Justitiedepartementet
Grundlagsenheten, L6
David Törngren,103 33 Stockholm

Er referens/dnr
Ju2017/0426/L6

Stockholm den 31 augusti 2017

Remissyttrande över ”En ny dataskyddslag – Kompletterande bestämmelser till EU:s dataskyddsförordning” (SOU 2017:39)

Sammanfattning

Beträffande betänkandet i sin helhet har Teknikföretagen och SOFF anslutit sig till det remissyttrande som inlämnats av Svenskt Näringsliv, men vi vill för egen del särskilt framhålla följande.

Teknikföretagen och Säkerhets- och Försvarsföretagen (SOFF) har granskat utredningens förslag mot bakgrund av de särskilda intressen som organisationerna företräder i enlighet med vad som framgår nedan under rubriken Bakgrund.

Det är Teknikföretagens och SOFF:s uppfattning att utredningens förslag bör förtydligas när det gäller hanteringen av känsliga personuppgifter som rör lagöverträdelser.

I de kompletterande bestämmelser som ska reglera hanteringen av personuppgifter som rör lagöverträdelser bör regeringen ge uttryck för att svenska företag ska tillåtas behandla uppgifter om lagöverträdeselser på sätt som gör det möjligt att efterfölja rättsliga och kontraktuella förpliktelser avseende exportkontroll när det gäller andra länders teknik, t.ex. de amerikanska regelverken avseende exportkontroll av amerikansk försvarsteknik och produkter med dubbla användningsområden. Detta bör ske genom en reglering i den kompletterande dataskyddslagen alternativt i förordningen till dataskyddslagen.

Om en sådan reglering inte skulle meddelas som komplement till artikel 10 i EU:s dataskyddsförordning riskerar detta att försvåra och i vissa fall omöjliggöra en stor del av den verksamhet som bedrivs hos Teknikföretagen och SOFF:s medlemmar.

Vidare bör utredningens förslag avseende möjligheten att sanktionsavgift ska få tas ut vid överträdelser av artikel 10 i dataskyddsförordningen inte införas.

Bakgrund

Teknikföretagen företräder ca 3 800 medlemsföretag. Flera av våra medlemsföretag är verksamma inom säkerhets- och försvarsområdet med utveckling och tillverkning av tekniskt avancerade produkter för såväl civila som militära ändamål. Flera av dessa företag företräds dessutom av

Teknikföretagen
Box 5510, 114 85 Stockholm
Storgatan 5, Stockholm
Telefon 08-782 08 00
Fax 08-782 09 00
www.teknikforetagen.se

branschorganisationen Säkerhets- & Försvarsföretagen (SOFF) som har ca 90 medlemsföretag.

Att det i Sverige finns företag som är verksamma inom säkerhets- och försvarsområdet är önskvärt av flera skäl. Genom tillgång till inhemskt utvecklade och tillverkade försvarsprodukter kan Sverige, inom vissa delområden, undvika att utveckla osunda beroendeförhållanden till andra länder. Vidare kan en stark och innovativ säkerhets- och försvarsindustriell bas bidra till bättre förutsättningar för svenskt deltagande i internationellt materielsamarbete och ytterst till att Försvarsmakten får tillgång till mer avancerad försvarsteknik.

Från ett bredare samhällsekonomiskt perspektiv är säkerhets- och försvarsföretag viktiga eftersom de genom extensiv forskning och produktutveckling bidrar till att upprätthålla svensk industri som en kunskapsintensiv bransch med förmåga att hävda sig i den internationella konkurrensen.

Säkerhets- och försvarsföretag i Sverige är emellertid i allt större omfattning i behov av internationellt samarbete för att utveckla de avancerade plattformar, system och produkter som efterfrågas på försvarsmarknaden. Det innebär att företagen även måste kunna få tillgång till försvarsteknik som utvecklats i andra länder.

Sverige har ett mycket omfattande försvarstekniskt samarbete med USA och flera europeiska länder. USA är den ledande tillverkaren av försvarsprodukter och står för en mycket stor del av den utveckling som bedrivs avseende säkerhets- och försvarsprodukter. Många av de plattformar, system och produkter som tillverkas i Sverige innehåller därför amerikanska delkomponenter. Sverige är härigenom starkt beroende av tillgång till amerikansk högteknologi. Det skulle till exempel vara omöjligt att producera och exportera Gripen utan godkännande från USA, då bland annat flygplanets motor är från USA. I själva verket är Gripen helt beroende av amerikansk försvarsteknik.

Av säkerhetspolitiska skäl finns det i USA sedan länge omfattande restriktioner avseende vilken försvarsteknik som får exporteras till andra länder samt även hur försvarstekniken får vidareexporteras. Detta gäller även teknik som kan ha så kallade dubbla användningsområden. De amerikanska exportrestriktionerna innebär bland annat att personer som finns med på vissa spärrlistor inte får ges tillgång till amerikansk försvarsteknik. Spärrlistornas syfte är att bekämpa terrorism och andra allvarliga brott och oegentligheter.

USA hävdar att det amerikanska regelverket i dessa delar har extraterritoriell tillämplighet, vilket innebär att också svenska företag måste förhålla sig till reglerna. Då begreppet ”export” enligt amerikansk lagstiftning innefattar varje situation när en person av annan nationalitet än amerikansk på något sätt kommer i kontakt med eller tar del av exportkontrollerade uppgifter eller materiel innebär detta att svenska företag måste kontrollera personer – anställda, leverantörer, kunder, samarbetspartners – gentemot spärrlistorna. Eftersom ett skäl till att dessa personer finns medtagna på spärrlistorna kan vara att de begått brott eller misstänks ha begått brott förutsätter denna kontroll en hantering av personuppgifter som kan innefatta uppgifter som rör lagöverträdelser. Nedan ges en kort beskrivning av de amerikanska regelverken och de konsekvenser som kan bli aktuella om regelverken inte efterföljs.

Personuppgifter som rör lagöverträdelser, Kompletterande bestämmelser till EU:s dataskyddsförordning 3 kap 9 – 12 §§

Artikel 10 i dataskyddsförordningen reglerar hanteringen av personuppgifter som rör lagöverträdelser. Utredningens uppdrag har i denna del varit att analysera behovet av kompletterande regler som ska tillåta behandling av uppgifter om lagöverträdelser som inte sker under kontroll av en myndighet.

Enligt utredningens förslag ska det vara möjligt för andra än myndigheter att behandla personuppgifter dels genom att Datainspektionen i enskilda fall meddelar beslut om att tillåta sådan behandling, dels genom att det framgår i förordning eller meddelade föreskrifter från Datainspektionen att behandling är tillåten.

När det gäller det senare skriver utredningen att det framkommit behov av en föreskrift som tillåter behandling av sådana uppgifter om lagöverträdelser som måste behandlas till följd av rättsliga förpliktelser och det konstateras att sådana förpliktelser exempelvis skulle kunna förekomma i regleringar som ”… syftar till att bekämpa t.ex. korruption, terrorism… och olämplig spridning av vapenteknologi” (s. 195). Utredningen uppger att de inte haft möjlighet att närmare utreda i vilken utsträckning sådana rättsliga förpliktelser redan förekommer och om de i så fall står i strid med dataskyddsförordningens och de av utredningen föreslagna bestämmelserna om behandling av personuppgifter som rör lagöverträdelser. Utredningen konstaterar dock att den typen av normkonflikt skulle vara problematisk.

Vi instämmer i utredningens bedömning att en normkonflikt på detta område skulle vara problematisk och vi förordar att regeringen i de kompletterande bestämmelser som ska reglera hanteringen av personuppgifter som rör lagöverträdelser bör ge uttryck för att svenska företag ska tillåtas behandla uppgifter om lagöverträdeselser på sätt som gör det möjligt att efterfölja de amerikanska regelverken avseende exportkontroll av amerikansk teknik. Detta bör i ske genom en reglering i förordningen till dataskyddslagen.

En anledning till att detta bör tydliggöras är att det av artikel 6.1 i dataskyddsförordningen framgår att varje behandling av personuppgifter måste vila på en rättslig grund och för det fall att den rättsliga grunden följer av artikel 6.1 c – behandlingen är nödvändig för att fullgöra en rättslig förpliktelse – ska grunden för behandlingen enligt artikel 6.3 första stycket dataskyddsförordningen fastställas i enlighet med unionsrätten eller den nationella rätten.

Utredningen konstaterar här att ett av syftena med artikel 6.3 första stycket har antagits vara att tydliggöra att en personuppgiftsansvarig inte får finna en rättslig grund för behandling av personuppgifter i tredje lands lagstiftning, då bestämmelsen innebär att en rättslig förpliktelse som följer av tredje lands lagstiftning inte utgör en rättslig grund för behandling av personuppgifter (s. 110).

Utredningen konstaterar även att det av skäl 41 till förordningen framgår att den rättsliga grunden bör vara tydlig och precis och dess tillämpning förutsägbar för dem som omfattas av den (s. 112).

Mot bakgrund av dessa skrivningar bör det i första hand genom förordningen till dataskyddslagen tydliggöras vilka rättsliga förpliktelser som kan ligga till grund för svenska företags behandling av uppgifter om lagöverträdelser och att dessa

innefattar rättsliga förpliktelser för uppfyllande av de amerikanska exportrestriktionerna.

I andra hand bör detta framgå av föreskrift som Datainspektionen har att meddela. Regeringen bör då på ett tydligare sätt än vad som framgår av utredningens förslag lämna uppdrag till Datainspektionen att på detta område meddela föreskrift med innebörd att företag tillåts behandla uppgifter om lagöverträdeselser på sätt som gör det möjligt att efterfölja de amerikanska regelverken på detta område.

Administrativa sanktionsavgifter, Kompletterande bestämmelser till EU:s dataskyddsförordning 7 kap 2 §

Utredningens förslag till lagtext i 7 kap 2 § innebär att sanktionsavgifter motsvarande den övre beloppsgränsen enligt artikel 83.5 i dataskyddsförordningen ska få tas ut även vid överträdelser av artikel 10 förordningen. Att det i dataskyddsförordningen inte är möjligt bedöms enligt utredningen vara ”… en oavsiktlig konsekvens…” (s. 280) att artikel 10 inte redan omfattas av de sanktioner som finns i artikel 83 dataskyddsförordningen.

Det kan inte uteslutas att det inte är ett misstag som skett på EU-nivå när artikel 10 i dataskyddsförordningen inte omnämns i artikel 83.

Vi ser inte någon anledning att redan i detta skede öka möjligheterna till administrativa sanktionsåtgärder. I den mån det skett ett misstag i EUs lagstiftningsarbete så är det ju självklart upp till EU att korrigera det. Från vårt perspektiv måste det vara uteslutet att endast Sverige på detta sätt utökar möjligheten till administrativa sanktionsavgifter.

Skulle förslaget bli lagstiftning kommer den av utredningen föreslagna sanktionsavgiften kommer enbart att drabba privata aktörer som behandlar personuppgifter i strid med artikel 10. Sanktionsavgifterna kan komma att bli mycket höga. För att inte svenska företag ska hamna i en märkbart sämre position jämfört med andra europeiska bolag måste det under alla omständigheter klarläggas att liknande utökning av möjligheten att besluta om administrativa sanktionsavgifter kommer att införas i övriga EU-länder. I annat fall skulle svenska företag inte enbart drabbas ekonomiskt vid en eventuell överträdelse utan regleringen i sig skulle kunna innebära en kraftig konkurrensbegränsning i förhållande till andra EU-länder. Så kan fallet bli mot bakgrund av vad som redovisats avseende den potentiella konflikten med amerikansk lagstiftning.

De amerikanska regelverken och konsekvenser som kan bli aktuella om regelverken inte efterföljs

De amerikanska exportrestriktionerna - regelverken och spärrlistorna

Som vi nämnt ovan har USA ett mycket omfattande exportkontrollsystem som även reglerar export till tredje land. Det innebär att export av svenska produkter som innehåller teknik eller produkter från USA kräver USA:s godkännande innan export till tredje land kan ske. Ett sådant godkännande sker genom avtal om exportlicenser.

En del av detta system hanteras av US Department of State och avser bland annat det så kallade ITAR-regelverket (International Traffic in Arms Regulations).

Dessa regler tar främst sikte på amerikansk utrikespolitik och intern säkerhet i USA (US national security). Produkterna som omfattas anges i US Munitions List (USML), dvs. försvarsrelaterade produkter.

Ytterligare en del av exportkontrollsystemet hanteras av US Department of Commerce, Bureau of Industry and Security (BIS) och avser bland annat EAR-regelverket (Export Administration Regulations). Dessa regler har även till mål att tillgodose USA:s ekonomiska intressen. Produkterna som omfattas anges i CCL (Commerce Control List). Eftersom USA har en s.k. catch-all klassificering i form av EAR99 gäller det nämnda regelverket för samtliga produkter som svenska företag köper från USA och som säljs till sanktionerade länder. Särskilt svårt kan detta då bli för företag som säljer produkter med dubbla användningsområden. Syftet med regelverken rörande produkter med dubbla användningsområden är att säkerställa att produkter eller teknik som kan användas för att utveckla, producera eller använda kemiska, biologiska eller nukleära vapen eller dess bärare inte ska falla i orätta händer, såsom till exempel terrorister, organiserade brottslingar eller icke önskvärda länder.

De amerikanska exportkontrollreglerna är som tidigare nämnts extraterritoriella, vilket innebär att USA anser att de är tillämpliga även utanför amerikanskt territorium, och reglerna innebär bland annat att personer som finns med på vissa spärrlistor inte får ges tillgång till amerikansk försvarsteknik. Spärrlistornas syfte är att bekämpa terrorism och andra allvarliga brott och oegentligheter.

Spärrlistor finns av flera olika slag. Även EU publicerar spärrlistor som bilagor till EU-förordningar då sanktioner beslutats inom ramen för EU. De amerikanska spärrlistorna är offentliga och innehåller uppgifter om både företag och enskilda individer med namn, adressuppgifter och organisationsanknytning. Dessa uppgifter ska beaktas i samband med internationella affärer, till exempel orderhantering och betalning, och företag och enskilda åläggs skyldigheter som till exempel anmälningsskyldighet eller förbud mot att handla med på listorna angivna personer.

Sanktionsprogrammen och tillhörande listor är som huvudregel tillämpliga på samtliga företag, både amerikanska och utländska, som handlar med amerikanskt kontrollerade produkter och teknologi som räknas som produkter med dubbla användningsområden samt militära produkter och teknologi. Även exempelvis rättshandlingar företagna av juridiska personer som är etablerade i USA (inklusive utländska filialer) inkluderas. Några av sanktionsprogrammen har ett ännu vidare tillämpningsområde och omfattar även utländska dotterbolag till amerikanska företag och på grund av den extraterritoriella tillämpningen länder som hanterar amerikanska produkter och teknik.

Ett annat regelverk som omfattar listor hanteras av myndigheten OFAC, Office of Foreign Assets Controls, som är organiserad under U.S. Department of the Treasury (US DoT), vilken administrerar och upprätthåller ekonomiska sanktioner och handelssanktioner. Dessa sanktioner kan avse alla typer av produkter, dvs. inte bara sådana som har strategisk betydelse. Sanktionerna innebär att transaktioner med s.k. Specially Designated Nationals and Blocked Persons (SDN) ska blockeras eller frysas. Detsamma gäller tillgångar som tillhör en SDN.

BIS Denied-Persons-listan administreras av BIS (Bureau of Industry and Security) och rör restriktioner för transaktioner med parter som nekats exporträttigheter på grund av brott mot amerikanska exportkontrollagar och

exportkontrollföreskrifter. Restriktionerna är tillämpliga vid transaktioner med varor/materiella tillgångar (inklusive mjukvara och teknologi) som är föremål för bestämmelserna i EAR, inklusive varor med ett amerikanskt ursprung oavsett var varan finns. Vidare omfattas utländska varor som innehåller mer än en miniminivå av amerikanska produkter som är föremål för amerikanska exportbestämmelser, samt vissa utlandstillverkade produkter som inbegriper amerikansk ursprungsteknik eller mjukvara.

Andra listor som omfattas är BIS Entity-listan och ISN Nonproliferation-listan bestående av både företag och enskilda personer.

För att kunna svara upp mot de amerikanska reglerna måste svenska företag säkerställa att reexport av amerikansk teknologi eller produkter inte sker till personer eller företag som finns på de aktuella spärrlistorna. Företagen kommer då att hantera personuppgifter som kan komma att innefatta uppgifter som rör lagöverträdelser.

Möjliga konsekvenser om de amerikanska regelverken inte efterföljs

När det gäller kontrollen av efterlevnaden av de amerikanska exportrestriktionerna kan nämnas att t.ex. den lista som kopplas mot ITAR-regelverket övervakas genom ett strikt kontrollprogram genomfört av USA:s utrikesdepartement genom de amerikanska ambassaderna i utlandet. Kontrollprogrammet kallas “Blue Lantern” och tillsynsbesök görs hos företag och slutanvändare i 80 – 100 länder årligen.

För det fall att ett svenskt företag inte skulle kunna efterleva den amerikanska lagstiftningen – t.ex. på grund av att det svenska företag inte får hantera personuppgifter som rör lagöverträdelser – kan konsekvenserna bli allvarliga för företaget.

Vid överträdelser av den amerikanska lagstiftningen i detta avseende riskerar företag att påföras höga böter - att bryta mot ITAR medför $1,000,000 i böter per förseelse och brott mot EAR innebär upp till $ 284,582 per förseelse. I båda fallen riskerar det svenska företaget även att förlora sina exportlicenser och olika andra typer av tillstånd samt att själv hamna på spärrlistan. Om ett företag förlorar sin exportlicens och därmed rätten att köpa amerikanska produkter och teknik kommer företag inte heller att kunna uppfylla skyldigheter i avtal, vilket i förlängningen t.ex. skulle kunna innebära uteblivna leveranser till det svenska försvaret och att den svenska staten inte längre kan säkerställa sin materielförsäljning, särskilt där staten har ett systemberoende.

Ytterligare en konsekvens för svenska företag med amerikanskt ägande kan bli att verksamhet inte längre kan bedrivas i Sverige utan måste flyttas till annat land. Detta då ett amerikanskt moderbolag – precis som det svenska dotterbolaget – kan förlora sin exportlicens för det fall att det svenska dotterbolaget inte efterlever de amerikanska regelverken.

Detta är konsekvenser som skulle kunna komma att drabba svenska företag generellt om inte svenska företag tillåts behandla uppgifter om lagöverträdeselser på sätt som gör det möjligt att efterfölja de amerikanska regelverken på detta område. Dessa konsekvenser har inte beaktats av utredningen i den ekonomiska konsekvensanalys för enskilda som utredningen presenterar (s. 349).

I sammanhanget vill vi framhålla att problematiken inte är ny. Teknikföretagen och SOFF har redan tidigare pekat på utmaningarna att efterleva utländska exportrestriktioner i Sverige, bl.a. vid besök på Näringsdepartementet för ett antal år sedan och i remissyttrande över förlag till en modernare säkerhetsskyddslag.

Vi har även noterat att andra organisationer har fått dispens från förbudet i nuvarande 21 § personuppgiftslagen för andra än myndigheter att behandla personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Som exempel kan nämnas att Bankföreningen i ett ansökningsförfarande avseende löpande kontroller av sina kunddatabaser mot den ovan nämnda OFAC-listan beviljades tillstånd att behandla personuppgifter om lagöverträdelser i syfte att kunna motverka penningtvätt och terrorism. För de syften som vi nämner i detta yttrande har det hittills inte varit möjligt att få gehör för ett sådant undantag, vilket förefaller märkligt. Liksom att motverka finansiering av terrorism måste det vara möjligt att motverka att vapenteknik och produkter med dubbla användningsområden sprids till personer som finns upptagna på listor med personer som inte ska få tillgång till sådan teknik.

Som ovan

Teknikföretagen

Klas Wåhlberg

Säkerhets- och försvarsföretagen

Robert Limmergård