SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Uttalande med beslut

2017-10-18 Dnr 65-2017

Bevarande av personuppgifter i Säkerhetspolisens dokument- och ärendehanteringssystem

1. SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat Säkerhetspolisens rutiner för bevarande av personuppgifter i myndighetens dokument- och ärendehanteringssystem (Systemet). Systemet används för att elektroniskt lagra, upprätta och dela allmänna handlingar. Det används bl.a. inom underrättelseverksamheten. Nämnden har också granskat vilka inom Säkerhetspolisen som ges tillgång till uppgifterna i Systemet.

Granskningen har visat att användare som har tillgång till uppgifter i Säkerhetspolisens underrättelsesystem i många fall automatiskt även får tillgång till de originalhandlingar i Systemet från vilka uppgifterna är hämtade. Det innebär att känsliga personuppgifter som bedömts inte vara tillåtna att behandla i underrättelsesystemen, och som har maskerats eller utelämnats i dessa, ändå kan läsas i Systemet av stora grupper av användare inom underrättelseverksamheten.

Säkerhetspolisens förklaring till denna ordning är att uppgifter i underrättelsesystemen måste kunna kvalitetssäkras. När det gäller sådana känsliga personuppgifter som har bedömts vara otillåtna att behandla i underrättelsesystemen är det angeläget att tillgången till uppgifterna begränsas till de användare som har ett verkligt behov av att kunna kvalitetssäkra dessa. Det är också viktigt att Säkerhetspolisen kontinuerligt kontrollerar att begränsningen iakttas.

Nämnden konstaterar också att Säkerhetspolisen bör införa rutiner så att personuppgifter i systemet inte fortsätter att vara tillgängliga i den brottsbekämpande verksamheten när de inte längre behövs där.

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

Innehåll

2. BAKGRUND

2.1. Syftet med granskningen

Säkerhetspolisens dokument- och ärendehanteringssystem (nedan kallat Systemet) innehåller ett stort antal personuppgifter. Många av dessa uppgifter är av särskilt integritetskänslig karaktär. Nämnden har tidigare kritiserat Säkerhetspolisens behandling av känsliga personuppgifter i Systemet.[1]

Den 29 mars 2017 beslutade Säkerhets- och integritetsskyddsnämnden att granska om Säkerhetspolisens rutiner för bevarande av personuppgifter i Systemet är förenliga med polisdatalagen (2010:361) (PDL) och polisdataförordningen (2010:1155) (PDF). Nämndens granskning har avsett sådan behandling av personuppgifter som sker i underrättelseverksamheten (6 kap. 1 § 1 PDL).

Frågan om hur personuppgifter bevaras i Systemet är nära sammankopplad med frågan om vilka inom Säkerhetspolisen som ges tillgång till uppgifterna. Även Säkerhetspolisens rutiner i denna del har granskats.

2.2. Rättsliga utgångspunkter

För behandlingen av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet gäller polisdatalagen. En grundläggande förutsättning för att personuppgifter ska få behandlas 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 att förebygga, förhindra eller upptäcka terrorbrott. Personuppgifter som behandlas med stöd av 6 kap. 1 § polisdatalagen får i många fall även behandlas för att tillhandahålla information till andra (6 kap. 2 § PDL).

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 det enskilda ärendet.[2]

---

[1] Se nämndens uttalande den 16 februari 2017 *Säkerhetspolisens behandling av känsliga personuppgifter i ett system för diarieföring m.m.* (dnr 143-2016).
[2] Prop. 2009/10:85 s. 325.

Personuppgifter får behandlas om det är nödvändigt för diarieföring, eller om uppgifterna har lämnats till Säkerhetspolisen i en anmälan eller liknande och behandlingen är nödvändig för handläggningen (6 kap. 3 § PDL). Att behandlingen ska vara nödvändig för handläggningen kan i ett enskilt fall innebära att personuppgifter i ett e-postmeddelande inte får behandlas på annat sätt än att uppgifterna tas emot och därefter omedelbart arkiveras eller gallras. I ett annat fall kan det innebära att personuppgifterna också får behandlas i samband med att framställan besvaras. Det är således inte möjligt för Säkerhetspolisen att med stöd av den bestämmelsen behandla uppgifter i en brottsutredning eller i underrättelseverksamhet. Sådan behandling förutsätts i stället ha stöd i bestämmelserna i 6 kap. 1-2 §§ polisdatalagen.[3]

Personuppgifter får inte bevaras under längre tid än vad som behövs för ändamålen med behandlingen (6 kap. 6 § PDL). Det finns också vissa tidsfrister som anger när uppgifterna senast ska gallras (6 kap. 7 och 12 §§ PDL). Riksarkivet får meddela föreskrifter om att uppgifter som ska gallras enligt dessa bestämmelser får bevaras för historiska, statistiska eller vetenskapliga ändamål (6 kap. 7 § tredje stycket och 14 § PDL samt 27 § PDF). I RA-MS 2015:61 har Riksarkivet meddelat föreskrifter om att handlingar och uppgifter i Systemet, med några få undantag, får bevaras för sådana ändamål. Uppgifterna får då arkiveras digitalt.[4] Vid digital arkivering ska uppgifterna avskiljas från Säkerhetspolisens brottsbekämpande verksamhet (19 § PDF).

Tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (6 kap. 4 § 5 och 2 kap. 11 § PDL).

3. UTREDNINGEN

3.1. Genomförande

Säkerhetspolisen har skriftligen besvarat frågor om myndighetens bevarande av – och tillgång till – personuppgifter i Systemet. En sammanfattning av Säkerhetspolisens svar återges i avsnitt 3.2. Av sekretesskäl har vissa detaljer utelämnats. Nämnden har även tagit del av ett antal av Säkerhetspolisens interna styrdokument som rör behandling av personuppgifter i Systemet.

3.2. Säkerhetspolisens svar

Säkerhetspolisen har bl.a. uppgett följande.

---

[3] Prop. 2009/10:85 s. 112, 259, 324 och 366.
[4] Prop. 2009/10:85 s. 212.

Systemet används i flera olika syften

Systemet används i full drift sedan år 2012 för att elektroniskt lagra, upprätta och dela allmänna handlingar. Det utgör även Säkerhetspolisens diarium. I systemet behandlas personuppgifter i inkomna och upprättade allmänna handlingar samt i arbetsdokument som ännu inte är upprättade. Behörigheter till uppgifter i Systemet tilldelas ofta grupper av användare som behöver tillgång till personuppgifterna för att kunna fullgöra sina arbetsuppgifter. Behörigheterna ger dem vanligen rätt att ta del av samtliga uppgifter i ett ärende.

Behandlingen i Systemet syftar i första hand till att uppfylla förvaltningsrättsliga krav på effektiv och spårbar handläggning samt diarieföring och hantering av allmänna handlingar. De allmänna handlingarna i Systemet är därför i original och Säkerhetspolisen ändrar inte på något sätt i dessa. Behandlingen i Systemet sker också till viss del inom ramen för den brottsbekämpande verksamheten.

När brottsbekämpande information ska analyseras, bearbetas och spridas använder Säkerhetspolisen främst centralregistret och it-systemet för bearbetning och analys av information (nedan kallade underrättelsesystemen). Också uppgifter i Systemet behandlas i underrättelseverksamheten. Det är nämligen endast ett urval av uppgifter som registreras i underrättelsesystemen och ibland behöver användarna ta del av originalhandlingarna som finns i Systemet. Syftet är att få en bättre bild av sammanhanget eller försäkra sig om att information inte har förvanskats eller missförståtts. De användare som har tillgång till uppgifter i underrättelsesystemen har därför i många fall även automatisk tillgång till de handlingar i Systemet som uppgifterna kommer ifrån.

Om en uppgift har registrerats i it-systemet för bearbetning och analys har i princip alla användare som arbetar inom det aktuella verksamhetsområdet tillgång till originalhandlingen i Systemet. Om en uppgift har registrerats i centralregistret har samtliga användare av det registret – dvs. i princip alla som arbetar i den operativa verksamheten – tillgång till den aktuella handlingen i Systemet, i vart fall efter det att ärendet avslutats i Systemet. De kan då direkt få tillgång till handlingen genom en länk från centralregistret.

Behandling av uppgifter sker för olika ändamål

Den som har behörighet att ta del av en handling i Systemet kan även ta del av sådana personuppgifter som har maskerats eller utelämnats i underrättelsesystemen på grund av att uppgifterna inte får behandlas där, t.ex. känsliga personuppgifter. Säkerhetspolisen bedömer dock att detta är förenligt med polisdatalagen. Skälet till detta är att personuppgifterna i

underrättelsesystemen och i Systemet behandlas för olika preciserade ändamål. Som nämnts ovan behandlas uppgifter i Systemet dels för att uppfylla vissa förvaltningsrättsliga krav, dels för ändamål som faller inom ramen för Säkerhetspolisens brottsbekämpande verksamhet. När en användare tar del av den bakomliggande handlingen till en registrering i underrättelsesystemen gör han eller hon det för det preciserade ändamålet att försäkra sig om att informationen i underrättelsesystemen inte har förvanskats, missförståtts eller för att få en bättre bild av sammanhanget (kvalitetsgranskning). Detta är särskilt viktigt inför att Säkerhetspolisen ska delge information utanför myndigheten eller vidta annan operativ åtgärd med anledning av den registrerade underrättelseinformationen. Utan möjlighet att kunna kvalitetssäkra informationen inför sådana beslut finns en konkret risk att Säkerhetspolisen vidtar obefogade åtgärder som kan få långtgående negativa konsekvenser för den enskilde och för Säkerhetspolisens eller andra nationella eller internationella myndigheters operativa verksamhet. Därutöver finns en påtaglig risk att bedömningen av uppgiftslämnarens trovärdighet och uppgifternas riktighet i sak blir felaktig.

Säkerhetspolisen har funnit att åtkomsten till handlingar i Systemet medför vissa risker för den enskildes integritet. Därför finns vissa begränsningar i Systemet. Det är t.ex. inte möjligt att söka efter uppgifter i handlingar. Vad gäller handlingar som upprättas vid Säkerhetspolisen finns det manualer och handböcker som syftar till att säkerställa att personuppgifter behandlas i enlighet med polisdatalagen. Varje åtgärd i systemet loggas på ett detaljerat sätt och det genomförs ändamålsenliga logguppföljningar.

Gallring och avställning för arkivering

I vissa situationer gallras uppgifter i Systemet genom att raderas. Som huvudregel avställs emellertid uppgifterna för arkivering i enlighet med 19 § polisdataförordningen och bevaras med stöd av Riksarkivets föreskrift RA-MS 2015:61. När uppgifter i Systemet avställs för arkivering tas tillgången till uppgifterna bort för alla utom huvudregistrator, samtidigt som en behörighetsgrupp för arkivarier läggs till. Arbete pågår med att utveckla ett separat e-arkiv till vilket alla uppgifter som är avställda för arkivering ska föras. Avställning för arkivering kan bara ske på ärendenivå. Det är dock möjligt att begränsa tillgången till enskilda handlingar i systemet utan att detta är att betrakta som avställning.

Ärenden i Systemet, som innehåller uppgifter som också har registrerats i centralregistret, avställs automatiskt för arkivering i samband med att uppgifterna gallras i centralregistret. I övrigt finns det inga särskilda arbetsrutiner för att se till att uppgifter i Systemet avställs. Det finns inte heller några arbetsrutiner för att ta bort tillgången till uppgifter i ärenden som inte har

avställts. Att ett ärende avslutas i Systemet medför inte automatiskt att uppgifterna avställs eller att tillgången till uppgifterna begränsas.

De flesta uppgifterna i Systemet ska gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Systemet har dock varit i full drift endast i cirka fem år. För vissa särskilda uppgifter gäller andra frister.

Utveckling av systemet

Systemet är inte i sig anpassat till de krav som polisdatalagen eller Säkerhetspolisens verksamhet ställer. Sedan Systemet togs i drift har Säkerhetspolisen därför stegvis utvecklat och anpassat det. I Systemet står hanteringen av allmänna handlingar i fokus. Alla allmänna handlingar registreras i ärenden. Det kan leda till problem med tillämpningen av polisdatalagen, som utgår ifrån att enskilda personuppgifter ska kunna gallras oavsett i vilket sammanhang de förekommer. För närvarande pågår emellertid flera lagstiftningsprojekt som kan komma att förändra villkoren för behandlingen. Säkerhetspolisen har därför valt att avvakta med mer omfattande utvecklingsprojekt avseende systemet till dess att förutsättningarna för den framtida behandlingen av personuppgifter har klargjorts.

4. NÄMNDENS BEDÖMNING

I Systemet behandlas personuppgifter i flera olika syften, däribland att diarieföra och elektroniskt lagra allmänna handlingar. Systemet används i både den brottsbekämpande och den administrativa verksamheten. I ett sådant system är det viktigt att kunna särskilja för vilket ändamål en viss behandling sker. Att personuppgifter får behandlas för att uppfylla krav på registrering och bevarande av allmänna handlingar innebär, som redan nämnts, inte att uppgifterna utan vidare får behandlas i brottsbekämpande syfte.

När personuppgifter i Systemet behandlas i underrättelseverksamheten måste behandlingen ha stöd i 6 kap. 1 § 1 polisdatalagen. Det är alltså bara personuppgifter som behövs för något av de syften som anges i den bestämmelsen som får behandlas. Känsliga personuppgifter får behandlas endast om det är absolut nödvändigt för syftet med behandlingen.

Eftersom nämndens tillsyn särskilt ska avse behandling av känsliga personuppgifter så koncentrerar nämnden sin prövning nedan till just sådan behandling.[5]

[5] Se 1 § andra stycket lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet.

När uppgifter från Systemet ska registreras i underrättelsesystemen gör Säkerhetspolisen en prövning av vilka känsliga personuppgifter som får behandlas där.[6] Sådana uppgifter som inte bedöms vara absolut nödvändiga för syftet med behandlingen registreras inte i underrättelsesystemen. Att en användare har tillgång till uppgifter i underrättelsesystemen medför emellertid i många fall att denne automatiskt får tillgång till de originalhandlingar i Systemet från vilka uppgifterna är hämtade. Det får till följd att de känsliga personuppgifter som bedömts inte vara tillåtna att behandla i underrättelsesystemen, och som har maskerats eller utelämnats i dessa, ändå kan läsas i Systemet av stora grupper av användare inom underrättelseverksamheten. Enligt nämndens mening innebär en sådan ordning en risk för att känsliga personuppgifter behandlas även när det inte är absolut nödvändigt för syftet med behandlingen.

Säkerhetspolisens förklaring till denna ordning är att uppgifter i underrättelsesystemen måste kunna kvalitetssäkras. Nämnden har förståelse för att vissa användare i underrättelseverksamheten har behov av att kunna ta del av originalhandlingar i kvalitetssäkringssyfte. När det gäller sådana känsliga personuppgifter som har bedömts vara otillåtna att behandla i underrättelsesystemen är det angeläget att tillgången till uppgifterna begränsas till de användare som har ett verkligt behov av att kunna kvalitetssäkra dessa. Det är också viktigt att Säkerhetspolisen kontinuerligt kontrollerar att begränsningen iakttas.

Säkerhetspolisen har redogjort för i vilka situationer myndigheten gallrar personuppgifter i Systemet genom radering och i vilka situationer uppgifterna istället avställs för arkivering i enlighet med 19 § polisdataförordningen. Säkerhetspolisen har vidare uppgett att den yttersta gallringfristen inte har inträtt för flertalet av de personuppgifter som behandlas i den brottsbekämpande verksamheten. Nämnden vill erinra om att uppgifter inte får behandlas under längre tid än vad som behövs för ändamålet med behandlingen (6 kap. 6 § första stycket PDL). Säkerhetspolisen bör därför införa rutiner så att personuppgifter i Systemet inte är tillgängliga i den brottsbekämpande verksamheten när de inte längre behövs i där.

Vad som förekommit i övrigt ger inte anledning till något uttalande från nämndens sida.

5. BESLUT

Med detta uttalande avslutas ärendet.

---

[6] Se t.ex. nämndens uttalande den 14 juni 2017 *Säkerhetspolisens behandling av känsliga personuppgifter i ett it-system för bearbetning och analys av information* (dnr 179-2016).

På Säkerhets- och integritetsskyddsnämndens vägnar

Sigurd Heuman

I avgörandet har deltagit: Sigurd Heuman (ordförande), Barbro Thorblad, Berit Jóhannesson, Zayera Khan, Christina Linderholm, Ewa Samuelsson, Mats Sander och Jonas Åkerlund (enhälligt).

Föredragande: Karin Tollbäck

Expedition till:
Säkerhetspolisen (dnr 2017-8254)

Kopia för kännedom till:
Datainspektionen