SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Uttalande med beslut

2016-06-14 Dnr 112-2015

Loggning och logguppföljning i Polismyndighetens säkerhetslogg

1. SAMMANFATTNING

Säkerhets- och integritetsskyddnämnden har granskat hur Polismyndigheten genomför loggning och logguppföljning i centrala säkerhetsloggen (CSL).

Nämnden konstaterar att CSL är ett viktigt verktyg som ger Polismyndigheten förutsättningar att i anslutna system kontrollera att personuppgiftsbehandlingen sker lagenligt. CSL ger alltså Polismyndigheten möjlighet att upprätthålla det integritetsskydd som föreskrivs i polisdatalagen.

Nämnden är dock starkt kritisk till att Polismyndighetens användning av logguppföljning i CSL fortfarande sker i begränsad omfattning. För att CSL ska utgöra det integritetsskydd som förutsattes vid lagens tillkomst måste loggutvärdering ske frekvent och göras såväl förebyggande som reaktivt. Polismyndigheten bör även överväga att införa fler automatgenererade larm, t.ex. vad gäller användning av känsliga personuppgifter som sökbegrepp.

Nämnden påtalar återigen behovet av ett förtydligande av lagstiftningen med avseende på förbudet att använda känsliga personuppgifter som sökbegrepp.

Polismyndigheten anmodas att senast den 31 januari 2017 till nämnden redovisa vilka åtgärder som har vidtagits för att få till stånd fler och tätare stickprovskontroller.

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

Polismyndigheten har utvecklat CSL för att förbättra den tekniska kontrollen över myndighetens egna it-användning. CSL samlar in, analyserar och arkiverar behandlingshistorik (loggar) från flera av polisens centrala it-system. Syftet med CSL är dels att skydda den personliga integriteten, dels att skydda den information som polisen behandlar mot otillåten behandling och angrepp.[1]

Tanken är att CSL ska logga all behandling som sker i Polismyndighetens it-system. Genom automatisk analys av inkomna loggar ska Polismyndigheten kunna följa upp och kontrollera dataanvändningen på ett mer systematiskt sätt. Systemet ska slå larm vid felaktig eller obehörig hantering, t.ex. obehörig inloggning.[2]

Nämnden har tidigare granskat Polismyndighetens användning av CSL. Då kontrollerades beställningar av loggutdrag från CSL som gjorts under vissa särskilt angivna perioder under åren 2012 och 2013[3]. Av granskningarna framgick att flertalet dåvarande polismyndigheter inte hade gjort någon logguppföljning alls för de it-system som var anslutna till CSL under den granskade perioden, och att logguppföljningen hade varit av mycket begränsad omfattning hos de övriga polismyndigheterna. De flesta beställningarna skedde på förekommen anledning, dvs. var reaktioner på misstänkt otillåtna slagningar och avsåg förfluten tid. Nämnden ansåg att polismyndigheterna skulle utnyttja möjligheten att begära loggutdrag från CSL i större utsträckning än vad som gjordes för att upprätthålla det integritetsskydd som föreskrivs i polisdatalagen.

3. RÄTTSLIGA UTGÅNGSPUNKTER

Polismyndigheten ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas (2 kap. 2 § första stycket 7 polisdatalagen [2010:361] [PDL] och 31 § personuppgiftslagen [1998:204] [PUL]).

Tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (2 kap. 11 § PDL). Bestämmelsen riktar sig till dem som deltar i polisens dagliga verksamhet, till dem som ansvarar för utformningen av nya datasystem liksom till dem som avgör vilken tillgång till personuppgifter respektive tjänsteman behöver. I förarbetena

---

[1] Prop. 2009/10:85 s. 271.
[2] A. prop. s. 271.
[3] Se nämndens uttalanden från den 4 september 2012 ”Granskning av polismyndigheternas användning av centrala säkerhetsloggen” (dnr 117-2012), och från den 15 november 2013 ”Uppföljning av polismyndigheternas användning av centrala säkerhetsloggen” (dnr 83-2013).

betonas att det åligger polisen att följa upp att lagstiftningen tillämpas med respekt för enskildas integritet samt att polisen genom tekniska åtgärder begränsar den enskilde tjänstemannens tillgång till information. Loggning nämns som ett sätt för polisen att försäkra sig om att varje användare bara får del av den information han eller hon behöver.[4]

Uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv får inte användas som sökbegrepp vid sökning i personuppgifter som har gjorts gemensamt tillgängliga, dvs. är tillgängliga för mer än ett fåtal personer (3 kap. 5 § första stycket PDL).

I Rikspolisstyrelsens (RPS) föreskrifter om säkerhet vid Polisens informationsbehandling med stöd av IT (RPSFS 2009:4, FAP 174-1)[5] finns bestämmelser om behörighetskontroll och loggning. Av föreskrifterna framgår bl.a. att myndigheten ska se till att loggar följs upp och vid behov analyseras.

Av föreskrifterna framgår vidare att loggning ska ske av varje åtkomst till och aktiviteter i it-system som är avsedda för behandling av särskilt skyddsvärda uppgifter. Användaraktiviteter som kan tolkas som försök till intrång eller brott mot behörighetsregler ska registreras i logg samt kunna generera larm.

4. UTREDNINGEN

4.1. Syfte

Granskningen har syftat till att kontrollera hur Polismyndigheten genomför loggning och logguppföljning i CSL. Frågor som har stått i fokus för nämndens granskning har varit följande.

- Vilka av Polismyndighetens it-system är anslutna till CSL?
- Hur är ansvaret för loggning och logguppföljning fördelat inom Polismyndigheten?
- Hur ser rutinerna ut för loggning och logguppföljning i CSL?
- Vilken information kan utläsas ur en logg?
- Hur ser rutinerna ut när det gäller bevarande av loggar från CSL?

4.2. Genomförande

Polismyndigheten har besvarat ett antal frågor rörande loggning och logguppföljning i CSL. Granskningen har således inte utförts på samma sätt

[4] Prop. 2009/10:85 s. 271.
[5] De föreskrifter och allmänna råd som Rikspolisstyrelsen utfärdat fortsätter att gälla även efter den 1 januari 2015, fram till dess att de upphävs.

som vid tidigare granskningar, där beställningar av loggutdrag från utvalda tidsperioder kontrollerades.

Polismyndigheten har även förevisat avidentifierade loggutdrag ur CSL från bl.a. systemet Surfa2. Nämnden har i anslutning till detta inhämtat ytterligare information.

Nämnden har slutligen tagit del av olika dokument och handlingar som rör loggning och logguppföljning, däribland en kravspecifikation för CSL och en intern rutinbeskrivning avseende beställning av loggutdrag.

4.3. Polismyndighetens svar

Polismyndigheten har sammanfattningsvis anfört följande.

It-system anslutna till CSL
För närvarande är 24 it-system, i vilka det sker personuppgiftsbehandling som regleras av polisdatalagen, anslutna till CSL. Anslutna system är bl.a. DurTvå (datoriserad utredningsrutin med tvångsmedelshantering), KUR (kriminalunderrättelseregistret), Obs-portalen (it-stöd för att internt sprida operativ brotts- och underrättelseinformation), RAR (rationell anmälningsrutin) och Surfa2 (särskild utredning, registrering, förundersökning, analys).

Ambitionen är att alla nya system, såväl de som köps in externt som de som skapas internt, ska anslutas till CSL, om det efter en bedömning anses nödvändigt. Även befintliga system och den s.k. mappstrukturen ska framöver anslutas till CSL så långt det tekniskt är möjligt.

Ansvarsfördelning
Av arbetsordningen för Polismyndigheten[6] framgår vilka befattningar som har behörighet att besluta om eller begära loggutdrag. Det är personuppgiftsombud, chefen för en avdelning, chefen för en polisregion eller av denne utsedd regional verksamhetsskyddschef samt verksamhetsskyddschefen vid rikspolischefens kansli som har denna behörighet. Beställningar av loggutdrag kommer framförallt från avdelningen för Särskilda utredningar och verksamhetsskyddsenheterna.

Rutiner för logguppföljning
Det finns för närvarande inga riktlinjer som reglerar när och på vems initiativ logguppföljning ska ske. Arbete pågår med att ta fram riktlinjer avseende personuppgiftsbehandling och registervård. Dessa riktlinjer kommer att

[6] PM 2015:39.

klargöra vem som ska ta initiativ till att beställa loggutdrag, inklusive stickprovskontroller. Arbetet förväntas vara klart under år 2016.

Information som kan utläsas ur CSL
Vilken information som kan utläsas från loggutdrag är olika beroende på vilket system det gäller. Ambitionen och utgångspunkten är att man ska kunna se vem som påverkat informationen som lagras i ett system samt vem som tagit del av informationen. Som exempel kan nämnas att i DurTvå och Surfa2 framgår vem som bl.a. har skapat, uppdaterat och tagit bort information medan det i RAR endast framgår att en viss användare har utfört en uppdaterande åtgärd.

Automatgenererade larm
Ett automatgenererande larm är en realtidsövervakning på en i förhand bestämd aktivitet som systemet automatiskt reagerar på vid en misstänkt överträdelse. Vid granskningen hade CSL två automatgenererande larm; ett när en användare försöker göra slagningar på sig själv och det andra om någon som är administratör för Surfa2 utvidgar sin egen behörighet i systemet.

Det är tekniskt möjligt att skapa ytterligare automatgenererande larm, t.ex. på ord som faller inom förbudet att använda känsliga personuppgifter som sökbegrepp. En sådan stående övervakning skulle dock i praktiken kunna innebära vissa praktiska svårigheter och vara resurskrävande. Det finns i nuläget inte någon avsikt att införa ett automatgenererat larm av det slaget.

Statistik logguppföljningsbeställningar
Antalet beställningar av loggutdrag från CSL (per år):
2012: 318 stycken
2013: 384 stycken
2014: 335 stycken
2015: 239 stycken

Under perioden 1 januari – 18 april 2016 gjordes 97 beställningar av loggutdrag från CSL. Beställningarna har ökat något jämfört med samma period år 2015.

Antalet beställningar som inkommer till CSL har totalt sett minskat sedan år 2014. En anledning till minskningen är att möjligheten att söka på sig själv blockerades år 2014 och att många av beställningarna innan dess berodde på att sådana sökningar gjorts. Det kan även förhålla sig så att det efter omorganisationen till en Polismyndighet, som trädde i kraft den 1 januari 2015, inte är helt klart vem som ska initiera loggbeställningarna.

Vanligast förekommande är att beställningar kommer från Särskilda utredningar och består av reaktioner på misstänkt otillåtna slagningar avseende förfluten tid. Det finns ingen statistik på hur många av beställningarna som är stickprovskontroller, men uppskattningsvis utgör de endast ett fåtal av det totala antalet.

Bevarande av loggen
Som huvudregel bevaras loggar i fem år. Därefter raderas de automatiskt.

5. NÄMNDENS BEDÖMNING

Granskningen visar att flera av Polismyndighetens mest centrala it-system som används inom den brottsbekämpande verksamheten är anslutna till CSL och att en omfattande mängd information kan utläsas av loggen. Som exempel kan nämnas att i Surfa2 kan bl.a. uppgifter om vilken användare som har skapat, ändrat, öppnat eller raderat ett dokument utläsas. Det går även att beställa loggutdrag utvisande vilka ord en användare har sökt på.

Mot bakgrund av vad som framkommit vid granskningen konstaterar nämnden att CSL är ett viktigt verktyg som ger Polismyndigheten förutsättningar att i anslutna it-system kontrollera att personuppgiftsbehandlingen sker lagenligt. CSL ger alltså Polismyndigheten möjlighet att upprätthålla det integritetsskydd som föreskrivs i polisdatalagen.

Nämnden har i flera uttalanden kritiserat Polismyndigheten för bristande logguppföljningar i vissa uppgiftssamlingar.[7] Även Datainspektionen har nyligen uttalat att Polismyndigheten behandlar personuppgifter i OBS-portalen i strid med gällande författning genom att inte genomföra regelbundna logguppföljningar avseende sökningar på känsliga personuppgifter i systemet.[8] Trots tidigare påpekanden konstaterar nämnden att beställningar av loggutdrag inte har ökat.

Nämnden noterar vidare att de logguppföljningar som görs oftast sker på förekommen anledning vid misstanke om oegentligheter och att stickprovskontroller endast utgör en begränsad del av beställningarna.
Som nämnden tidigare uttalat måste loggutvärdering ske frekvent och göras såväl förebyggande som reaktivt om CSL ska utgöra det integritetsskydd som förutsattes vid lagens tillkomst. Polismyndigheten bör således verka för att fler

[7] Se t.ex. nämndens uttalanden den 17 februari 2016 ”Polismyndighetens behandling av känsliga personuppgifter i uppgiftssamling om inhemsk extremism” (dnr 87-2015) och den 18 februari 2015 ”Uppföljning av tidigare granskning avseende Rikspolisstyrelsens behandling av personuppgifter i penningtvättregistret” (dnr 2095-2014) samt däri hänvisade uttalanden.
[8] Datainspektionens yttrande från den 18 april 2016 ”Tillsyn enligt polisdatalagen (2010:361) och personuppgiftslagen (1998:204) avseende Polismyndighetens personuppgiftsbehandling i OBS-portalen” (dnr 211-2015).

och tätare stickprovskontroller görs. Polismyndigheten bör även överväga att införa fler automatgenererade larm, t.ex. vad gäller sökning på känsliga personuppgifter.

Avslutningsvis ska även nämnas att vid förevisningen av CSL framkom i ett avidentifierat loggutdrag att en person gjort sökningar på flera typer av känsliga personuppgifter. Polismyndigheten har uppgett att detta troligen skett i samband med registervård.

Som tidigare redovisats föreligger ett förbud mot att använda känsliga personuppgifter som sökbegrepp i gemensamt tillgängliga uppgiftssamlingar. Bestämmelsens ordalydelse medger inte undantag för sökningar som sker i registervårdande syfte. Nämnden anser dock att det ur ett integritetsperspektiv är olyckligt om sökförbudet omöjliggör en effektiv registervård. Nämnden har påtalat detta i samband med en tidigare granskning och fäste då Justitiedepartementets uppmärksamhet på behovet av ett förtydligande av bestämmelsen.[9] Något förslag till klargörande har såvitt känt inte lagts fram. Nämnden finner därför anledning att återigen aktualisera frågan. Det är av stor vikt att sådana registervårdande åtgärder närmare regleras.

6. BESLUT

1. Polismyndigheten anmodas att senast den 31 januari 2017 till nämnden redovisa vilka åtgärder som har vidtagits för att få till stånd fler och tätare stickprovskontroller.

2. Med anledning av vad nämnden uttalat om behovet av ett förtydligande av en lagbestämmelse ska en kopia av detta uttalande med beslut överlämnas till Justitiedepartementet.

3. Med detta uttalande avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Sigurd Heuman

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

[9] Se nämndens uttalande från den 11 december 2012 ”Rikspolisstyrelsens rutiner för kontroll av behandling av känsliga personuppgifter i det centrala kriminalunderrättelseregistret, KUR” (dnr 231-2012).

Föredragande: Jenny Fromin

Expedition till:
Polismyndigheten, Rättsavdelningen, enheten för rättslig styrning och stöd (A391.314/2015)
Justitiedepartementet

Kopia för kännedom till:
Datainspektionen