



## **Polismyndigheten i Östergötlands läns behandling av personuppgifter i underrättelseverksamheten**

---

### **1 SAMMANFATTNING**

Säkerhets- och integritetsskyddsnämnden har granskat Polismyndigheten i Östergötlands läns behandling av personuppgifter i underrättelseverksamheten.

Nämnden riktar kritik mot polismyndigheten på följande punkter.

- Känsliga personuppgifter har i flera fall behandlats utan att det har varit absolut nödvändigt.
- 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 har funnits något konkret behov av dem.
- Det närmare ändamålet med behandlingen har i vissa fall inte framgått tillräckligt tydligt.
- I vissa fall har det inte framgått tillräckligt tydligt 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
4	PERSONUPPGIFTSBEHANDLING I POLISMYNDIGHETENS UNDERRÄTTELSEVERKSAMHET .....	6
4.1	Beslut om särskilda uppgiftssamlingar .....	6
4.2	SURFA2.....	6
4.3	Y-servern.....	6
5	BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER .....	7
5.1	Rättsliga utgångspunkter .....	7
5.2	Vad granskningen har visat.....	8
5.3	Nämndens bedömning.....	8
6	GEMENSAMT TILLGÄNGLIGA PERSONUPPGIFTER.....	10
6.1	Rättsliga utgångspunkter .....	10
6.2	Vad granskningen har visat.....	10
6.3	Nämndens bedömning.....	11
7	ÄNDAMÅL OCH BEHOV .....	12
7.1	Rättsliga utgångspunkter .....	12
7.2	Vad granskningen har visat.....	13
7.3	Nämndens bedömning.....	14
8	UPPLYSNINGAR OM ÄNDAMÅLET MED BEHANDLINGEN .....	15
8.1	Rättsliga utgångspunkter .....	15
8.2	Vad granskningen har visat.....	16
8.3	Nämndens bedömning.....	16
9	UPPLYSNINGAR OM PERSONER SOM INTE ÄR MISSTÄNKTA .....	17
9.1	Rättsliga utgångspunkter .....	17
9.2	Vad granskningen har visat.....	17
9.3	Nämndens bedömning.....	18
10	GALLRING AV PERSONUPPGIFTER .....	19
10.1	Rättsliga utgångspunkter .....	19
10.2	Vad granskningen har visat.....	19
10.3	Nämndens bedömning.....	20
11	AVSLUTANDE KOMMENTARER .....	20

## 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 behandlat personuppgifter i underrättelseverksamheten. Den 15 november 2013 riktade nämnden allvarlig kritik mot Polismyndigheten i Skåne för behandlingen i uppgiftssamlingen ”Kringresande”.<sup>1</sup> Nämnden inledde i samband med detta en översiktlig granskning av underrättelseverksamheten vid landets länspolismyndigheter i syfte att hämta in underlag för kommande granskningar.<sup>2</sup>

Den 13 februari 2014 beslutade nämnden att granska personuppgiftsbehandlingen med stöd av polisdatalagen (2010:361) (PDL) i underrättelseverksamheten vid Polismyndigheten i Östergötlands län (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* endast när det är absolut nödvändigt som komplement till annan behandling? (Avsnitt 5)

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

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

- Vilka personuppgifter är *gemensamt tillgängliga*? Får dessa uppgifter vara gemensamt tillgängliga? (Avsnitt 6)
- 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 Y-servern).<sup>3</sup>

Delar av nämndens kansli genomförde en inspektion vid polismyndighetens kriminalunderrättelsetjänst den 1 och 22 april 2014. Vid inspektionen gjordes en översiktlig granskning av fler än 200 dokument och filer från SURFA2 och Y-servern. Vissa granskade dokument valdes ut slumpmässigt. Andra dokument valdes ut med hjälp av i förväg bestämda sökkriterier, däribland att de innehöll känsliga personuppgifter, ett stort antal personuppgifter eller särskilt gamla uppgifter.

Tjugofyra av dessa dokument blev sedan föremål för en närmare granskning, eftersom de illustrerade vissa återkommande eller särskilt allvarliga problem. Polismyndigheten har, på nämndens begäran, fått besvara olika frågor om personuppgiftsbehandlingen i dessa tjugofyra dokument.

I följande avsnitt används åtta av de tjugofyra 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. Av sekretesskäl kan någon närmare förklaring av vad dokumenten gäller inte lämnas. I samtliga fall rör det sig emellertid om uppgifter om personer som har pekats ut med namn och personnummer eller födelsedatum.

<sup>3</sup> Se avsnitt 4.2 och 4.3 för mer information om SURFA2 och Y-servern.

Följande exempel har hämtats från SURFA2.

- **Exempel 1** innehåller information om att en person som har lämnat uppgifter till polisen ”har flera diagnoser, bland annat Aspergers.” Dokumentet är från år 2014.  
Se bedömning i avsnitt 5.
- **Exempel 2** innehåller information om att en person som kan misstänkas för stöld går ”på kontroller vid ett par ggr/år [...] för sin medicinerande sjukdom. Friskförklarad.”. Dokumentet är från år 2014.  
Se bedömning i avsnitt 5.

Följande exempel har hämtats från Y-servern.

- **Exempel 3** innehåller information om att ett sällskap av ”romsk härkomst” har besökt ett hotell. Dokumentet är från år 2013.  
Se bedömning i avsnitt 5.
- **Exempel 4** innehåller information om att en person som kan misstänkas för narkotikabrott har ”konverterat till islam”. Dokumentet är från år 2013.  
Se bedömning i avsnitt 5.
- **Exempel 5** innehåller ett så kallat länkschema som visar länkar mellan olika personer. Länkschemat innehåller uppgifter om personernas namn, personnummer och kön samt visar vilka relationer de olika personerna har till varandra. I anslutning till vissa personer står det ”muslimsk kurd”. Dokumentet är från år 2012 och ingår i ett pågående ärende hos polismyndigheten.  
Se bedömningar i avsnitt 5, 7, 8 och 9.
- **Exempel 6** innehåller information om var en person som kan misstänkas för vissa trafikbrott brukar parkera sin moped. Dokumentet är från år 2014.  
Se bedömningar i avsnitt 6, 7 och 8.
- **Exempel 7** innehåller endast en lista med namn och personnummer i anslutning till en viss adress. Dokumentet är från år 2012 och ingick i ett ärende som avslutades samma år.  
Se bedömning i avsnitt 7, 8 och 9.
- **Exempel 8** innehåller information om ett antal personer som kan misstänkas för narkotikabrott. Dokumentet är senast ändrat år 2000.  
Se bedömning i avsnitt 10.

## **4 PERSONUPPGIFTSBEHANDLING I POLISMYNDIGHETENS UNDERRÄTTELSEVERKSAMHET**

### **4.1 Beslut om särskilda uppgiftssamlingar**

Polismyndigheten har fattat beslut om att inrätta ett antal 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 som ska få *tillgång* till uppgifterna, hur de ska göras *tillgängliga*, hur och när *gallring* ska ske samt för vilket *närmare ändamål* de får behandlas.

Enligt SUS-besluten ska både SURFA2 och Y-servern användas för de flesta uppgiftssamlingar. Fyra av uppgiftssamlingarna ska dock endast behandlas i SURFA2.

### **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 är personuppgiftsansvarig 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 Y-servern**

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

Polismyndigheten har uppgett följande. Samtliga tjänstemän vid polismyndighetens kriminalunderrättelsetjänst har tillgång till Y-servern. Normalt är det däremot endast ett fåtal tjänstemän som arbetar i respektive mapp på Y-servern. Innan SURFA2 togs i bruk användes Y-servern för att sortera, dela, bearbeta och visualisera information i underrättelseverksamheten. Våren 2014 inleddes ett arbete med att föra över relevanta uppgifter på Y-servern till SURFA2. All ny underrättelseinformation läggs numera i regel in direkt i SURFA2. Det förekommer dock alltjämt att information tillfälligt läggs på Y-servern under en beredning. Det kommer även fortsättningsvis att finnas ett behov av att kunna föra över information från SURFA2 till Y-servern för vidare bearbetning eller analys som inte är möjlig att genomföra i SURFA2.

## 5 BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER

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

### 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 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 bara behandlas 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 dessutom prövas noga i det enskilda fallet.<sup>4</sup>

Känsliga personuppgifter får dock behandlas om det är nödvändigt för diarieföring eller om uppgiften har lämnats till polisen i en anmälan eller liknande och det är nödvändigt för handläggningen att behandla uppgiften (2 kap. 9 § och 10 § 2 st. PDL). Undantaget gäller bara sådan behandling som krävs för att inkomna handlingar ska kunna hanteras på ett korrekt sätt. Det är alltså inte möjligt att behandla uppgifter i exempelvis arbetet med att bearbeta underrättelser med stöd av denna bestämmelse.<sup>5</sup>

---

<sup>4</sup> Prop. 2009/10:85 s. 325.

<sup>5</sup> Prop. 2009/10:85 s. 112.

Personuppgifter får bara behandlas om det är lagligt (2 kap. 2 § 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**

Polismyndigheten har uppgett följande. Det saknas centrala direktiv från Rikspolisstyrelsen om behandlingen av känsliga personuppgifter i underrättelseverksamheten. Det är något som polismyndigheten tidigare har efterlyst. När känsliga personuppgifter behandlas i SURFA2 ska det enligt polismyndighetens interna rutiner finnas ett dokument länkat till varje känslig personuppgift. Av dokumentet ska det gå att utläsa varför det bedöms vara absolut nödvändigt att behandla uppgiften. Vid behandling av känsliga personuppgifter på Y-servern finns det inga motsvarande rutiner. Det pågår emellertid en diskussion inom polismyndigheten om att införa rutiner som innebär att beslut om registrering av känsliga personuppgifter ska fattas av en chef eller en särskild tjänsteman.

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 1–5.

Polismyndighetens svar kan sammanfattas på följande sätt. Polismyndigheten bedömer att det finns känsliga personuppgifter i dokumenten som inte har varit absolut nödvändiga för ändamålet med behandlingen. Att uppgifterna ändå har behandlats beror i vissa fall på bristande kunskap om hur undantagen från förbudet mot behandling av känsliga personuppgifter får tillämpas, till exempel undantaget i 2 kap. 9 § och 10 § 2 st. PDL om uppgifter i inkomna handlingar. I andra fall beror det på felbedömning eller förbiseende från den handläggande tjänstemannens sida. Eftersom det inte har varit absolut nödvändigt att behandla de känsliga personuppgifterna borde dessa ha gallrats. Det kommer nu att ske.

## **5.3 Nämndens bedömning**

Nämnden anser att det har förekommit brister i hanteringen av känsliga personuppgifter i polismyndighetens underrättelseverksamhet.

Vid granskningen har det inte framkommit något som tyder på att personuppgifter har behandlats enbart på grund av en persons ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv. Känsliga personuppgifter har emellertid behandlats som ett komplement till behandling som sker för andra syften.



Nämnden bedömer att det i flera fall inte har varit absolut nödvändigt att behandla de känsliga personuppgifterna för de ändamål som polismyndigheten har angett. Det gäller bland annat uppgifterna om hälsa, etnicitet respektive religiös åskådning i exempel 1–5. Nämnden förutsätter att dessa känsliga personuppgifter nu kommer att gallras utan dröjsmål.

Det undantag som möjliggör behandling av känsliga uppgifter i inkomna handlingar, 2 kap. 9 § och 10 § 2 st. PDL, har enligt nämnden tillämpats alltför vitt i polismyndighetens underrättelseverksamhet. Om behandlingen inte sker för diariesändamål eller liknande får känsliga personuppgifter bara behandlas om det är *absolut nödvändigt* för ändamålet med behandlingen. Det gäller även om uppgifterna har sitt ursprung i information som en utomstående person har lämnat till polisen.

Med anledning av vad polismyndigheten har uppgett om orsakerna till den felaktiga behandlingen vill nämnden även betona vikten av utbildning och interna diskussioner om behandling av känsliga personuppgifter.

Det måste också finnas fungerande rutiner som säkerställer att känsliga personuppgifter inte behandlas i strid med lag. Nämnden har i flera andra sammanhang förordat att rutiner införs som innebär att beslut om registrering av känsliga personuppgifter alltid ska fattas av särskilt utsedda personer samt att besluten ska dokumenteras och motiveras.<sup>6</sup> Nämnden noterar att polismyndigheten har infört eller har för avsikt att införa sådana rutiner för behandlingen av personuppgifter i SURFA2. Nämnden förutsätter att motsvarande rutiner även kommer att gälla för den behandling som sker på Y-servern.

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

---

<sup>6</sup> 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 Y-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 vissa högre krav på behandlingen av uppgifter som är *gemensamt tillgängliga* (3 kap. 1 § PDL).<sup>7</sup>

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 obestämd 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.<sup>8</sup>

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

Av polismyndighetens olika SUS-beslut framgår vilka uppgiftssamlingar som ska vara gemensamt tillgängliga och vilka som inte ska vara det. I de beslut som gäller för uppgiftssamlingar som inte ska vara gemensamt tillgängliga uppges, som ovan nämnts, i samtliga fall att uppgifterna ska behandlas både på Y-servern och i SURFA2. Enligt polismyndigheten är emellertid i princip alla uppgifter på Y-servern gemensamt tillgängliga, eftersom samtliga medarbetare vid kriminalunderrättelsetjänsten har tillgång till dem.

<sup>7</sup> Prop. 2009/10:85 s. 125. Se även avsnitt 8 och 9.

<sup>8</sup> Se 3 kap. 1 § PDL och prop. 2009/10:85 s. 334 f.

I SURFA2 finns det uppgifter som enligt polismyndigheten inte är gemensamt tillgängliga. I mars 2014 var det mellan fyra och nio personer som hade tillgång till dessa. Även om vissa medarbetare kan behöva bytas ut över tid menar polismyndigheten att detta inte ensamt kan vara avgörande för om uppgifterna ska anses vara gemensamt tillgängliga eller inte.

Nämnden har begärt att polismyndigheten ska utveckla om personuppgifter i vissa granskade dokument får vara gemensamt tillgängliga, eftersom det inte har framgått att uppgifterna har samband med den typ av brottsliga verksamhet som krävs eller att de behövs för övervakning. Det gäller bland annat exempel 6.

Polismyndigheten har svarat att det saknats förutsättningar att göra personuppgifterna i bland annat exempel 6 gemensamt tillgängliga och att felbedömningar ligger till grund för att det ändå har skett.

### **6.3 Nämndens bedömning**

Nämnden konstaterar att det inte har funnits lagliga förutsättningar för att göra alla uppgifter på Y-servern gemensamt tillgängliga. Det gäller bland annat exempel 6. I detta fall framgår det inte att uppgifterna har samband med brottslighet av tillräckligt allvarligt slag eller att de får vara gemensamt tillgängliga av något annat skäl.

Nämnden utgår ifrån att det inte har varit polismyndighetens avsikt att göra uppgifter gemensamt tillgängliga i den stora utsträckning som har skett. Det har emellertid blivit konsekvensen av att behörigheterna till de olika mapparna på Y-servern inte har begränsats till de tjänstemän som ska arbeta med informationen. Uppgifter som hör till uppgiftssamlingar som enligt SUS-besluten inte ska vara gemensamt tillgängliga har därmed ändå blivit det. Om Y-servern även fortsättningsvis ska användas för behandling av alla typer av underrättelseinformation måste tillgången till dokumenten därför begränsas.

Nämnden vill även påminna om att tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Det kan ifrågasättas om alla tjänstemän vid polismyndighetens kriminalunderrättelsetjänst har behov av alla uppgifter på Y-servern i sitt arbete. Tillgången till uppgifterna måste begränsas även av det skälet.

Med anledning av vad polismyndigheten har svarat om hur en hög personrörlighet påverkar bedömningen av vilka uppgifter som är gemensamt tillgängliga, vill nämnden framhålla följande. Uppgifter som behandlas en längre tid kan anses vara gemensamt tillgängliga trots att antalet personer som

har tillgång till dem vid varje givet tillfälle är få.<sup>9</sup> Vid bedömningen av vilka uppgifter som är gemensamt tillgängliga bör fler faktorer beaktas än vad polismyndigheten hittills verkar ha gjort. Det kan till exempel finnas skäl att ta hänsyn till den faktiska eller förväntade årliga omsättningen på de tjänstemän som har tillgång till uppgifterna. Vilka gallringsbestämmelser och -rutiner som gäller för den aktuella uppgiftssamlingen kan också vara av betydelse.

## 7 ÄNDAMÅL OCH BEHOV

Polismyndigheten har fattat beslut om för vilka *närmare ändamål* uppgifter får samlas in och behandlas i underrättelseverksamheten. Nämnden bedömer att de flesta av dessa närmare ändamål har formulerats på ett godtagbart sätt. I vissa fall bedömer nämnden emellertid att de beslutade närmare ändamålen 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 för vilket uppgifterna samlades in (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.<sup>10</sup> 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).

<sup>9</sup> 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.

<sup>10</sup> Prop. 2009/10:85 s. 317 f.

När en personuppgift görs gemensamt tillgänglig ska det alltid framgå för vilket närmare ändamål som behandlingen sker.<sup>11</sup> Utöver detta finns det inget krav i PDL på att det närmare ändamålet ska dokumenteras.<sup>12</sup> 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 behandlas samtliga uppgifter i underrättelseverksamheten inom ramen för någon av de uppgiftssamlingar som den har fattat beslut om. Genom att uppgifterna ingår i uppgiftssamlingar menar polismyndigheten att det går att ta reda på för vilka närmare ändamål varje personuppgift behandlas. Detta eftersom de närmare ändamålen framgår av respektive SUS-beslut.

Av sekretesskäl kan beskrivningen av de närmare ändamålen i de olika SUS-besluten inte återges i sin helhet. Nedan beskrivs istället vissa gemensamma nämnare som återkommer i flera SUS-beslut.

- Behandlingen ska syfta till en viss typ av *resultat*. Arbetet i vissa uppgiftssamlingar ska exempelvis syfta till att fatta beslut om operativa åtgärder, till exempel att inleda en förundersökning.
- Informationen ska ha en viss *geografisk anknytning*. Den information som behandlas ska ha betydelse för verksamheten inom ett visst geografiskt område.
- Informationen ska röra vissa *typer av brott*. Till exempel kan ändamålet vara att samla in och bearbeta information om våldsbrott eller narkotikabrott.
- Informationen ska röra viss *brottslighet*. Utmärkande för den aktuella brottsligheten kan vara att den utförs av vissa *personer* eller *organisationer*, har viss *omfattning* eller att en viss *påföljd* kan följa på den. Till exempel kan ändamålet vara att samla in och bearbeta information om vissa kriminella nätverk eller om brott som sker systematiskt.

När en uppgift behandlas i SURFA2 framgår det vilken uppgiftssamling den tillhör. Dessutom kan användaren välja vilka uppgiftssamlingar en viss sökning ska omfatta, förutsatt att han eller hon har tillgång till dem.

---

<sup>11</sup> Se avsnitt 8.

<sup>12</sup> Prop. 2009/10:85 s. 98.

Någon motsvarande tydlighet finns inte när en personuppgift behandlas på Y-servern. Enligt polismyndigheten ska alla personuppgifter som finns på Y-servern gå att hänföra till en eller flera uppgiftssamlingar. Mapparnas namn motsvarar i princip uppgiftssamlingarnas, men det finns även mappar som inte har någon tydlig koppling till någon uppgiftssamling. Polismyndigheten har enligt uppgift för avsikt att anpassa namnen på mapparna på Y-servern så att de överensstämmer bättre med namnen på de beslutade uppgiftssamlingarna.

Nämnden har begärt att myndigheten ska uppge vilken uppgiftssamling vissa granskade dokument tillhör, bland annat exempel 5–7. Myndigheten har i samtliga fall kunnat uppge vilka uppgiftssamlingar dokumenten tillhör.

Nämnden har även frågat polismyndigheten om – och i så fall varför – det finns behov av att behandla uppgifter i vissa dokument för det närmare ändamål som anges i respektive SUS-beslut. Det gäller bland annat exempel 5–7. Polismyndigheten har förklarat vari behovet att samla in uppgifterna bestod, att det inte längre finns något behov av att behandla uppgifterna i exempel 6 och 7 samt att dessa uppgifter borde ha gallrats.

### **7.3 Nämndens bedömning**

Nämnden anser att de närmare ändamål som anges i de granskade SUS-besluten i några fall är för 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. De flesta av dessa beslut har utformats på ett godtagbart sätt.

I några fall förefaller de beskrivna ändamålen dock vara så vitt formulerade att de inte utgör någon effektiv garant mot ”bra att ha”-uppgiftssamlingar. De

ändamålsbeskrivningar som nämnden anser är för allmänna omfattar ett flertal olika brottstyper som inte har någon uppenbar koppling till varandra. Det finns risk att dessa uppgiftssamlingar innehåller fler uppgifter än vad som behövs i verksamheten. I flera fall är ändamålsbeskrivningarna i SUS-besluten också svåra att förstå rent språkligt. Mot bakgrund av detta bör ändamålsbeskrivningen i vissa SUS-beslut formuleras om och preciseras.

Nämnden bedömer att det inte finns något behov av att behandla uppgifterna i exempel 6 och 7 för de närmare ändamål som polismyndigheten har uppgett för respektive behandling. Nämnden förutsätter att uppgifterna nu gallras. Det måste också finnas fungerande rutiner för gallring av personuppgifter som inte längre behövs.

## 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.

När det gäller de uppgifter som behandlas på Y-servern är det emellertid inte alltid möjligt att avgöra vilken uppgiftssamling de hör till och därmed inte heller vilket SUS-beslut som gäller för behandlingen.

### 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.<sup>13</sup> 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).

Om det inte framgår på något annat sätt, 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

<sup>13</sup> Prop. 2009/10:85 s. 147.

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.<sup>14</sup>

## 8.2 Vad granskningen har visat

Granskningen har visat att det närmare ändamålet oftast inte framgår tydligt av träffbilden vid en sökning eller av den text som uppgiften finns i. Genom att uppgifterna är kopplade till uppgiftssamlingar menar polismyndigheten emellertid att det går att ta reda på för vilka närmare ändamål de behandlas.

Nämnden har frågat polismyndigheten på vilket sätt det närmare ändamålet framgår för behandlingen av personuppgifter i vissa dokument på Y-servern, bland annat exempel 5-7.

Polismyndigheten har sammanfattningsvis svarat att de närmare ändamålen inte framgår i något av de aktuella dokumenten, men att behandlingen sker för det närmare ändamål som angivits i SUS-beslutet för den uppgiftssamling som respektive dokument tillhör.

## 8.3 Nämndens bedömning

Nämnden konstaterar att det inte alltid framgår för vilket närmare ändamål uppgifter behandlas. Det gäller i synnerhet när uppgifter behandlas på Y-servern.

Eftersom i princip alla uppgifter på Y-servern och många av uppgifterna i SURFA2 är gemensamt tillgängliga gäller kravet att det närmare ändamålet ska framgå i stora delar av polismyndighetens underrättelseverksamhet.

Om det närmare ändamålet inte framgår tydligt redan av träffbilden vid en sökning eller av den text som uppgiften finns i, måste det framgå på något annat sätt. I polismyndighetens underrättelseverksamhet går det närmare ändamålet i och för sig att utläsa av 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 framgår på ett godtagbart sätt. En förutsättning är dock att det i SUS-beslutet angivna närmare ändamålet är tillräckligt preciserat.<sup>15</sup>

När det gäller uppgifter som behandlas på Y-servern är det inte alltid möjligt att avgöra vilken uppgiftssamling de hör till och därmed inte heller vilket SUS-

---

<sup>14</sup> Prop. 2009/10:85 s. 148 och s. 339.

<sup>15</sup> Se avsnitt 7.



beslut som gäller för behandlingen. Det gäller bland annat exempel 5–7. Beträffande exempel 6 och 7 framgår det närmare ändamålet med behandlingen inte heller på något annat sätt.

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 misstänka 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.<sup>16</sup>

### 9.2 Vad granskningen har visat

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 personuppgifter som behandlas på Y-servern saknas det särskilda funktioner för att visa vilka personer som inte är misstänkta. Enligt polismyndigheten går det istället att förstå av sammanhanget vilka som är misstänkta för brott och vilka som inte är det.

Som ovan nämnts är i princip alla uppgifter på Y-servern gemensamt tillgängliga. Därför gäller kravet att det ska framgå vilka personer som inte är misstänkta även för dessa uppgifter.

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 Y-servern. Det gäller bland annat exempel 5 och 7.

Polismyndigheten har sammanfattningsvis uppgett följande. I exempel 5 går det inte att utläsa av dokumentet vilka personer som inte är misstänkta för

<sup>16</sup> Prop. 2009/10:85 s. 149 f.

brott. Av den samlade dokumentationen i ärendet framgår det vilken roll respektive person har. I exempel 7 finns det anteckningar i dokumentet om att vissa personer förekommer i andra polisiära register som innehåller misstankar om brott. Det får anses framgå motsatsvis att övriga personer inte var misstänkta för brott när listan upprättades.

### **9.3 Nämndens bedömning**

Nämnden konstaterar att det i flera granskade dokument på Y-servern inte har framgått vilka personer som inte är misstänkta.

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. Den som tar del av en uppgift ska inte behöva leta i ett omfattande material för att få reda på om den som uppgiften avser är misstänkt eller inte.

Nämnden anser att det inte framgår av exempel 5 och 7 vilka personer som inte är misstänkta. Beträffande exempel 5 är det inte tillräckligt att det framgår av den samlade dokumentationen i ärendet vilka som inte är misstänkta. Enligt nämnden ställer PDL högre krav än så. Upplysningarna bör finnas i dokumentet, dess rubrik eller i någon annan information som visas för den som tar del av uppgiften.

Anteckningar om att vissa personer i ett dokument förekommer i andra register leder inte heller nödvändigtvis till slutsatsen att övriga personer som omnämns där inte är misstänkta för brott. Av dokumentet i exempel 7 framgår därför inte tillräckligt tydligt vilka personer som inte är misstänkta.

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

## 10 GALLRING AV PERSONUPPGIFTER

Uppgifter på Y-servern har i flera fall inte gallrats i tid. I vissa fall borde uppgifterna 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 tidsbegränsningar för bevarande av gemensamt tillgängliga uppgifter (3 kap. 14 § PDL) och sådana som inte är det (2 kap. 13 § PDL). Dessa bestämmelser anger den *längsta tid* en uppgift får bevaras. Gallringsfristerna i PDL 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 Y-servern sker gallring däremot helt manuellt. Gallringen på Y-servern har emellertid inte fullt ut skett i enlighet med gällande rutiner, vilket kan bero på bristande uppföljning eller otillräckliga resurser. I vissa fall beror den uteblivna gallringen på tekniska hinder som polismyndigheten inte kan avhjälpa på egen hand.

De regler som gäller för gallring och förlängning av gallringsfrister i uppgiftssamlingarna beskrivs i respektive SUS-beslut, bland annat genom hänvisningar till gallringsbestämmelserna i PDL.

På fråga från nämnden har polismyndigheten svarat att uppgifterna i vissa äldre dokument på Y-servern borde ha gallrats. Det gäller bland annat exempel 8.

Utöver de granskade dokumenten har nämnden bland annat noterat en databasfil på Y-servern som upptog ett stort lagringsutrymme. Vid nämndens

inspektion hade ingen av polismyndighetens närvarande personal tillgång till filen. Nämnden har därför inte haft möjlighet att granska innehållet närmare. Av information som visades i anslutning till filen gick det emellertid att se att den innehöll en databas samt att den inte hade används sedan år 2011. På fråga från nämnden har polismyndigheten uppgett att filen har fungerat som en samlingsplats för uppgifter om viss brottslig verksamhet som skulle analyseras samt att filen borde ha gallrats.

### **10.3 Nämndens bedömning**

Nämnden konstaterar att gallringen av uppgifter på Y-servern har brustit.

Trots att polismyndigheten har rutiner för gallring på Y-servern har många uppgifter uppenbarligen inte gallrats i rätt tid. Bland annat borde uppgifterna i exempel 8 ha gallrats för flera år sedan. Detsamma gäller den stora databasfilen på Y-servern.

Nämnden förutsätter att det nu tillsätts resurser för att genomföra den nödvändiga gallringen på Y-servern.

Vidare konstaterar nämnden att de gallringsbestämmelser som gäller för uppgifter som inte är gemensamt tillgängliga beskrivs på ett felaktigt sätt i flera av de SUS-beslut som gäller för sådana uppgifter. I flera fall beskrivs eller hänvisas till fel gallringsbestämmelse i PDL. Nämnden förutsätter att gallring i de berörda uppgiftssamlingarna ändå sker i enlighet med PDL:s regler samt att besluten anpassas efter lagstiftningen i dessa delar.

## **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, i förhållande till den totala mängden uppgifter, endast utgör en liten del av den information som behandlas i verksamheten. Trots det menar nämnden att de iakttagelser som har gjorts tyder på att det finns vissa systematiska felaktigheter med behandlingen av personuppgifter i den granskade verksamheten. Det gäller i synnerhet behandlingen av personuppgifter på Y-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.