrelsens (RPS) rutiner för och kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättsregistret, KUR. Granskningen – som har avgränsats till ärenden som initierats av Rikskriminalpolisen (RKP) – har skett dels genom enkätfrågor, dels genom inspektion vid RKP den 14 november 2012. Nämnden konstaterar att behandling av känsliga personuppgifter tycks ske i liten omfattning i den granskade delen av KUR. Nämnden bedömer dock att registrering av känsliga personuppgifter har skett utan att det framstår som absolut nödvändigt för syftet med behandlingen i tre av fem granskade ärenden, samt konstaterar att RPS saknar särskilda rutiner för den prövning som enligt polisdatalagen (2010:361) (PDL) ska göras i samband med en registrering av känsliga personuppgifter. Nämnden anser att sådana rutiner bör införas samt att användarna kontinuerligt bör få utbildning i identifiering och behandling av känsliga personuppgifter. RPS föreskrifter på området bör vidare uppdateras för att avspegla regleringen i PDL. Nämnden förutsätter även att RPS fortsättningsvis kommer att genomföra logguppföljning avseende sökning på känsliga personuppgifter i KUR, liksom att införa regelbunden internkontroll i form av stickprov eller liknande i syfte att minska risken för att känsliga personuppgifter behandlas i strid med PDL.

2 BAKGRUND OCH AVGRÄNSNING

Syftet med PDL är att ge polisen möjlighet att behandla personuppgifter på ett ändamålsenligt sätt i sin brottsbekämpande verksamhet och att skydda människor mot att deras personliga integritet kränks vid en sådan behandling.¹ I PDL, liksom i annan lagstiftning om behandling av personuppgifter på internationell och nationell nivå, har känsliga personuppgifter en särställning som innebär att sådana uppgifter endast får behandlas i undantagsfall och under särskilda förutsättningar.

¹ Prop. 2009/10:85 s. 66.

Nämnden beslutade den 28 mars 2012 att granska föreskrifter och rutiner för samt interna kontrollfunktioner vid RPS behandling av känsliga personuppgifter i det centrala kriminalunderrättelseregistret (KUR), det allmänna spaningsregistret (ASP) samt personefterlysning- och U-boksregistret (EPU). Nämnden tar i detta uttalande endast upp den del av granskningen som rör behandling av känsliga personuppgifter i KUR. Under tillsynsprojektets gång har det framkommit att det finns en oklarhet rörande personuppgiftsansvaret för uppgifter i KUR. Nämnden har därför valt att i detta projekt endast granska ärenden i KUR som initierats av RKP, för vilka det står klart att RPS är personuppgiftsansvarig. RKP är en del av RPS.

KUR är ett nationellt kriminalunderrättelseregister som förs och används gemensamt av polismyndigheterna och RPS. Registret har funnits i sin nuvarande form sedan slutet av 90-talet och används för att dokumentera och sprida underrättelseuppslag över hela landet. Enligt RPS har enbart anställda hos kriminalunderrättelsetjänsterna vid de olika polismyndigheterna och RKP tillgång till registret, totalt ca 800 användare. Uppskattningsvis mellan 80 och 100 personer har s.k. registratorsbehörighet, dvs. kan registrera uppgifter i registret. RPS avsikt är att KUR i en nära framtid ska ersättas med modernare system, men när detta kan ske är ännu så länge oklart.

3 RÄTTSLIG REGLERING

Enligt artikel 8 Europeiska konventionen för de mänskliga rättigheterna och de grundläggande friheterna (EKMR) har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Rätten får enligt andra stycket i samma artikel inskränkas av offentlig myndighet endast under vissa angivna förutsättningar. EKMR gäller som lag i Sverige. Genom Europarådets konvention från 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (dataskyddskonventionen) har Europarådet preciserat vad skyddet i artikel 8 EKMR innebär i dataskyddshänseende, bl.a. genom att slå fast att känsliga personuppgifter som huvudregel inte får behandlas, men att vissa undantag kan tillåtas. Dataskyddskonventionen har ratificerats av samtliga EU-länder. Utöver dataskyddskonventionen har Europarådet tagit fram en rekommendation (No. R (87) 15) som reglerar användningen av personuppgifter inom polissektorn. I rekommendationen preciseras bl.a. att undantag från förbudet mot behandling av känsliga personuppgifter enligt dataskyddskonventionen endast får ske om det är absolut nödvändigt (artikel 2.4). Bestämmelserna i 5 § i den äldre polisdatalagen (1998:622), som reglerade förutsättningarna för polisens behandling av känsliga personuppgifter, motsvarar Europarådets rekommendation i detta avseende. Den äldre polisdatalagens reglering fördes, med endast en viss språklig justering, över till 2 kap. 10 § PDL.

Enligt 2 kap. 10 § första stycket PDL 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). Det är alltså inte tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån något i paragrafen angivet förhållande kan hänföras till en viss kategori av människor.²

Huvudregeln i 2 kap. 10 § första stycket PDL kompletteras med två undantag i paragrafens andra stycke. Uppgifter om en person, om de behandlas på annan grund, får kompletteras med sådana uppgifter som avses i första stycket när det är *absolut nödvändigt* för syftet med behandlingen. Bestämmelsen innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får dessa kompletteras med känsliga personuppgifter om det är av avgörande betydelse för utredningen. Med hänsyn till den restriktivitet som ligger i begreppet ”absolut nödvändigt” måste behovet av att göra sådana kompletteringar prövas noga i det enskilda ärendet.³

Enligt 3 kap. 5 § första stycket PDL får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv inte användas som sökbegrepp vid sökning i personuppgifter som har gjorts gemensamt tillgängliga, dvs. är tillgängliga för mer än ett fåtal personer. Sådana sökningar skulle kunna möjliggöra exempelvis kartläggning av personer med en viss politisk ståndpunkt eller religiös inriktning. Enligt andra stycket i paragrafen hindrar förbudet dock inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp. Vid remissbehandlingen av förslaget till ny polisdatalag framförde RPS att det var viktigt för polisen att i vissa situationer kunna använda sig av känsliga personuppgifter som sökbegrepp. Regeringen bedömde dock att integritetsintresset vägde över och att ett förbud skulle införas.⁴

Behandlingen av uppgifter i KUR regleras vidare av RPS föreskrifter RPSFS 2008:9 FAP 447-1. I föreskrifterna nämns ingenting om behandlingen av känsliga personuppgifter generellt, om förutsättningar för att få registrera sådana uppgifter eller om det ovannämnda sökförbudet. Föreskrifterna har inte uppdaterats sedan PDL:s ikraftträdande.

² Prop. 2009/10:85 s. 149 och 150.

³ A. prop. s. 325.

⁴ A. prop. s. 156.

4 GRANSKNINGEN

RPS har efter anmodan av nämnden besvarat ett antal frågor rörande rutinerna för och kontrollen av RPS behandling av känsliga personuppgifter bl.a. i KUR. Vidare har nämnden den 14 november 2012 genomfört en inspektion vid RKP. Vid inspektionen har företrädare för RKP gett en beskrivning av personuppgiftsbehandlingen, särskilt avseende känsliga personuppgifter, i KUR samt förevisat registret. Enligt uppgift från företrädare för RPS och RKP sker behandling av känsliga personuppgifter i mycket liten uträkning i KUR. RKP har vid inspektionstillfället även förevisat och redogjort för bakgrunden till fem ärenden i KUR som innehåller känsliga personuppgifter. Ärendena hade tidigare valts ut av nämndens kansli. Vid urvalet har kansliet använt vissa känsliga personuppgifter som sökord, eftersom ärenden i KUR som innehåller känsliga personuppgifter inte är markerade på något särskilt sätt. Sökningen har gjorts bland ärenden som initierats av RKP från den 1 januari 2006 till den 12 oktober 2012.

5 NÄMNDENS IAKTTAGELSER

Nämnden kan inledningsvis konstatera att KUR är ett omfattande system med ett stort antal användare och att uppgifter i systemet således är gemensamt tillgängliga. Nämnden kan vidare konstatera att den sökning på känsliga personuppgifter som nämndens kansli genomfört har genererat mycket få träffar, i relation till den stora mängd ärenden som registrerats av RKP under den period som sökningarna omfattat.

Nämnden har tagit del av relevanta delar av användarhandboken för KUR. Nämnden noterar att handboken inte är uppdaterad efter det att nu gällande PDL trädde i kraft. Handboken innehåller inte några instruktioner om behandling av känsliga personuppgifter eller förbudet mot att söka på sådana uppgifter. Vid granskningen har vidare framkommit att RPS inte heller har några särskilda rutiner för behandling av känsliga personuppgifter i KUR i någon annan form.

RPS har uppgett att samtliga användare av KUR genomgår en obligatorisk utbildning där bl.a. PDL:s reglering av känsliga personuppgifter tas upp, innan de får tillgång till registret. Enligt uppgift från företrädare för RKP förekommer i stort sett inga diskussioner internt kring identifiering och registrering av känsliga personuppgifter i KUR, men medvetenheten om regleringen av känsliga personuppgifter är generellt sett högre nu än innan PDL trädde ikraft.

I RPS enkätsvar till nämnden angav myndigheten att användarna inte kan söka på känsliga personuppgifter i KUR. Vid granskningen har framkommit att vissa åtgärder har vidtagits av RPS inför PDL:s ikraftträdande för att försvåra sökning

på känsliga personuppgifter i systemet. Av kansliets sökningar i och RKP:s förevisning av KUR framgår dock att det för alla användare av systemet är tekniskt möjligt att fritextsöka på känsliga personuppgifter i vissa delar av ärendena.

KUR är anslutet till RPS centrala säkerhetslogg (CSL), som är ett system för logganalys som är kopplat till ett flertal av polisens större uppgiftssamlingar. Enligt uppgifter från RPS har logguppföljning aldrig beställts från CSL avseende KUR. Enligt RPS görs inte heller någon egen logguppföljning eller annan intern kontroll avseende KUR, med undantag för att det görs vissa stickprov i undervisningssyfte omedelbart efter det att nya användare har fått behörighet att registrera uppgifter i KUR.

6 NÄMNDENS BEDÖMNING

Lagstiftaren har, med stöd i internationella rättsligt bindande instrument, infört en mycket restriktiv reglering när det gäller behandlingen av känsliga personuppgifter i polisens brottsbekämpande verksamhet. Genom PDL:s reglering har man velat omöjliggöra en kartläggning av människor utifrån exempelvis etnicitet, politisk ståndpunkt eller religiös inriktning. Från integritetssynpunkt är denna reglering av fundamental betydelse. Det åligger RPS att se till att reglerna efterlevs vid behandling av uppgifter där RPS har personuppgiftsansvar.

Vid den granskning av fem enskilda ärenden som nämnden genomfört har registrering av etniskt ursprung (rom, kurd) i två fall och registrering av religiös övertygelse (shiamuslim) i ett fall skett utan att det, enligt nämndens mening, framstått som absolut nödvändigt för syftet med behandlingen mot bakgrund av de skäl som har framförts för registreringarna. Nämnden vill betona att rekvisitet ”absolut nödvändigt” är ett mycket högt ställt krav. För att en känslig personuppgift ska få behandlas är det inte tillräckligt att den har betydelse för ett ärende. De aktuella ärendena registrerades visserligen före PDL:s ikraftträdande, men förutsättningarna för registrering enligt den äldre polisdatlagen var i sak desamma som enligt PDL. RPS behandling har enligt nämnden i ovannämnda fall inte uppfyllt de högt ställda krav som lagstiftaren förutsatt. Enligt uppgift har varken utbildning eller rutiner kring registrering förändrats på något genomgripande sätt sedan dessa registreringar skedde.

Det kan konstateras att RPS helt saknar särskilda rutiner för behandlingen av känsliga personuppgifter i KUR. De rutiner som gäller för registrering generellt innebär att RPS har lagt hela ansvaret för att säkerställa att känsliga personuppgifter inte tillförs KUR i större omfattning än PDL medger på var och en av de personer som har behörighet att registrera uppgifterna.

Eftersom det är tekniskt möjligt för alla användare att söka i KUR på känsliga personuppgifter i vissa delar av ärendena, ligger ett tungt ansvar på den personuppgiftsansvarige att på andra sätt säkerställa att sökförbudet i PDL efterlevs. Såvitt framkommit vid granskningen är den enda åtgärd som vidtagits av RPS i detta avseende att tillhandahålla ett obligatoriskt utbildningstillfälle för alla användare där bl.a. sökförbudet tas upp.

Nämndens uppfattning är att det varken vid registrering av eller vid sökning på känsliga personuppgifter är tillräckligt att ansvaret läggs på den enskilde användaren. Detta ansvar måste kompletteras med återkommande utbildning, tydliga rutiner och en effektiv internkontroll. Det krävs därför att såväl personer med registratorsbehörighet som andra användare har tillräckliga kunskaper om vad som utgör en känslig personuppgift, under vilka förutsättningar en sådan uppgift får behandlas och att det gäller ett absolut sökförbud för sådana uppgifter. Nämnden anser att alla användare kontinuerligt bör få utbildning i dessa avseenden. Därutöver bör särskilda rutiner inrättas för den noggranna prövning i varje enskilt fall som ska ske innan en känslig personuppgift registreras. Denna prövning kan lämpligen föregås av ett samråd med annan än den som ska utföra registreringen, såsom närmaste chef. De närmare förutsättningarna för registrering av känsliga personuppgifter och rutinerna kring ett sådant beslut bör dokumenteras och spridas på lämpligt sätt, exempelvis genom användarhandboken för KUR. Att rutinerna följts i det enskilda fallet bör dessutom dokumenteras genom anteckning eller liknande i själva systemet. RPS föreskrifter på området bör vidare uppdateras för att avspegla regleringen i PDL.

Av nämndens granskning framgår visserligen att RPS synes behandla känsliga personuppgifter i liten utsträckning i den granskade delen av KUR. Att behandling av känsliga personuppgifter sker sällan gör dock snarast att behovet av utbildning och tydliga rutiner för sådan behandling är större än i system där sådan behandling är mer vanligt förekommande.

Enligt uppgift genomför RPS ingen logguppföljning i KUR på eget initiativ. Interna kontrollfunktioner, såsom exempelvis logguppföljning, är ett viktigt verktyg för att säkerställa en lagenlig personuppgiftsbehandling. För att loggning ska bli ett effektivt sätt att upprätthålla integritetsskyddet måste loggutvärdering ske frekvent och såväl förebyggande som reaktivt. Verksamheten vid CSL bygger till stor del på beställningar om logguppföljning från polismyndigheterna. Nämnden förutsätter att RPS fortsättningsvis kommer att utnyttja de möjligheter CSL ger för att genomföra logguppföljning i KUR, inte minst beträffande efterlevnaden av sökförbudet i PDL avseende känsliga personuppgifter. Även i övrigt bör rutiner för internkontroll i form av stickprov

införas, för att minska riskerna för att känsliga personuppgifter fortsättningsvis behandlas i strid med PDL.

Nämnden avser följa upp vilka åtgärder RPS har vidtagit med anledning av ovannämnda synpunkter.

Avslutningsvis kan nämnas att RPS menar att sökförbudet i 3 kap. 5 § PDL möjliggör en effektiv registervård när det gäller känsliga personuppgifter, såsom radering av känsliga personuppgifter som behandlas utan stöd i PDL. Nämnden instämmer i att regleringen är otydlig i detta avseende och vill understryka att en konsekvens som den RPS nämner är olycklig ur ett integritetsperspektiv, varför ett förtydligande av regleringen bör övervägas.

Säkerhets- och integritetsskyddsnämnden beslutar att delge Regeringskansliet, RPS och samtliga polismyndigheter uttalandet.