



Polismyndigheten i Västra Götalands behandling av personuppgifter i underrättelseverksamheten

1 SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat Polismyndigheten i Västra Götalands behandling av personuppgifter i underrättelseverksamheten.

Nämnden riktar allvarlig kritik mot polismyndighetens behandling av känsliga personuppgifter. I ett flertal av de dokument som nämnden granskat har uppgifter om personers etniska ursprung, politiska åsikter, religiösa övertygelse eller hälsa behandlats utan att det varit absolut nödvändigt. Uppgifterna i ett av dokumenten har, enligt nämndens bedömning, behandlats *enbart* på grund av en persons religiösa övertygelse (personen hade konverterat till islam). Eftersom denna olagliga behandling kan utgöra brott, anmäler nämnden den till Åklagarmyndigheten.

Nämnden riktar även kritik mot polismyndigheten på följande punkter.

- Uppgifter har varit tillgängliga i en alltför vid krets.
- Det närmare ändamålet med behandlingen av personuppgifter i vissa uppgiftssamlingar har varit alltför vitt.
- Uppgifter har behandlats utan att det funnits ett konkret behov av dem.
- I vissa fall har det inte framgått tillräckligt tydligt för vilket närmare ändamål uppgifter behandlas eller vilka personer som inte är misstänkta för brott.
- Uppgifter har inte gallrats i rätt tid.

Nämnden förutsätter att den nya Polismyndigheten som bildas vid årsskiftet åtgärdar de brister som har uppmärksammats vid granskningen. Den nya Polismyndigheten måste också säkerställa att motsvarande problem inte förekommer i underrättelseverksamheten i övriga delar av landet. Nämnden avser att granska vilka åtgärder som den nya Polismyndigheten vidtar för att säkerställa att personuppgiftsbehandlingen sker i enlighet med polisdatalagen.

Innehållsförteckning

1	SAMMANFATTNING.....	1
2	BAKGRUND	3
3	NÄMNDENS GRANSKNING.....	3
3.1	Omfattning.....	3
3.2	Genomförande	4
3.3	Exempel.....	4
3.4	Polismyndighetens anmälan om brott.....	6
3.5	Polismyndighetens arbete med att gallra uppgifter.....	6
4	PERSONUPPGIFTSBEHANDLING I POLISMYNDIGHETENS UNDERRÄTTELSEVERKSAMHET	7
4.1	Beslut om särskilda uppgiftssamlingar	7
4.2	SURFA2	7
4.3	Z-servern	7
5	BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER	8
5.1	Rättsliga utgångspunkter	8
5.2	Vad granskningen har visat	8
5.3	Nämndens bedömning	9
6	GEMENSAMT TILLGÄNGLIGA PERSONUPPGIFTER.....	12
6.1	Rättsliga utgångspunkter	12
6.2	Vad granskningen har visat	12
6.3	Nämndens bedömning	13
7	ÄNDAMÅL OCH BEHOV	14
7.1	Rättsliga utgångspunkter	14
7.2	Vad granskningen har visat	15
7.3	Nämndens bedömning	16
8	UPPLYSNINGAR OM ÄNDAMÅLET MED BEHANDLINGEN.....	18
8.1	Rättsliga utgångspunkter	18
8.2	Vad granskningen har visat	19
8.3	Nämndens bedömning	19
9	UPPLYSNINGAR OM PERSONER SOM INTE ÄR MISSTÄNKTA	20
9.1	Rättsliga utgångspunkter	20
9.2	Vad granskningen har visat	20
9.3	Nämndens bedömning	21
10	GALLRING AV PERSONUPPGIFTER	21
10.1	Rättsliga utgångspunkter.....	21
10.2	Vad granskningen har visat.....	21
10.3	Nämndens bedömning	22
11	AVSLUTANDE KOMMENTARER	22

2 BAKGRUND

Underrättelseverksamhet innebär att polisen samlar in och bearbetar uppgifter som tyder på brottslig verksamhet utan att det finns någon misstanke om ett konkret brott. Verksamheten syftar till att skapa en bild av brottsligheten, som kan användas som underlag för olika beslut, till exempel om att inleda förundersökning eller att genomföra insatser för att förebygga, förhindra eller upptäcka brott. Uppgifter om personer får i många fall samlas in även om personerna inte är misstänkta för brott. Det är inte ovanligt att så kallade känsliga personuppgifter, det vill säga uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa eller sexualliv, behandlas i underrättelseverksamheten. Underrättelseverksamheten är inte heller reglerad i samma utsträckning som utredningsverksamheten. Därför är behandlingen av personuppgifter i underrättelseverksamhet särskilt känslig ur ett integritetsperspektiv.

Under de senaste åren har Säkerhets- och integritetsskyddsnämnden i olika sammanhang granskat hur både Rikspolisstyrelsen och vissa länspolismyndigheter har behandlat personuppgifter i underrättelseverksamheten. Den 15 november 2013 riktade nämnden allvarlig kritik mot Polismyndigheten i Skåne för behandlingen av personuppgifter i uppgiftssamlingen ”Kringresande”.¹ Nämnden inledde i samband med detta en översiktlig granskning av underrättelseverksamheten vid landets länspolismyndigheter i syfte att hämta in underlag för kommande granskningar.²

Den 13 februari 2014 beslutade nämnden att granska personuppgiftsbehandlingen med stöd av polisdatalagen (2010:361) (PDL) i underrättelseverksamheten vid Polismyndigheten i Västra Götaland (polismyndigheten).

3 NÄMNDENS GRANSKNING

3.1 Omfattning

Nämnden har avgränsat sin granskning till vissa frågor som är särskilt viktiga ur ett integritetsperspektiv.

- Behandlas *känsliga personuppgifter* bara när det är absolut nödvändigt som komplement till annan behandling? (Avsnitt 5)
- Vilka personuppgifter får anses vara *gemensamt tillgängliga*? Har dessa uppgifter fått göras gemensamt tillgängliga? (Avsnitt 6)

¹ Se nämndens uttalande den 15 november 2013 ”Polismyndigheten i Skånes behandling av personuppgifter i uppgiftssamlingen benämnd ’Kringresande’” (dnr 173-2013).

² Se nämndens uttalande den 23 januari 2014 ”Kartläggning av polismyndigheternas behandling av känsliga personuppgifter i underrättelseverksamhet” (dnr 200-2013).

- Finns det ett *närmare ändamål* med behandlingen av personuppgifter? Finns det ett *konkret behov* av behandlingen för det närmare ändamålet? (Avsnitt 7)
- *Framgår* det närmare ändamålet med behandlingen tillräckligt tydligt när personuppgifter är gemensamt tillgängliga? (Avsnitt 8)
- Framgår det tillräckligt tydligt vilka personer som *inte är misstänkta* för brott när personuppgifter är gemensamt tillgängliga? (Avsnitt 9)
- Gallras personuppgifter i rätt tid? (Avsnitt 10)

3.2 Genomförande

I polismyndighetens underrättelseverksamhet behandlas personuppgifter dels med hjälp av en IT-plattform som kallas SURFA2, dels i olika dokument som finns i en mappstruktur på en av polismyndighetens servrar (här kallad Z-servern).³

Delar av nämndens kansli genomförde en inspektion vid polismyndighetens kriminalunderrättelsetjänst den 13 och 14 maj 2014. Vid inspektionen gjordes en översiktlig granskning av fler än 200 dokument och filer från SURFA2 och Z-servern. Vissa granskade dokument valdes ut slumpmässigt. Andra dokument valdes ut med hjälp av i förväg bestämda sökkriterier, däribland att dokumentet innehöll känsliga personuppgifter, ett stort antal personuppgifter eller särskilt gamla uppgifter.

Trettio av dessa dokument blev sedan föremål för en närmare granskning, eftersom de illustrerade vissa återkommande eller särskilt allvarliga problem. Polismyndigheten har därför, på nämndens begäran, besvarat olika frågor om personuppgiftsbehandlingen i dessa trettio dokument.

I följande avsnitt används nio av de trettio dokumenten som exempel på olika typer av brister. I nästa avsnitt presenteras exemplen närmare.

3.3 Exempel

Nedan följer en kort beskrivning av de dokument som nämnden kommer att använda som exempel i ett eller flera av de avsnitt som följer. I samtliga fall rör det sig om uppgifter om personer som har pekats ut med namn och personnummer eller på något annat sätt.

³ Se avsnitt 4.2 och 4.3 för mer information om SURFA2 och Z-servern.

Följande exempel har hämtats från Z-servern.

- **Exempel 1** innehåller en lista över ca 180 personer samt webbadresser knutna till respektive person. Vissa av personerna uppges ha kopplingar till *kristna*, *icke-autonoma* eller *autonoma* grupperingar. Några personer uppges ha kopplingar till såväl icke-autonoma som autonoma grupperingar. Det finns också uppgifter som får förstås som att personerna på olika sätt har haft kopplingar till protester mot utvisningar eller avvisningar enligt utlänningslagen (2005:716). Enligt polismyndigheten översändes dokumentet från en annan polismyndighet i december 2012 efter att en tjänsteman vid kriminalunderrättelsetjänsten hade frågat efter material till en så kallad riskanalys inför en avvisning.

Se bedömningar i avsnitt 5, 6, 7, 8 och 9.

- **Exempel 2** är ett dokument från år 2004 med filnamnet *Kurdgänget*. Dokumentet innehåller uppgifter om ett flertal olika personer och telefonnummer. Enligt polismyndigheten har dokumentet upprättats inom ramen för en brottsutredning.

Se bedömningar i avsnitt 5 och 7.

- **Exempel 3** är ett dokument från år 2006 med ordet *psyksjuk* i filnamnet. Dokumentet innehåller uppgifter om att en person som har sagt sig vara utsatt för brott är förvirrad och enligt uppgift även *svårt alkoholiserad*. Enligt polismyndigheten har en tjänsteman vid kriminalunderrättelsetjänsten upprättat dokumentet i sin tidigare tjänst.

Se bedömningar i avsnitt 5, 7, 8 och 10.

- **Exempel 4** är ett dokument från år 1999 med en kort anteckning från ett förhör i en brottsutredning. Enligt polismyndigheten har en tjänsteman vid kriminalunderrättelsetjänsten upprättat anteckningen i sin tidigare tjänst.

Se bedömningar i avsnitt 7, 8 och 10.

Följande exempel har hämtats från SURFA2.

- **Exempel 5** är ett dokument från år 2013 med uppgifter om att en ung man har *konverterat till islam*. Uppgifterna har antecknats i samband med att tjänstemän från en polismyndighet besökt mannens hem i ett ärende som rörde en annan person. Den som har antecknat uppgifterna har angett att de kanske kan vara av intresse, eftersom mannen är ”svensk och ensam i familjen som konverterat till islam i så ung ålder”.

Se bedömningar i avsnitt 5 och 7.

- **Exempel 6** är ett dokument från år 2013 med uppgifter om att vissa personer, enligt en källa, begår olika typer av inbrott. En av personerna uppges vara *zigenare*.

Se bedömning i avsnitt 5.

- **Exempel 7** är ett dokument från år 2011 med uppgifter om att vissa personer, enligt en källa, är inblandade i häleriverksamhet. En av personerna uppges vara *jude*.

Se bedömning i avsnitt 5.

- **Exempel 8** är ett dokument från år 2013 med uppgifter om att vissa personer misstänks vara inblandade i narkotikaförsäljning. Vissa av personerna uppges vara *romer*.

Se bedömning i avsnitt 5.

- **Exempel 9** är ett dokument från år 2013 som bara innehåller en uppgift om att en person, som är född år 2008, är barn till en annan registrerad person.

Se bedömning i avsnitt 7.

3.4 Polismyndighetens anmälan om brott

Polismyndigheten har efter nämndens inspektion själv gjort en anmälan om brott. Anmälan avsåg den behandling av personuppgifter som beskrivs i exempel 1 och några ytterligare dokument som enligt polismyndigheten hade anknytning till samma händelse. En förundersökning har inletts med anledning av anmälan.

3.5 Polismyndighetens arbete med att gallra uppgifter

Polismyndigheten har angett följande. Vid nämndens inspektion pågick redan ett omfattande arbete med att gallra sådana uppgifter, främst på Z-servern, som det inte fanns stöd för att fortsätta behandla enligt PDL. Efter inspektionen har polismyndigheten sparat de dokument som nämnden granskat närmare för att kunna besvara nämndens frågor. Många andra dokument och mappar har dock gallrats efter inspektionen. Polismyndigheten har därför i vissa delar besvarat nämndens frågor med reservation för att den saknat vetskap om vad som kan ha framgått av andra dokument.

4 PERSONUPPGIFTSBEHANDLING I POLISMYNDIGHETENS UNDERRÄTTELSEVERKSAMHET

4.1 Beslut om särskilda uppgiftssamlingar

Polismyndigheten har fattat ett antal beslut om att inrätta så kallade särskilda uppgiftssamlingar (SUS-beslut). I besluten fastslås vilka regler som gäller för den behandling av personuppgifter som sker i respektive uppgiftssamling, exempelvis vilka tjänstemän som ska få *tillgång* till uppgifterna, hur uppgifterna ska göras *tillgängliga*, hur och när *gallring* ska ske samt för vilket *närmare ändamål* uppgifterna får behandlas.

Vid nämndens inspektion behandlades alla uppgifter på Z-servern med stöd av ett enda SUS-beslut. För de uppgifter som behandlades i SURFA2 gällde däremot flera olika SUS-beslut.

4.2 SURFA2

Polismyndigheten började använda SURFA2 i underrättelseverksamheten år 2013. SURFA2 är en IT-plattform som har tagits fram av Rikspolisstyrelsen för att underlätta behandling av personuppgifter i enlighet med PDL. Rikspolisstyrelsen äger och förvaltar SURFA2-plattformen, men den används även av andra polismyndigheter. Den polismyndighet som för in eller på annat sätt behandlar personuppgifter i en uppgiftssamling i SURFA2 har personuppgiftsansvar för behandlingen.

I SURFA2 kan information till exempel delas, länkas, bearbetas, visualiseras och sorteras genom att kopplas till olika typer av kategorier. En uppgift måste alltid kopplas till en eller flera uppgiftssamlingar i SURFA2. En användare kan bara se information som finns i uppgiftssamlingar som han eller hon har tilldelats behörighet till.

Det pågår för närvarande ett arbete med att vidareutveckla SURFA2. Inom ramen för det här uttalandet beskrivs emellertid bara de funktioner och arbetssätt som fanns vid tiden för nämndens inspektion.

4.3 Z-servern

På Z-servern finns det ett stort antal filer med underrättelseuppslag och arbetsdokument sorterade i olika mappar. I mapparna finns exempelvis Word-, Excel- och PDF-filer men även filer som används med olika analysprogram. Till skillnad från SURFA2 har Z-servern inte några särskilda funktioner som är anpassade efter de krav som PDL ställer.

Polismyndigheten har uppgett följande. Z-servern användes för att sortera, dela, bearbeta och visualisera information i underrättelseverksamheten innan SURFA2 togs i bruk. Numera läggs i princip all ny underrättelseinformation in direkt i SURFA2. Det kommer dock även fortsättningsvis att finnas ett behov av att föra över information från SURFA2 till Z-servern för vidare bearbetning eller analys som inte är möjlig att genomföra i SURFA2.

5 BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER

Polismyndigheten har i ett flertal fall behandlat känsliga personuppgifter utan att det har varit *absolut nödvändigt* för ändamålet med behandlingen.

Uppgifterna i ett dokument har enligt nämndens bedömning behandlats *enbart* på grund av att en person har konverterat till islam. Eftersom behandlingen av personuppgifter i det dokumentet kan utgöra brott anmäler nämnden förhållandena till Åklagarmyndigheten.

5.1 Rättsliga utgångspunkter

Möjligheterna att behandla uppgifter om en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (*känsliga personuppgifter*) med stöd av PDL är mycket begränsade. Det är till exempel aldrig tillåtet att samla in uppgifter om enskilda *enbart* på grund av deras politiska åsikter eller för att de tillhör en viss etnisk grupp. Känsliga uppgifter om en person får behandlas endast som komplement till behandling som sker för andra syften om det är *absolut nödvändigt* för syftet med den behandlingen (2 kap. 10 § PDL). Med hänsyn till den restriktivitet som ligger i begreppet absolut nödvändigt måste behovet av att komplettera med sådana uppgifter prövas noga i det enskilda fallet.⁴

Personuppgifter får bara behandlas om det är lagligt (2 kap. 2 § 1 st. 3 PDL och 9 § 1 st. a personuppgiftslagen [1998:204] [PUL]). Om känsliga personuppgifter behandlas i strid med 2 kap. 10 § PDL, ska de därför gallras så snart som möjligt.

5.2 Vad granskningen har visat

Nämnden har begärt att polismyndigheten ska förklara om – och i så fall varför – det har varit absolut nödvändigt att behandla känsliga personuppgifter i vissa granskade dokument. Det gäller bland annat exempel 1–3 och 5–8.

⁴ Prop. 2009/10:85 s. 325.

Polismyndighetens svar kan sammanfattas på följande sätt. Det har *inte varit absolut nödvändigt* för ändamålet med behandlingen att komplettera med känsliga personuppgifter i de flesta av dokumenten, däribland exempel 1–3 och 5–8. Det kan dock ifrågasättas om vissa av dokumenten, däribland exempel 2, innehåller känsliga personuppgifter, eftersom uppgifterna om etniskt ursprung bara finns med i filnamnet och inte i själva dokumentet. Vad gäller exempel 1 gör polismyndigheten bedömningen att uppgifter om både religiös övertygelse och politiska åsikter har behandlats i dokumentet. Vad gäller exempel 3 kan de känsliga personuppgifterna om hälsa ha varit absolut nödvändiga att behandla för sitt ursprungliga ändamål men det har inte funnits något behov av att behandla dem i underrättelseverksamheten.

Utöver frågorna om de granskade dokumenten har nämnden även ställt frågor om en särskild mapp på Z-servern som upptäcktes vid inspektionen. Mappen var benämnd ”gallring” och innehöll bland annat ett flertal olika dokument med känsliga personuppgifter. Polismyndigheten har sammanfattningsvis svarat följande. Mappen innehöll dokument som hade sorterats ut under polismyndighetens pågående arbete med att gallra sådana uppgifter som inte får behandlas enligt PDL. På grund av ett förbiseende hade uppgifterna dock inte gallrats.

Enligt polismyndigheten har rutinerna för behandling av känsliga personuppgifter tidigare varit otillräckliga. Polismyndigheten har därför haft interna diskussioner om hur tjänstemännen bör och får formulera sig i dokument som ska behandlas i underrättelseverksamheten. Polismyndigheten har också infört en ny rutin som innebär att tjänstemän vid kriminalunderrättelsetjänsten kan skicka tillbaka dokument som kommer in från andra tjänstemän vid myndigheten för omformulering om de innehåller känsliga personuppgifter. Tjänstemännen vid kriminalunderrättelsetjänsten gör också alltid en egen bedömning av vilka uppgifter som slutligen ska registreras.

5.3 Nämndens bedömning

Nämnden anser att det har förekommit allvarliga brister i polismyndighetens behandling av känsliga personuppgifter.

I ett flertal granskade dokument har polismyndigheten behandlat uppgifter om personers etniska ursprung, politiska åsikter, religiösa övertygelse eller hälsa utan att det har varit absolut nödvändigt för ändamålet med behandlingen. Bland dessa finns exempel 1–3 och 5–8.

Att uppgifterna om etniskt ursprung i vissa fall bara har funnits med i filnamnet behöver inte ha någon betydelse för bedömningen av om känsliga personuppgifter har behandlats. Det avgörande är att uppgifterna kan kopplas ihop med personerna i dokumentet. Så har varit fallet i exempel 2.

I de flesta dokumenten har den olagliga behandlingen av känsliga personuppgifter skett som ett *komplement* till behandling som skett för något berättigat ändamål. Uppgifterna i exempel 8 har till exempel behandlats i underrättelseverksamheten på grund av att personerna har haft kopplingar till misstänkt narkotikaförsäljning. Det är den kompletterande uppgiften om att vissa av personerna är romer som har varit olaglig, eftersom den inte har varit absolut nödvändig för ändamålet med behandlingen av övriga uppgifter.

Vad gäller *exempel 5* har polismyndigheten däremot inte kunnat ange något ändamål för behandlingen över huvud taget.⁵ Den enda anledningen till att uppgifter om personen har behandlats tycks vara att personen, enligt den som har antecknat uppgifterna, är ”svensk och ensam i familjen som konverterat till islam i så ung ålder”. Uppgifternas koppling till misstänkt brottslig verksamhet framstår som obefintlig. Polismyndigheten har inte heller bedömt att det finns någon sådan koppling. Mot bakgrund av detta bedömer nämnden att uppgifterna har behandlats hos polismyndigheten *enbart* på grund av att personen har konverterat till islam, det vill säga på grund av hans religiösa övertygelse. Denna olagliga behandling av känsliga personuppgifter är särskilt allvarlig.

Om nämnden vid en granskning uppmärksammar något som kan utgöra brott, ska en anmälan göras till Åklagarmyndigheten. Nämnden bedömer att den behandling av personuppgifter som beskrivs i exempel 5 kan utgöra brott. Den anmälan som polismyndigheten själv har gjort omfattar inte behandlingen i exempel 5. Nämnden anmäler därför förhållandena till Åklagarmyndigheten enligt 20 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

Beträffande uppgifterna i *exempel 1* har ändamålet, som nämnden uppfattat det, varit att förebygga, förhindra eller upptäcka någon form av brottslig verksamhet i samband med en avvisning. I dokumentet förekommer bland annat uppgifter om att vissa personer har koppling till en *kristen* gruppering, vilket får anses avslöja dessa personers *religiösa övertygelse*.

Det finns även uppgifter i exempel 1 som skulle kunna avslöja personers *politiska åsikter*, så som kopplingen till protester mot avvisningar och uppgifterna om att vissa personer har koppling till en autonom gruppering. De uppgifter som nämnden har tillgång till är dock knapphändiga och – med avseende på personers kopplingar till grupperingar – motsägelsefulla. Nämndens möjligheter att inhämta kompletterande information efter det att förundersökning inletts har varit begränsade. Polismyndigheten, som torde ha

⁵ Se avsnitt 7.2.

bättre underlag för bedömningen, har dock bedömt att dokumentet innehåller uppgifter om personers politiska åsikter.

Enligt polismyndigheten har det inte varit absolut nödvändigt att behandla de känsliga personuppgifterna i dokumentet. Ingenting har framkommit som föranleder någon annan bedömning från nämndens sida. Nämnden konstaterar därför att behandlingen av uppgifter om religiös övertygelse och politiska åsikter i exempel 1 har varit olaglig.

Som framgår i kommande avsnitt har polismyndigheten behandlat uppgifterna i exempel 1 utan att det har funnits något som tyder på att personerna har varit inblandade i brottslig verksamhet och utan att det över huvud taget har funnits något behov av uppgifterna i arbetet med den riskanalys som de samlats in för.⁶ Uppgifterna har också varit gemensamt tillgängliga utan att de särskilda krav som gäller för sådana uppgifter har varit uppfyllda.⁷ Personuppgiftsbehandlingen i exemplet har alltså varit olaglig på flera sätt.

Som har nämnts ovan har en förundersökning inletts om den behandling av uppgifter som beskrivs i exempel 1, efter en anmälan från polismyndigheten. Nämnden gör därför inte någon egen bedömning av om den behandlingen kan utgöra brott.

Polismyndigheten har angett att uppgifterna i exempel 1 har gallrats i samband med att polismyndigheten lämnat över dokumentet till Polisens avdelning för interna utredningar. Nämnden förutsätter att de känsliga personuppgifter i andra dokument som fortfarande behandlas i strid med lag nu kommer att gallras utan dröjsmål. Detta gäller även uppgifterna i mappen ”gallring”.

Fungerande rutiner måste också införas för att säkerställa att känsliga personuppgifter inte behandlas i strid med lag. De rutiner som polismyndigheten nyligen har infört framstår som ett första steg för att uppnå detta men är enligt nämnden otillräckliga. Nämnden har i flera andra sammanhang rekommenderat att rutiner införs som innebär att beslut om registrering av känsliga personuppgifter alltid ska fattas av särskilt utsedda personer och att besluten ska dokumenteras och motiveras.⁸ Nämnden rekommenderar att sådana rutiner införs.

Det måste också finnas fungerande rutiner för gallring av känsliga personuppgifter som behandlas utan lagligt stöd.

⁶ Se avsnitt 7.

⁷ Se avsnitt 6 och 8-9.

⁸ Se exempelvis nämndens uttalande den 11 december 2012 ”Rikspolisstyrelsens rutiner för och kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättelseregistret, KUR” (dnr 231-2012).

6 GEMENSAMT TILLGÄNGLIGA PERSONUPPGIFTER

Det har inte funnits lagliga förutsättningar för att göra alla uppgifter på Z-servern tillgängliga för ett flertal personer, det vill säga *gemensamt tillgängliga*.

6.1 Rättsliga utgångspunkter

I förarbetena till PDL framhålls att risken för intrång i den personliga integriteten är större när uppgifter används av flera gemensamt i verksamheten än när personuppgifter behandlas av en enskild tjänsteman vid den egna datorn. Utöver de minimikrav som gäller för all behandling av personuppgifter ställer PDL därför högre krav på behandlingen av uppgifter som är *gemensamt tillgängliga* (3 kap. 1 § PDL).⁹

Personuppgifter är gemensamt tillgängliga om ett *flertal personer* har möjlighet att ta del av dem eller om avsikten är att uppgifterna ska vara åtkomliga för en *i förväg obestämmd krets*. I förarbetena till PDL anges att personuppgifter som fler än ett tiotal personer har eller avses få tillgång till i regel ska anses vara gemensamt tillgängliga.¹⁰

Det är inte alla typer av personuppgifter som får göras gemensamt tillgängliga. I underrättelseverksamhet får uppgifter göras gemensamt tillgängliga på två olika grunder. Den ena är att uppgifterna *kan antas ha samband med misstänkt brottslig verksamhet* som har ett års fängelse eller däröver i straffskalan eller sker systematiskt (3 kap. 2 § 1 st. 1 PDL). Den andra är att uppgifterna *behövs för övervakningen av en person* som är allvarligt kriminellt belastad eller farlig och som kan antas ägna sig åt allvarlig brottslighet (3 kap. 2 § 1 st. 2 PDL).

Tillgången till personuppgifter ska också begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (2 kap. 11 § 1 st. PDL).

6.2 Vad granskningen har visat

Vid nämndens inspektion hade samtliga medarbetare vid kriminalunderrättelse-tjänsten tillgång till i princip hela Z-servern. Detta gällde även uppgifter som exempelvis fanns i olika tjänstemäns personliga mappar.

Enligt polismyndigheten var alla uppgifter som fanns på Z-servern vid nämndens inspektion gemensamt tillgängliga. Polismyndigheten har dock dragit slutsatsen att det inte är möjligt att ha uppgifter på Z-servern gemensamt

⁹ Prop. 2009/10:85 s. 125. Se även avsnitt 8–9.

¹⁰ Se 3 kap. 1 § PDL och prop. 2009/10:85 s. 334 f.

tillgängliga på ett sätt som lever upp till PDL:s krav. Efter inspektionen har polismyndigheten därför organiserat om Z-servern så att varje mapp bara är tillgänglig för mellan två och åtta tjänstemän. De SUS-beslut som för närvarande gäller för mapparna är också tidsbegränsade så att uppgifter bara får tillföras under åren 2014 och 2015 och ska gallras senast vid utgången av år 2016. Efter omorganisationen bedömer polismyndigheten att inga av uppgifterna på Z-servern är gemensamt tillgängliga.

I SURFA2 fanns det vid inspektionen både sådana uppgiftssamlingar som enligt polismyndigheten var gemensamt tillgängliga och sådana som inte var det. Mellan två och nio personer hade tillgång till de uppgifter som enligt polismyndigheten inte var gemensamt tillgängliga. Enligt de SUS-beslut som gällde för dessa uppgiftssamlingar fick uppgifter bara tillföras under antingen år 2013 eller år 2014 och skulle gallras ett år efter registreringsdatum.

Nämnden har begärt att polismyndigheten ska utveckla om personuppgifterna i vissa granskade dokument på Z-servern har fått göras gemensamt tillgängliga, eftersom det inte har framgått att uppgifterna har samband med den typ av brottslig verksamhet som krävs eller att de behövs för övervakning. Det gäller bland annat exempel 1.

Polismyndigheten har sammanfattningsvis svarat att uppgifterna i vissa av dokumenten, däribland exempel 1, inte har fått göras gemensamt tillgängliga.

6.3 Nämndens bedömning

Nämnden konstaterar att det inte har funnits lagliga förutsättningar för att göra alla uppgifter på Z-servern gemensamt tillgängliga. Detta gäller bland annat uppgifterna i exempel 1, där polismyndigheten inte har kunnat redogöra för något samband mellan uppgifterna och misstänkt brottslig verksamhet över huvud taget. Det är inte heller sannolikt att alla tjänstemän vid polismyndighetens kriminalunderrättelsetjänst har haft behov av alla uppgifter på Z-servern i sitt arbete.

Nämnden ser därför positivt på att polismyndigheten redan har begränsat tillgången till uppgifterna på Z-servern så att uppgifterna inte längre ska vara gemensamt tillgängliga och så att tjänstemännens tillgång till personuppgifter bättre ska motsvara deras behov av uppgifterna.

Vad gäller polismyndighetens bedömning av vilka uppgifter som *inte är gemensamt tillgängliga* vill nämnden emellertid påminna om att uppgifter som behandlas en längre tid kan anses vara gemensamt tillgängliga på grund av att

ett flertal personer sammanlagt kan få tillgång till dem över tid.¹¹ För att undvika detta har polismyndigheten beslutat att uppgifterna bara får behandlas med stöd av varje SUS-beslut under en relativt kort tid. Polismyndigheten bör dock överväga om vissa av uppgifterna ändå kan bedömas vara gemensamt tillgängliga på grund av tidsaspekten.

7 ÄNDAMÅL OCH BEHOV

Polismyndigheten har fattat beslut om för vilka *närmare ändamål* uppgifter får samlas in och behandlas i underrättelseverksamheten. Nämnden bedömer dock att vissa av dessa närmare ändamål är alltför vida.

Polismyndigheten har i flera fall behandlat uppgifter utan att det har funnits ett *konkret behov* av dem för de angivna ändamålen.

7.1 Rättsliga utgångspunkter

En grundläggande förutsättning för att personuppgifter ska få behandlas enligt PDL är att de behövs i polisens brottsbekämpande verksamhet, exempelvis i underrättelseverksamheten (2 kap. 7 § 1 PDL).

Dessutom får personuppgifter samlas in endast för särskilda, uttryckligt angivna och berättigade ändamål (*närmare ändamål*). Fler uppgifter än vad som är nödvändigt med hänsyn till dessa närmare ändamål får inte behandlas. Uppgifter får heller inte behandlas för ändamål som är oförenliga med det ändamål som uppgifterna samlades in för (2 kap. 2 § 1 st. 3 PDL och 9 § 1 st. c, d och f PUL).

För att en uppgift ska få behandlas måste det också alltid finnas ett *konkret behov* av uppgiften. Behovet måste svara mot det närmare ändamålet med behandlingen i det aktuella sammanhanget. I ett underrättelseprojekt som rör en viss typ av brottslighet får polisen till exempel inte behandla uppgifter som inte har samband med just det projektet.¹² Om det inte finns ett konkret behov av att behandla en viss uppgift får den inte samlas in. Insamlade uppgifter som det inte längre finns behov av ska gallras (2 kap. 12 § 1 st. PDL).

När en personuppgift görs gemensamt tillgänglig ska det alltid framgå för vilket närmare ändamål som behandlingen sker.¹³ Utöver detta finns det inget

¹¹ Prop. 2009/10:85 s. 128 f. och 335. Jfr även Datainspektionens beslut den 26 november 2013 i ärende 279-2013, Tillsyn av personuppgiftsbehandlingen vid Polismyndigheten Gotland, s. 10.

¹² Prop. 2009/10:85 s. 317 f.

¹³ Se avsnitt 8.

krav i PDL på att det närmare ändamålet ska dokumenteras.¹⁴ Den som behandlar en viss uppgift måste emellertid alltid ha klart för sig för vilket eller vilka närmare ändamål som behandlingen sker.

7.2 Vad granskningen har visat

Enligt polismyndigheten har samtliga uppgifter i underrättelseverksamheten behandlats inom ramen för någon av de uppgiftssamlingar som den har fattat beslut om. I SUS-besluten har angetts för vilka närmare ändamål uppgifter får behandlas.

Av sekretesskäl kan polismyndighetens olika SUS-beslut inte beskrivas närmare. I flera av de beslut som gällde vid nämndens inspektion var emellertid de närmare ändamålen inte avgränsade till vissa typer av brott eller brottslig verksamhet. Besluten innehöll i de fallen i princip bara geografiska avgränsningar. Ett exempel på detta är det SUS-beslut som gällde för behandlingen av alla uppgifter på Z-servern.¹⁵ Det närmare ändamål som angavs i det beslutet var att uppgifterna skulle göras gemensamt tillgängliga i underrättelseverksamhet med stöd av bestämmelsen i 3 kap. 2 § 1 PDL om samband med brottslig verksamhet. I beslutet angavs också att syftet var att bekämpa brottsligheten inom polismyndighetens geografiska område.

Nämnden har begärt att polismyndigheten ska utveckla om – och i så fall varför – det har funnits ett konkret behov av att behandla personuppgifterna i vissa dokument för de ändamål som har angetts. Det gäller bland annat exempel 1–5 och 9.

Polismyndigheten har sammanfattningsvis svarat följande. Flera av dokumenten innehåller uppgifter som det aldrig har funnits något behov av att behandla. Bland dessa finns exempel 1, 5 och 9. Vad gäller uppgifterna i exempel 1 har ändamålet med behandlingen varit att göra en riskanalys inför en avvisning men det har aldrig funnits något behov av uppgifterna för detta ändamål. Vad gäller exempel 5 har uppgifterna över huvud taget inte behandlats för något i PDL tillåtet ändamål och dokumentet som helhet borde aldrig ha registrerats.

Vad gäller uppgifterna i vissa dokument på Z-servern har polismyndigheten svarat att tjänstemän vid kriminalunderrättelsetjänsten vid någon tidpunkt har haft ett behov av dem för *andra ändamål än underrättelseverksamhet*, till exempel för att utreda brott. Bland dessa finns exempel 2–4.

¹⁴ Prop. 2009/10:85 s. 98.

¹⁵ Efter inspektionen har polismyndigheten organiserat om Z-servern så att uppgifterna behandlas med stöd av flera olika SUS-beslut. Se även avsnitt 6.2.

Exempel 9 var vid nämndens inspektion kopplat till en uppgiftssamling i SURFA2 som bara ett fåtal tjänstemän hade tillgång till men som innehöll uppgifter om ett mycket stort antal personer. Vad gäller den uppgiftssamlingen har polismyndigheten angett följande. Uppgiftssamlingen hade sin bakgrund i ett nationellt projekt i Rikspolisstyrelsens regi där uppgifterna behandlades av ett flertal olika polismyndigheter. När projektet avslutades år 2013 fördes alla uppgifter över till den aktuella uppgiftssamlingen. I samband med detta gjordes inte någon omedelbar bedömning av om polismyndigheten hade behov av alla uppgifterna, som alltså i många fall kunde ha samlats in och registrerats av andra polismyndigheter. Polismyndigheten har därför inte haft behov av alla uppgifterna, däribland de om barnet i exempel 9. Vid utgången av år 2014 ska hela uppgiftssamlingen gallras.

7.3 Nämndens bedömning

Nämnden anser att de närmare ändamål som polismyndigheten har angett i sina SUS-beslut i vissa fall har varit alltför vida.

Noga formulerade och preciserade närmare ändamål är viktiga för att säkerställa att varje registrering av en ny personuppgift fyller ett reellt och legitimt behov. På det sättet kan polismyndigheten styra dem som behandlar personuppgifter så att de inte samlar in eller behandlar fler uppgifter än vad som behövs i den brottsbekämpande verksamheten. Behovet av den typen av styrning är särskilt stort i underrättelseverksamheten, eftersom det saknas andra begränsande regler av det slag som finns i utredningsverksamheten. Om det närmare ändamålet är alltför allmänt eller otydligt formulerat, finns det en risk att det skapas ”bra att ha”-uppgiftssamlingar med personuppgifter som det egentligen inte finns något behov av. Enligt nämnden innebär en brist på precisering av det närmare ändamålet därför att PDL:s integritetsskydd i praktiken sätts ur spel.

Nämnden konstaterar att polismyndigheten genom SUS-besluten har bestämt för vilka närmare ändamål uppgifter får samlas in och behandlas i underrättelseverksamheten. Nämnden anser dock att de beskrivna ändamålen i vissa fall har varit så vitt formulerade att de inte kunnat utgöra någon effektiv garant mot ”bra att ha”-uppgiftssamlingar. Detta gäller bland annat det SUS-beslut som tidigare gällde för behandlingen av alla uppgifter på Z-servern. Mot bakgrund av detta bör polismyndigheten formulera om och precisera ändamålsbeskrivningarna i de SUS-beslut där det i stort sett bara finns en geografisk avgränsning.

De alltför vida och otydliga ändamål som angetts i SUS-besluten kan ha bidragit till att polismyndigheten i ett flertal fall har behandlat uppgifter i underrättelseverksamheten som det aldrig har funnits något behov av.

Uppgifterna i exempel 1 och 5 har enligt uppgift aldrig behövts hos polismyndigheten. De har därför aldrig fått behandlas i den brottsbekämpande verksamheten.¹⁶ De närmare ändamål som har angetts i de SUS-beslut som har gällt för respektive exempel har också varit så vida att de inte har gett någon ledning alls för vilken behandling som har varit tillåten, exempelvis vilken typ av brottslighet uppgifterna ska ha samband med för att få behandlas.

Även uppgifterna om barnet i exempel 9 har behandlats trots att det inte har funnits något behov av det. Mot bakgrund av vad polismyndigheten har svarat gäller detta sannolikt även för ett stort antal andra uppgifter i samma uppgiftssamling. Polismyndigheten har över huvud taget haft en mycket begränsad kontroll över vilka uppgifter som har funnits i den uppgiftssamlingen. Det är inte godtagbart att en personuppgiftsansvarig myndighet har sådan bristande kontroll över sin behandling av personuppgifter.

Uppgifterna i vissa dokument, däribland exempel 2–4, kan vissa tjänstemän vid kriminalunderrättelsetjänsten ha behövt för något annat ändamål än underrättelseverksamhet. Något behov av att behandla uppgifterna i underrättelseverksamheten har dock inte funnits enligt polismyndigheten. Det SUS-beslut som gällde för behandlingen av uppgifter på Z-servern, där dokumenten har lagrats, har inte heller gett stöd för att behandla uppgifter för något annat ändamål än underrättelseverksamhet.

Nämnden förutsätter att de uppgifter som det inte finns något konkret behov av nu gallras. Det måste också införas fungerande rutiner för att säkerställa att bara sådana uppgifter som det finns ett konkret behov av behandlas i underrättelseverksamheten.

¹⁶ Inkomna handlingar har dock fått diarieföras med stöd av 2 kap. 9 § 1 PDL. Prop. 2009/10:85 s. 113.

8 UPPLYSNINGAR OM ÄNDAMÅLET MED BEHANDLINGEN

I vissa fall har det inte *framgått* tillräckligt tydligt för vilket närmare ändamål uppgifter har behandlats.

Om det tydligt framgår vilket SUS-beslut som gäller för behandlingen, kan det närmare ändamålet sägas framgå på ett godtagbart sätt. Det förutsätter emellertid att det i beslutet angivna närmare ändamålet är tillräckligt preciserat.

8.1 Rättsliga utgångspunkter

Som framgår av avsnitt 7 måste det vid varje tidpunkt vara känt för vilket närmare ändamål en viss personuppgift behandlas. När en uppgift behandlas i en enskild tjänstemans dator eller i en liten, klart avgränsad projektgrupp vet den handläggande tjänstemannen varför uppgiften behandlas.¹⁷ När uppgifter är gemensamt tillgängliga blir det däremot svårare för de personer som kan komma i kontakt med uppgiften att få sådana upplysningar. Enligt PDL ska därför det närmare ändamålet alltid *framgå* i anslutning till sådana uppgifter (3 kap. 3 § PDL).

Av PDL:s förarbeten kan utläsas att det normalt ska framgå på vilken grund uppgifterna har gjorts gemensamt tillgängliga. Om grunden är att uppgifterna kan antas ha samband med misstänkt brottslig verksamhet, ska det också vara tydligt för *vilket slag av brottslig verksamhet* som behandlingen sker, exempelvis ett underrättelseprojekt om vapensmuggling från Y-land. Om uppgifterna har samlats in för ett visst ändamål men senare kommer att användas för något nytt ändamål, måste det framgå att den senare behandlingen sker för ett nytt ändamål.¹⁸

Om det inte framgår av sammanhanget, måste en särskild upplysning om det närmare ändamålet lämnas. Om polisen möjliggör så kallade fritextsökningar i ett flertal sammanlänkade system, bör det redan av träffbilden framgå för vilket eller vilka ändamål en viss personuppgift behandlas. Om det till exempel framgår att uppgiften behandlas i ett underrättelseprojekt som har ett tydligt definierat ändamål, är detta normalt tillräckligt.¹⁹

¹⁷ Prop. 2009/10:85 s. 147.

¹⁸ Prop. 2009/10:85 s. 339 f.

¹⁹ Prop. 2009/10:85 s. 148 och s. 339.

8.2 Vad granskningen har visat

Eftersom i princip alla uppgifter på Z-servern och många av uppgifterna i SURFA2 var gemensamt tillgängliga vid nämndens inspektion gällde kravet – att det närmare ändamålet ska *framgå* – i stora delar av polismyndighetens underrättelseverksamhet.

Enligt polismyndigheten har de närmare ändamålen med behandlingen av uppgifter på Z-servern framgått av det SUS-beslut som gällde för behandlingen tillsammans med innehållet i registrerade dokument och namnen på de mappar som uppgifterna fanns i. Vad gäller uppgifter i SURFA2 har de närmare ändamålen enligt polismyndigheten framgått av SUS-besluten tillsammans med innehållet i registrerade dokument och viss annan information som kan anges när dokument registreras i SURFA2.

På fråga från nämnden har polismyndigheten angett att det närmare ändamålet med behandlingen av uppgifterna i flera dokument på Z-servern i vart fall inte framgår längre.²⁰ Bland dessa finns exempel 1, 3 och 4.

8.3 Nämndens bedömning

Nämnden konstaterar att det inte alltid har framgått för vilket närmare ändamål uppgifter har behandlats i polismyndighetens underrättelseverksamhet.

Om det närmare ändamålet inte framgår tydligt redan av träffbilden vid en sökning eller av den text som uppgiften finns i, måste detta framgå på något annat sätt. I polismyndighetens underrättelseverksamhet har närmare ändamål angetts i de olika SUS-besluten. I de fall det tydligt går att utläsa – av träffbilden eller av texten i ett visst dokument – vilket SUS-beslut som gäller för behandlingen menar nämnden att det närmare ändamålet kan anses framgå på ett godtagbart sätt. Det förutsätter dock att det närmare ändamålet i SUS-beslutet är tillräckligt preciserat.

Som påpekats ovan har de närmare ändamål som angetts i polismyndighetens SUS-beslut i vissa fall varit alltför vida och otydliga.²¹ Det gäller bland annat det beslut som tidigare gällde för behandlingen av alla uppgifter på Z-servern. Enligt det beslutet fick uppgifter i princip behandlas om de hade samband med *någon* misstänkt brottslig verksamhet. Även om det i och för sig har framgått vilket SUS-beslut som gällde för behandlingen av uppgifterna på Z-servern har det alltså inte genom detta beslut framgått *vilken typ* av misstänkt brottslig verksamhet som uppgifterna har haft samband med.

²⁰ Se avsnitt 3.5 om den gallring som polismyndigheten har genomfört.

²¹ Se avsnitt 7.

För uppgifterna på Z-servern kan det närmare ändamålet med behandlingen alltså inte anses ha framgått genom SUS-beslutet. För vissa av de granskade dokumenten har det närmare ändamålet inte heller framgått tillräckligt tydligt på något annat sätt. Det gäller bland annat exempel 1, 3 och 4.

Nämnden förutsätter att åtgärder vidtas för att komma till rätta med dessa brister.

9 UPPLYSNINGAR OM PERSONER SOM INTE ÄR MISSTÄNKTA

I vissa fall har det inte *framgått* tillräckligt tydligt vilka personer som inte är misstänkta för brott.

9.1 Rättsliga utgångspunkter

Om en uppgift som är gemensamt tillgänglig avser en person som inte är misstänkt för brott, eller för att ha utövat eller komma att utöva brottslig verksamhet, ska det alltid *framgå* att personen inte är misstänkt (3 kap. 4 § 1 st. PDL). Om det inte framgår av sammanhanget, måste en särskild upplysning om att personen inte är misstänkt lämnas.²²

9.2 Vad granskningen har visat

Som nämnts ovan var i princip alla uppgifter på Z-servern och många av uppgifterna i SURFA2 gemensamt tillgängliga vid nämndens inspektion. Därför gällde även kravet – att det ska framgå vilka personer som inte är misstänkta – i stora delar av polismyndighetens underrättelseverksamhet.

När uppgifter behandlas i SURFA2 använder polismyndigheten en speciell länk för att visa vilka personer som är misstänkta för brott i ett visst sammanhang. För uppgifter som behandlas på Z-servern saknas det däremot särskilda funktioner för att visa vilka personer som inte är misstänkta.

Nämnden har begärt att polismyndigheten ska utveckla om – och i så fall på vilket sätt – det har framgått vilka personer som inte är misstänkta i vissa dokument på Z-servern. Det gäller bland annat exempel 1.

Polismyndigheten har sammanfattningsvis svarat följande. I flera av dokumenten framgår det i vart fall inte längre om personerna är misstänkta eller inte.²³ Bland dessa finns exempel 1, där det inte framgår om några av de

²² Prop. 2009/10:85 s. 149 f.

²³ Se avsnitt 3.5 om den gallring som polismyndigheten har genomfört.

ca 180 personerna är misstänkta. Såvitt känt finns det dock ingenting som tyder på att några av personerna i exempel 1 skulle vara misstänkta.

9.3 Nämndens bedömning

Det är av stor betydelse för skyddet av den personliga integriteten att det framgår om uppgifter om en person behandlas för att han eller hon är misstänkt för att ha utövat eller komma att utöva brottslig verksamhet eller om behandlingen sker av någon annan anledning.

Nämnden konstaterar att det i flera granskade dokument på Z-servern inte har framgått vilka personer som inte är misstänkta. Det gäller bland annat exempel 1.

Nämnden förutsätter att åtgärder vidtas för att komma till rätta med dessa brister.

10 GALLRING AV PERSONUPPGIFTER

Uppgifter på Z-servern har i flera fall inte gallrats i tid. I vissa fall borde uppgifter ha gallrats för flera år sedan.

10.1 Rättsliga utgångspunkter

Gallringsbestämmelserna i PDL syftar i första hand till att skydda den enskildes integritet genom att sätta en yttersta tidsgräns för det intrång som behandlingen innebär. Att en uppgift gallras innebär att den inte längre finns digitalt åtkomlig. Gallrade uppgifter ska alltså inte gå att söka fram eller sammanställa i den brottsbekämpande verksamheten.

Uppgifter som *inte längre behövs* för något av de i PDL tillåtna ändamålen ska gallras (2 kap. 12 § 1 st. PDL). Därutöver finns olika tidsbegränsningar för bevarande av uppgifter i underrättelseverksamheten beroende på om de är gemensamt tillgängliga (3 kap. 14 § PDL) eller inte (2 kap. 13 § PDL). Dessa bestämmelser anger den *längsta tid* en uppgift får bevaras. Gallringsfristerna har satts till ett, tre, fem eller tio år, beroende på vad uppgiften gäller.

10.2 Vad granskningen har visat

Polismyndigheten har uppgett följande. I SURFA2 gallras uppgifter automatiskt efter en viss tid, i enlighet med de gallringsfrister som finns i PDL. När det sker beror dels på om uppgifterna är gemensamt tillgängliga eller inte, dels på vad uppgifterna gäller. Tidpunkten för gallring kan också flyttas fram

automatiskt om nya uppgifter om samma person börjar behandlas i samma uppgiftssamling. Det går även att gallra uppgifter manuellt i SURFA2. På Z-servern måste uppgifter gallras helt manuellt. Det har dock saknats fungerande rutiner för detta. En omfattande genomgång av uppgifterna på Z-servern har därför genomförts efter nämndens inspektion och sådana uppgifter som inte längre får behandlas enligt PDL har gallrats.

På fråga från nämnden har polismyndigheten angett att uppgifterna i vissa äldre dokument på Z-servern borde ha gallrats, antingen på grund av PDL:s gallringsfrister eller på grund av att uppgifterna inte har fått behandlas längre av andra skäl. Det gäller bland annat exempel 3 och 4.

10.3 Nämndens bedömning

Nämnden konstaterar att gallringen av uppgifter på Z-servern har brustit. Uppgifter har i flera fall inte gallrats i tid. Det gäller bland annat uppgifterna i exempel 3 och 4. I vissa fall, däribland exempel 4, borde uppgifterna ha gallrats för flera år sedan.

Nämnden förutsätter att det införs fungerande rutiner så att uppgifter gallras i tid. Detta gäller särskilt för de nya mapparna på Z-servern där uppgifterna inte gallras automatiskt efter en viss tid.

11 AVSLUTANDE KOMMENTARER

Nämndens granskning har visat på olika brister i personuppgiftsbehandlingen i polismyndighetens underrättelseverksamhet. Granskningen har i huvudsak utgått ifrån ett antal dokument som endast innehåller en liten del av den totala mängden uppgifter som behandlas i verksamheten. Trots det menar nämnden att de iakttagelser som har gjorts tyder på att det har funnits vissa systematiska felaktigheter med behandlingen av personuppgifter i den granskade verksamheten. Det gäller i synnerhet behandlingen av personuppgifter på Z-servern.

Nämnden konstaterar att det pågår ett arbete med att på olika sätt anpassa polismyndighetens underrättelseverksamhet till de krav som PDL ställer, bland annat genom introduktionen och vidareutvecklingen av SURFA2. Vid inspektionstillfällena var detta arbete inte slutfört. Det kan förklara vissa av de felaktigheter som har iakttagits, men långt ifrån alla. Felaktigheterna verkar även bero på ett flertal andra faktorer, så som resursbrist i verksamheten, otillräckliga kunskaper om innebörden av vissa bestämmelser, bristande rutiner eller avsaknaden av relevanta och uppdaterade myndighetsföreskrifter.

Den 1 januari 2015 kommer de nuvarande polismyndigheterna att slås samman till en ny myndighet. Nämnden förutsätter att den nya Polismyndigheten åtgärdar de brister som har uppmärksammats vid granskningen och säkerställer att motsvarande problem inte förekommer i underrättelseverksamheten i övriga delar av landet.

Nämnden avser att granska vilka åtgärder som den nya Polismyndigheten vidtar för att säkerställa att personuppgiftsbehandlingen i underrättelseverksamheten sker i enlighet med PDL.

Sändlista:

Polismyndigheten i Västra Götaland

Kopia för kännedom:

Rikspolisstyrelsen

Datainspektionen