SÄKERHETS- OCH INTEGRITETSSKYDDSNÄMNDEN

Samrådsyttrande

2013-03-21 Dnr 230-2012

Rikspolisstyrelsens IT-system OBS-portalen

1 SAMMANFATTNING

Säkerhets- och integritetsskyddsnämnden rekommenderar Rikspolisstyrelsen att:

- Införa tekniska lösningar för att förhindra eller i vart fall försvåra möjligheterna till sökning på känsliga personuppgifter i OBS-portalen.
- Differentiera behörigheterna i den del av systemet som har störst spridning, OBS-info, i högre utsträckning för att ett tillräckligt skydd för den personliga integriteten ska uppnås.
- Införa och dokumentera särskilda rutiner för den noggranna prövning som ska ske innan en känslig personuppgift registreras.

2 OM SAMRÅDET

Rikspolisstyrelsen är enligt 2 § polisdataförordningen (2010:1155) skyldig att samråda med nämnden i fråga om behandling av känsliga person-uppgifter när vissa nya IT-system planeras.

Rikspolisstyrelsen har i skrivelse, som inkom till nämnden den 29 november 2012, begärt samråd avseende IT-systemet OBS-portalen. OBS-portalen är ett nytt nationellt system för att sprida operativ brotts-, spanings- och kriminalunderrättelseinformation, där känsliga personuppgifter kommer att behandlas. Nämndens kansli har ställt vissa kompletterande frågor till Rikspolisstyrelsen, som inkommit med svar.

Nedanstående yttrande baseras på den skriftliga information som nämnden fått av Rikspolisstyrelsen. Yttrandet innebär inte att nämnden uttalar sig om lagligheten av den behandling av uppgifter som kommer att ske i systemet.

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

3 NÄMNDENS BEDÖMNING

3.1 Förbudet mot att söka på känsliga personuppgifter

Tekniska hinder mot att söka på känsliga personuppgifter bör införas

Enligt Rikspolisstyrelsen saknas det tekniska hinder mot att söka på känsliga personuppgifter i OBS-portalen. Nämnden rekommenderar i första hand att Rikspolisstyrelsen inför tekniska lösningar för att förhindra eller i vart fall försvåra möjligheterna till sökning på känsliga personuppgifter i OBS-portalen.

I ett så omfattande system som OBS-info är det särskilt angeläget att förbudet mot sökning på känsliga personuppgifter följs. Förbudet – som är absolut – syftar till att förhindra att integritetskänsliga sammanställningar av information kan göras, exempelvis kartläggningar av personer med viss politisk ståndpunkt eller religiös inriktning. Från integritetssynpunkt är denna reglering av fundamental betydelse. Ansvaret för att sökförbudet efterlevs bör därför inte enbart läggas på den enskilde tjänstemannen. En utgångspunkt måste istället vara att Rikspolisstyrelsen aktivt söker tekniska lösningar som omöjliggör otillåtna sökningar.

Behovet av information, utbildning och logguppföljning

Om det inte införs tekniska hinder mot att söka på känsliga personuppgifter i ett IT-system måste det enligt nämnden ställas särskilt höga krav på information och utbildning om vad som är en känslig personuppgift och om sökförbudet samt på myndighetens uppföljning av användarnas sökningar.

Enligt Rikspolisstyrelsen kommer användarna kunna få information om sökförbudet och en upplysning om att samtliga sökningar loggas genom att klicka på en länk intill sökfältet i OBS-portalen. Nämnden ser positivt på att användaren informeras, men anser att informationen i länken bör utvecklas med exempel på känsliga personuppgifter för att ge användaren ett bättre underlag för sin bedömning av om ett visst sökbegrepp är en känslig person-uppgift. Även metodhandboken för OBS-portalen bör uppdateras på motsvarande sätt för att ge ett bättre stöd till redaktörer och läsare.

Nämnden har inte fått någon information om vilken utbildning användare med läsbehörighet i de delar av portalen som innehåller personuppgifter kommer att få. Nämnden rekommenderar att användarna återkommande utbildas om vad som är en känslig personuppgift och om sökförbudet.

Nämndens tillsyn över den öppna polisens personuppgiftsbehandling har hittills visat att den interna kontrollen i form av stickprov och logguppföljning alltför ofta brister (se nämndens redovisning av tillsynsverksamheten avseende

polisens personuppgiftsbehandling, dnr 35-2013). Om det inte införs tekniska hinder mot sökningar på känsliga personuppgifter i OBS-portalen, anser nämnden att logguppföljning och stickprov måste genomföras mer frekvent och effektivt än vad nämndens granskning visat hittills.

Sökningar som avser en gärningsmans tillvägagångssätt

Enligt Rikspolisstyrelsen ska det vara möjligt att söka på exempelvis ordet bög i OBS-portalen eftersom ordet skulle kunna registreras om det ingår i en beskrivning av en eftersökt gärningsmans tillvägagångssätt, såsom att ordet alltid yttras i samband med misshandel. Ordet är i det fallet inte hänförligt till någon enskild person och alltså inte en personuppgift. Nämnden anser inte att sådana sökningar bör tillåtas. Även om registreringen av ett ord – som skulle ha varit en känslig personuppgift om det kopplats till en viss person – inte innebär en behandling av en känslig personuppgift, skulle sökningar på sådana ord innebära en risk för träffar som avslöjar känsliga personuppgifter och därmed omfattas av förbudet i 3 kap. 5 § första stycket polisdatalagen (2010:361).[1]

4.2 Alltför vida behörigheter

Nämnden anser att den presenterade behörighetstilldelningen, i framför allt den del av portalen som kallas OBS-info, framstår som alltför vid ur ett integritetsskyddsperspektiv. Nämnden rekommenderar därför Rikspolisstyrelsen att införa en mer differentierad behörighetstilldelning.

Vid personuppgiftsbehandling i stora uppgiftssamlingar är begränsningar av tillgängligheten för användarna ett viktigt integritetsskydd, vilket avspeglas i polisdatalagens krav på att tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att fullgöra sina arbetsuppgifter (2 kap. 11 § polisdatalagen). Enligt förarbetena riktar sig kravet på begränsning bland annat till dem som ansvarar för utformningen av nya datasystem, och det betonas att polisdatalagen ställer högre krav än tidigare på att polisen genom tekniska åtgärder begränsar den enskilde tjänstemannens tillgång till information.[2]

I OBS-portalen är användarens behörighet knuten till flikar i gränssnittet. Under flikarna KUT-sam och OBS-info kommer personuppgifter att behandlas. Enligt Rikspolisstyrelsen ger behörighet till KUT-sam respektive OBS-info åtkomst till samtliga uppgifter från hela landet. KUT-sam kommer enligt Rikspolisstyrelsen att ha 500 behöriga användare inom kriminal-underrättelsetjänsten (KUT). OBS-info ersätter de regionala KUT-infosystemen och kommer enligt Rikspolisstyrelsen att ha 20 000 till 25 000

[1] Jfr. prop. 2009/10:85 s. 156.
[2] A. prop. s. 270 och 326.

behöriga användare. Nämndens tidigare granskning har visat att känsliga personuppgifter förekommit i inte obetydlig omfattning i KUT-info (Polismyndigheternas behandling av känsliga personuppgifter i KUT-info, dnr 176-2012). När nu KUT-info ersätts av OBS-info och informationen därmed får nationell spridning är en differentierad behörighetstilldelning nödvändig för att tillvarata integritetsintresset. Nämnden ifrågasätter om 20 000 till 25 000 användare har behov av behörighet till alla uppgifter i OBS-info för att kunna fullgöra sina arbetsuppgifter. Även om tillgången till personuppgifter i KUT-sam är betydligt mer begränsad vill nämnden uppmana RPS att överväga om så många som 500 KUT-anställda har behov av full behörighet till KUT-sam för att kunna fullgöra sina arbetsuppgifter, och om integritetsskyddsintresset har beaktats i tillräcklig mån.

4.3 Rutiner i samband med registrering av känsliga personuppgifter

Nämnden rekommenderar att särskilda rutiner införs för den noggranna prövning som ska ske innan en känslig personuppgift registreras och att rutinen dokumenteras. Såväl nämnden som Datainspektionen har tidigare pekat på behovet av sådana rutiner (ovannämnda uttalande, samt Datainspektionens beslut den 20 november 2012, dnr 604-2012 och 605-2012). Som nämnden har konstaterat tidigare bör prövningen föregås av ett samråd med annan än den som ska utföra registreringen, såsom närmaste chef. Dessa rutiner bör dokumenteras och spridas på lämpligt sätt bland redaktörerna. Att rutinerna följts och beslut fattats i det enskilda fallet bör dessutom dokumenteras genom en anteckning eller liknande i själva systemet.

Nämndens rekommendation i detta avseende är föranledd av den restriktivitet som ligger i begreppet ”absolut nödvändigt”, vilket enligt förarbetena innebär att en noggrann prövning måste ske i varje enskilt fall innan en registrering av känsliga personuppgifter görs.[3] Nämnden menar att en sådan noggrann prövning förutsätter tydliga rutiner och någon form av intern beredning.

Detta samrådsyttrande har beslutats av Säkerhets- och integritetsskyddsnämnden. I beslutet har ledamöterna Sigurd Heuman, ordförande, Susanne Nylund, Leif Hallberg, Berit Jóhannesson, Alf Karlsson, Eric Myrin och Stefan Tornberg deltagit. Föredragande har varit Elisabeth Hedborg.

Sigurd Heuman

Elisabeth Hedborg

[3] Prop. 2009/10:85 s. 325.

Sändlista:
Rikspolisstyrelsen

Kopia för kännedom:
Datainspektionen