

Polismyndigheten i Jämtlands län
Att: NN
Box 707
831 28 ÖSTERSUND

Tillsyn av personuppgiftsbehandlingen vid Polismyndigheten i Jämtlands län

Datainspektionen meddelar följande

BESLUT

1. Datainspektionen förelägger Polismyndigheten i Jämtlands län att senast den 15 februari 2013 beträffande KUT-info införa rutiner som säkerställer att nödvändighetsprövningen enligt 2 kap. 10 § polisdatalagen (2010:361) alltid föregår en behandling av känsliga personuppgifter i KUT-info.
2. Den personuppgiftsbehandling som Polismyndigheten i Jämtlands län utför i den särskilda undersökningen i kriminalunderrättelseverksamhet, dnr. HD 09/08, är enligt Datainspektionen inte förenlig med 14-16 §§ polisdatalagen (1998:622) och punkten 4 i övergångsbestämmelserna till polisdatalagen (2010:361), främst med avseende på kraven om misstänkt allvarlig brottslighet, att de personer som inte är misstänkta i undersökningen förses med en upplysning om detta förhållande, samt gallring. Datainspektionen förelägger därför Polismyndigheten i Jämtlands län att senast den 15 februari 2013 inrätta personuppgiftsbehandlingen i undersökningen i enlighet med 14-16 §§ polisdatalagen (1998:622), för det fall undersökningen den 15 februari 2013 alltjämt förs med stöd av den lagen.
3. Datainspektionen förelägger Polismyndigheten i Jämtlands län att senast den 15 februari 2013, för det fall polismyndigheten vid den

tidpunkten alltjämt behandlar personuppgifter i särskilda undersökningar i kriminalunderrättelseverksamhet med stöd av bestämmelserna i polisdatalagen (1998:622) och övergångsbestämmelserna till polisdatalagen (2010:361), införa rutiner som säkerställer att prövningen rörande särskilda undersökningars fortsättning eller avslutande (s.k. förlängningsbeslut) sker minst en gång per år.

4. Polismyndigheten i Jämtlands län behandlar personuppgifter i sin kriminalunderrättelseverksamhet utanför såväl särskilda undersökningar enligt polisdatalagen (1998:622), som uppgiftssamlingar enligt polisdatalagen (2010:361). Datainspektionen förelägger därför polismyndigheten att senast den 15 februari 2013 säkerställa att all personuppgiftsbehandling som utförs i myndighetens kriminalunderrättelseverksamhet sker i enlighet med en tydligt angiven rättslig grund.
5. Datainspektionen förelägger Polismyndigheten i Jämtlands län att senast den 15 mars 2013 inkomma till inspektionen med en beskrivning av de åtgärder som polismyndigheten har vidtagit med anledning av punkterna 1-4, samt de påpekanden som återfinns nedan.

Datainspektionen lämnar de påpekanden som återfinns på sid. 4 och 5 (PUST), sid. 5, 6 och 7 (KUT-info), samt sid. 11 (Behandling av personuppgifter i polismyndighetens kriminalunderrättelseverksamhet).

SKÄL FÖR BESLUTET

Redogörelse för tillsynsärendet

I enlighet med beslutad tillsynsplan har Datainspektionen genomfört tillsyn av personuppgiftsbehandlingen vid Polismyndigheten i Jämtlands län (i det följande polismyndigheten). Således har Datainspektionen den 30 maj 2012 på plats i Östersund utfört en inspektion i syfte att granska huruvida den personuppgiftsbehandling som polismyndigheten utför är förenlig med gällande rätt. Inom ramen för tillsynsärendet har personuppgiftsbehandlingen inom främst följande system/behandlingsgranskats:

- Polisens Utredningsstöd (PUST)
- Lokalt system för arbetsskador (LISA)
- Intrapolis och Internet
- Polisens underrättelsemodell – applikationer (PUM-A)
- KUT-info
- Särskilda undersökningar i kriminalunderrättelseverksamhet (SUR)

I samband med inspektionen har Datainspektionen utfört slagningar samt förevisats hur polismyndigheten behandlar personuppgifter i en majoritet av de utvalda systemen.

Över inspektionen har protokoll förts. Polismyndigheten har beretts tillfälle att yttra sig över protokollet och gjort så i yttrande som inkom till Datainspektionen den 30 juli 2012.

Datainspektionens överväganden

PUST

Rationell Anmälningsrutin (RAR) och Datoriserad UtredningsrutinTvångsmedel (DurTvå) är centrala polisiära IT-system i vilka det behandlas mycket stora mängder personuppgifter av integritetskänslig natur. RAR utgör polismyndigheternas anmälningsregister och kriminaldiarium; DurTvå är ett utredningsstöd som i huvudsak används för att bygga upp och färdigställa förundersökningsprotokoll. I DurTvå registreras också reella och personella tvångsmedel. Det relativt nyligen införda systemet PUST kommer på sikt att helt ersätta RAR och DurTvå, men i dagsläget hanteras endast ärenden av enklare beskaffenhet i PUST. PUST gör det möjligt för polisen att i princip slutföra en utredning i fält. Polismyndigheten är personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför i PUST.

I PUST och DurTvå, samt numera även i RAR, behandlar polisen personuppgifter med stöd av polisdatalagen (2010:361), som trädde ikraft den 1 mars 2012. I de tre systemen gör polisen personuppgifter gemensamt tillgängliga. Vissa bestämmelser i polisdatalagen (2010:361), bl.a. om bevarande och sökning, behöver inte tillämpas förrän den 1 januari 2015 (se övergångsbestämmelserna).

Datainspektionens bedömning av polismyndighetens personuppgiftsbehandling i PUST är att behandlingen sker i enlighet med de regler som gäller idag. Det ska i detta sammanhang rätteligen understrykas att landets enskilda polismyndigheter har mycket små om alls några möjligheter att, utöver registreringen av uppgifter, påverka PUST i egentlig mening, eftersom det är fråga om ett centralt system som har utvecklats av och drivs via Rikspolisstyrelsen. De enskilda polismyndigheterna är dock, som nämnts ovan, personuppgiftsansvariga för den behandling som respektive myndighet utför och vissa möjligheter till lokala variationer finns. Mot den angivna bakgrunden vill Datainspektionen inledningsvis göra följande påpekande. Vid inspektionen framgick att polismyndigheten i samband med registrering namnger utredningar i PUST (i fältet "Utredningens namn") bl.a. till den misstänktes efternamn (men förfarandet varierar inom myndigheten). Genom att namnge ärendena på det beskrivna sättet, kan man vid sökning i polismyndighetens PUST, i sökfältet "Utredningens namn", söka fram ärenden som annars inte hade varit sökbara (t.ex. efter det att förundersökningsledaren har fattat ett nedläggningsbeslut). Sökningar efter sådana ärenden utfördes vid inspektionen. Det innebär således i praktiken att bestämmelsen i 3 kap. 13 § polisdatalagen (2010:361) (som inte behöver

tillämpas förrän den 1 januari 2015) om att en person i vissa fall inte får vara sökbar som misstänkt riskerar att sättas ur spel. Datainspektionens bedömning är, att om polismyndigheten fortsätter att namnge ärenden som i vissa fall görs nu, kommer det efter den 1 januari 2015 att finnas uppgifter som riskerar att blir åtkomliga i strid med 3 kap. 13 § polisdatalagen (2010:361). En sådan konsekvens kan polismyndigheten förhindra genom att ändra sitt förfarande vid registrering redan nu. Således anser Datainspektionen att polismyndigheten bör upphöra med att namnge ärenden i PUST med hjälp av personuppgifter i fältet "Utredningens namn".

Datainspektionen konstaterade att inga stickprovskontroller avseende uppföljning av loggar sker i PUST, men vid misstanke om obehöriga slagningar beställer polismyndigheten loggutdrag. Datainspektionen vill påpeka att det ankommer på polismyndigheten att följa upp loggar på sådant sätt att det finns en reell upptäcktsrisk för personer som gör obehöriga slagningar i polisens IT-system.

KUT-info

Polismyndigheten har ingen egen server för KUT-info. Som en följd av detta skickas KUT-info ut cirka en gång per vecka till ungefär 200 mottagare. Vid KUT:en sparas den utskickade informationen i upp till två år i oförändrat skick (råmaterial). Datainspektionen har följande synpunkter på polismyndighetens behandling av personuppgifter inom ramen för KUT-info.

För det första innebär det förfarande som polismyndigheten nu använder sig av att myndigheten i praktiken frånhänder sig kontrollen över informationen i samband med att e-postmeddelandena skickas iväg till mottagarna. Det finns således ingen möjlighet att kontrollera och följa upp hur informationen används vidare, om den skrivs ut, ändras eller andra åtgärder vidtas med materialet. I 2 kap. 11 § polisdatalagen (2010:361), som är tillämplig på behandlingen av personuppgifter i KUT-info, uppställs ett grundläggande krav som innebär att tillgången till personuppgifter i polisens brottsbekämpande verksamhet ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. KUT-infon vid polismyndigheten skickas ut till ca. 200 mottagare där alla får del av samma information, vilket innebär att någon föregående prövning utifrån bestämmelsen i 2 kap. 11 § polisdatalagen inte sker i det enskilda fallet, utan endast generellt i samband med att behörigheten till KUT-info i sig prövas. Mot den angivna bakgrunden vill Datainspektionen göra följande påpekande. Det ankommer enligt Datainspektionen på polismyndigheten att begränsa åtkomsten till personuppgifter i KUT-info till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Vägledande i den delen bör vara att ju mer stringent, genomtänkt och relevant för olika brottsbekämpande ändamål som informationen på KUT-info är, desto lättare

blir det för polismyndigheten att säkerställa att den information som sprids är av betydelse för lösande av mottagarnas arbetsuppgifter. Det kan dock inte uteslutas att en väldigt spridd krets av mottagare med starkt varierande arbetsuppgifter (varav en del med arbetsuppgifter helt utanför den utskickande myndighetens verksamhetsområden) kan kräva att det upprättas olika versioner av KUT-info. En sådan prövning görs av polismyndigheten i egenskap av personuppgiftsansvarig för behandlingen (se även vidare nedan avseende känsliga personuppgifter i KUT-info).

För det andra finns det enligt Datainspektionen anledning att anta att det råmaterial som sparas vid underrättsroteln (men även hos mottagarna) i vissa fall riskerar att behandlas i strid med 9 § g) personuppgiftslagen (1998:204) (jfr. 2 kap. 2 § polisdatalagen (2010:361)), dvs. över tiden inte är riktigt och aktuellt. KUT-info används främst för identifiering och efterlysningar. När t.ex. en efterlyst person grips, bör man enligt Datainspektionen inte behandla uppgifter som ger upplysning om ett vid den tidpunkten felaktigt förhållande. Bristande uppgiftskvalitet innebär en risk för otillbörliga intrång i den personliga integriteten och gagnar inte heller de operativa mål som finns med verksamheten (behandlingen). Mot den bakgrunden gör Datainspektionen följande påpekande. Datainspektionen anser att polismyndigheten, mot bakgrund av bestämmelsen i 9 § g) personuppgiftslagen (1998:204), bör överväga hur behandlingen av personuppgifter inom ramen för KUT-info kan inrättas på ett sådant sätt att skyddet för den personliga integriteten säkerställs samtidigt som ändamålet med behandlingen kan upprätthållas. En del av det arbetet består i att vidta åtgärder som så långt det är praktiskt möjligt säkerställer att informationen i KUT-info (vid KUT:en och hos mottagarna) över tiden är riktig och aktuell.

För det tredje anser Datainspektionen att det finns anledning att beröra frågan om polismyndighetens behandling av personuppgifter i KUT-info mot bakgrund av ändamålsbestämmelserna i 2 kap. 7 och 8 §§ polisdatalagen (2010:361). För sin brottsbekämpande verksamhet såvitt avser polisens egen verksamhet får polisen behandla personuppgifter i enlighet med de s.k. primära ändamålen i 2 kap. 7 § polisdatalagen (uttömmande), dvs. för att förebygga, förhindra, utreda och beivra brott. Dessutom får personuppgifter som behandlas för de primära ändamålen, med stöd av 2 kap. 8 § polisdatalagen (2010:361), även behandlas när det är nödvändigt för att tillhandahålla information som behövs i den brottsbekämpande verksamheten hos ett antal myndigheter (t.ex. andra polismyndigheter; s.k. sekundära ändamål). Slutligen får polisen behandla uppgifter för andra sekundära ändamål (tillhandahållande till andra myndigheter) än de som nämns i 2 kap. 8 § polisdatalagen (2010:361), under förutsättning att behandlingen i det enskilda fallet inte är oförenlig med insamlingsändamålet (finalitetsprincipen; se vidare prop. 2009/10:85, sid. 97-99).

Vid inspektionen kunde konstateras att en del av de noteringar som skickas ut via KUT-info i princip avser kompletta analysbesked i ärenden om ringa

narkotikabrott där namn, personnummer, K-nummer och substanser framgick, men även domar från Östersunds tingsrätt som polismyndigheten får expedierade till sig. Gemensamt för dessa noteringar var att de förekom utan ytterligare upplysningar som satte dem i ett operativt sammanhang. Datainspektionen uppfattar att ändamålet med behandlingen av personuppgifter i KUT-info i allt väsentligt är brottsbekämpande verksamhet i polismyndighetens egen verksamhet (dvs. 2 kap. 7 § polisdatalagen (2010:361)) i och med att det ska skapa underlag för operativa insatser för polismyndighetens personal, samt för att bidra med relevanta uppgifter som kan effektivisera polisarbetet och göra detta framgångsrikt. Mot den bakgrunden anser Datainspektionen att all personuppgiftsbehandling i KUT-info ska rymmas inom ramen för de ändamål som anges i 2 kap. 7 och 8 §§ polisdatalagen (2010:361).

Datainspektionen bedömer att det idag behandlas personuppgifter i KUT-info som i vissa fall i vart fall tenderar att hamna utanför ändamålen i 2 kap. 7 och 8 §§ polisdatalagen. Det handlar då framför allt om uppgifter av ren informativ karaktär utan ytterligare upplysningar. I de fallen är det svårt att se och bedöma varför uppgifterna behandlas i KUT-info. Om den personuppgiftsansvarige inte säkerställer att all information i KUT-info har ett uttalat syfte med en viss inriktning, finns risken att behandlingen till slut hamnar utanför polisdatalagens tillämpningsområde. Om så blir fallet är det i praktiken omöjligt för mottagarna och den personuppgiftsansvarige att fullt ut säkerställa att olika bestämmelser om grundläggande krav på behandlingen, sökning, bevarande och gallring beaktas på rätt sätt, med risk för otillbörliga intrång i de registrerades personliga integritet som följd. Frågan har också betydelse för bedömningen av om mottagarna till KUT-info har behov av uppgifterna för att kunna lösa sina arbetsuppgifter. Datainspektionen bedömer att t.ex. spridande till 200 mottagare av detaljerad information kring ringa narkotikabrott (inkl. analysbesked) närmast har ett rent informativt syfte som feed-back till de befattningshavare som har kännedom om vissa konkreta ärenden. Rapportering av trender m.m. i narkotikasammanhang torde kunna genomföras utan så detaljerad information som nu är aktuellt. Mot den angivna bakgrunden vill Datainspektionen påpeka att polismyndigheten bör göra en prövning av vilka personuppgifter som är nödvändiga att behandla för att uppnå det syfte som finns med KUT-info och då även beakta den spridning som materialet ges. I detta arbete ligger självklart även att säkerställa att den typ av personuppgifter som förekommer i KUT-info och det sammanhang i vilket uppgifterna presenteras sammantaget gör att behandlingen faller inom polisdatalagens (2010:361) tillämpningsområde.

För det fjärde kan Datainspektionen konstatera att polismyndigheten behandlar känsliga personuppgifter i KUT-info, t.ex. i form av de ovan nämnda analysbeskeden. Polisen får behandla känsliga personuppgifter i den brottsbekämpande verksamheten endast om de krav som ställs upp i 2 kap. 10 § polisdatalagen (2010:361) är uppfyllda, vilket innebär att uppgifterna får behandlas bara om det är absolut nödvändigt för syftet med behandlingen

och då som ett komplement till andra uppgifter om den registrerade. Datainspektionen anser att den behandling av känsliga personuppgifter i KUT-info som kunde observeras vid inspektionen inte uppfyller kraven i 2 kap. 10 § polisdatalagen (2010:361), samt att det vid polismyndigheten inte finns rutiner som säkerställer att de känsliga personuppgifternas särställning beaktas såvitt avser KUT-info. Mot den bakgrunden förelägger Datainspektionen polismyndigheten att införa rutiner som säkerställer att den nödvändighetsprövning som polisdatalagen (2010:361) föreskriver alltid föregår en behandling av känsliga personuppgifter i KUT-info. Datainspektionen vill dessutom påpeka att förekomsten av känsliga personuppgifter i utskickat KUT-info också har bäring på den ovan berörda frågan om kretsen av mottagare.

Datainspektionen vill avslutningsvis på ett generellt plan också beröra frågan om att KUT-info innehåller personuppgifter som polismyndigheten har gjort gemensamt tillgängliga i sin brottsbekämpande verksamhet. Relevanta bestämmelser för sådan behandling finns i 3 kap. polisdatalagen (2010:361). Personuppgiftsbehandlingen i KUT-info sker i många fall inte inom ramen för en förundersökning, vilket i korthet bl.a. innebär att kraven i 3 kap. 2, 5-7 och 14 §§ polisdatalagen (2010:361) måste vara uppfyllda i tillämpliga delar. Enligt Datainspektionen kan det finnas anledning att i ett annat sammanhang djupare och på ett nationellt plan beröra denna fråga närmare, men redan nu kan konstateras att det kan ifrågasättas om den behandling som idag sker i KUT-info i alla delar uppfyller kraven i 3 kap. 2 § polisdatalagen (2010:361) när det bl.a. gäller straffskalor och krav på anknytning till brottslig verksamhet.

Informationssäkerhet

Polismyndigheten saknar egna särskilda rutiner och instruktioner för användning av mobila lagringsmedia, mobil IT-utrustning samt privat IT-utrustning i tjänsten. Enligt 31 § personuppgiftslagen (1998:204), som är tillämplig på behandling av personuppgifter enligt polisdatalagen (2010:361), ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas (säkerhetsåtgärder). När åtgärderna vidtas ska bland annat beaktas vilka särskilda risker som finns med behandlingen och hur pass känsliga de behandlade personuppgifterna är. Den information som polismyndigheten hanterar i sin brottsbekämpande verksamhet är ofta integritetskänslig. När personuppgifter flyttas och sprids med hjälp av mobil IT-utrustning finns det inneboende risker att information i vart fall oavsiktligt hamnar i orätta händer eller sammanblandas med privat material.

Polismyndigheten har uppgett att den tillämpar de föreskrifter på informationssäkerhetsområdet som Rikspolisstyrelsen har meddelat. Datainspektionen godtar polismyndighetens sätt att arbeta i denna del, men förutsätter att polismyndigheten, i den mån myndigheten inte avser att närmare reglera de aktuella frågorna, tillser att de befattningshavare som behandlar personuppgifter i mobil IT-utrustning över tiden (när ny teknik tillförs eller görs tillgänglig) utbildas för att upprätthålla en säker behandling av personuppgifter.

Behandling av personuppgifter i polismyndighetens kriminalunderrättelseverksamhet

Inledning

Inom ramen för polisens kriminalunderrättelseverksamhet förekommer bland den mest integritetskänsliga behandlingen av personuppgifter som sker i samhället. Syftet med kriminalunderrättelseverksamheten är att genom insamling, bearbetning och analys kunna hitta samband mellan olika personer och brott för att i senare led kunna delge informationen och skapa underlag för förundersökningar (polisutredningar avseende konkreta brott) eller för att bl.a. kunna förhindra brott. Behandlingen sker i polisens brottsbekämpande verksamhet. I och med att polisen inom ramen för kriminalunderrättelseverksamheten har getts långtgående befogenheter att, även när det föreligger endast svaga misstankar om olika personers inblandning i brottslighet som dessutom inte behöver vara konkret angiven, kartlägga ett stort antal personer, är det mycket viktigt att samtliga skyddsmekanismer som ska förebygga otillbörliga intrång i den personliga integriteten iakttas.

I polisdatalagen (2010:361) finns bestämmelser om behandling av personuppgifter utanför en förundersökning. I den mån det är fråga om s.k. gemensamt tillgängliga uppgifter (fler än ett tiotal personer som har tillgång till uppgifterna) gäller de mer begränsande bestämmelserna i 3 kap. polisdatalagen, annars gäller reglerna i 2 kap. polisdatalagen. Polisen får dock, fram till utgången av 2014, med stöd av övergångsbestämmelserna till polisdatalagen (2010:361), behandla personuppgifter i s.k. särskilda undersökningar i kriminalunderrättelseverksamhet (SUR:ar) enligt reglerna i 3 och 14-16 §§ polisdatalagen (1998:622). Trots att de nya och mer tillåtande bestämmelserna avseende kriminalunderrättelseverksamhet i polisdatalagen (2010:361) beslutades redan 2010 för att träda ikraft i mars 2012, behandlar polisen i Sverige idag personuppgifter i kriminalunderrättelseverksamhet i stort sett uteslutande i enlighet med det äldre regelverket (dvs. i SUR:ar). Polismyndigheten har uppgett att några uppgiftssamlingar enligt polisdatalagen (2010:361) inte förekom vid myndigheten vid tiden för inspektionen.

I en särskild undersökning i kriminalunderrättelseverksamhet ska uppgifter insamlas, bearbetas och analyseras i syfte att ge underlag för beslut om förundersökning eller om särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. En särskild undersökning får föras om polismyndigheten beslutat om en sådan undersökning och det finns anledning att anta att allvarlig brottslighet har utövats eller kan komma att utövas. Med allvarlig brottslighet avses att det rör sig om brottslig verksamhet som innefattar brott för vilket är föreskrivet fängelse i två år eller däröver. Om uppgifterna avser en person som det inte finns någon misstanke mot (s.k. kringperson vilket kan vara en arbetsgivare, bekant eller släkting som bedöms ha en relevant anknytning till den misstänktes brottsliga verksamhet) ska detta särskilt anges i undersökningen. Enligt 16 § första stycket polisdatalagen (1998:622) ska personuppgifter i särskilda undersökningar gallras senast ett år efter det att behandlingen har beslutats, men om det är av särskild betydelse för att en särskild undersökning ska kunna avslutas får uppgifterna behandlas under längre tid. I praktiken går detta till på så sätt att polismyndigheterna fattar s.k. förlängningsbeslut en gång per år och i samband härmed utförs även gallringsåtgärder. Särskilda undersökningar som pågår under endast ett år är således ovanliga inom polisen.

Datainspektionens granskning

I den särskilda undersökningen som bedrivs vid polismyndigheten behandlas personuppgifter utan att de personer som inte är misstänkta för brottslig allvarlig brottslig verksamhet förses med en sådan särskild upplysning som följer av 14 § andra stycket polisdatalagen (1998:622). Således går det i polismyndighetens behandling inte att se om en registrerad person kan misstänkas ägna sig åt brottslig verksamhet, eller om grunden för registrering endast är att personen är länkad till en viss misstänkt. Vid polismyndigheten registreras även personer som saknar koppling till allvarlig brottslig verksamhet i polisdatalagens (1998:622) mening. Vid inspektionen påträffades bl.a. ett flertal registreringar av barn som uppenbarligen inte hade någon annan koppling till allvarlig brottslig verksamhet än att de t.ex. var släkt med en person som misstänktes för sådan verksamhet. Det rörde sig bl.a. om små barn. Vad gäller gallring av personuppgifter har polismyndigheten i samband med inspektionen hänvisat till dokument som beskriver rutiner för detta samt uppgett att rutinerna tillämpas. Under inspektionen kunde det emellertid konstateras att samtliga poster som hade valts ut för gallring sedan den särskilda undersökningen påbörjades alltjämt fanns kvar i kriminalunderrättelsetjänstens IT-miljö (och således endast hade flyttats). Datainspektionen anser att de aktuella bristerna, som ju innebär en behandling som står i strid med polisdatalagens (1998:622) bestämmelser, är allvarliga eftersom de avser en grundläggande del av integritetsskyddet och att

myndigheten inte kan fortsätta att behandla personuppgifter i verksamheten utan att bristerna avhjälps. Det sagda innebär att det är av väsentlig betydelse att polismyndigheten snarast inrättar behandlingen i enlighet med lagens krav. Mot den bakgrunden förelägger Datainspektionen polismyndigheten att beträffande kraven på allvarlig brottslig verksamhet, uppmärkning av icke misstänkt, samt gallring, inrätta behandlingen i enlighet med 14-16 §§ polisdatalagen (1998:622). Inspektionen förutsätter att de personuppgifter som redan har valts ut för gallring omgäende raderas om så inte redan har skett.

Vidare kunde Datainspektionen vid inspektionen konstatera brister när det gäller polismyndighetens prövning enligt 16 § första stycket polisdatalagen (1998:622) (förlängningsbeslut), trots att det har tagits fram skriftliga rutiner för detta (TjF 171-3). Bristerna består i att förlängningsbeslut i flera fall inte har fattats i rätt tid vilket i sin tur innebär att de rutiner som finns inte fungerar fullt ut i det praktiska arbetet. Förseningarna uppgår till mellan tre och drygt sex månader. Datainspektionen anser att polismyndigheten, i syfte att upprätthålla ettårsfristen, som har stor betydelse för intrånget i den personliga integriteten, måste införa rutiner som säkerställer att förlängningsbesluten *i praktiken* fattas i rätt tid. Polismyndigheten föreläggs följaktligen att inrätta sådana rutiner.

Vid inspektionen kunde dessutom konstateras att polismyndigheten enligt Datainspektionen behandlar personuppgifter i sin kriminalunderrättelseverksamhet utanför såväl särskilda undersökningar enligt polisdatalagen (1998:622), som uppgiftssamlingar enligt polisdatalagen (2010:361). Det rör sig om personuppgifter som påträffades i olika mappar (vid sidan av behandling i särskild undersökning) i kriminalunderrättelsetjänstens IT-system och där uppgifternas ursprung eller ändamålet för behandlingen inte framgick. För att de befattningshavare som behandlar personuppgifter vid polismyndigheten ska veta vilka bestämmelser som gäller för en viss behandling, får det inte råda något tvivel om vilken rättslig grund som gäller för behandlingen. Enligt Datainspektionen råder det, i de aktuella delarna, oklarheter kring den rättsliga grunden. Mot den bakgrunden förelägger Datainspektionen polismyndigheten att tillse att all behandling av personuppgifter i kriminalunderrättelseverksamheten sker i enlighet med en tydligt angiven och giltig rättslig grund.

Polismyndigheten utför inga kontroller av enskilda användares aktiviteter (loggning/logguppföljning) såvitt avser de personuppgifter som behandlas i myndighetens kriminalunderrättelseverksamhet. Mot bakgrund av att polisen, som det i vart fall får bedömas, kommer att få en ny IT-plattform för den aktuella behandlingen, vill Datainspektionen i detta skede i vart fall påpeka att polismyndigheten alltid ska sträva efter att inrätta behandlingen av

integritetskänsliga personuppgifter på ett sådant sätt att användarnas aktiviteter kan kontrolleras genomloggning och logguppföljning.

Enligt Datainspektionen finns det skäl att följa upp de åtgärder som polismyndigheten ska vidta med anledning av detta beslut. Polismyndigheten föreläggs därför att inkomma till inspektionen med en redovisning av de åtgärder som myndigheten vidtar med anledning av beslutet.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, tillsynschefen Britt Marie Wester, samt juristerna Maria Karlströms, Anna Larsson Stattin och Nicklas Hjertonsson, föredragande.

Göran Gräslund

Nicklas Hjertonsson

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet ska ha kommit in till Datainspektionen senast tre veckor från den dag beslutet meddelades för att kunna prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Kopia till:

Personuppgiftsombudet NN, genom Polismyndigheten i Jämtlands läns försorg.

Säkerhets- och integritetsskyddsnämnden, Box 22523, 104 22 STOCKHOLM
(för kännedom)

Rikspolisstyrelsen, Rättsavdelningen, Box 12256, 102 26 STOCKHOLM (för kännedom)