



**Säkerhetspolisens behandling av känsliga personuppgifter i ett system för
diarieföring m.m.**

1. SAMMANFATTNING

Säkerhets- och integritetsskyddsmyndigheten har granskat Säkerhetspolisens behandling av känsliga personuppgifter i myndighetens it-system för ärende- och dokumenthantering samt diarieföring.

Nämnden riktar kritik mot Säkerhetspolisens behandling av känsliga personuppgifter i it-systemet. I flera fall har uppgifter om personers etnicitet eller hälsotillstånd behandlats utan att det varit absolut nödvändigt för syftet med behandlingen. Behandlingen av känsliga personuppgifter har därmed skett i strid med polisdatalagen.

Nämnden noterar att Säkerhetspolisen har påbörjat ett arbete i syfte att minska risken för felaktig personuppgiftsbehandling i anteckningsfältet i it-systemet. Nämnden avser att följa upp vilka åtgärder som Säkerhetspolisen vidtar.

Innehåll

1. SAMMANFATTNING.....	1
2. BAKGRUND	3
2.1. Inledning	3
2.2. Rättsliga utgångspunkter.....	3
3. UTREDNINGEN	3
3.1. Om it-systemet för diarieföring m.m.	3
3.2. Genomförande.....	4
3.3. Nämndens iakttagelser	4
3.4. Säkerhetspolisens svar	5
4. NÄMNDENS BEDÖMNING	6
5. BESLUT	6

2. BAKGRUND

2.1. Inledning

Säkerhets- och integritetsskyddsmyndigheten beslutade den 14 juni 2016 att granska om känsliga personuppgifter behandlas i Säkerhetspolisens it-system för diarieföring av handlingar, och om behandlingen i så fall är förenlig med polisdatalagens (2010:361) (PDL) bestämmelser.

2.2. Rättsliga utgångspunkter

En grundläggande förutsättning för att Säkerhetspolisen ska få behandla personuppgifter enligt polisdatalagen är att de behövs i den brottsbekämpande verksamheten (6 kap. 1 § PDL). Behovet ska vara konkret och svara mot något av de ändamål som anges i paragrafen, exempelvis brott mot riket säkerhet (6 kap. 1 § 1 a PDL).

Säkerhetspolisen får även behandla personuppgifter om det är nödvändigt för diarieföring (6 kap. 3 § 1 PDL). När personuppgifter behandlas för diarieföringsändamål ska reglerna om gemensamt tillgängliga uppgifter inte tillämpas (6 kap. 8 § 2 PDL). Säkerhetspolisen är som huvudregel, i likhet med alla myndigheter, skyldig att registrera, dvs. diarieföra, allmänna handlingar som kommer in till eller upprättas vid myndigheten (5 kap. 1 § offentlighets- och sekretesslagen [2009:400]).

Uppgifter om en person får 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*) (6 kap. 4 § 4 och 2 kap. 10 § första stycket PDL).

Om uppgifter om en person behandlas på annan grund får de *kompletteras* med känsliga personuppgifter när det är *absolut nödvändigt* för syftet med behandlingen (6 kap. 4 § 4 och 2 kap. 10 § andra stycket PDL). Med hänsyn till den restriktivitet som ligger i begreppet ”absolut nödvändigt” måste behovet av att göra sådana kompletteringar prövas noga i varje enskilt fall.¹ Känsliga personuppgifter får också behandlas om det är nödvändigt för diarieföring (6 kap. 4 § 4, 2 kap. 9 § p. 1 och 2 kap. 10 § PDL).

3. UTREDNINGEN

3.1. Om it-systemet för diarieföring m.m.

Säkerhetspolisen har bl.a. uppgett följande.

¹ Prop. 2009/10:85 s. 325.

It-systemet används både som ett dokument- och ärendehanteringssystem och som myndighetens diarium. Det används i första hand för att lagra inkomna, upprättade och expedierade handlingar elektroniskt samt för att sprida informationen vidare internt och externt. För att analysera och bearbeta brottsbekämpande information används andra it-system. En stor del av den information som finns i it-systemet rör den brottsbekämpande verksamheten.

I it-systemet finns ett antal standardfält som gäller för alla ärenden och handlingar. Uppgifter om den enskilda handlingen finns i det s.k. handlingskortet. Där registreras uppgifter om datum för när handlingen kom in eller upprättades, diarienummer, uppgifter om handlingens avsändare eller mottagare samt i korthet vad handlingen rör, dvs. diarieföringsuppgifter.

I it-systemet finns även ett anteckningsfält där det är möjligt att föra in uppgifter om ärendet. Anteckningsfältet används för tjänsteanteckningar som rör ärendet, dokumentation av beslut om att känsliga personuppgifter får behandlas, kommunikation mellan befattningshavare vid olika avdelningar om ärendets handläggning samt för instruktioner till medarbetare.

3.2. Genomförande

Den 6 oktober 2016 genomfördes en inspektion vid Säkerhetspolisen. Vid inspektionen granskades behandlingen av känsliga personuppgifter som registrerats i handlingskort och anteckningsfält i it-systemet. Granskningen omfattade således inte själva dokumenten.

Vid inspektionen användes ord som kan utgöra känsliga personuppgifter om etnicitet och hälsotillstånd som sökbegrepp. Därefter granskades vissa personregistreringar närmare. Totalt granskades 19 registreringar innehållandes känsliga personuppgifter, varav 6 behandlades i handlingskort, och 13 i anteckningsfält.

Säkerhetspolisen har efter inspektionen skriftligen besvarat frågor med anledning av nämndens iakttagelser avseende nio granskade registreringar i anteckningsfälten. En sammanfattning av Säkerhetspolisens svar återges i avsnitt 3.4.

3.3. Nämndens iakttagelser

De granskade *handlingskort* innehöll diarieföringsuppgifter. I det fält där handlingen beskrivs fanns känsliga personuppgifter om etnicitet, t.ex. uppgift om att en handling rörde ett möte mellan befattningshavare vid Säkerhetspolisen och företrädare för en förening för en etnisk folkgrupp. I den diarieförda handlingen angavs att syftet med mötet var att inhämta

upplysningar inom ramen för Säkerhetspolisens arbete mot terrorism och brott mot rikets säkerhet.

De registreringar som granskades i *anteckningsfälten* utgjordes av tjänsteanteckningar, intern kommunikation inom Säkerhetspolisen samt information om ärendet. Registreringarna innehöll känsliga personuppgifter om etniskt ursprung och hälsotillstånd. Från granskningen noterades bl.a. följande.

Exempel 1 rörde en iakttagelse om en person som närmat sig ett skyddsobjekt. Personens etniska ursprung angavs. Uppgifterna behandlades för ändamålet personskydd.

Exempel 2 rörde sig om två personer som var misstänkta för brottslig verksamhet innefattande terrorbrott. De två personernas etnicitet angavs. Uppgifterna behandlades för ändamålet kontraterror.

Exempel 3 rörde en förfrågan från utländsk säkerhetstjänst. Befattningshavare vid Säkerhetspolisen diskuterade en namngiven person och dennes etnicitet angavs. Uppgifterna behandlades för ändamålet kontraterror.

Exempel 4 rörde en person som anmälts för olaga hot mot en grupp. Enligt uppgift hade denna person ”en sjukdomsbild”. Uppgifterna behandlades för ändamålet författningsskydd.

Exempel 5 rörde en person som kontaktat Säkerhetspolisen med anledning av mottagna hot av politisk eller religiös karaktär. Personen befann sig på ”psykakuten”. Uppgifterna behandlades för ändamålet kontraterror.

Det finns inte några särskilda rutinbeskrivningar för personuppgiftsbehandlingen i det aktuella it-systemet. Säkerhetspolisen har dock ett rutindokument som ska tillämpas vid all behandling av känsliga personuppgifter inom myndighetens brottsbekämpande verksamhet.

3.4. Säkerhetspolisens svar

Vad gäller exempel 1–5 har behandlingen av de känsliga personuppgifterna i anteckningsfälten inte varit absolut nödvändig för syftet med respektive behandling. Uppgifterna har därför raderats efter nämndens inspektion. Däremot är de känsliga personuppgifter som förekommer i exempel 2–4 absolut nödvändiga att behandla i andra sammanhang, t.ex. i andra it-system.

Säkerhetspolisen ser allvarligt på de felaktiga registreringarna. Felen har uppkommit trots att rutiner införts och omfattande utbildningsinsatser

genomförts på området. Vissa brister uppmärksammades i anteckningsfälten redan före nämndens granskning. Det pågår ett arbete i syfte att minska risken för den här typen av brister, inklusive hur anteckningsfältet ska användas, och för att se om det behövs förändringar i systemets tekniska utformning. I sammanhanget vill Säkerhetspolisen poängtera att det förekommer hundratusentals uppgifter i fälten i it-systemet och att det finns en risk att enskilda medarbetare kan göra fel.

Tillgången till uppgifterna i it-systemet styrs genom behörighetsgrupper. Mellan 56 och 709 personer har haft tillgång till de nio registreringar som nämnden ställt frågor om.

Efter nämndens inspektion har Säkerhetspolisen informerat om att det numera finns en text vid anteckningsfältet som uppmanar användaren att inte registrera känsliga personuppgifter i detta fält.

4. NÄMNDENS BEDÖMNING

Nämnden instämmer i Säkerhetspolisens bedömning att de känsliga personuppgifter som har behandlats i anteckningsfälten i exempel 1–5 inte har varit absolut nödvändiga för ändamålet med behandlingen. Uppgifterna om etnicitet och hälsotillstånd har därmed behandlats i strid med polisdatalagen i dessa fall. Avseende exempel 3 anser nämnden att det är särskilt allvarligt att den felaktiga registreringen har varit tillgänglig för över 700 personer vid Säkerhetspolisen.

Nämnden noterar att Säkerhetspolisen har påbörjat ett arbete i syfte att minska risken för felaktig personuppgiftsbehandling i anteckningsfältet i it-systemet. Nämnden avser att följa upp vilka åtgärder som Säkerhetspolisen vidtar.

Nämnden finner inte anledning att ifrågasätta behandlingen av de granskade registreringarna i handlingskorten eller de övriga åtta granskade registreringarna i anteckningsfälten.

5. BESLUT

Med detta uttalande avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Sigurd Heuman

I avgörandet har deltagit: Sigurd Heuman (ordförande), Barbro Thorblad, Cecilia Dalman Eek, Linnéa Darell, Berit Jóhannesson, Christina Linderholm, Ewa Samuelsson, Mats Sander och Jonas Åkerlund (enhälligt).

Föredragande: Ylva Marsh

Expedition till:
Säkerhetspolisen (dnr 2016-12016)

Kopia för kännedom till:
Datainspektionen