

Polismyndigheten Gotland
Box 1153
621 22 VISBY

Tillsyn av personuppgiftsbehandling vid Polismyndigheten Gotland

Datainspektionen meddelar följande

BESLUT

1. Polismyndigheten Gotland föreläggs att, senast den 28 februari 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 Gotland föreläggs att, senast den 28 februari 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, DurTvå och PUST samt registreras i systemen senast i samband med att ett ärende slutredovisas.
3. Polismyndigheten Gotland föreläggs att, senast den 28 februari 2014, i enlighet med 2 kap. 2 § första stycket 7 polisdatalagen (2010:361) och 31 § personuppgiftslagen (1998:204) utarbeta skriftliga rutiner som innehåller säkerhetsåtgärder avseende behandling av personuppgifter på mobila enheter (mobila lagringsmedia).
4. Polismyndigheten Gotland föreläggs att, senast den 28 februari 2014, i enlighet med 2 kap. 2 § första stycket 7 polisdatalagen (2010:361) och

31 § personuppgiftslagen (1998:204) införa loggning och logguppföljning av enskilda användares aktiviteter för att upptäcka och beivra obehörig åtkomst till personuppgifter i systemen.

5. Polismyndigheten Gotland föreläggs att, senast den 28 februari 2014, i enlighet med 2 kap. 11 § polisdatalagen (2010:361) genomföra en översyn av åtkomsten till arkiverade personuppgifter med utgångspunkt i att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.
6. Polismyndigheten Gotland föreläggs att snarast radera de personuppgifter i den särskilda uppgiftssamlingen som inte borde ha registrerats samt upprätta rutiner som säkerställer att behandlingen av personuppgifter som sker i den särskilda uppgiftssamlingen i kriminalunderrättelseverksamhet föregås av en prövning av att varje registrering är förenlig med 2 kap. 7 § polisdatalagen (2010:361).
7. Polismyndigheten Gotland 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 A012.020/2013 som bedrivs med stöd av polisdatalagen.
8. Polismyndigheten Gotland föreläggs att senast den 28 mars 2014 komma in till Datainspektionen med en åtgärdsplan som innehåller en redovisning av de åtgärder som polismyndigheten har vidtagit med anledning av föreläggandena enligt punkterna 1-7.

Redogörelse för tillsynsärendet

I enlighet med beslutad tillsynsplan har Datainspektionen genomfört tillsyn av personuppgiftsbehandlingen vid Polismyndigheten Gotland (i det följande polismyndigheten). Datainspektionen har den 3 maj 2013 på plats i Visby genomfört en övergripande inspektion med stickprovsvisa kontroller av:

- Polisens Utredningsstöd (PUST)
- Internet (publicering av okända gärningsmän)
- KUT-info (KUT = kriminalunderrättelsetjänst)
- Särskilda undersökningar i kriminalunderrättelseverksamheten (SUR)
- Särskilda uppgiftssamlingar i kriminalunderrättelseverksamheten (SUS)

Någon fullständig genomgång av dessa system har inte skett.

Vid inspektionen gjorde Datainspektionen stickprovsvisa slagningar och polismyndigheten förevisade hur personuppgifter behandlas i ovanstående system.

Datainspektionen har upprättat protokoll över inspektionen.

Polismyndigheten, som beretts tillfälle att yttra sig över protokollet, kom in med yttrande den 17 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, enligt 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 § 10 polisdatalagen och 42 § personuppgiftslagen är skyldig att till var och en som begär det lämna upplysningar om myndighetens behandlingar av personuppgifter.

Datainspektionen gör följande bedömning

Vid inspektionen konstaterades att polismyndigheten inte genomfört någon översyn av förteckningen i samband med den nya polisdatalagens ikraftträdande. I förteckningen saknas också IT-systemet RAR, publiceringen

av information på polismyndighetens Facebook-sida samt publiceringen av misstänkta gärningsmän på Internet.

Datainspektionen anser att de brister som förteckningen uppvisar är allvarliga. Det är särskilt anmärkningsvärt att förteckningen inte är uppdaterad i förhållande till polisdatalagen, som trädde i kraft den 1 mars 2012. Det är visserligen personuppgiftsombudet som ska föra förteckningen men det förutsätter att polismyndigheten förser denne med uppgifter 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.

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 polismyndighetens anmälningsregister och kriminaldiarium och DurTvå är ett utredningsstöd som i huvudsak används för att bygga upp och färdigställa förundersökningsprotokoll. I DurTvå registreras också reella och personella tvångsmedel. Polisens utredningsstöd (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. I dessa system behandlar polisen personuppgifter med stöd av polisdatalagen. I de tre IT-systemen gör polisen personuppgifter gemensamt tillgängliga.

PUST

Polismyndigheten har på grund av störningar i datasystemen använt PUST endast i begränsad utsträckning.

Vid inspektionen framgick att polismyndigheten namngett ett antal ärenden i fältet "Utredningens namn" med namn och/eller personnummer.

Polismyndigheten har i yttrande över protokollet uppgett att efter inspektionen har en ny rutin införts som innebär att ärendet namnges med datum samt plats för brottet/händelsen i fältet "Utredningens namn" och inte med namn och/eller personnummer. Rutinen har kommunicerats till samtliga medarbetare som använder PUST. Den på polismyndigheten ansvarige tjänstemannen för PUST har ändrat samtliga öppna ärenden där namn och/eller personnummer registrerats i fältet "Utredningens namn" till datum samt plats för brottet/händelsen.

Datainspektionen gör följande bedömning

Genom att namnge ärendena med personuppgifter, kan man vid sökning i polismyndighetens PUST, i sökfältet "Utredningens namn", söka fram ärenden som annars inte skulle vara sökbara, efter det att förundersökningsledaren har lagt ner förundersökningen. Att kunna göra sökningar på detta sätt innebär att bestämmelsen i 3 kap. 13 § polisdatalagen (som dock inte behöver tillämpas förrän den 1 januari 2015) sätts ur spel. Datainspektionen anser att det är positivt att polismyndigheten infört nya rutiner som medför att ärenden inte namnges med personuppgifter.

Hantering av skyddade personuppgifter i RAR, DurTvå och PUST

Datainspektionen efterfrågade under inspektionen hur personer med skyddade personuppgifter hanteras samt hur de personer som får skyddade personuppgifter under utredningens gång hanteras i RAR, DurTvå och PUST. Vad gäller RAR och DurTvå har polismyndigheten inga rutiner för att hantera de situationer då en person erhåller skyddade personuppgifter under ärendets handläggning. Polismyndigheten har skriftligen angett att av en lokal rutinhandbok för PUST framgår att PUST inte ska användas när en person har skyddade personuppgifter. Om en person får skyddade personuppgifter under utredningens gång ansvarar handläggaren för att ärendet makuleras och att uppgifterna överförs till RAR och DurTvå. Polismyndigheten har idag ingen skriftlig rutin för detta.

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. Att skyddade personuppgifter inte behandlas på rätt sätt innebär att behandlingen riskerar att stå i strid med 9 § första stycket g personuppgiftslagen (se 2 kap. 2 § första stycket 3 polisdatalagen), eftersom uppgifterna i registret, utan upplysning om sekretessmarkering, inte är riktiga och aktuella. Mot bakgrund av ovanstående ska polisen föreläggas att införa rutiner som säkerställer att en tillförd sekretessmarkering uppmärksammas samt registreras i systemen senast i samband med att ett ärende slutredovisas.

Publicering av okända gärningsmän på Internet

Beslut om publicering av okända gärningsmän på Internet föregås av en noggrann prövning och beslut fattas av förundersökningsledaren. Informationen publiceras i maximalt en månad och raderas därefter automatiskt. Om personen identifieras innan dess tas informationen omedelbart bort efter beslut av förundersökningsledaren. Polismyndigheten

följer Rikspolisstyrelsens föreskrifter, det vill säga FAP 188-1 vid internetpubliceringar samt de riktlinjer som polismyndigheten i Stockholm tagit fram. Polismyndigheten har inte beslutat om några lokala tjänsteföreskrifter på detta område. Polismyndigheten har vid ett tillfälle publicerat information om okända gärningsmän på Internet i samband med en notis om en mordbrand. Vid det tillfället ville polismyndigheten komma i kontakt med en person som kan ha bevittnat händelsen.

Datainspektionen gör följande bedömning

Datainspektionen anser det positivt att en publicering av okända gärningsmän föregås av en noggrann prövning av polismyndigheten. Datainspektionen vill dock poängtera vikten av att en noggrann prövning också ska göras avseende andra involverade personer, såsom vittnen och målsäganden.

Av FAP 188-1, punkt 8, framgår att polismyndigheten i lokala föreskrifter bör meddela de ytterligare bestämmelser som behövs för tillämpningen av FAP 188-1. Datainspektionen rekommenderar polismyndigheten att upprätta lokala skriftliga rutiner avseende publicering av okända gärningsmän på Internet. Detta kan exempelvis ske genom att ett beslut fattas om att en viss polismyndighets rutiner ska gälla även för Gotland.

IT-säkerhet och loggning

Vid inspektionen konstaterades att polismyndigheten i stora delar saknar lokala tjänsteföreskrifter för användning av mobila enheter. Polismyndigheten följer dock de riktlinjer som Rikspolisstyrelsen tagit fram samt de riktlinjer som polismyndigheten i Stockholm har.

Vidare konstaterades att polismyndigheten aldrig gjort några kontroller, varken stickprovskontroller eller kontroller på förekommen anledning, av loggarna avseende de IT-system som är anslutna till polisens centrala säkerhetslogg (CSL) eller lokala IT-system. Polismyndigheten har uppgett att sådana kontroller är ”på gång” och att två personer har genomgått utbildning avseende logguppföljning.

Datainspektionen gör följande bedömning

Enligt 31 § personuppgiftslagen, som är tillämplig på behandling 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 (säkerhetsåtgärder). 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 ofta integritetskänslig. Det finns betydande risker 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 som tagits fram lokalt för denna hantering.

Polismyndigheten har rutiner för användningen av mobila enheter men har inte själv tagit fram någon lokal tjänsteföreskrift. Polismyndigheten Gotland ska därför föreläggas att upprätta skriftliga rutiner innehållande säkerhetsåtgärder avseende behandling av personuppgifter på mobila enheter (mobila lagringsmedia). Detta kan exempelvis ske genom att ett beslut fattas om att en viss polismyndighets rutiner ska gälla även för Gotland.

Med anledning av att polismyndigheten inte utför några kontroller av enskilda användares aktiviteter ska polisen föreläggas att införa loggning och logguppföljning för att upptäcka och beivra obehörig åtkomst till personuppgifter i systemen.

Arkivariebehörigheter

Sammanlagt 10 personer har behörighet "arkivarie" i RAR och DurTvå och har åtkomst till ärenden som inte längre är åtkomliga i den dagliga brottsbekämpande verksamheten. Det är förundersökningsledare och tjänstemän på expeditionen som innehar behörigheten. Det är polismyndighetens uppfattning att samtliga som har arkivariebehörigheten har ett behov av åtkomst till sådana ärenden. Polismyndigheten har inte genomfört någon strukturerad analys/genomgång av vem/vilka som har ett behov av att ha en arkivariebehörighet. Polismyndigheten uppger att de kommer att genomföra en översyn i denna del.

Datainspektionen gör följande bedömning

Enligt 2 kap. 11 § polisdatalagen ska tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. När det gäller behandlingen av personuppgifter i äldre avslutade ärenden kan nämnas att tilldelandet av behörigheter inte innebär att behörigheter får användas fritt. Det är endast i de fall då undantagen i 3 kap. 7 § andra stycket polisdatalagen är tillämpliga som sökningar i äldre ärenden får ske. Det finns annars en risk för att arkivariebehörigheten används i situationer där det saknas rättsliga förutsättningar för polisen att behandla sådana uppgifter. Det är polismyndighetens uppgift som personuppgiftsansvarig att genom utbildning och kontroll så långt det är möjligt och rimligt säkerställa att regelverket följs. Med hänsyn till omfattningen av de personuppgifter som en "arkivarie" har tillgång till är det av största vikt att behörigheten är begränsad till det antal personer på polismyndigheten som har ett klart motiverat behov

vilket kräver en noggrann analys innan behörigheter delas ut. Polismyndigheten har uppgett att en översyn av arkivariebehörigheten kommer att genomföras. Mot bakgrund av detta ska polismyndigheten föreläggas att redovisa resultatet av översynen till Datainspektionen med utgångspunkt i att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter.

Behandling av personuppgifter i polismyndighetens kriminalunderrättelseverksamhet

Inledning

I polisdatalagen finns bestämmelser om behandling av personuppgifter utanför en förundersökning. I den mån det är fråga om s.k. gemensamt tillgängliga uppgifter gäller de mer begränsade 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, behandla personuppgifter i s.k. särskilda undersökningar i kriminalunderrättelseverksamhet enligt reglerna i 3 och 14-16 §§ gamla polisdatalagen (1998:622). Polismyndigheten uppgav vid tiden för inspektionen att de behandlar personuppgifter inom kriminalunderrättelseverksamheten både enligt det nya och enligt det äldre regelverket.

KUT-info

KUT-info används av polismyndigheten för att snabbt publicera väsentlig information av operativ karaktär som polisanställda har behov av i sin tjänst. I KUT-info behandlar polisen personuppgifter med stöd av polisdatalagen och polisen gör personuppgifterna gemensamt tillgängliga. Informationen publiceras i notiser i en pdf-fil som nås via polismyndighetens intranät. KUT-info innehåller information om exempelvis brott som inträffat, varningar för farliga personer, personer som är häktade/anhållna samt villkorligt frigivna personer.

Sex personer som arbetar med kriminalunderrättelseverksamhet har behörighet att publicera information. Vad som ska publiceras beslutas på gemensamma morgonmöten av polismyndighetens kriminalunderrättelsetjänst. Poliser, civilutredare och länskommunikationscentralen på Gotland har läsbehörighet till KUT-info.

Informationen publiceras på intranätet under ett par veckor. I samband med att informationen tas bort skrivs en kopia ut som förvaras i en pärm. Informationen i pärmarna gallras inte, de arkiveras efter ca ett år.

Datainspektionen tog del av samtliga notiser som publicerades på KUT-info vid tidpunkten för inspektionen. En notis med syfte att identifiera en misstänkt person låg fortfarande kvar trots att personen identifierats. Vidare fanns en notis som innehöll information om en person som dömts för fyra trafikbrott. Notisen har publicerats eftersom polismyndigheten anser att det är fråga om upprepad brottslighet som gör att brottet anses ske systematiskt.

Datainspektionen gör följande bedömning

Polismyndigheten får publicera personuppgifter i KUT-info om uppgifterna kan antas ha samband med misstänkt brottslig verksamhet, om den misstänkta verksamheten innefattar brott för vilket är föreskrivet fängelse i ett år eller däröver, eller om det sker systematiskt (3 kap. 2 § första stycket 1 a-b polisdatalagen). Enligt polismyndigheten publiceras många av notiserna med stöd av att den misstänkta brottsliga verksamheten sker systematiskt. Med anledning av detta vill Datainspektionen peka på det resonemang som förs i förarbetena till polisdatalagen avseende misstänkt brottslighet som sker systematiskt. En verksamhet kan misstänkas ske systematiskt när det är fråga om ligor som satt i system att begå snatterier eller när det handlar om ekonomisk brottslighet, där bland annat osant intygande, som inte är grovt, utgör ett betydande problem och där brottsligheten ofta bedrivs systematiskt och kan kräva kartläggning. Det nämns att intresset av en effektiv brottsbekämpning talar för att polisen bör kunna göra även uppgifter med anknytning till sådan systematisk brottslighet gemensamt tillgängliga (prop. 2009/10:38, s. 134).

Mot denna bakgrund rekommenderar Datainspektionen polismyndigheten att ta fram rutiner för att kvalitetssäkra informationen innan publicering sker på KUT-info så att publiceringen uppfyller kraven enligt 3 kap. 2 § polisdatalagen och för att säkerställa att uppgifter tas bort när de inte längre är aktuella.

Polismyndighetens särskilda uppgiftssamling

Polismyndigheten upphörde i april 2013 med att behandla uppgifter i fem särskilda undersökningar och övergick till att foga samman informationen i dessa till en gemensam särskild uppgiftssamling. Polismyndigheten avser att fortsättningsvis behandla kriminalunderrättelseinformation i denna "berednings-SUS" och föra in information, såsom underrättelseuppslag, tips m.m. löpande. I uppgiftssamlingen finns sammanlagt 3 800 personer registrerade för någon form av brottslighet. Det är polismyndighetens bedömning att den särskilda uppgiftssamlingen inte är att anse som gemensamt tillgänglig, då endast sex personer har tillgång till informationen. Uppgifterna i uppgiftssamlingen gallras efter ett år. Gallringen sker manuellt och kontrolleras varannan månad. Informationen i den särskilda

uppgiftssamlingen kommer att gås igenom kontinuerligt och kan leda till förundersökningar eller att en ny särskild uppgiftssamling avseende ett begränsat fenomen, t.ex. ett kriminellt nätverk, startas.

Polismyndigheten markerar inte personer som inte är misstänkta för brott. Polisen anser att IT-systemet Surfai inte tillåter sådan markering och har avvaktat att Rikspolisstyrelsen ska lösa detta problem inom ramen för Surfaz.

Vid Datainspektionens stickprovskontroll noterades två registreringar av personer under 15 år som enligt polismyndigheten inte borde ha registrerats på samma sätt som någon som är misstänkt för brott.

Datainspektionen gör följande bedömning

Mycket talar för att polismyndighetens särskilda uppgiftssamling är gemensamt tillgänglig. Polismyndigheten anser att den särskilda uppgiftssamlingen inte är gemensamt tillgänglig eftersom endast sex personer har åtkomst till uppgifterna. I förarbetena nämns som tumregel att uppgifter normalt bör anses gemensamt tillgängliga när fler än ett tiotal personer har tillgång till dem men tidsaspekten kan också ha betydelse för bedömningen. Uppgifter som behandlas under längre tid kommer typiskt sätt fler till del, exempelvis för att personer i en från början begränsad krets med tiden byts ut. Projekt inom underrättelseverksamheten har inte sällan obestämd varaktighet och kan därför komma att löpa under en längre tid. Även om tanken från början har varit att endast en liten avgränsad krets ska syssla med projektet är det därför långtifrån alltid möjligt att upprätthålla det kravet (prop. 2009/10:85, s. 128 ff.). Med anledning av den omfattande mängd personuppgifter som behandlas i polismyndighetens uppgiftssamling kan man utgå från att personuppgifterna kommer behandlas under en längre tid, och att personerna som arbetar med uppgiftssamlingen kommer att bytas ut.

Eftersom uppgifterna torde vara gemensamt tillgängliga blir 3 kap. tillämpligt och polismyndigheten måste därmed förse de personer som inte är misstänkta för allvarlig brottslig verksamhet (kringpersoner) med en sådan särskild upplysning som följer av 3 kap. 4 § första stycket polisdatalagen.

Hur polismyndigheten arbetar i kriminalunderrättelseverksamhet med stöd av den nya lagstiftningen och om uppgifterna är att anse som gemensamt eller icke gemensamt tillgängliga är en principiell och stor fråga som Datainspektionen har för avsikt att ta upp med Rikspolisstyrelsen, då den inte är specifik för polismyndigheten Gotland utan berör alla polismyndigheter. Datainspektionen riktar därför inte någon anmärkning i nuläget mot polismyndigheten i denna del.

Polismyndigheten får behandla personuppgifter om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet, för att utreda eller beivra brott eller fullgöra förpliktelser som följer av internationella åtaganden (2 kap. 7 § polisdatalagen). Denna bestämmelse gäller oavsett om uppgifterna är gemensamt eller icke gemensamt tillgängliga. Vid inspektionen påträffades bland annat två registreringar av personer under 15 år som uppenbarligen inte hade någon annan koppling till brottslig verksamhet än att de till exempel var släkt med en person som misstänktes för sådan verksamhet. I dessa fall uppgav polismyndigheten att personerna inte borde ha registrerats. Polismyndigheten ska därför föreläggas att snarast radera de personuppgifter som inte borde ha registrerats samt upprätta rutiner som säkerställer att behandlingen av personuppgifter i den särskilda uppgiftssamlingen föregås av en prövning som säkerställer att varje registrering är förenlig med 2 kap. 7 § polisdatalagen.

Polismyndighetens särskilda undersökning

Polismyndigheten behandlar personuppgifter i en särskild undersökning med stöd av övergångsbestämmelserna i polisdatalagen (2010:361) enligt 3 och 14-16 §§ i den gamla polisdatalagen (1998:622). Den särskilda undersökningen förs som pilotdrift i Surfa 2 på uppmaning av Rikskriminalpolisen och det är endast KUT-chefen som har åtkomst till undersökningen på polismyndigheten. Det pågår inget aktivt analysarbete eller annat arbete i den särskilda undersökningen. Polismyndigheten har efter inspektionen varit i kontakt med Rikskriminalpolisen som meddelat att undersökningen kommer avslutas. Polismyndigheten avser att föra den särskilda undersökningen så länge polisen har uppdraget av Rikskriminalpolisen.

Datainspektionen gör följande bedömning

Polismyndigheten, som är personuppgiftsansvarig för behandlingen av personuppgifter, har uppgett att det inte pågår något aktivt analysarbete i den särskilda undersökningen. En särskild undersökning som innehåller personuppgifter kan enligt Datainspektionen inte ligga vilande. Detta följer av 3 § och 14 § polisdatalagen (1998:622). Vidare ska personuppgifter i en särskild undersökning 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 (16 § polisdatalagen). Eftersom uppgifterna inte bearbetas överhuvudtaget innebär det att uppgifterna inte heller gallras. Datainspektionen bedömer att det inte är förenligt med polisdatalagen (1998:622) att enbart samla in personuppgifter utan att bearbeta eller analysera dem. Polismyndigheten ska därför föreläggas att upphöra med behandlingen av personuppgifter i den särskilda undersökningen A012.020/2013.

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 inkomma med en åtgärdsplan som innehåller de åtgärder som polismyndigheten vidtagit med anledning av beslutet.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö i närvaro av chefsjuristen Hans-Olof Lindblom, enhetschefen Britt Marie Wester, samt juristerna Jonas Agnvall, Cecilia Bergman och Anna Larsson Stattin, föredragande.

Kristina Svahn Starrsjö

Anna Larsson Stattin

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.