Ert tjänsteställe, handläggare
Justitiedepartementet

Ert datum
2017-05-15

Er beteckning
Ju2017/04264/L6

Vårt tjänsteställe, handläggare
HKV LEDS JUR Anna Saarikoski,
08-788 96 09, anna.saarikoski@mil.se

Vårt föregående datum

Vår föregående beteckning

Remissyttrande över betänkandet Ny dataskyddslag (SOU 2017:39)

Försvarsmakten har fått betänkandet *Ny dataskyddslag - Kompletterande bestämmelser till EU:s dataskyddsförordning*[1] på remiss och lämnar följande yttrande. Yttrandet följer betänkandets disposition.

Sammanfattning av Försvarsmaktens förslag och synpunkter

Personuppgiftsbehandlingen i delar av Försvarsmaktens kärnverksamhet – försvarsunderrättelseverksamhet och militär säkerhetstjänst – regleras av en heltäckande särreglering genom lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, FM-PUL. Med hänsyn till detta och till att det har tillsatts en utredning om Försvarsmaktens personuppgiftsbehandling[2] vars uppdrag bl.a. innefattar en översyn av rådande särreglering och en analys av en utökning av den samt att försvarssektorns behov av särreglering och sekretess inte har beaktats vare sig i förordningsarbetet eller i betänkandet föreslår Försvarsmakten att tillämpningsområdet begränsas på sätt att dataskyddsförordningen inte ska gälla vid personuppgiftsbehandling som regleras i FM-PUL. Med hänsyn till pågående utredning föreslår Försvarsmakten även en övergångsbestämmelse som rör Försvarsmaktens behandling av personuppgifter i övrig verksamhet som är av betydelse för Sveriges säkerhet. Se närmare under avsnitt 6.4.2 respektive avsnitt 20.

[1] 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).
[2] Fö 2017:03 Behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt, Dir. 2017:42.

- Försvarsmakten anser alltså att 1 kap. 2 § förslaget till dataskyddslag ska kompletteras med ett nytt andra stycke:

  Bestämmelserna i dataskyddsförordningen ska dock inte gälla vid personuppgiftsbehandling som regleras i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

- Försvarsmakten menar även att övergångsbestämmelserna i dataskyddslagen ska kompletteras med en bestämmelse med innebörden att för Försvarsmaktens del ska personuppgiftslagen (1998:204) fortsatt gälla för de delar av myndighetens verksamhet som är av betydelse för Sveriges säkerhet.

- Försvarsmakten menar att det av 1 kap. 2 § förslaget till dataskyddslag uttryckligen ska framgå vilka delar av dataskyddsförordningen som är tillämplig även utanför dataskyddsförordningens tillämpningsområde (med det undantag avseende tillämpningsområdet som Försvarsmakten föreslår ovan), se närmare under avsnitt 6.4.2.

- Försvarsmakten anser att det av dataskyddslagen ska framgå att incidentrapportering och information till den registrerade enligt artiklarna 33 respektive 34 i dataskyddsförordningen inte ska tillämpas i verksamhet som är av betydelse för Sveriges säkerhet, se närmare nedan under avsnitt 6.4.2.

- Försvarsmakten anser att 5 kap. 1 § förslaget till dataskyddslag ska kompletteras så att motsvarande begränsning som föreslås för information till de registrerade enligt artiklarna 13-15 ska gälla avseende information till den registrerade enligt artikel 34, se närmare under avsnitt 13.4.1.

- Försvarsmakten föreslår att undantag i enlighet med artikel 23 ska framgå av dataskyddslagen avseende artikel 21, se närmare under avsnitt 13.4.3.

- Försvarsmakten motsätter sig förslaget att tillsynsmyndigheten ges befogenhet att rikta sanktionsavgifter mot myndigheter, se närmare under avsnitt 18.5.3.

6. Behandling av personuppgifter utanför dataskyddsförordningens tillämpningsområde

6.4.2 Ska förordningens bestämmelser göras gällande utanför deras tillämpningsområde?

Av artikel 2.2 i dataskyddsförordningen framgår att förordningen inte är tillämplig inom verksamhet rörande nationell säkerhet. Av dataskyddsförordningens skäl 16 framgår att

> ”Denna förordning är inte tillämplig på frågor som rör skyddet av grundläggande rättigheter och friheter eller det fria flödet av personuppgifter på områden som inte omfattas av unionsrätten, såsom verksamhet rörande nationell säkerhet. Denna förord-

ning är inte tillämplig på medlemsstaternas behandling av personuppgifter när de agerar inom ramen för unionens gemensamma utrikes- och säkerhetspolitik."

I betänkandet uttalas att det inte är klart exakt vilka verksamheter som faller utanför unionsrättens tillämpningsområde och därmed inte omfattas av dataskyddsförordningen, förutom när det gäller sådan verksamhet som rör nationell säkerhet.[3]

Utredningen föreslår trots detta att dataskyddsförordningen ska göras tillämplig för verksamhet som faller utanför unionsrättens tillämpningsområde, jfr. 1 kap. 2 § förslaget till dataskyddslag. Försvarsmakten motsätter sig en sådan utsträckning av tillämpningsområdet och föreslår att 1 kap. 2 § förslaget till dataskyddslag kompletteras med ett nytt andra stycke:

Bestämmelserna i dataskyddsförordningen ska dock inte gälla vid personuppgiftsbehandling som regleras i lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

Försvarsmaktens kärnuppgift är att upprätthålla och utveckla ett militärt försvar som ytterst kan möta ett väpnat angrepp. Grunden för Försvarsmaktens verksamhet ska vara förmågan till väpnad strid, se förordningen (2007:1266) med instruktion för Försvarsmakten. Den kärnverksamhet som bedrivs av Försvarsmakten faller alltså utanför det som regleras av unionsrätten.

Personuppgiftsbehandlingen i delar av Försvarsmaktens kärnverksamhet – försvarsunderrättelseverksamhet och militär säkerhetstjänst – regleras av en heltäckande särreglering genom lagen (2007:258) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, FM-PUL, med tillhörande förordning.[4] FM-PUL innehåller en uttömmande reglering av förutsättningarna för Försvarsmakten att behandla personuppgifter i försvarsunderrättelseverksamheten och den militära säkerhetstjänsten.[5] Detta särskiljer lagen från registerlagstiftningar. Motsvarande förhållande gäller även för den särreglering som finns för behandling av personuppgifter i delar av Försvarets radioanstalts verksamhet genom lagen (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

Av förarbetena till FM-PUL framgår bl.a. följande.

"Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst och Försvarets radioanstalts underrättelseverksamhet utgör grundläggande och viktiga samhällsfunktioner för Sveriges oberoende och yttre säkerhet. ---
I verksamheterna behandlas en stor mängd personuppgifter och det är nödvändigt för myndigheterna att behandla även känsliga sådana uppgifter. Genom att samla alla

[3] *Ny dataskyddslag - Kompletterande bestämmelser till EU:s dataskyddsförordning* (SOU 2017:39) sid. 91.
[4] Förordningen (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.
[5] Prop. 2006/07:46 sid. 43.

> tillämpliga bestämmelser om behandling av personuppgifter i en lag för Försvarsmakten och en för Försvarets radioanstalt och i därtill hörande förordningar blir det överskådligt och tydligt för myndigheterna vad som gäller, vilket underlättar tillämpningen."[6]

Av datalagsutredningen framgår inte att personuppgiftsbehandlingen i delar av Försvarsmaktens och i Försvarets radioanstalts verksamhet regleras av en heltäckande särreglering som innehåller alla de bestämmelser som ska vara tillämpliga för behandlingen. Utredningen diskuterar heller inte de skäl som lagstiftaren[7] anfört för att inom ramen för dessa områden – vilka faller utanför unionsrätten – uttömmande reglera förutsättningarna för verksamheten i en särlagstiftning för respektive myndighet. Detta borde ha behandlats och medför att utredningens resonemang kring utökning av dataskyddsförordningens tillämpningsområde inte riktigt är fullständigt.

Viktigt att framhålla är även att eftersom dataskyddsförordningen inte omfattar nationell säkerhet har försvarssektorns särskilda behov av särreglering och sekretess inte analyserats i förordningsarbetet.

En utredning har tillsatts om behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt (Fö 2017:03 Behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt, Dir. 2017:42). Utredaren kommer bl.a. att kartlägga Försvarsmaktens personuppgiftsbehandling och analysera om rådande lagstiftning är ändamålsenlig för Försvarsmakten. Utredaren ska även analysera vilket utrymme det finns för nationell reglering av den personuppgiftsbehandling i Försvarsmakten och Försvarets radioanstalt som idag regleras i personuppgiftslagen, och utifrån den analysen bedöma om behandlingen helt eller delvis bör regleras särskilt. Utredaren ska vidare lämna de författningsförslag som behövs och är lämpliga. Utredningen ska redovisa sitt arbete den 31 maj 2018.

Pågående utredningsuppdrag innefattar alltså bl.a. en översyn av gällande reglering och behov av ny lagstiftning, innefattande en analys av en utökad särreglering. Mot bakgrund av föreliggande utredningsuppdrag och att försvarssektorns behov av särreglering och sekretess inte har beaktats vare sig i förordningsarbetet eller i betänkandet föreslår Försvarsmakten att tillämpningsområdet begränsas på sätt att dataskyddsförordningen inte ska gälla vid personuppgiftsbehandling som regleras i FM-PUL. Med hänsyn till pågående utredning föreslår Försvarsmakten även en ytterligare övergångsbestämmelse som rör Försvarsmaktens behandling av personuppgifter i övrig verksamhet som är av betydelse för Sveriges säkerhet, se närmare under avsnitt 20.

[6] Prop. 2006/07:46 sid. 45.
[7] Se prop. 2006/07:46.

Avgränsningen av det utsträckta tillämpningsområdet ska framgå av dataskyddslagen

Av 1 kap. 2 § förslaget till dataskyddslag framgår att dataskyddsförordningen ska utsträckas till att "i tillämpliga delar" gälla utanför unionsrätten. I författningskommentaren till bestämmelsen anges att kapitel VII och kapitel X i dataskyddsförordningen inte utgör tillämpliga delar. Det uttalas vidare att det även i övrigt kan finnas bestämmelser i dataskyddsförordningen som inte kan tillämpas i rent nationell verksamhet och att det därför i varje enskilt fall får göras en bedömning av om en viss förordningsbestämmelse kan gälla (sid. 354, se även sid. 92-93).

Att föreslå att ett regelverk görs tillämpligt utanför dess ursprungliga tillämpningsområde utan att på förhand utreda vilka delar som rättsligt kan göras tillämpliga enligt nationell rätt, vilket först då möjliggör en full överblick av konsekvenserna av en sådan ordning, är inte tillfredsställande. Vidare leder nu föreslagen lydelse av 1 kap. 2 § förslaget till dataskyddslag till osäkerhet i rättstillämpningen.

Enligt Försvarsmaktens uppfattning ska det därför av 1 kap. 2 § i förslaget till dataskyddslagen uttryckligen framgå vilka delar av dataskyddsförordningen som är tillämpliga även utanför dataskyddsförordningens tillämpningsområde (med det undantag avseende tillämpningsområdet som Försvarsmakten föreslår ovan genom ett nytt andra stycke i 1 kap. 2 § i förslaget till dataskyddslag).

Ett exempel på denna otydlighet är avsnitt 19.6.3 i betänkandet (sid. 323) som refererar till artikel 62.3 dataskyddsförordningen. Enligt artikeln får en tillsynsmyndighet tilldela befogenheter, även utredningsbefogenheter, till ledamöter eller personal från en annan medlemsstats tillsynsmyndighet som deltar i gemensamma insatser. Utredningen konstaterar att bestämmelser innebär att företrädare för en utländsk tillsynsmyndighet kan ges befogenhet att utöva offentlig makt i Sverige.

Avsnittet innehåller ingen påminnelse om att artikeln ingår i ett kapitel som inte kan göras tillämpligt utanför unionsrättens tillämpningsområde och detta framgår som sagt inte heller av 1 kap. 2 § förslaget till dataskyddslag. Denna otydlighet leder till tillämpningsproblem och är otillfredsställande. Inte minst mot bakgrund av att vid en tillsyn av verksamhet som omfattar Sveriges säkerhet kan tillsynsmyndigheten komma att ta del av information som omfattas av försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen (2009:400).

Artiklarna 33 och 34 om personuppgiftsincidenter och information till den registrerade – bör inte göras tillämpliga i verksamhet som är av betydelse för Sveriges säkerhet

Försvarsmakten motsätter sig att artikel 33 i dataskyddsförordningen – som rör rapportering av personuppgiftsincidenter till tillsynsmyndigheten – ska göras tillämplig i verksamhet som är av betydelse för Sveriges säkerhet. Detsamma gäller kravet på information till den registrerade enligt artikel 34 i dataskyddsförordningen.

Enligt 10 a § säkerhetsskyddsförordningen (1996:633) ska myndigheter rapportera it-incidenter som bl.a. allvarligt kan påverka säkerheten i ett system som behandlar hemliga uppgifter i en omfattning som inte är ringa. Rapportering ska ske till Försvarsmakten eller Säkerhetspolisen inom ramen för respektive myndighets tillsynsområde enligt 39 § säkerhetsskyddsförordningen. I 20 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen) regleras en skyldighet för myndigheter att rapportera it-incidenter till Myndigheten för samhällsskydd och beredskap. Incidentrapporteringen enligt denna förordning omfattar emellertid inte sådana incidenter som ska rapporteras enligt säkerhetsskyddsförordningen.

I sammanhanget kan även nämnas att för den it-incidentrapportering som föreslås i samband med införandet av det s.k. NIS-direktivet[8] undantas it-incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.[9] Detsamma gäller avseende den rapportering av personuppgiftsincidenter som föreslås i betänkandet *Brottsdatalag* (SOU 2017:29).[10]

En samlad dokumentation av personuppgiftsincidenter för försvarssektorn, i vilken även totalförsvaret inbegrips, är information som samtidigt kan röja uppgifter som är av betydelse för rikets säkerhet jfr. 15 kap. 2 § offentlighets- och sekretesslagen. Dokumentation kring incidenter kommer att visa på sårbarheter i berörda system och kan till exempel visa på hur man kan kringgå skyddsåtgärder för att få obehörig tillgång till systemen. Kunskap om en personuppgiftsincident kan på så vis ge en motståndare uppgifter som underlättar vidare angrepp och inhämtning.

Just risken för informationsspridning uppmärksammades av den nyligen redovisade brottsdatalagsutredningen. Utredningen ansåg att behovet av att skydda hemliga uppgifter som rör Sveriges säkerhet var så viktigt att endast den myndighet som utövar tillsyn över säkerhetsskyddet skulle få del av dessa. Brottsdatalagsutredningen konstaterade även att eftersom nationell säkerhet låg utanför tillämpningsområdet för det direktiv[11] som brottsdatalagen föreslås implementera skulle personuppgiftsincidenter som ska anmälas enligt 10 a § säkerhetsskyddsförordningen inte anmälas till tillsynsmyndigheten för den föreslagna brottsdatalagen.[12]

Incidentrapporteringen enligt säkerhetsskyddsförordningen eller krisberedskapsförordningen tar visserligen inte främst sikte på säkerhetsincidenter där personuppgifter på olika sätt röjts, jfr. artikel 4.12 dataskyddsförordningen. Oavsett anledningen till att en it-incident rapporteras syftar en sådan rapportering till att uppmärksamma brister i skyddet av information för att därefter vidta åtgärder för att säkerställa detta. Om en it-incident inträffar i ett sy-

[8] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.
[9] *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36) sid. 87.
[10] Se 3 kap. 9 § förslaget till brottsdatalag och sid. 331 f.
[11] Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.
[12] *Brottsdatalag* (SOU 2017:29) sid. 331.

stem med personuppgifter kommer alltså de skyddsåtgärder och säkerhetshöjande åtgärder som vidtas med anledning av incidenten att stärka skyddet även för personuppgifterna och därmed för den personliga integriteten.

Med hänsyn till riskerna för informationsspridning, se resonemang ovan, tillsammans med att befintliga regelverk redan tillhandahåller system för att säkerställa att it-incidenter – även sådana rörande personuppgifter – uppmärksammas och omhändertas, bör artiklarna 33 och 34 i dataskyddsförordningen undantas för verksamhet som är av betydelse för Sveriges säkerhet genom en bestämmelse i dataskyddslagen. Exempel på verksamhet som är av betydelse för Sveriges säkerhet *kan* vara it-incidenter som ska rapporteras enligt 10 a § säkerhetsskyddsförordningen.[13]

Försvarsmakten föreslår att tillämpningsområdet ska avgränsas avseende "verksamhet som är av betydelse för Sveriges säkerhet." En sådan avgränsning följer den föreslagna inskränkningen för tillämpningsområdet för den lag som ska implementera det NIS-direktivet.[14] Uppgifter som omfattas av försvarssekretess enligt 15 kap. 2 § offentlighets- och sekretesslagen kan förekomma hos andra myndigheter än Försvarsmakten. Den valda avgränsningen säkerställer att personuppgiftsincidenter som röjer försvarssekretess även hos andra myndigheter inte sprids annat än till den myndighet som utövar tillsyn över säkerhetsskyddet. Mot denna bakgrund föreslås att motsvarande begrepp används i dataskyddslagen för att avgränsa dataskyddsförordningens tillämpningsområde.

13. Begränsningar av vissa rättigheter och skyldigheter i dataskyddsförordningen

Dataskyddsförordningen ger medlemsstaterna möjlighet att begränsa omfattningen av vissa av de skyldigheter och rättigheter som förordningen föreskriver. Utredningen föreslår i 5 kap. 3 § förslaget till dataskyddslag ett bemyndigande för regeringen att meddela föreskrifter om ytterligare begränsningar enligt artikel 23 i dataskyddsförordningen. Försvarsmakten ställer sig positiv till ett sådant bemyndigande men menar att dataskyddslagen även borde innehålla en begränsning enligt artikel 23 i dataskyddsförordningen för artiklarna 21 och 34 i dataskyddsförordningen.

[13] Tillämpningsområdet för nuvarande säkerhetsskyddslagstiftning är dock inte ensamt är avgörande för vad som utgör verksamhet som är av betydelse för Sveriges säkerhet. Säkerhetsskyddslagstiftningen omfattar exempelvis inte system som inte innehåller hemliga uppgifter men vars funktion eller tillgänglighet är av avgörande betydelse för totalförsvaret eller det militära försvaret. Värt att nämna är att i betänkandet *En ny säkerhetsskyddslag* (SOU 2015:25) föreslås ett bredare tillämpningsområde som innebär att sådana system kommer att omfattas av den nya säkerhetsskyddslagen.

[14] I betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster* (SOU 2017:36) föreslås att lagen inte ska vara tillämplig på verksamhet som är av betydelse för Sveriges säkerhet, jfr. 6 § i lagförslaget. Denna avgränsning speglar även artikel 1.6 i NIS-direktivet vari det anges att direktivet inte påverkar medlemsstaternas åtgärder för att skydda sina väsentliga statliga funktioner, särskilt för att skydda den nationella säkerheten, inklusive åtgärder för skydd av information vars avslöjande medlemsstaterna anser strida mot sina väsentliga säkerhetsintressen.

13.4.1 Sekretess och tystnadsplikt ska gå före informationsplikten

5 kap. 1 § förslaget till dataskyddslag innebär att skyldigheten för den personuppgiftsansvarige att lämna information om och tillgång till de personuppgifter som behandlas i enlighet med artiklarna 13-15, inte ska gälla uppgifter som på grund av sekretess eller tystnadsplikt inte får lämnas ut till den registrerade. Motsvarande reglering återfinns även i 27 § personuppgiftslagen och i 2 kap. 4 § FM-PUL.

Eftersom sekretess även kan aktualiseras för information om dataskyddsincidenter bör 5 kap. 1 § i förslaget till dataskyddslag kompletteras så att motsvarande begränsning även gäller avseende information till den registrerade enligt artikel 34 dataskyddsförordningen. En sådan begränsning av information till den registrerade vid en personuppgiftsincident har föreslagits av brottsdatalagsutredningen för brottsdatalagen.[15]

13.4.3 Något om rätten att göra invändningar

Dataskyddsförordningen innehåller genom artikel 21 en bestämmelse om rätten att göra invändningar mot bl.a. en myndighets personuppgiftsbehandlingar (behandlingar som grundar sig på artikel 6.1e, allmänt intresse eller myndighetsutövning). Utredningen konstaterar att rätten att invända mot en personuppgiftsbehandling föreskrivs redan i dataskyddsdirektivet och att denna rätt endast är genomförd i personuppgiftslagen avseende direkt marknadsföring, se 11 § personuppgiftslagen.

Utredningen slår vidare fast att det enligt gällande svensk rätt inte finns någon generell rätt för den registrerade att invända mot behandling av personuppgifter som sker hos myndigheter. Försvarsmakten vill i sammanhanget framhålla att det som utmärker en myndighets personuppgiftsbehandling är att den är föranledd av de uppdrag som riksdag och regering genom författningar har givit åt myndigheten att lösa.

Dataskyddsförordningen innehåller – på motsvarande sätt som gäller idag – en rad rättigheter för den registrerade att åstadkomma ändring av en felaktig personuppgiftsbehandling genom rätten till information (artikel 15), rätten till rättelse (artikel 16), rätten till radering (artikel 17) och rätten till begränsning av behandling (artikel 18).

Mot bakgrund av att myndigheternas personuppgiftsbehandling i princip uteslutande sker inom ramen för ett offentligrättsligt uppdrag och den registrerades möjligheter att åtgärda en felaktig personuppgiftsbehandling tillgodoses genom artiklarna 15-18 i dataskyddsförordningen anser Försvarsmakten att undantag i enlighet med artikel 23 ska meddelas avseende artikel 21.

[15] *Brottsdatalag* (SOU 2017:29), se i författningsförslaget 3 kap. 11 § och sid. 337.

18.5 Sanktionsavgift inom offentlig sektor

18.5.3 Överväganden och förslag

Försvarsmakten motsätter sig utredningens förslag att införa en ny administrativ sanktion för myndigheter. I betänkandet *Myndighetsdatalag* (SOU 2015:39, sid. 631-632) diskuterades frågan om tillsynsmyndighetens befogenheter att rikta beslut om vite, som är en annan typ av ekonomisk sanktion, gentemot en annan myndighet.

Myndighetsdatalagsutredningens förslag var på denna punkt motsatt förslaget i förevarande betänkande – tillsynsmyndigheten skulle inte ges befogenhet att besluta om vite. Myndighetsdatalagsutredningen konstaterade att behandling av personuppgifter hos myndigheter i princip uteslutande sker inom ramen för ett offentligrättsligt uppdrag. Myndighetsdatalagsutredningen uttalade vidare följande.

> ”Enligt vår uppfattning innebär statliga myndigheters behandling av personuppgifter, som är en integrerad del i en myndighets hela verksamhet och myndighetsutövning, inte på något sätt att myndigheter kan anses agera på en marknad eller av annat skäl bör jämställas med eller anses agera som ett privaträttsligt subjekt. Eftersom dessa 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 finns inga bärande skäl för att i alla delar ha samma sanktionsmöjligheter mot både myndigheter och enskilda. Det finns därmed 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.”

Det som framförs av myndighetsdatalagsutredningen ifråga om möjligheten att rikta viten mot myndigheter är av relevans även för frågan om sanktionsavgifter. Förevarande betänkande tar emellertid inte upp det som myndighetsdatalagsutredningen lyfter på sidorna 631-632 vilket borde ha behandlats.

Försvarsmakten delar myndighetsdatalagsutredningens uppfattning att tillsynsmyndigheten inte ska ges befogenhet att rikta olika former av ekonomiska sanktioner mot myndigheter. Som framhålls i datalagsutredningen (sid. 296) kan överträdelser ifråga om personuppgiftsbehandling för myndigheters del – utöver skadestånd enligt dataskyddsförordningen och flera straffsanktioner i brottsbalken – beivras med ansvar för tjänstefel. Mot denna bakgrund avstyrker Försvarsmakten förslaget om sanktionsavgifter för offentlig sektor.

20. Ikraftträdande- och övergångsbestämmelser

Av de föreslagna övergångsbestämmelserna framgår att dataskyddslagen träder i kraft den 25 maj 2018, samma dag som dataskyddsförordningen träder ikraft, och att personuppgiftslagen samtidigt upphävs. Det framgår vidare att personuppgiftslagen fortsatt kommer att gälla i

den utsträckning som det i en annan lag eller förordning finns bestämmelser som innehåller hänvisningar till personuppgiftslagen.

Som ovan nämnts har en utredning tillsatts om behandling av personuppgifter inom Försvarsmakten och Försvarets radioanstalt. Utredningsuppdraget innefattar bl.a. en översyn av rådande lagstiftning och en analys av en utökad särreglering.

Som nämnts under avsnitt 6.4.2 har försvarssektorns behov av särreglering och sekretess inte beaktats vare sig i arbetet med dataskyddsförordningen – eftersom dessa områden faller utanför tillämpningsområdet – eller i betänkandet. Mot denna bakgrund och med hänsyn till pågående utredningsuppdrag menar Försvarsmakten att dataskyddslagen ska kompletteras med en övergångsbestämmelse av innebörden att för Försvarsmaktens del ska personuppgiftslagen fortsatt gälla för de delar av myndighetens verksamhet som är av betydelse för Sveriges säkerhet (d.v.s. som faller utanför unionsrätten).

I beredningen av detta yttrande har Zenobia Rosander, avdelningsdirektör tillika personuppgiftsombud, Catharina Hammarström, byrådirektör, Jan Wünsche, it-säkerhetsstrateg, Alexandra Larsson, strategisk arkitekt för informationshantering, och Anna Karlheden, verksamhetsutvecklare, deltagit.

Detta remissyttrande har beslutats av Carin Bratt, chefsjurist. I den slutliga handläggningen har dessutom deltagit Anna Asp, ställföreträdande chef Juridiska avdelningen, Annika Grahn Sulusi, sektionschef, och som föredragande Anna Saarikoski, försvarsjurist tillika personuppgiftsombud.

Carin Bratt
Chefsjurist

Anna Saarikoski

Sändlista
Regeringskansliet (Justitiedepartementet)

För kännedom
Försvarsdepartementet
HKV LEDS STAB ÖB GD
HKV LEDS CIO
MUST