Datainspektionen

Datum	Diarienr
2014-01-30	280-2013

Polismyndigheten i Uppsala län
Box 3007
750 03 Uppsala

Tillsyn av personuppgiftsbehandling vid Polismyndigheten i Uppsala län

Datainspektionen meddelar följande

BESLUT

1. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014 och därefter fortlöpande, förse personuppgiftsombudet med de uppgifter som behövs för att denne i enlighet med 2 kap. 2 § första stycket 9 polisdatalagen (2010:361) och 39 § personuppgiftslagen (1998:204) ska kunna föra en aktuell förteckning över de behandlingar av personuppgifter som polismyndigheten genomför.

2. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014, i enlighet med 2 kap. 2 § första stycket 7 polisdatalagen (2010:361) och 31 § personuppgiftslagen (1998:204) utarbeta skriftliga rutiner om säkerhetsåtgärder vid behandling av personuppgifter på mobila enheter (mobila lagringsmedia).

3. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014, i enlighet med 2 kap. 2 § första stycket 3 polisdatalagen (2010:361) och 9 § första stycket g personuppgiftslagen (1998:204) införa rutiner som säkerställer att en tillförd sekretessmarkering i folkbokföringsregistret uppmärksammas i RAR och DurTvå och registreras i systemen senast i samband med att ett ärende slutredovisas.

4. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014, införa gallringsrutiner för Sko-/spårregistren i enlighet med vad som

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

anges i 2 kap. 12 § polisdatalagen (2010:361) och att gallra personuppgifter ur registren.

5. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014, upphöra med att behandla personuppgifter i Daktyloskopieringsregistret för ändamålet fotokonfrontation.

6. Polismyndigheten i Uppsala län föreläggs att, senast den 30 april 2014, se över myndighetens rutiner vid publicering av notiser innehållande personuppgifter i KUT-info, där notisen publicerats i ett återkopplingssyfte för personalen.

7. Polismyndigheten i Uppsala län föreläggs att omgående, i enlighet med 14 § polisdatalagen (1998:622), inrätta behandlingen i den särskilda undersökningen H-19-08 på ett sådant sätt att det säkerställs att de personer som inte är misstänkta för brott (s.k. kringpersoner) förses med en notering om detta förhållande.

8. Polismyndigheten i Uppsala län föreläggs att omgående, i enlighet med 3 § och 14 §§ polisdatalagen (1998:622), upphöra med behandlingen av personuppgifter i den särskilda undersökningen i kriminalunderrättelseverksamhet med dnr H-20-08 som bedrivs med stöd av polisdatalagen (1998:622).

9. Polismyndigheten i Uppsala län föreläggs att senast den 28 maj 2014 komma in till Datainspektionen en redovisning av de åtgärder som polismyndigheten har vidtagit med anledning av föreläggandena enligt punkterna 1-8.

Redogörelse för tillsynsärendet

I enlighet med beslutad tillsynsplan har Datainspektionen genomfört tillsyn av personuppgiftsbehandling vid Polismyndigheten i Uppsala län (i det följande polismyndigheten). Datainspektionen har den 22 april 2013 på plats i Uppsala utfört en inspektion i syfte att granska om den personuppgiftsbehandling som polismyndigheten utför är förenlig med gällande rätt. Tillsynen inleddes med en genomgång av integritetsskyddsarbetet och den förteckning som polismyndigheten för över behandlingarna vid myndigheten. Därefter har personuppgiftsbehandlingen inom följande IT-stöd/behandlingar granskats:

- Polisens utredningsstöd (PUST)
- Sko-/spårregistren
- Daktyloskopieringsregister

- Arrestliggaren
- Digital Bandinspelning
- KUT-info (KUT= kriminalunderrättelseverksamhet)
- Särskilda undersökningar i kriminalunderrättelseverksamhet

Vid inspektionen har Datainspektionen gjort stickprovsvisa kontroller och polismyndigheten har förevisat hur myndigheten behandlar personuppgifter i de utvalda IT-systemen.

Vidare har Datainspektionen, avseende IT-systemen Rationell Anmälansrutin (RAR) och Datoriserad Utredningsrutin Tvångsmedel (DurTvå), kontrollerat hur myndigheterna avställer uppgifter i systemen samt ställt frågor om hur personer med skyddade personuppgifter hanteras.

Utöver de ovan angivna systemen har Datainspektionen ställt frågor kring IT-systemen Daktningsregister och Dagbesked Arresten som båda funnits med på den förteckning som Datainspektionen tagit del av inför inspektionen. Båda dessa system var enligt polismyndigheten avvecklade vid inspektionstillfället.

Hanteringen av information på mobila enheter har granskats ur ett IT-säkerhetsperspektiv.

Datainspektionen har upprättat protokoll över inspektionen. Polismyndigheten, som beretts tillfälle att yttra sig över protokollet, kom in med ett yttrande den 18 juni 2013.

Skäl för beslutet

Allmänt om integritetsarbetet vid polismyndigheten

Polismyndigheten har i enlighet med kraven i 2 kap. 5 § polisdatalagen (2010:361) utsett ett personuppgiftsombud. En av personuppgiftsombudets uppgifter är, i enlighet med 39 § personuppgiftslagen (1998:204), att föra en förteckning över de personuppgiftsbehandlingar som sker vid myndigheten. Det förutsätter att polismyndigheten förser personuppgiftsombudet med nödvändiga uppgifter om de behandlingar av personuppgifter som myndigheten genomför. Behovet av att föra en sådan förteckning följer också av att polismyndigheten enligt 2 kap. 2 § första stycket 10 polisdatalagen och 42 § personuppgiftslagen är skyldig att till var och en som begär det lämna upplysningar om myndighetens behandling av personuppgifter.

Datainspektionen gör följande bedömning
Vid inspektionen konstaterades att polismyndigheten inte genomfört någon översyn av förteckningen i samband med den nya polisdatalagens ikraftträdande. Datainspektionen konstaterade också att förteckningen har följande brister:

- IT-systemet RAR och behandlingen av personuppgifter vid publicering av misstänkta gärningsmän på Internet saknas.
- Daktningsregistret finns upptagen i förteckningen trots att registret avvecklats.
- Dagbesked arresten finns upptagen i förteckningen trots att registret avvecklats.
- Daktyloskopieringsregistret saknas i förteckningen (se avsnittet nedan som avser Daktyloskopieringsregistret).
- Fel grund för behandlingen är angiven avseende Sko/spårregistret. Den rätta grunden ska enligt Datainspektionens bedömning vara polisdatalagen och inte personuppgiftslagen. Följaktligen saknas också en rättslig analys i förhållande till polisdatalagen (för bedömningen se vad som särskilt anges under avsnittet nedan som behandlar Sko/spårregistret).
- Polisdatalagen måste läggas till som grund för behandlingen vad avser Arrestliggaren. Följaktligen saknas också en rättslig analys i förhållande till polisdatalagen (för bedömningen se vad som särskilt anges under avsnittet nedan som behandlar Arrestliggaren).
- Polisdatalagen måste läggas till som grund för behandlingen vad avser KUT-info (för bedömningen se vad som särskilt anges under avsnittet nedan som behandlar KUT-info). Följaktligen saknas också en rättslig analys i förhållande till polisdatalagen.

Datainspektionen anser att de brister som förteckningen uppvisar är allvarliga. Det är anmärkningsvärt att förteckningen inte är uppdaterad i förhållande till polisdatalagen, som trädde ikraft den 1 mars 2012. Det är visserligen personuppgiftsombudet som ska föra förteckningen men det förutsätter att polismyndigheten förser denne med uppgifterna om myndighetens behandling. Mot denna bakgrund finner Datainspektionen skäl att förelägga polismyndigheten att förse personuppgiftsombudet med de uppgifter som behövs för att leva upp till skyldigheten enligt 39 § personuppgiftslagen.

IT-säkerhet i mobil lagringsmedia och mobil IT-utrustning
Vid inspektionen konstaterades att polismyndigheten i stora delar saknar särskilda rutiner eller instruktioner för användning av mobila lagringsmedia och mobil IT-utrustning. Det finns dock ett dokument ”Goda råd om hur du

använder mobiltelefonen” som bland annat ger råd om säker hantering av mobiltelefoner och hur information ska hanteras på mobiltelefoner. Dokumentet är framtaget av verksamhetsskyddsenheten på Rikspolisstyrelsen. I övrigt har polismyndigheten beskrivit hur man hanterar material på mobila lagringsmedier i vissa situationer.

Datainspektionen gör följande bedömning
Enligt 31 § personuppgiftslagen, som är tillämplig på behandlingen av personuppgifter enligt 2 kap. 2 § första stycket 7 polisdatalagen, ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. När åtgärder vidtas ska bland annat beaktas vilka särskilda risker som finns med behandlingen och hur pass känsliga de behandlade personuppgifterna är.

Den information polismyndigheten hanterar i den brottsbekämpande verksamheten är integritetskänslig. Det finns betydande risker för att uppgifterna sprids på ett icke avsiktligt sätt vid mobil hantering. För att säkerhetsnivån ska anses tillräcklig krävs därför att det finns genomtänkta skriftliga instruktioner för denna hantering. Det dokument som Rikspolisstyrelsen tagit fram är inte tillräckligt. Mot denna bakgrund finns det skäl att förelägga polismyndigheten att, i enlighet med 2 kap. 2 § första stycket 7 polisdatalagen och 31 § personuppgiftslagen, utarbeta skriftliga rutiner om säkerhetsåtgärder vid behandling av personuppgifter på mobila enheter (mobila lagringsmedia).

Allmänt om RAR, DurTvå och PUST
Rationell Anmälansrutin (RAR) och Datoriserad Utredningsrutin Tvångsmedel (DurTvå) är centrala polisiära IT-system i vilka det behandlas mycket stora mängder personuppgifter av integritetskänslig natur. RAR utgör polismyndigheternas anmälningsregister och kriminaldiarium och DurTvå är ett utredningssystem som i huvudsak används för att bygga upp och färdigställa förundersökningsprotokoll. I DurTvå registreras också reella och personella tvångsmedel. IT-systemet Polisens utredningsstöd (PUST) kommer på sikt helt att ersätta RAR och DurTvå, men vid inspektionstillfället hanterades 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 RAR, DurTvå och PUST.

I PUST och DurTvå, samt numera även i RAR, behandlar polisen personuppgifter med stöd av polisdatalagen, som trädde ikraft den 1 mars 2012. I de tre IT-systemen gör polisen personuppgifter gemensamt tillgängliga. Vissa

bestämmelser i polisdatalagen, bl.a. om bevarande och sökning, behöver inte tillämpas förrän den 1 januari 2015 (se övergångsbestämmelserna).

Datainspektionen gör följande bedömning
Datainspektionens bedömning av polismyndighetens personuppgiftsbehandling i PUST är att behandlingen sker i enlighet med polisdatalagen.

Vid inspektionen konstaterades dock att polismyndigheten, i strid med den interna rutinen hos polismyndigheten som anvisar att personuppgifter inte ska behandlas i fältet ”utredningens namn”, hade en del utredningar som döpts med förnamn, efternamn, personnummer eller en kombination av alla tre. Som Datainspektionen tidigare konstaterat i tillsynsärenden gentemot andra polismyndigheter (se t.ex. Datainspektionens beslut den 20 november 2012, dnr 605-2012) kan man genom att namnge ärendena på det beskrivna sättet i sökfältet ”Utredningens namn”, söka fram ärenden som annars inte hade varit sökbara (t.ex. efter det att förundersökningsledaren har fattat ett nedläggningsbeslut). Det innebär således i praktiken att bestämmelsen i 3 kap. 13 § polisdatalagen, som dock 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. Således anser Datainspektionen att polismyndigheten inte bör namnge ärenden i PUST med hjälp av personuppgifter i fältet ”Utredningens namn”. Polismyndigheten rekommenderas att se över hur den interna rutinen tillämpas i denna del. Datainspektionen ser positivt på att polismyndigheten varit i kontakt med Rikspolisstyrelsen och lagt fram ett förbättringsförslag som innebär att användarna ska varnas om personuppgifter skrivs in i fältet för utredningen namn.

Hantering av s.k. skyddade personuppgifter i RAR, DurTvå och PUST
Polismyndigheten saknar rutiner, vid registrering av uppgifter i RAR och DurTvå, för att hantera de fall då de involverade personerna i en förundersökning erhåller skyddade personuppgifter under ett ärendes handläggning. Vid inspektionen framkom vidare att ärenden i vilka det förekommer skyddade personuppgifter inte får registreras i PUST från start. Det gäller oavsett vilken av de involverade personerna som har skyddade personuppgifter. Sådana ärenden ska istället registreras i RAR och DurTvå. I PUST finns enligt polismyndigheten en automatisk kontroll gentemot folkbokföringsregistret, varför systemet kan uppdatera informationen när en person får skyddade personuppgifter under utredningens gång.

Datainspektionen gör följande bedömning
Om det saknas rutiner för att hantera de fall då en involverad person i en förundersökning erhåller skyddade personuppgifter under handläggningen riskerar en tillförd sekretessmarkering att inte upptäckas innan ärendet

slutredovisas till åklagare. Enligt Datainspektionen innebär det i sin tur att registrerade personer riskerar att drabbas av otillbörliga intrång i den personliga integriteten. Till exempel riskerar en målsägande, som begär och erhåller skyddade personuppgifter med anledning av hot som denne utsätts för i samband med en brottsutredning, att få sekretesskyddade uppgifter rörande adress m.m. röjda. Att skyddade personuppgifter inte behandlas på rätt sätt innebär att behandlingen riskar att stå i strid med 9 § första stycket g personuppgiftslagen (se 2 kap. 2 § första stycket polisdatalagen), eftersom uppgifterna i registret, utan upplysning om sekretessmarkering, inte är riktiga och aktuella. Mot denna bakgrund föreläggs polismyndigheten att, i enlighet med 2 kap. 2 § första stycket 3 polisdatalagen och 9 § första stycket g personuppgiftslagen, införa rutiner som säkerställer att en tillförd sekretessmarkering i folkbokföringsregistret uppmärksammas i RAR och DurTvå senast i samband med att ett ärende slutredovisas.

Vad avser PUST utgår Datainspektionen från att den automatiska funktionen i PUST som polismyndigheten redogjort för klarar av att hantera de situationer där involverade personer får skyddade personuppgifter under ett ärendes behandling. Datainspektionen har därför inga synpunkter i denna del.

Sko-/spårregistren
Syftet med registren är, enligt polismyndighetens förteckning, att kunna identifiera vilken sko eller skomodell som lämnat spår på brottsplatser och därigenom kunna knyta en misstänkt gärningsman till en brottsplats. Det finns två register, ett avseende skospår från brottsplatser och ett avseende skor. I registret för spår registreras, förutom spåret/mönstret på skon, koder för mönstren. I registret avseende skor sparas bland annat bilder på beslagtagna skor och skomodeller. I båda registren registreras ärendenummer (K-nummer), beslagsnummer, brottskod, brottsdatum och område/distrikt. Genom ärendenummer och beslagsnummer går det att koppla uppgifterna i registren till personer, vilket medför att personuppgifter behandlas i registren.

Datainspektionen gör följande bedömning
Polismyndigheten har i förteckningen över registren angett att den lagliga grunden för behandling av personuppgifter i registren är personuppgiftslagen. En behandling av spår från en brottsplats, där syftet är att kunna koppla ihop spåren med gärningsmän, hör till polisens brottsbekämpande verksamhet. Polisdatalagen gäller, enligt 1 kap. 2 §, när polisen behandlar personuppgifter automatiskt i den brottsbekämpande verksamheten. Följaktligen gäller polisdatalagen för behandlingen av personuppgifter i registren.

Vid inspektionen kunde det konstateras att polismyndigheten saknar rutiner för att gallra uppgifter ur registren och att någon gallring inte har genomförts

sedan 2008, då registren skapades. I polisdatalagen finns bestämmelser om hur länge personuppgifter får sparas. Mot denna bakgrund föreläggs polismyndigheten att införa gallringsrutiner för Sko-/spårregistren i enlighet med vad som anges i 2 kap. 12 § polisdatalagen och att gallra personuppgifter ur registren.

Daktyloskopieringsregister
Daktyloskoperingsregistret är ett register som polismyndigheten fört sedan 1989 med Datainspektionens tillstånd (Datainspektionens beslut den 29 augusti 1989, dnr 1416-89). Ändamålet med registret är att vara ett administrativt hjälpmedel vid arkivhantering av fotografier beträffande daktyloskopierade personer misstänkta för brott. Polismyndighetens Daktyloskoperingsregistret innehåller personuppgifter i form av förnamn, efternamn, personnummer, fotonummer, datum och brottskod. Varje digitalt fotografi tilldelas ett fotonummer och kan, vid sökning, hittas genom koppling mellan Daktyloskoperingsregistret och fotonumret. Fotografierna, som idag är digitala, sparas i en bildfil på en nätverksserver. Polismyndigheten har uppgett att ändamålet med registret är att kunna hitta själva bildfilerna där fotografierna finns lagrade. Fotografierna används också enligt polismyndigheten för framtagning av fotokonfrontationer som sker inom ramen för en förundersökning.

Datainspektionen uppfattar att bakgrunden till inrättandet av registret är den skyldighet som en polismyndighet har att skicka fotografier på daktyloskopierade personer, som misstänks för brott, till Rikspolisstyrelsen. Enligt 7 § förordning (1992:824) om fingeravtryck m.m. ska fotografier som tas med stöd av föreskrifterna i 28 kap. 14 § rättegångsbalken skickas skyndsamt till Rikspolisstyrelsen tillsammans med en beskrivning av personen. Uppgifterna registreras i signalements- och känneteckensregistret och får behandlas av en polismyndighet för att underlätta identifiering av personer i samband med brott. Enligt övergångsbestämmelserna till polisdatalagen (2010:361) för Rikspolisstyrelsen signalements- och känneteckenregister med stöd av den upphävda datalagen (1973:289) och tillstånd från Datainspektionen.

Datainspektionen gör följande bedömning
I samband med polisdatalagen (2010:361) ikraftträdande den 1 mars 2012 upphörde polismyndighetens tidigare tillstånd för Daktyloskopieringsregistret att gälla. Det framgår av punkten 3 i ikraftträdande- och övergångsbestämmelserna till polisdatalagen. Registret måste därför vara förenligt med polisdatalagens bestämmelser.

Frågan är då om den behandling av personuppgifter som polismyndigheten utför i Daktyloskoperingsregistret är förenlig med bestämmelserna i polisdatalagen.

I polisdatalagen finns särskilda bestämmelser i fjärde kapitlet om fingeravtrycks- eller signalementsregister. Rikspolisstyrelsen får föra sådana register enligt 4 kap. 11 § polisdatalagen. Det är också Rikspolisstyrelsen som är personuppgiftsansvarig för signalements- och känneteckensregistret som ännu så länge förs med stöd av Datainspektionens tillstånd.

Enligt Datainspektionens bedömning ger polisdatalagstiftningen inte stöd för en polismyndighet att föra ett eget lokalt signalementsregister. I bedömningen väger Datainspektionen in följande faktorer.

Av 4 kap. 11 § polisdatalagen följer att Rikspolisstyrelsen får föra ett fingeravtrycks- eller signalementsregister enligt 28 kap. rättegångsbalken. Enligt förordningen om fingeravtryck ska polismyndigheterna skicka uppgifterna till Rikspolisstyrelsen. Det finns ingen motsvarande bestämmelse i polisdatalagen som anger att andra polismyndigheter får inrätta ett lokalt fingeravtrycks- och signalementsregister. Det är också Rikspolisstyrelsens register som är en förutsättning för det internationella samarbetet med utbyte av information (se bland annat art 8 i Rådets beslut 2008/615/RIF av den 23 juni 2008 om fördjupat gränsöverskridande samarbete, särskilt för bekämpning av terrorism och gränsöverskridande brottslighet, det s.k. Prümrådsbeslutet).

Fingeravtrycks- och signalementsregister inrymmer särskilda integritetsrisker och regleras i fjärde kapitlet i polisdatalagen. I förhållande till andra och tredje kapitlet polisdatalagen innehåller det fjärde kapitlet särskilda regler om innehåll, gallring och direktåtkomst. Om en polismyndighet skulle kunna föra ett lokalt signalementsregister med stöd av antingen andra eller tredje kapitlet i polisdatalagen skulle det innebära att det integritetsskydd som motiverat särskilda bestämmelser i fjärde kapitlet skulle gå förlorat.

Vidare är systematiken i polisdatalagen på flera ställen uppbyggd på så sätt att polismyndigheter uttryckligen medges en rätt att ta del av informationen i fingeravtrycks- eller signalementsregister. Det framgår exempelvis av 4 kap. 17 § polisdatalagen som anger att polismyndigheter får medges direktåtkomst till registren. Det saknas en bestämmelse i polisdatalagen som medger Rikspolisstyrelsen en motsvarande möjlighet till direktåtkomst till fingeravtrycks- eller signalementsregister. Här är det relevant att jämföra med 3 kap. 8 § polisdatalagen i vilken Rikspolisstyrelsen är uppräknad bland de myndigheter som får medges direktåtkomst. Vidare anger den

sekretessbrytande bestämmelsen i 2 kap. 18 § polisdatalagen endast att polismyndigheter och inte Rikspolisstyrelsen har rätt att ta del av personuppgifter som behandlas i fingeravtrycks- eller signalementsregister enligt 4 kap. polisdatalagen.

Polismyndigheten använder Daktyloskoperingsregistret vid fotokonfrontationer bland annat eftersom de fotografier som Rikspolisstyrelsen tillhandahåller genom signalements- och känneteckensregistret håller lägre kvalité. Att fotografierna har lägre kvalité beror på det förfarande och format som Rikspolisstyrelsen anvisar när polismyndigheten ska skicka in uppgifter. Datainspektionen har förståelse för att polismyndigheten önskar ha material av hög kvalité i samband med fotokonfrontationer. Daktyloskoperingsregistret är dock, vid en sådan användning, att ses som ett lokalt signalementsregister. Enligt Datainspektionens bedömning saknar polismyndigheten ett lagligt stöd för att behandla personuppgifter i Daktyloskoperingsregistret för ändamålet fotokonfrontation. I avsaknad av lagligt stöd föreläggs polismyndigheten att upphöra med att behandla personuppgifter i Daktyloskoperingsregistret för ändamålet fotokonfrontation.

Arrestliggaren
Enligt polismyndigheten är arrestliggarens syfte att vara ett administrativt stöd för att hålla reda på och bevaka tidfrister i samband med att polismyndigheten frihetsberövat en person. Det avser framförallt personer som anhållits. Häktade personer antecknas inte i arrestliggaren eftersom Kriminalvården ansvarar för dessa. I arrestliggaren antecknas även personer som omhändertas med stöd av lagen (1976:511) om omhändertagande av berusade personer och omhändertagande av personer med stöd av lagen (1991:1128) om psykiatrisk tvångsvård.

De personuppgifter som registreras är efternamn, förnamn och personnummer. Därtill registreras skälet till frihetsberövandet och bedömning/åtgärd samt lagstöd. Under bedömning/åtgärd antecknas ibland känsliga personuppgifter, exempelvis sjukdomar och mediciner. Arrestliggaren är gemensam för arrestlokalerna i länet.

Datainspektionen gör följande bedömning
Polismyndigheten har i förteckningen över registren angett att den lagliga grunden för behandling av personuppgifter i Arrestliggaren är personuppgiftslagen. I de delar som uppgifter om personer som är anhållna behandlas i Arrestliggare, är det Datainspektionens bedömning att behandlingen hör till polisens brottsbekämpande verksamhet. För denna behandling gäller polisdatalagen. Behandling som sker utanför den brottsbekämpande verksamheten, t.ex. ett omhändertagande enligt lagen om psykiatrisk tvångs-

vård, faller utanför polisdatalagen och kan styras av bestämmelserna i personuppgiftslagen.

Vid inspektionen konstaterades att vakthavande befäl samt inspektörer och chefer vid länskommunikationscentraler, totalt ca 20 personer, har full behörighet till arrestliggaren. Ytterligare cirka 20 personer bestående av inre befäl, personal vid kriminalunderrättelsetjänsten och pressansvarig, har läsbehörighet till en digital kopia av arrestliggaren. Datainspektionen vill påminna om att det är viktigt att polismyndigheten löpande prövar vilka som ska ha behörighet att läsa informationen i arrestliggaren och att endast de som behöver informationen för fullgörande av arbetsuppgifter tilldelas behörighet.

Datainspektionen ifrågasätter också om polisen överhuvudtaget ska ha ett IT-system i vilket personuppgifter behandlas med stöd av olika rättsliga grunder (se Datainspektionens beslut i samrådsärende avseende OBS-portalen, dnr 1741-2012). Dubbla rättsliga grunder gör det svårt för den personuppgiftsansvarige att fullt ut säkerställa att olika bestämmelser avseende grundläggande krav på behandlingen, sökning, bevarande och gallring beaktas på rätt sätt med risk för intrång i de registrerades personliga integritet som följd. Datainspektionen rekommenderar Polismyndigheten att noga pröva lämpligheten av att behandla personuppgifter med stöd av olika rättsliga grunder i ett och samma IT-system.

KUT-info
KUT-info användes vid inspektionstillfället av polismyndigheten för att snabbt publicera väsentlig information av operativ karaktär som polisanställda har behov av i sin tjänst. Informationen publiceras i Pdf-dokument, för vilka krävs särskild behörighet. Varje fredag publiceras ett nytt pdf-dokument. Nästan 700 personer har behörighet att ta del av informationen. Gallring sker två månader efter publicering.

Vid inspektionen konstaterades att polismyndigheten publicerar notiser med information om personer som dömts för brott med bild, namn, brottsrubricering och påföljd. Vidare upptäcktes en notis med information om personer som häktats. Vid inspektionen konstaterades även en notis med information om att en person, som polismyndigheten tidigare efterfrågat identiteten på, var identifierad. I notisen publicerades namn och bild. Enligt polismyndigheten har notiserna publicerats i återkopplingssyfte för personalen.

Polismyndigheten har i förteckningen över registren angett att den lagliga grunden för behandling av personuppgifter i KUT-info är personuppgiftslagen.

Datainspektionen gör följande bedömning.
Mot bakgrund av karaktären på de notiser som publiceras i KUT-info är polisdatalagen tillämplig på behandlingen. I den mån det kan förekomma publiceringar som inte hör till den brottsbekämpande verksamheten gäller personuppgiftslagens regler. Datainspektionen vill i detta sammanhang hänvisa till vad som framförts ovan angående dubbla rättsliga grunder i avsnittet avseende Arrestliggaren och rekommenderar polismyndigheten att noga pröva lämpligheten av att behandla personuppgifter med stöd av olika rättsliga grunder i ett och samma IT-system.

Datainspektionen har förståelse för att det kan finnas ett behov av återkoppling på utförda arbetsinsatser, inte minst för att motivera personalen. Det kan dock utföras på annat sätt än att sprida informationen utöver den krets som rimligen har ett konkret behov av uppgifterna för lösande av sina arbetsuppgifter och i så fall utan att personuppgifter behandlas.

Datainspektionen ifrågasätter således behovet av att publicera personuppgifter i notiser som syftar att ge återkoppling till personalen. En sådan behandling kan stå i strid med de grundläggande kraven i 9 § personuppgiftslagen som bland annat anger att inte fler uppgifter än vad som behövs för ändamålet får behandlas.

Mot denna bakgrund finner Datainspektionen skäl att förelägga polismyndigheten att se över sina rutiner vid publicering av notiser innehållande personuppgifter i KUT-info, där notisen publicerats i ett återkopplingssyfte för personalen.

Behandling av personuppgifter i polismyndighetens kriminalunderrättelseverksamhet

Inledning
Inom ramen för polisens kriminalunderrättelseverksamhet förekommer mycket integritetskänslig behandling av personuppgifter. 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 t.ex. för att kunna förhindra brott. Behandlingen sker i polisens brottsbekämpande verksamhet.

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 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) så länge beslutet om att behandla personuppgifterna fattats före den 1 mars 2012 då den nya polisdatalagen trädde ikraft. Polismyndigheten har uppgett att några uppgiftssamlingar enligt nya polisdatalagen (2010:361) inte förekom vid myndigheten vid tiden för inspektionen.

I en särskild undersökning i kriminalunderrättelseverksamhet får 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 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. 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.

Datainspektionens granskning
Vid polismyndigheten bedrevs den 22 april 2013 sammanlagt fyra särskilda undersökningar med stöd av polisdatalagen (1998:622), varav tre granskades vid inspektionen.

Datainspektionen gör följande bedömning
Polisen har fått långtgående befogenheter inom kriminalunderrättelseverksamheten att, även när det endast föreligger svaga misstankar om personers inblandning i brott som dessutom inte behöver vara konkret angivna, kartlägga ett stort antal personer. Det är därför mycket viktigt att samtliga skyddsmekanismer som ska förebygga otillbörliga intrång i den personliga integriteten iakttas.

Polisen kommer att få en ny IT-plattform för behandling av personuppgifter i myndighetens kriminalunderrättelseverksamhet. Mot den bakgrunden vill Datainspektionen påminna om att polismyndigheten behöver inrätta

behandlingen av integritetskänsliga personuppgifter på ett sådant sätt att användarnas aktiviteter kan kontrolleras genom loggning.

Enligt polismyndigheten gallras uppgifter manuellt ur de särskilda undersökningarna ungefär en gång per kvartal efter det att ärendet funnits i 12 månader. Huvudregeln är att gallringsprövningen sker av respektive handläggare och slutligen av den som är ansvarig för den särskilda undersökningen. En gång i kvartalet får handläggarna en lista på personer som kan vara aktuella att gallra. I tveksamma fall ska handläggarna diskutera gallringen med närmast chef. Datainspektionen har inga synpunkter på dessa rutiner.

När det gäller de tre särskilda undersökningarna som kontrollerades på plats genom stickprovskontroller är det Datainspektionens bedömning att två undersökningar (H-19-08 och H-20-08) har brister.

För det första behandlar polismyndigheten, i den särskilda undersökningen H-19-08, personuppgifter om personer som inte är misstänkta för allvarlig brottslig verksamhet (kringpersoner) utan att personerna försetts med en sådan särskild upplysning som följer av 14 § andra stycket polisdatalagen (1998:622). Således går det i polismyndighetens särskilda undersökning inte att se om en registrerad person kan misstänkas för att ägna sig åt brottslig verksamhet eller om grunden för registrering endast är att personen är en s.k. kringperson. Bristen är allvarlig eftersom den avser en grundläggande del av integritetsskyddet. Polismyndigheten ska därför föreläggas att i de aktuella delarna inrätta personuppgiftsbehandlingen på så sätt att det säkerställs att de personer som inte är misstänkta för brott (kringpersoner) förses med en notering om detta förhållande.

Vidare konstaterar Datainspektionen att polismyndigheten, i den särskilda undersökningen H-20-08, behandlar uppgifter om en person, som när anteckningen skrevs i september 2010, misstänktes för brott. Enligt polismyndigheten har dock inget analysarbete skett sedan registreringen och ingen ytterligare information har tillförts. Polismyndigheten har uppgett att ”undersökningen inte är så aktiv och att polismyndigheten funderar på att avsluta den”.

En särskild undersökning som innehåller personuppgifter kan enligt Datainspektionen inte ligga vilande. Det framgår av 3 § och 14 § polisdatalagen (1998:622). Det är således inte förenligt med lagstiftningen att enbart samla in personuppgifter utan att bearbeta eller analysera informationen. Om bearbetning och analys inte sker i undersökningen ska undersökningen avslutas. Mot den bakgrunden ska polismyndigheten föreläggas att omgående avsluta den särskilda undersökningen H-20-08.

I två av de särskilda undersökningarna, H-19-08 och H-01-10, fanns, vid inspektionstillfället, barn registrerade. I H-19-08 fanns ett 20-tal barn under 15 år registrerade och i H-01-10 fanns ett barn fött 2009 registrerat.

Polismyndigheten har uppgett att det kan finnas behov av att kartlägga och registrera även barn i särskilda undersökningar. Myndigheten har hänvisat till att registreringen kan behövas för att kunna avslöja och bekämpa brott där barnen själva är redskap vid andras brottslighet. Datainspektionen kan inte på befintligt underlag ifrågasätta de förklaringar som polismyndigheten lämnat i ärendet till varför barnen registrerats. Datainspektionen rekommenderar dock polismyndigheten att gå igenom och kontrollera registreringarna av barn och behovet av att ha kvar dessa i de särskilda undersökningarna.

Uppföljning av genomförda åtgärder
Enligt Datainspektionen finns det skäl att följa upp de åtgärder som polismyndigheten ska vidta i enlighet med detta beslut. Polismyndigheten föreläggs därför att komma in med en redovisning av de åtgärder som myndigheten vidtagit med anledning av föreläggandena i detta beslut.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö i närvaro av chefsjuristen Hans-Olof Lindblom, enhetschefen Britt Marie Wester och Jonas Agnvall, föredragande.

Kristina Svahn Starrsjö

Jonas Agnvall

Hur man överklagar
Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Överklagandet skall 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.

Bilaga:

1. Datainspektionens beslut dnr 1741-2012