



## **Säkerhetspolisens behandling av känsliga personuppgifter i fristående databaser**

---

### **1 SAMMANFATTNING**

Säkerhets- och integritetsskyddsnämnden har granskat Säkerhetspolisens behandling av känsliga personuppgifter i fristående databaser. Granskningen har omfattat Säkerhetspolisens interna styrdokument samt 20 slumpvis utvalda personobjekt i en av de fristående databaserna. Nämnden har vid en inspektion den 18 juni 2013 granskat fyra av dessa personobjekt närmare.

Nämnden uppmanar Säkerhetspolisen att uppdatera sina interna bestämmelser så att det där framgår att dokumentation av beslut om behandling av känsliga personuppgifter ska ske, och att prövningen av om det är absolut nödvändigt för syftet med behandlingen att behandla den känsliga personuppgiften bör göras så snart som möjligt efter det att en sådan uppgift läggs in i systemet.

Säkerhetspolisen synes i övrigt ha goda rutiner för behandling av känsliga personuppgifter i de fristående databaserna. Nämnden bedömer också att Säkerhetspolisen vidtar adekvata utbildnings- och logguppföljningsinsatser för att säkerställa att reglerna om behandling av känsliga personuppgifter efterlevs. Nämnden vill dock betona vikten av riktad logguppföljning för att säkerställa att sökning på känsliga personuppgifter enbart görs när det är absolut nödvändigt.

Vid granskningen av personobjekt i den databas som omfattats av den aktuella tillsynen har enligt nämndens bedömning inte framkommit något som tyder på att känsliga personuppgifter behandlas i strid med polisdatalagen (2010:361) (PDL).

## 2 BAKGRUND OCH AVGRÄNSNING

I PDL, liksom i annan lagstiftning om behandling av personuppgifter på internationell och nationell nivå, har känsliga personuppgifter en särställning som innebär att sådana uppgifter endast får behandlas i undantagsfall och under särskilda förutsättningar.

Nämnden beslutade den 4 september 2012 att granska Sakerhetspolisens behandling av känsliga personuppgifter i de uppgiftssamlingar som förs vid sidan av centralregistret, så kallade fristående databaser. Granskningen har därefter begränsats till en av dessa databaser.

Fristående databaser används av Sakerhetspolisen för att bearbeta och bedöma information i syfte att avgöra om informationen ska tillföras centralregistret. Sakerhetspolisen håller för närvarande på att byta ut det IT-system som används för att bearbeta och analysera informationen i databaserna.

## 3 RÄTTSLIGA UTGÅNGSPUNKTER

Enligt 2 kap. 10 § första stycket PDL, som enligt 5 kap. 4 § PDL är tillämplig även vid behandling av personuppgifter hos Sakerhetspolisen, får uppgifter om en person inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (känsliga personuppgifter). Det är alltså inte tillåtet att föra register över eller på annat sätt göra anteckningar om enskilda enbart på den grunden att de utifrån något i paragrafen angivet förhållande kan hänföras till en viss kategori av människor. Bestämmelsen hindrar emellertid inte behandling av uppgifter om en persons nationalitet och i regel faller också uppgifter om att en viss person kommer från en viss världsdel eller ett visst land utanför förbudet mot behandling av känsliga personuppgifter.<sup>1</sup>

2 kap. 10 § andra stycket PDL innehåller vissa undantag från huvudregeln. Här föreskrivs bl.a. att uppgifter om en person, om de behandlas på annan grund, får kompletteras med sådana uppgifter som avses i första stycket när det är absolut nödvändigt för syftet med behandlingen. Bestämmelsen innebär att om andra uppgifter om en person samlas in i samband med t.ex. en förundersökning får dessa kompletteras med känsliga personuppgifter om det är av avgörande betydelse för utredningen. Med hänsyn till den restriktivitet som ligger i begreppet ”absolut nödvändigt” måste behovet av att göra sådana kompletteringar prövas noga i det enskilda ärendet.<sup>2</sup>

---

<sup>1</sup> Prop. 2009/10:85 s. 325.

<sup>2</sup> A. prop. s. 325.

Enligt 5 kap. 11 § första stycket PDL får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv – vid sökning i personuppgifter som har gjorts gemensamt tillgängliga, dvs. är tillgängliga för mer än ett fåtal personer – endast användas som sökbegrepp när det är absolut nödvändigt för de ändamål som anges i 5 kap. 1 § PDL.<sup>3</sup> Enligt 5 kap. 11 § andra stycket PDL hindrar detta inte att brottsrubriceringar eller uppgifter som beskriver en persons utseende används som sökbegrepp.

Säkerhetspolisen är enligt 5 kap. 5 § PDL personuppgiftsansvarig för den behandling av personuppgifter som Säkerhetspolisen utför.

#### **4 GRANSKNINGEN**

Säkerhetspolisen har efter anmodan inkommit till nämnden med interna styrdokument och rutinbeskrivningar avseende behandlingen av känsliga personuppgifter i fristående databaser. Vidare har nämnden den 18 juni 2013 genomfört en inspektion vid Säkerhetspolisen. Vid inspektionen har företrädare för Säkerhetspolisen gett en beskrivning av personuppgiftsbehandlingen, särskilt avseende känsliga personuppgifter, i den granskade databasen samt förevisat databasen.

Säkerhetspolisen har vid inspektionstillfället även förevisat och redogjort för bakgrunden till registreringar avseende fyra personobjekt i databasen som innehåller känsliga personuppgifter. Personobjekten hade tidigare valts ut av nämndens kansli. Initialt granskades 20 personobjekt översiktligt. Dessa bestod av de fem först registrerade personobjekten med känsliga personuppgifter varje kalendermånad, från och med april 2012 till och med juli 2012.

#### **5 NÄMNDENS IAKTTAGELSER**

Säkerhetspolisen har beslutat interna bestämmelser och rutiner avseende behandling av känsliga personuppgifter i fristående databaser.

Enligt Säkerhetspolisens interna bestämmelser behöver inte något formellt beslut fattas när det gäller behandling av känsliga personuppgifter som sker i ett inledande skede, innan det har bedömts om uppgifterna ska fortsätta att behandlas och om uppgifterna ska registreras i centralregistret.

Bestämmelserna anger att det är den som registrerar uppgiften som ansvarar för att uppgiften är korrekt. Vidare får enligt bestämmelserna känsliga personuppgifter endast registreras i fristående databaser om de får registreras i centralregistret. Det ska framgå i de fristående databaserna om det har fattats

---

<sup>3</sup> A. prop. s. 127 ff.

ett särskilt beslut om att känsliga personuppgifter får behandlas avseende en person i centralregistret.

Säkerhetspolisen har efter inspektionstillfället lämnat den kompletterande upplysningen att det nya IT-system som ska användas för bearbetning och analys av informationen i de fristående databaserna kommer att ha en funktion som innebär att beslut om behandling av känsliga personuppgifter måste dokumenteras.

I Säkerhetspolisens skriftliga rutiner för behandling av känsliga personuppgifter ges exempel på vad som utgör känsliga personuppgifter. Vidare anges hur bedömningen om det är absolut nödvändigt att komplettera med känsliga personuppgifter görs och exempel på under vilka omständigheter det kan vara tillåtet att behandla sådana uppgifter. Rutinerna beskriver även under vilka förutsättningar sökning med känsliga personuppgifter som sökbegrepp får ske.

Anställda får enligt Säkerhetspolisen genomgå utbildning i förutsättningarna för behandling av känsliga personuppgifter samt kunskapstest innan de får tillgång den granskade databasen. Loggning och logguppföljning sker regelbundet avseende användarnas aktiviteter i databasen, men uppföljningen är inte särskilt riktad mot behandlingen av känsliga personuppgifter.

Enligt uppgifter från Säkerhetspolisen innehåller den granskade databasen känsliga personuppgifter i relativt stor utsträckning. Främst rör det sig om uppgifter om politiska åsikter samt religiös eller filosofisk övertygelse. Samtliga granskade registreringar av personobjekt innehåller känsliga personuppgifter.

## **6 NÄMNDENS BEDÖMNING**

Av Säkerhetspolisens interna bestämmelser framgår att det inte behöver fattas något formellt beslut om att känsliga personuppgifter får behandlas i ett inledande skede. Säkerhetspolisen har dock uppgett att det nya IT-systemet för bearbetning och analys har en funktion som innebär att de tjänstemän som gör prövningen av om känsliga personuppgifter får registreras i den granskade databasen måste ange i IT-systemet om ett beslut om behandling av känsliga personuppgifter har fattats. Säkerhetspolisen bör därför uppdatera sina interna bestämmelser så det där tydligt framgår att dokumentation av sådana beslut ska ske.

Nämnden erinrar i detta sammanhang om den synpunkt som nämnden framförde i samrådsyttrande den 18 april 2013 över Säkerhetspolisens planerade IT-system för bearbetning och analys (dnr 17-2013). I yttrandet

uttalade nämnden bl.a. att den anser att Säkerhetspolisen ska införa rutiner och anta interna styrdokument för att säkerställa att en prövning enligt 2 kap. 10 § PDL, dvs. en prövning av om det är absolut nödvändigt för syftet med behandlingen att behandla den känsliga personuppgiften, görs så snart som möjligt efter det att en sådan uppgift läggs in i den del av det nya IT-systemet som innehåller så kallad obedd information. Den ståndpunkt som nämnden framförde i samrådsyttrandet gör sig alltså gällande. Detta bör också återspeglas i de interna bestämmelserna.

Säkerhetspolisen synes i övrigt ha goda rutiner för behandling av känsliga personuppgifter i de fristående databaserna. Nämnden bedömer också att Säkerhetspolisen vidtar adekvata utbildnings- och logguppföljningsinsatser för att säkerställa att reglerna om behandling av känsliga personuppgifter efterlevs. Nämnden vill dock betona vikten av riktad logguppföljning för att säkerställa att sökning på känsliga personuppgifter enbart görs när det är absolut nödvändigt.

Vid granskningen av personobjekt i den databas som omfattats av den aktuella tillsynen har det enligt nämndens bedömning inte framkommit något som tyder på att känsliga personuppgifter behandlas i strid med PDL.

---

Sändlista:

Säkerhetspolisen

Kopia för kännedom:

Datainspektionen