FRA

REMISSYTTRANDE

2017-08-31

FRA beteckning
20 400:3498/ 7:2

Justitiedepartementet
Grundlagsenheten
103 33 Stockholm

Er handläggare	Ert datum	Er beteckning
Manne Heimer	2017-05-15	Ju2017/04264/L6
FRA handläggare	FRA föreg. datum	FRA föreg. beteckning
Kári Ólafsson		

Remittering av betänkandet SOU 2017:39 Ny dataskyddslag

Försvarets radioanstalt (FRA) har – från de utgångspunkter myndigheten har att beakta – följande synpunkter på betänkandet Ny dataskyddslag (SOU 2017:39).

Sammanfattning

Följande bör framgå direkt av 1 kap. 2 § dataskyddslagen.[1]

a) Att dataskyddsförordningen[2] inte ska gälla vid personuppgiftsbehandling som regleras enligt lagen (2007:259) om behandling av personuppgifter i Förvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet (FRA-PUL) (se nedan 6.4.2).

b) Att incidentrapportering enligt artikel 33 dataskyddsförordningen och information till registrerade om sådan incident enligt artikel 34 dataskyddsförordningen inte ska gälla om rapporteringsskyldighet följer av 10 a § säkerhetsskyddsförordningen (1996:633) (se nedan 6.4.2).

[1] Förslag till lag med kompletterande bestämmelser till EU:s dataskyddsförordning.
[2] Europaparlamentets och rådets förordning (EU 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

FRA
Box 301
161 26 BROMMA

Telefon
08 - 471 46 00

Telefax

Org.nr
20 21 00 - 0365

För verksamhet som dataskyddsförordningen ska gälla bör följande begränsning införas i dataskyddslagen.

- Information till registrerade om personuppgiftsincidenter enligt artikel 34 i dataskyddsförordningen ska inte krävas om uppgifterna avseende incidenten omfattas av sekretess (se nedan 13.4.1).

FRA ifrågasätter förslaget att sanktionsavgifter ska få tas ut av myndigheter (se nedan 18.5.3).

Det bör tillkomma en övergångsbestämmelse med innebörden att personuppgiftslagen (1998:204) (PUL) ska gälla behandling av personuppgifter inom FRA:s informationssäkerhetsverksamhet längst till och med den 25 maj 2020 (se nedan 20.2).

FRA:s synpunkter nedan följer betänkandets disposition.

6.4.2 Ska förordningens bestämmelser göras gällande utanför deras tillämpningsområde? (s. 91 ff.)

a) Det bör framgå direkt av dataskyddslagen att dataskyddsförordningen inte ska gälla verksamhet som regleras av FRA-PUL.

FRA är en svensk underrättelsetjänst med uppgift att bl.a. bedriva signalspaning enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet och till lagen anslutande förordning. FRA bedriver signalspaning i syfte att kartlägga bl.a. yttre militära hot, hot mot svensk personal under internationella insatser, internationell terrorism, främmande underrättelseverksamhet mot svenska intressen och övriga internationella företeelser som har betydelse för svensk utrikes-, säkerhets- och försvarspolitik. All signalspaning är riktad mot utländska förhållanden och sker på uppdrag av bl.a. regeringen.

FRA:s försvarsunderrättelse- och utvecklingsverksamhet faller utanför unionsrätten och regleras såvitt gäller behandling av personuppgifter av en särskild lagstiftning – FRA-PUL. Lagen skiljer sig från s.k. registerförfattningar på det sätt att den är heltäckande och innehåller alla de bestämmelser som är tillämpliga för behandling av personuppgifter i FRA:s försvarsunderrättelse- och utvecklingsverksamhet. Personuppgiftsbehandling i andra delar av FRA:s verksamhet, såsom administration, omfattas av PUL.

FRA

Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst regleras på motsvarande sätt i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (FM-PUL).

I förarbetena[3] till FRA-PUL och FM-PUL motiveras denna ordning på följande sätt på s. 41.

> Inom [...] Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet är det nödvändigt med en särskild författningsreglering av personuppgiftsbehandlingen av såväl effektivitets- som integritetsskäl. Omfattningen av verksamheterna, deras speciella inriktning samt den stora mängden uppgifter av ofta känslig natur och behandlingar som förekommer talar för en särskild författningsreglering. Det är för allmänhetens förtroende för [...] Försvarets radioanstalt och de nu aktuella verksamheterna, vilka av naturliga skäl till största delen är sekretessbelagda, viktigt med en hög nivå på integritetsskyddet.

Vidare anförs följande på s. 45.

> Genom att samla alla tillämpliga bestämmelser om behandling av personuppgifter i en lag [...] och i därtill hörande förordningar blir det överskådligt och tydligt för myndigheterna vad som gäller, vilket underlättar tillämpningen.
>
> [...] Försvarets radioanstalts försvarsunderrättelseverksamhet är omgärdade av sekretessbestämmelser som försvårar möjligheten till den insyn som annars är möjlig i offentlig verksamhet. Det är därför särskilt viktigt att lagstiftningen utformas på ett sätt som underlättar för den enskilde att få klart för sig under vilka förutsättningar [...] Försvarets radioanstalt kan komma att behandla personuppgifter som rör honom eller henne, samt under vilka förutsättningar den enskilde kan utnyttja de rättigheter som han eller hon har. En heltäckande lagstiftningslösning kan i detta perspektiv vara till fördel också för den enskilde.

Dessa skäl gör sig alltjämt gällande. Det bör därför uttryckligen framgå av dataskyddslagen att dataskyddsförordningen inte ska gälla verksamhet som regleras av FRA-PUL.

I sammanhanget vill FRA uppmärksamma att FRA-PUL är föremål för översyn av en särskild utredare. Uppdraget ska redovisas senast den 31 maj 2018. Utredningen ska bl.a. bedöma om den reglering som gäller vid behandling av personuppgifter i FRA:s

[3] Se prop. 2006/07:46 Personuppgiftsbehandling hos Försvarsmakten och Försvarets radioanstalt.

försvarunderrättelse- och utvecklingsverksamhet är ändamålsenligt utformad och tillräcklig vad gäller skyddet för den enskildas personliga integritet samt lämna de författningsförslag som behövs och är lämpliga.[4]

b) Artikel 33 och artikel 34 bör inte gälla incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen (1996:633), vilket bör framgå direkt av dataskyddslagen.[5]

Enligt artikel 33 dataskyddsförordningen ska personuppgiftsincidenter rapporteras till tillsynsmyndigheten.

Det håller på att växa fram ett flertal parallella system för rapportering av incidenter i it-system.

- Idag ska myndigheter rapportera it-incidenter enligt 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen).
- Motsvarande bestämmelser om rapportering av personuppgiftsincidenter i dataskyddsförordningen finns i förslag till brottsdatalag avseende brottsbekämpande myndigheters verksamhet.[6]
- Vidare föreslås incidentrapporteringsplikt för leverantörer av samhällsviktiga och digitala tjänster i samband med införandet av EU:s NIS-direktiv.[7]

De skyldigheter att rapportera incidenter som kommer följa av de olika författningarna kommer delvis att överlappa varandra. En och samma incident kan komma att rapporteras enligt flera olika lagar och till olika tillsynsmyndigheter.[8] Denna ordning är inte lätt att överblicka.

För FRA:s del är det viktigt att rapportering enligt nämnda författningar och författningsförslag inte ska ske för det fall rapporteringsskyldighet föreligger enligt 10 a §

---

[4] Uppdraget anges i kommittédirektivet Behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (Dir. 2017:42).

[5] Jämför vad som anges i 3 kap. 9 § förslag till brottsdataförordning i betänkandet Brottsdatalag (SOU 2017:29).

[6] Se betänkandet Brottsdatalag (SOU 2017:29).

[7] Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensamt nivå på säkerhet i nätverks- och informationssystem i hela unionen. Se betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36).

[8] Incidenter enligt krisberedskapsförordningen och den föreslagna lagen om vissa tillhandahållare av samhällsviktiga tjänster och digitala tjänster ska rapporteras till Myndigheten för samhällsskydd och beredskap. I nu aktuellt betänkande och betänkandet Brottsdatalag framgår att personuppgiftsincidenter troligen kommer rapporteras till Datainspektionen.

säkerhetsskyddsförordningen. Detta förhållande har reglerats eller kommer att regleras i de författningar som redovisas i det följande.

Rapporteringsskyldigheten enligt krisberedskapsförordningen omfattar inte sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen. Detsamma föreslås gälla enligt betänkandet Ny brottsdatalag (SOU 2017:29), s. 331 f., vari följande anges.

> En personuppgiftsincident uppfyller kriterierna för en it-incident. Det innebär att de flesta behöriga myndigheter kommer att behöva anmäla sådana incidenter enligt två olika förfaranden och till olika myndigheter. It-incidenter som kan antas påverka säkerheten för hemliga uppgifter som rör Sveriges säkerhet ska dock enbart anmälas enligt säkerhetsskyddsförordningen. Behovet av att skydda sådan information anses vara så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet ska få ta del av den. Även om den rapporteringen har ett annat syfte än rapporteringen av personuppgiftsincidenter, anser utredningen att behovet av skydd för uppgifter som rör Sveriges säkerhet väger tyngre än behovet av att skydda enskilda från eventuella intrång i den personliga integriteten. Eftersom nationell säkerhet ligger utanför direktivets tillämpningsområde anser utredningen att sådana personuppgiftsincidenter som ska anmälas enligt 10 a § säkerhetsskyddsförordningen inte bör anmälas till tillsynsmyndigheten.

Även i betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster SOU (2017:36), s. 87, anges att incidentrapportering enligt den föreslagna s.k. NIS-lagen inte ska tillämpas på sådana incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

Något sådant undantag som anges ovan finns dock inte i förslaget till dataskyddslag.

Incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen gäller Sveriges säkerhet och omfattas inte av unionsrätten. I linje med vad som gäller idag och som föreslås i de ovan nämnda betänkandena bör inte artikel 33 dataskyddsförordningen gälla för det fall en personuppgiftsincident ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

Av samma skäl bör inte heller artikel 34 dataskyddsförordningen om information till en registrerad vid en personuppgiftsincident gälla incidenter som ska rapporteras enligt nämnda bestämmelse i säkerhetsskyddsförordningen.

Mot denna bakgrund bör det av 1 kap. 2 § förslag till dataskyddslag framgå att artikel 33 och 34 inte ska gälla personuppgiftsincidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.

13.4.1 Sekretess och tystnadsplikt ska gå före informationsplikten (s. 204)

För verksamhet som dataskyddsförordningen ska gälla bör information till registrerade om personuppgiftsincidenter enligt artikel 34 dataskyddsförordningen inte krävas om uppgifterna avseende incidenten omfattas av sekretess. En begränsning med detta innehåll bör, med stöd av artikel 23 dataskyddsförordningen införas i dataskyddslagen.

Dataskyddsförordningen kommer att gälla en mängd verksamheter av varierande slag. Information om en personuppgiftsincident skulle kunna röja uppgifter som omfattas av sekretess. Därför bör det införas en bestämmelse som begränsar information till den registrerade på samma sätt som föreslås gälla artiklarna 13-15 i dataskyddsförordningen enligt 5 kap. 1 § dataskyddslagen.[9]

18.5 Sanktionsavgifter inom offentlig sektor

18.5.3 Överväganden och förslag (s. 287 ff.)

FRA ifrågasätter om det är lämpligt att sanktionsavgifter ska kunna tas ut av myndigheter. Motsvarande fråga har tidigare behandlats i betänkandet Myndighetsdatalag (SOU 2015:39). I betänkandet (s. 630 ff.) anges att det följer av allmänna rättsgrundsatser att vite inte bör användas som sanktionsmedel mellan statliga myndigheter. Vidare påtalas att myndigheters behandling av personuppgifter sker i en verksamhet som i allmänhet inte förekommer utanför det allmänna och som omgärdas av helt andra krav och regler än vad som annars är fallet. I betänkandet anges att det inte finns några bärande skäl för att i alla delar ha samma sanktionsmöjligheter mot både myndigheter och enskilda. Konklusionen i betänkandet, s. 632, är följande.

> Det finns [...] inget sådant starkt vägande skäl som talar för att myndigheters behandling av personuppgifter utgör ett sådant undantagsfall att man bör avvika från den allmänna rättsgrundsatsen att staten inte kan rikta viten mot sig själv.

[9] Jfr även den föreslagna begränsningen av information till registrerade vid personuppgiftsincident i 3 kap. 11 § brottsdatalagen, se SOU 2017.

Sanktionsavgifter är ett effektivt rättsmedel att komma till rätta med överträdelser hos enskilda, t.ex. privata bolag, som enligt förslaget till ny dataskyddslag inte längre riskerar dömas straff för att bryta mot dataskyddsförordningen. För ansvariga vid statliga myndigheter kan dock alltjämt tjänstemannaansvar utkrävas. Därutöver har den registrerade möjlighet att utkräva skadestånd av myndigheter vid överträdelser av dataskyddsförordningen. Regeringen har också möjlighet att ställa krav på myndigheter genom allmänna direktiv och förordningar för att komma tillrätta med överträdelser.

Mot bakgrund av det ovan angivna ifrågasätter FRA förslaget att tillsynsmyndighet ska få ta ut sanktionsavgifter av myndigheter.

20.2 Ikraftträdande- och övergångsbestämmelser i förordningen (s. 339)

Utöver försvarsunderrättelse- och utvecklingsverksamhet bedriver FRA informationssäkerhetsverksamhet som syftar till att stödja de mest skyddsvärda verksamheterna bland statliga myndigheter och statligt ägda bolag.

FRA ska således ha hög teknisk kompetens inom informationssäkerhetsområdet i enlighet med 4 § förordningen (2007:937) med instruktion för Försvarets radioanstalt. FRA får efter begäran stödja sådana statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhet- eller försvarspolitiskt hänseende. FRA ska särskilt kunna stödja insatser vid nationella kriser med it-inslag, medverka till identifiering av inblandade aktörer vid it-relaterade hot mot samhällsviktiga system, genomföra it-säkerhetsanalyser, och ge annat tekniskt stöd.

Regeringen har, som angetts ovan, gett en särskild utredare i uppdrag att göra en översyn av den lagstiftning som gäller för personuppgiftsbehandling inom bl.a. FRA.[10] Uppdraget ska redovisas senast den 31 maj 2018. Utredaren ska bl.a. analysera vilket utrymme det finns för en nationell reglering av FRA:s informationssäkerhetsverksamhet som idag regleras av PUL.

Det tar tid och resurser att anpassa en verksamhet till en ny rättslig ordning. Det kan därför ifrågasättas om det är lämpligt att FRA:s informationssäkerhetsverksamhet ska tillämpa dataskyddsförordningen innan det står klart vilken personuppgiftslagstiftning som ska gälla för denna verksamhet. För att på bästa sätt utnyttja samhällets resurser och för att underlätta rättstillämpningen bör PUL gälla FRA:s informationssäker-

[10] Behandlingen av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (Dir. 2017:42).

FRA

hetsverksamhet tills dess att det lagstiftningsarbete som utredarens förslag föranleder har genomförts.

Mot bakgrund av att FRA:s informationssäkerhet således är föremål för översyn och kan komma att regleras i nationell lagstiftning på samma sätt som FRA:s försvarsunderrättelse- och utvecklingsverksamhet bör det införas en övergångsbestämmelse med innebörden att personuppgiftslagen alltjämt ska gälla för FRA:s informationssäkerhetsverksamhet. Detta bör gälla längst till och med 25 maj 2020.[11]

I detta ärende har generaldirektören Dag Hartelius beslutat. I den slutliga handläggningen har också deltagit chefsjuristen Michaela Dráb, planeringschefen Johan Dahlstedt, avdelningscheferna ~~Gustaf Wallerfelt (Sigund) Charlotte Lindgren (Cyber)~~ och Gunnar Hellenius (avd T), ~~tjf avdelningschefen Eva Hallberg (avd V)~~, kontorschefen Bergquist Frederiksen (avd V/Rätts) samt juristen Kári Ólafsson (avd V/Rätts), tillika föredragande.

Försvarets radioanstalt

Dag Hartelius

Kári Ólafsson

[11] I skäl 171 dataskyddsförordningen anges att behandling som redan pågår den dag då förordningen börjar tillämpas bör bringas i överensstämmelse med förordningen inom en period av två år från det att förordningen träder i kraft.

FRA

Sändlista
För kännedom
Försvarsdepartementet/Sund
Försvarsdepartementet/Rättssekretariatet

Internt FRA
GD
ÖD
Chefsjuristen
C Plan
Informationschefen
Säkerhetsskyddschefen
AC
KC Rätts (Avd V/Rättskontoret)