

2018-12-11

Diarienummer
71-2018Ö:2



Försvarsdepartementet
Ref: Fö2018/00999/RS
103 33 Stockholm

Betänkandet Behandlingen av personuppgifter vid Försvarsmakten och Försvarets radioanstalt (SOU 2018:63)

Statens inspektion för försvarsunderrättelseverksamheten (Siun) har enligt förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten till uppgift att kontrollera försvarsunderrättelseverksamheten hos de myndigheter som enligt förordningen (2000:131) om försvarsunderrättelseverksamhet bedriver sådan verksamhet. Siun ska även granska behandlingen av uppgifter enligt lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (FM) samt enligt lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA).

Siun har tagit del av betänkandet och välkomnar de delar i förslaget som bidrar till att tydliggöra de berörda myndigheternas förutsättningar för personuppgiftsbehandling inom sina verksamheter och samtidigt klargöra för allmänheten vilka olika typer av personuppgiftsbehandling som kan förekomma. Samtidigt noterar Siun att betänkandets förslag medför utökade möjligheter till såväl behandling som utbyte av personuppgifter. I förslaget har även vissa gallringsfrister tagits bort och istället har en behovsrelaterad bestämmelse om längsta tid för behandling införts. Sammantaget innebär förändringarna att försvarsunderrättelseverksamhetens förutsättningar att verka utökas, genom hantering och spridning av information, vilket sannolikt kommer att få viss negativ påverkan på den personliga integriteten. Utöver dessa övergripande iakttagelser lämnar Siun

följande synpunkter. I rubriksättningen nedan hänvisas till kapitel i de föreslagna registerförfattningarna, benämnda FM-PuL resp. FRA-PuL.

1. Rättsliga grunder för behandling i försvarsunderrättelseverksamhet

2 kap. 2-3 §§ FM-PuL, 2 kap. 1-2 §§ FRA-PuL

De förändringar som föreslås innebär dels att kravet på anknytning till den preciserade inriktningen tas bort, dels att myndigheterna får fortsätta behandla de personuppgifter som man fått tillgång till i försvarsunderrättelseverksamheten om det behövs för att fullgöra densamma.

Enligt Siun fungerar kravet på anknytning till en preciserad inriktning som ett stöd för myndigheterna i deras personuppgiftsbehandling. Detta beror på att regeringen genom sitt årliga beslut, utöver bestämmelserna i lagen och förordningen om försvarsunderrättelseverksamhet, styr försvarsunderrättelseverksamhetens inriktning vilken myndigheterna utgår ifrån när de själva producerar interna styrdokument. I dessa styrdokument/preciserade inriktningar görs ytterligare en precisering i förhållande till regeringens inriktning. De preciserade inriktningarna utgör sedan i sin tur grund för bl.a. personuppgiftsbehandlingen. På detta sätt styr regeringen vilken försvarsunderrättelseverksamhet myndigheterna ska ägna sig åt vilket samtidigt, genom den preciserade inriktningen, sätter en yttre ram för personuppgiftsbehandlingen. Om kravet på anknytning till den preciserade inriktningen tas bort kommer behandlingen istället att prövas direkt mot regeringens inriktning vilken är vidare än den preciserade inriktningen. Effekten av detta blir sannolikt en mer generös bedömning av vad som är nödvändig behandling för verksamheten. I prop. 2006/07:46 Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt, s. 65 betonades bl.a. vikten av den myndighetsinterna inriktningen med dess preciserade ändamålsangivelse som en väsentlig utgångspunkt för kontrollen av personuppgiftsbehandlingen. Ytterligare en effekt av att den preciserade inriktningen tas bort är således att denna utgångspunkt för Siuns kontroll av personuppgiftsbehandlingen uteblir.

Den nya bestämmelsen som innebär att myndigheterna får fortsätta behandla de personuppgifter som man fått tillgång till i försvarsunderrättelseverksamheten om det behövs för att fullgöra densamma möjliggör fortsatt behandling av uppgifter som behandlats med stöd av tidigare gällande inriktningsbeslut från regeringen. Myndigheterna får således behandla uppgifter inom områden som regeringen inte längre prioriterar i aktuell inriktning.

Sammantaget innebär de nya bestämmelserna sannolikt att fler personuppgifter kommer att behandlas eftersom de inte begränsas av myndigheternas preciserade inriktningar/produktionsplaner för innevarande år samt då äldre personuppgifter kan behandlas för ”gamla behov” som regeringen bedömer inte längre är aktuella att bedriva försvarsunderrättelseproduktion mot. Detta leder förmodligen till viss ökning av integritetsintrånget.

2. Ny rättslig grund avseende FM

2 kap. 1 och 22 §§ FM-PuL

I den nya bestämmelsen föreslås att FM ska få behandla personuppgifter om det är nödvändigt för att planera, förbereda och genomföra verksamhet som rör Sveriges försvar och säkerhet eller internationellt försvars- och säkerhetssamarbete. Med anledning av följande avsnitt i betänkandet finner Siun tillämpningsområdet för den nya bestämmelsen oklart. I avsnitt 6.3.1 anges att den föreslagna bestämmelsen i och för sig också omfattar FM:s försvarsunderrättelseverksamhet och militära säkerhetstjänst men att dessa verksamheter även i den föreslagna lagen ska regleras särskilt med hänsyn till dessa verksamheters karaktär och till att de hittills reglerats i FM-PUL. I avsnitt 6.4.7 kommenteras den nya bestämmelse som ersätter nuvarande bestämmelse i 1 kap.17 § FM-PUL om överföring av personuppgifter till andra länder m.m. Där anges att utredningen anser att en bestämmelse som motsvarar 1 kap. 17 § FM-PUL bör tas in i den nya lagen. Med hänsyn till det vidgade tillämpningsområdet för behandlingen av personuppgifter vid Försvarsmakten bör dock ”försvarsunderrättelse- och säkerhetssamarbetet” ersättas med ”försvars- och säkerhetssamarbetet”.

Tillämpningsområdet för den nya rättsliga grunden bör förtydligas. Utredningen är otydlig i dessa avseenden, vilket öppnar för olika tolkningar och missförstånd. Det är nödvändigt att klargöra om behandling av personuppgifter avseende försvarsunderrättelseverksamhet eller militär säkerhetstjänst även kan ske med stöd av denna nya grund och inte enbart med stöd av den särskilda regleringen av försvarsunderrättelseverksamhet och militär säkerhetstjänst.

3. Ny rättslig grund och preciserad finalitet avseende FRA

2 kap. 3, 5-7 och 20 §§ samt 3 kap. 4 § FRA-PuL

I de föreslagna bestämmelserna återfinns bl.a. en reglering avseende informationssäkerhetsverksamhet vilken inte regleras i FRA:s nuvarande registerförfattning. En av bestämmelserna medger utländsk organisation direktåtkomst till personuppgifter som behandlas i informationssäkerhetsverksamheten. Vidare föreslås att personuppgifter som behandlas med stöd av den föreslagna lagen bl.a. ska kunna lämnas ut till en utländsk organisation inom informationssäkerhetsområdet. Det finns också bestämmelser om utbyte av personuppgifter mellan försvarsunderrättelse-, utvecklings- och informationssäkerhetsverksamhet. Av bestämmelserna framgår att det i flera fall är aktuellt med behandling av personuppgifter för andra ändamål än de ursprungliga. Som exempel kan nämnas utbytet mellan försvarsunderrättelseverksamheten och det tekniska detekterings- och varningssystemet (TDV) inom informationssäkerhetsverksamheten. Siun har inte fått till uppgift att granska informationssäkerhetsverksamheten vilket får till följd att om personuppgifter från försvarsunderrättelseverksamheten förs över till informationssäkerhetsverksamheten kommer dessa försvarsunderrättelseuppgifter inte att kontrolleras av Siun. En liknande situation förekommer visserligen redan idag då uppgifter kan rapporteras till andra myndigheter som inte granskas av Siun. En omfattande behandling av personuppgifter för andra ändamål än de ursprungliga skapar emellertid en rundgång och sammanblandning av integritetskänsliga uppgifter vilket kan innebära ”glapp” i kontrollen av dessa. I övrigt finns sannolikt en risk för att vissa av dessa utbyten kommer att innebära ett ökat intrång i den personliga integriteten då flödet av personuppgifter innebär att uppgifterna kommer fler till del. Om utbytet innebär att uppgifter delas med verk-

samheter utanför FRA minskar FRA:s kontroll över uppgifterna och därmed ökar även risken för felaktig behandling och spridning av uppgifterna.

4. Behandling av personuppgifter i allmänt tillgänglig information

2 kap. 8 § FM-PuL, 2 kap. 8 § FRA-PuL

För såväl FM som FRA föreslås en ny bestämmelse som möjliggör behandling av personuppgifter som utgör allmänt tillgänglig information. I betänkandet noteras att antalet personuppgifter i dessa referensdatabaser kan bli mycket stort vilket innebär en form av integritetsintrång även om uppgifterna är allmänt tillgängliga. Enligt Siuns bedömning kan det finnas skäl att överväga någon form av reglering av längsta tid för behandling. Utan någon form av begränsning kan det finnas risk att personuppgifter behandlas i dessa stora databaser under lång tid utan att de lagstadgade kraven på nödvändighet uppfylls. En reglering får till effekt att myndigheterna går igenom och bedömer uppgifterna och på så sätt säkerställer att kraven på nödvändighet uppfylls.

5. Behandling av personuppgifter i vissa fall

2 kap. 20 § FM-PuL, 2 kap. 18 § FRA-PuL

Den nya paragrafen har anpassats till de behov myndigheterna har bl.a. med hänsyn till de stora mängder data som inkommer till dem. Även i detta fall kan det finnas skäl att överväga någon form av reglering av längsta tid för behandling istället för att endast begränsa den tillåtna behandlingen, enligt denna "lätnadsregel", till det skede då det inte kunnat fastställas vilka personuppgifter informationen innehåller. Ett skede öppnar för tolkning och skulle kunna leda till långa perioder av personuppgiftsbehandling utan att alla bestämmelser i respektive registerlagstiftning behöver beaktas vilket inte är lämpligt från ett integritetsskyddsperspektiv.

6. Utökade möjligheter till direktåtkomst

3 kap. 3 § FM-PuL, 3 kap. 3 § FRA-PuL

I betänkandet presenteras förslag om att medge utländska underrättelse- och säkerhetstjänster direktåtkomst bl.a. för samarbete mot terrorism eller internationellt säkerhetssamarbete. Det konstateras att ökade möjligheter till direkt-

åtkomst kan innebära att intrånget i den personliga integriteten i viss mån kan öka. Enligt Siuns uppfattning bör analysen avseende såväl behovet som konsekvenserna av direktåtkomst för utländska underrättelse- och säkerhetstjänster fördjupas. Den föreslagna direktåtkomsten avseende personuppgifter av den känsliga karaktär det är fråga om kan öka integritetsintrånget dels till följd av ökad spridning av uppgifterna, dels till följd av ökad risk för felaktig hantering av uppgifterna då det är svårt att kontrollera hur dessa används och sprids hos utländska tjänster.

7. Ändring i 2 a § lagen (2008:717) om signalspaning

Den föreslagna ändringen gäller ett undantag avseende andra stycket i 2 a § i fråga om signaler som utväxlas autonomt mellan tekniska system i sådana fall där signalerna inte innehåller personuppgifter. I betänkandet nämns bl.a. att det även i andra sammanhang än vid teknisk signalspaning till stöd för produktion av signalreferensbibliotek förekommer signaler som utväxlas autonomt i och mellan tekniska system där ingen mänsklig information förekommer och där inga integritetsaspekter gör sig gällande. Enligt Siuns uppfattning bör detta förtydligas och utvecklas så att det framgår vilka andra sammanhang som avses.

8. Siuns nya uppgift (Siuns instruktion 1 §)

I betänkandet föreslås en ändring i 1 § Siuns instruktion som innebär att Siun ska lämna försvarsunderrättelsemyndigheterna råd och stöd beträffande deras skyldigheter i den verksamhet som inspektionen har till uppgift att kontrollera och granska. Betänkandet hänvisar i denna del till avsnittet som avser Datainspektionens roll. Den föreslagna ändringen är placerad i 1 § och träffar därmed all försvarsunderrättelseverksamhet hos samtliga myndigheter som Siun kontrollerar och inte enbart personuppgiftsbehandlingen hos FRA och FM. Siuns uppgift är att utföra en laglighetsgranskning i efterhand vilket inte innefattar sådana uppgifter som ankommer på en tillsynsmyndighet såsom rådgivning eller utfärdande av varningar eller förelägganden. Förslaget är således inte förenligt med de uppgifter Siun har idag. Vidare är Siun inte dimensionerad för en sådan verksamhet. Siuns konstruktion och storlek har utformats med hänsyn till uppgiften att granska och kontrollera verksamheter av särskilt känslig karaktär. Vad

gäller rådgivning och stöd till de myndigheter som har särskilda registerförfattningar utförs den uppgiften av Datainspektionen. Ur den aspekten vore det inte lämpligt med en liknande uppgift för Siun. Sammanfattningsvis anser Siun inte att den föreslagna uppgiften är lämplig för ett kontrollorgan av Siuns karaktär och avstyrker förslaget.

I detta beslut har vice ordförande Jan Öhman, ledamöterna ClasGöran Carlsson, Inge Garstedt, Helene Petersson, Anders Schröder och Per Westerberg deltagit.

I den slutliga handläggningen har även Maria Broms, Annika Jäderlund (föredragande), Jessica Ovin och Jörgen Yng deltagit.

På nämndens uppdrag



Jan Öhman


Annika Jäderlund