SÄKERHETS- OCH
INTEGRITETSSKYDDSNÄMNDEN

Uttalande

2013-11-15 Dnr 151-2012

Tillgången till personuppgifter i Säkerhetspolisens uppgiftssamlingar

1 SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat tillgången till personuppgifter i Säkerhetspolisens uppgiftssamlingar. Granskningen har omfattat Säkerhetspolisens interna styrdokument avseende tillgång till personuppgifter i centralregistret och fristående databaser. Säkerhetspolisen har i samband med inspektion utförd av nämndens kansli besvarat ett antal frågor om behörighet och logguppföljning avseende centralregistret och en fristående databas.

Nämnden bedömer att de granskade styrdokumenten är ändamålsenligt utformade. Nämnden anser dock att vissa rutiner avseende centralregistret bör fastställas i interna styrdokument.

Nämnden bedömer vidare att Säkerhetspolisens utbildnings- och logguppföljningsinsatser är tillfredsställande när det gäller att säkerställa att tjänstemännen använder centralregistret och den granskade fristående databasen enbart när de har behov av det i sin tjänst. Nämnden vill dock betona vikten av riktad logguppföljning för att tillförsäkra att behörigheten att söka på känsliga personuppgifter används uteslutande i tjänsten och när förutsättningarna för att få göra sådana sökningar är uppfyllda i övrigt.

Slutligen anser nämnden att åtkomsten till känsliga personuppgifter som ännu inte prövats enligt 2 kap. 10 § polisdatalagen (2010:361) (PDL) bör begränsas till ett absolut minimum. Detta bör återspeglas i de interna bestämmelserna avseende de fristående databaserna.

Postadress Box 22523, 104 22 Stockholm
Telefon 08-617 98 00
E-post sakint@sakint.se
Organisationsnummer 202100-5703
Besöksadress Norr Mälarstrand 6, Stockholm
Telefax 08-617 98 88
Webbplats www.sakint.se
Bankgiro 782-4329

2 BAKGRUND OCH AVGRÄNSNING

2.1 Säkerhetspolisens uppgiftssamlingar

Centralregistret är den databas som huvudsakligen används i Säkerhetspolisens verksamhet och utgör ett spaningsregister för att bl.a. förebygga och avslöja brott mot rikets säkerhet och för att bekämpa terrorism. Databasen innehåller bl.a. uppgifter om personer mot vilka det föreligger misstankar om brottslig verksamhet, som inte behöver vara preciserade till vissa konkreta brott, och uppgifter om personer som har samband med någon som antecknats på grund av en misstanke.

En fristående databas är en uppgiftssamling som förs vid sidan av centralregistret. Fristående databaser används av Säkerhetspolisen för att bearbeta och bedöma information i syfte att avgöra om informationen ska tillföras centralregistret.

2.2 Vikten av att begränsa tillgången till personuppgifter

PDL:s krav på att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter är av central betydelse från integritetssynpunkt. I förarbetena betonas därför vikten av att polisen organiserar sin verksamhet på ett sådant sätt att obefogad spridning av personuppgifter motverkas.[1]

Säkerhetspolisen behandlar stora mängder information som är samlad på ett sådant sätt att uppgifter enkelt är sökbara elektroniskt. Informationen är ofta av känslig karaktär från ett integritetsperspektiv. Utformningen av behörigheter utifrån vad tjänstemannen behöver för att kunna fullgöra sina arbetsuppgifter blir därmed ett viktigt verktyg för att upprätthålla integritetsskyddet vid Säkerhetspolisens behandling av personuppgifter enligt PDL.

2.3 Avgränsning

Nämnden beslutade den 4 september 2012 att granska tillgången till personuppgifter i Säkerhetspolisens uppgiftssamlingar. Granskningen har avsett interna styrdokument och rutiner och har begränsats till centralregistret och en fristående databas.

3 RÄTTSLIGA UTGÅNGSPUNKTER

Enligt 2 kap. 11 § PDL, som enligt 5 kap. 4 § PDL är tillämplig även vid behandling av personuppgifter hos Säkerhetspolisen, ska tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter. Bestämmelsen riktar sig till dem som deltar i polisens dagliga verksamhet, till dem som ansvarar för utformningen av

[1] Prop 2009/10:85 s. 94.

nya datasystem liksom till dem som avgör vilken tillgång till personuppgifter respektive tjänsteman behöver.[2] I förarbetena betonas att det åligger polisen att följa upp att lagstiftningen tillämpas med respekt för enskildas integritet samt att PDL ställer högre krav än tidigare på att polisen genom tekniska åtgärder begränsar den enskilde tjänstemannens tillgång till information. Loggning nämns som ett sätt för polisen att kontrollera att varje användare bara får del av den information han eller hon behöver för sitt arbete. Vidare framhålls vikten av att polisen noga kontrollerar och följer upp tilldelningen av behörigheter.[3]

I 2 kap. 1 och 2 §§ PDL föreskrivs att 31 § personuppgiftslagen (1998:204) gäller för polisens personuppgiftsbehandling enligt PDL. Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Bestämmelserna ska enligt 5 kap. 4 § PDL även tillämpas vid behandling av personuppgifter hos Säkerhetspolisen.

I 5 kap. 5 § första stycket PDL föreskrivs att Säkerhetspolisen är personuppgiftsansvarig för den behandling som Säkerhetspolisen utför.

Enligt 4 § polisdataförordningen (2010:1155) ansvarar Säkerhetspolisen för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst av personuppgifter i den egna verksamheten. Av 3 § polisdataförordningen framgår att Rikspolisstyrelsen får meddela närmare föreskrifter om tillgången till personuppgifter för personer som är verksamma inom polisväsendet.

Rikspolisstyrelsen har utfärdat föreskrifter om säkerhet vid Polisens informationsbehandling med stöd av IT (RPSFS 2009:4, FAP 174-1) och föreskrifter och allmänna råd om användningen av IT-system inom Polisen (RPSFS 2005:8, FAP 170:1), vilka bl.a. reglerar behörighet och loggning.

4 GRANSKNINGEN

Nämnden har efter tagit del av interna styrdokument avseende tillgången till personuppgifter i Säkerhetspolisens uppgiftssamlingar. Nämndens kansli har därefter ställt skriftliga frågor som besvarats av ansvariga befattningshavare i samband med två inspektioner. Vid inspektionerna har företrädare för Säkerhetspolisen gett en beskrivning av personuppgiftsbehandlingen, särskilt avseende behörighet och

[2] A. prop. s. 326.
[3] A. prop. s. 270 f.

logguppföljning kopplad till centralregistret och den granskade fristående databasen.

5 NÄMNDENS IAKTTAGELSER

5.1 Tillgången till uppgifter i centralregistret

På Säkerhetspolisens intranät anges vilka typer av behörigheter som användare kan få i centralregistret och vad varje behörighetstyp innebär. Därutöver anges bl.a. att den som i sitt arbete har behov av att göra slagningar i centralregistret kan få behörighet efter att ha genomgått den behörighetsgrundande centralregisterutbildningen. Vidare framgår där att den som vill genomgå utbildningen ska kontakta sin enhetschef, som utfärdar ett intyg på att medarbetaren behöver utbildning om centralregistret samt att enhetschefen ansvarar för att samtliga på enheten har korrekt behörighet inom centralregistret och använder centralregistret uteslutande i sin tjänst.

Säkerhetspolisen har uppgett att en särskild befattningshavare beslutar om medarbetaren ska få tillgång till centralregistret. Vid beslutet överväger befattningshavaren om behörigheten är rimlig i förhållande till personens arbetsuppgifter. Befattningshavaren kontrollerar även om den som beslutet avser har genomgått centralregisterutbildning och blivit certifierad. En person kan få certifiering efter att ha klarat ett kunskapstest om hur centralregistret får användas inklusive bestämmelserna om tillgång till personuppgifter.

Enligt Säkerhetspolisen kan en anställd som inte har nödvändig behörighet till centralregistret begära extrahering (utdrag) av uppgifter från centralregistret. Begäran om extrahering av uppgifter prövas av särskilt utpekade personer.

Säkerhetspolisen har vidare uppgett att behörigheter till centralregistret omprövas var sjätte månad och när en anställd byter tjänst eller arbetsuppgift. Vid omprövningen var sjätte månad tas behörigheten bort för de användare som inte har använt sina behörigheter under de senaste sex månaderna.

Säkerhetspolisen har också uppgett att logguppföljning sker regelbundet genom stickprovskontroller avseende användarnas aktiviteter i centralregistret, men att uppföljningen inte är särskilt riktad mot behandling av känsliga personuppgifter.

5.2 Tillgången till uppgifter i fristående databaser

I Säkerhetspolisens interna styrdokument regleras tilldelning, förändring, borttagning och uppföljning av behörigheter i fristående databaser. Enligt styrdokumenten tilldelas behörighet endast den som har adekvat utbildning för begärd behörighetsnivå och har genomgått certifiering samt har ett belagt behov av den begärda behörigheten för att utföra sina arbetsuppgifter. En medarbetare kan bli certifierad efter att ha klarat ett kunskapstest.

Enligt Säkerhetspolisens interna styrdokument är behörigheter till fristående databaser behovsbaserade och ska omprövas minst en gång per halvår eller vid annat tillfälle som viss angiven beslutsfattare bestämmer. Om en medarbetare har varit inaktiv i fristående databaser de senaste sex månaderna ska behörigheten upphöra och tas bort. Om en medarbetare inte längre har behov av tilldelad behörighet för att utföra sina arbetsuppgifter, exempelvis till följd av byte eller ändring av tjänst, ska borttagning av behörigheten ske. Vidare framgår av rutinbeskrivningen att medarbetaren ansvarar för att meddela om behov av befintlig tilldelning inte längre finns.

Säkerhetspolisen har uppgett att logguppföljning sker regelbundet avseende användarnas aktiviteter i den granskade fristående databasen, men uppföljningen är inte särskilt riktad mot behandling av känsliga personuppgifter.

6 NÄMNDENS BEDÖMNING

Nämnden bedömer att de granskade interna styrdokumenten är ändamålsenligt utformade. Nämnden anser dock att de rutiner avseende behörighet till centralregistret som framgår av Säkerhetspolisens intranät och av Säkerhetspolisens muntliga uppgifter också bör framgå av något mer formaliserat internt styrdokument.

Säkerhetspolisens utbildnings- och logguppföljningsinsatser är enligt nämnden tillfredsställande när det gäller att säkerställa att tjänstemännen använder centralregistret och den granskade fristående databasen enbart när de har behov av det för sin tjänst. Nämnden vill dock betona vikten av riktad logguppföljning för att tillförsäkra att behörigheten att söka på känsliga personuppgifter används uteslutande i tjänsten och när förutsättningarna för att få göra sådana sökningar är uppfyllda i övrigt.

Nämnden erinrar om den synpunkt som nämnden framförde i samrådsyttrandet den 18 april 2013 över Säkerhetspolisens planerade IT-system för bearbetning och analys (dnr 17-2013). I yttrandet uttalade nämnden bl.a. att åtkomsten till känsliga personuppgifter som ännu inte prövats enligt 2 kap. 10 § PDL bör

begränsas till ett absolut minimum. Den ståndpunkt som nämnden framförde i samrådsyttrandet gäller alltjämt. Nämndens ståndpunkt bör också återspeglas i de interna bestämmelserna avseende de fristående databaserna.

_____

Sändlista:
Säkerhetspolisen

Kopia för kännedom:
Datainspektionen