SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Uttalande med beslut

2017-05-04 Dnr 24-2017

Loggning och logguppföljning inom Säkerhetspolisens brottsbekämpande verksamhet

1. SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden har granskat hur Säkerhetspolisen genomför loggning och logguppföljning i den brottsbekämpande verksamheten.

Av Säkerhetspolisens uppgifter framgår att de flesta centrala it-system, som används inom den brottsbekämpande verksamheten, är anslutna till ett loggsystem och att nästintill varje aktivitet som äger rum loggas. Enligt nämndens uppfattning synes loggningen innebära en reell möjlighet för Säkerhetspolisen att upptäcka överträdelser av polisdatalagens bestämmelser.

Säkerhetspolisen har beskrivit att logguppföljning sker kontinuerligt och såväl förebyggande som reaktivt. Sammanfattningsvis anser nämnden att den ordning för loggning och logguppföljning som Säkerhetspolisen redovisat framstår som ändamålsenlig.

Nämnden understryker att sökningar i Säkerhetspolisens it-system med sökbegrepp som kan avslöja känsliga personuppgifter inte får ske rutinmässigt utan först efter en prövning i varje enskilt fall.

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

Nämnden beslutade den 25 januari 2017 att granska hur Säkerhetspolisen använder loggning och logguppföljning i den brottsbekämpande verksamheten.

3. RÄTTSLIGA UTGÅNGSPUNKTER

Säkerhetspolisen är skyldig att vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas i verksamheten (se 2 kap. 2 § första stycket 7 och 6 kap. 4 § första stycket 1 polisdatalagen [2010:361; PDL] samt 31 § personuppgiftslagen [1998:204]). Loggning är ett exempel på en sådan teknisk åtgärd.

Vid sökning i personuppgifter som har gjorts gemensamt tillgängliga vid Säkerhetspolisen får uppgifter som avslöjar ras, etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller som rör hälsa eller sexualliv (känsliga personuppgifter) användas som sökbegrepp endast om det är absolut nödvändigt för de ändamål som gäller för Säkerhetspolisens behandling av personuppgifter (6 kap. 11 § PDL).

4. UTREDNINGEN

4.1. Genomförande

Säkerhetspolisen har skriftligen besvarat frågor bl.a. om i vilken omfattning som Säkerhetspolisen loggar användarnas aktiviteter i it-systemen, vilka rutiner som finns för loggning och logguppföljning samt vilka rutiner som finns för bevarande av logguppgifter. Säkerhetspolisen har vid ett möte den 8 mars 2017 även lämnat muntlig information som sammanställts i ett protokoll. Nämnden har även tagit del av ett styrdokument för loggning och logguppföljning samt en skrivelse om loggsystemet. Av sekretesskäl är nedanstående beskrivningar av loggsystemet, rutiner och nämndens bedömning i vissa delar tämligen kortfattade.

4.2. Information från Säkerhetspolisen

Om den centrala säkerhetsloggen

Säkerhetspolisen använder ett centralt loggsystem, här benämnt centrala säkerhetsloggen (CSL). Syftet med CSL är dels att skydda Säkerhetspolisens användare, dels att skydda de registrerades personliga integritet. CSL samlar in, analyserar och arkiverar loggar från anslutna it-system. Analysen i CSL sker automatiskt och omfattar varje loggpost. Grunden för den automatiska analysen bestäms av bl.a. personuppgiftsombudet och enheten för intern

säkerhet och riskhantering. Genom CSL kan risken för informationsläckage och integritetskränkningar minimeras.[1] CSL har varit i drift i drygt två år. Behörigheten till information i CSL är ytterst begränsad. Loggarna bevaras i tio år, därefter gallras uppgifterna i CSL.

I vilken omfattning sker loggning?

Samtliga större it-system vid Säkerhetspolisen är anslutna till CSL. När nya it-system tas i bruk kopplas de till CSL. Det pågår även ett arbete med att, i den mån det är möjligt, ansluta äldre it-system till CSL. Vilken information som kan utläsas från loggarna beror på vilket it-system det gäller. I de största it-systemen generar nästintill varje aktivitet en loggpost. Enligt Säkerhetspolisens interna styrdokument för hantering av CSL krävs att anslutna system ska generera vissa loggdata om t.ex. ändringar av dokument, tidpunkt för vidtagna aktiviteter, IP-adress och försök till åtkomst av viss information.

Vilka rutiner finns för logguppföljning?

Från de anslutna it-systemen kommer det kontinuerligt in en stor mängd loggdata till CSL. I CSL bearbetas och analyseras informationen framförallt automatiskt. Även manuell analys sker av logganalytiker. Det sker både förebyggande kontroller och kontroller på förekommen anledning. I syfte att upptäcka överträdelser finns ett flertal automatiska larm, som löses ut vid exempelvis felaktiga inloggningsförsök.[2] Vidare tas loggrapporter fram avseende slumpvis utvalda medarbetares aktiviteter. Loggrapporterna skickas en gång per vecka till personalansvariga enhetschefer som ansvarar för att avvikande händelser följs upp. Vid behov har enhetscheferna även möjlighet att begära riktad logguppföljning avseende den personal de ansvarar för. Vid en misstänkt överträdelse inleds en undersökning som kan överlämnas till åklagare för utredning om ett eventuellt brott har begåtts.

Sker logguppföljning av sökningar på känsliga personuppgifter?

Det görs ett stort antal sökningar i Säkerhetspolisens it-system med sökord som kan avslöja känsliga personuppgifter. Riktad logguppföljning avseende sådana sökningar görs dagligen i de större it-systemen. Logganalytiker bedömer efter i förväg bestämda kriterier om en användare kan ha haft behov av att göra en viss sökning.

---

[1] Skrivelse från Säkerhetspolisen ”Begäran om samråd enligt 2 § polisdataförordningen” (dnr 2153-2014) 2014-12-18, s. 5.

[2] Automatiska larm är en realtidsövervakning på en i förhand bestämd aktivitet som systemet automatiskt reagerar på vid en misstänkt överträdelse.

5. NÄMNDENS BEDÖMNING

Av Säkerhetspolisen uppgifter framgår att de flesta centrala it-system, som används inom den brottsbekämpande verksamheten, är anslutna till CSL. Det pågår också ett arbete med att ansluta fler it-system till CSL. Nästintill varje aktivitet som äger rum i de centrala it-systemen loggas i CSL. Enligt nämnden synes loggningen vid Säkerhetspolisen innebära en reell möjlighet att upptäcka överträdelser av polisdatalagens bestämmelser.

Säkerhetspolisen har uppgett att det sker en kontinuerlig logguppföljning av användarnas aktiviteter genom såväl automatisk som manuell analys. Genom ett flertal automatiska larm kan avvikande användarbeteenden upptäckas. Loggutdrag kan tas fram vid misstanke om att personuppgifter behandlats felaktigt. Logguppföljning sker således både förebyggande och reaktivt.

Sammanfattningsvis anser nämnden att den ordning för loggning och logguppföljning som Säkerhetspolisen redovisat framstår som ändamålsenlig.

Säkerhetspolisen har uppgett att det görs ett stort antal sökningar med sökord som kan avslöja känsliga personuppgifter. Med anledning därav vill nämnden understryka att sådana sökningar inte får ske rutinmässigt utan först sedan det vid en prövning i det enskilda fallet fastställts att det finns ett påtagligt behov.[3]

6. BESLUT

Med detta uttalande avslutas ärendet.

På Säkerhets- och integritetsskyddsnämndens vägnar

Sigurd Heuman

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

Föredragande: Ylva Marsh

[3] Prop. 2009/10:85 s. 266

Expedition till:
Säkerhetspolisen, Rättsenheten (dnr 2017-2754)

Kopia för kännedom till:
Datainspektionen