SVENSKT NÄRINGSLIV

Justitiedepartementet
Grundlagsenheten, L6
David Törngren

103 33 Stockholm

Vår referens/dnr:
86/2017

Er referens/dnr:
Ju2017/04264/L6

2017-08-31

Remissvar

Betänkandet "Ny dataskyddslag - Kompletterande bestämmelser till EU:s dataskyddsförordning (SOU 2017:39)

Svenskt Näringsliv inkommer med remissvar uppdelat i två delar. Del 1 innehåller näringspolitiska aspekter och del 2 innehåller kommentarer ur ett arbetsrättsligt perspektiv.

DEL 1: Näringspolitiska synpunkter

Denna del av remissyttrande har tagits fram i samverkan med Svenskt Näringslivs branschövergripande digitala policygrupp.

Sammanfattning

Svenskt Näringsliv tillstyrker föreslagen 13 års gräns för inhämtande av samtycke.
Svenskt Näringsliv anser att absolut sekretess bör gälla vid tillsynsmyndighetens hantering av tillståndsärenden, tillsyn, förhandssamråd samt dataincidentrapportering.
Svenskt Näringsliv avstyrker föreslagen implementering av artikel 10 dataskyddsförordningen om behandling av personuppgifter som rör fällande domar i brottmål samt lagöverträdelser, vilket utvecklas nedan och i bilaga 1.
Svenskt Näringsliv tillstyrker tystnadsplikt för dataskyddsombud men förordar annan utformning.
Svenskt Näringsliv avstyrker sanktionsavgift för brott mot 10 § dataskyddsförordningen.
Svenskt Näringsliv anser att preskriptionstiden för överträdelser bör sänkas till tre år.

I detta sammanhang vill vi påminna om vikten av överblickbara regelverk med enhetlig definition av begrepp, tillämpning och koordinering mellan tillsynsmyndigheterna inom det digitala regelverksområdet. Det är centralt för företagens möjlighet till regelefterlevnad. Myndigheter behöver öka sin information och rådgivning. Informationssäkerheten kan förstärkas genom uppdrag till myndigheter att skydda och stötta näringslivet mot dataintrång och industrispionage.

Åldersgräns för samtycke till behandling
Svenskt Näringsliv tillstyrker utredningens förslag att 13 år bör gälla som gräns för inhämtande av samtycke, artikel 6.1 a dataskyddsförordningen.

Artikel 8 dataskyddsförordningen är olycklig eftersom det gör att företag som riktar sig mot unga måste anpassa sig till olika nationella lagstiftningar. Ur ett internationellt perspektiv motsvarar betänkandets 13-årsgräns den amerikanska Children's Online Privacy Protection Rule, COPPA, vilket i praktiken samtliga bolag som riktar sig till unga med digitala varor och tjänster utgår ifrån. Det vore därför mest naturligt att arbeta för en internationell 13-årsgräns.

Nättjänster som riktar sig till barn skall utformas varsamt. Den möjlighet som ges har bidragit till stora exportframgångar då flera svenska företag är marknadsledande i att locka en ung publik, se till exempel Minecraft från Mojang.

Det finns en överhängande risk att den åldersgräns som införs i praktiken blir en åldersgräns för att använda olika nättjänster. Det skulle begränsa ungdomars tillgång till bland annat sociala media, utbildningsappar och spel och därigenom deras yttrandefrihet och delaktighet på nätet.

Sekretess hos tillsynsmyndigheten
Svenskt Näringsliv delar inte utredningens bedömning att den befintliga sekretessbestämmelsen räcker för att skydda konfidentiell information, SOU 2017:39 s. 257–259.

Enligt artikel 54.2 i dataskyddsförordningen ska verksamma inom tillsynsmyndigheten omfattas av tystnadsplikt vad avser konfidentiell information som de fått kunskap om under utförande av sitt arbete. Tystnadsplikten ska i synnerhet gälla rapportering från fysiska personer om överträdelser av dataskyddsförordningen. Offentlighetsprincipen medför att tillsynsmyndighetens hantering av företagsuppgifter behöver sekretessbeläggas för att inte i sig bli en säkerhetsrisk för företag och kunder då uppgifter om tekniska brister och säkerhetsåtgärder kan försämra skyddet mot hackerattacker och spionage.

För att undvika osäkerhet i fråga om sekretessens omfattning anser Svenskt Näringsliv att absolut sekretess bör gälla vid tillsynsmyndighetens hantering av ärenden om tillstånd, tillsyn, förhandssamråd och dataincidentrapportering. Svenskt Näringsliv delar Datainspektionens uppfattning i dessa delar, se skrivelsen Vissa frågor om sekretess med anledning av EU:s dataskyddsreform till Justitiedepartementet 2017-07-07 med diarienummer 1704–2017.

Ett svagt sekretesskydd för incidentrapporter riskerar att begränsa innehållet i personuppgiftsansvarigas rapporter till tillsynsmyndigheten.

Vi välkomnar Datainspektionens förslag att en lagreglerad generell tystnadsplikt för leverantörer av IT-tjänster bör utredas så teknikskiften inte förhindras på grund av krav på tystnadsplikt i artikel 9.3 dataskyddsförordnigen.

Svenskt Näringsliv vill också understryka vikten av att den offentliga sektorn tillhandahåller säkra kommunikationskanaler för näringslivets leverans av information till tillsynsmyndigheter.

Tystnadsplikt för dataskyddsombud
Svenskt Näringsliv tillstyrker tystnadsplikt för dataskyddsombud men förordar annan utformning likt tystnadsplikt för revisor.

Enligt artikel 38.5 dataskyddsförordnigen ska dataskyddsombudet, när det gäller genomförandet av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

I SOU 2017:39 s 261 framförs att "Sannolikt syftar bestämmelsen till att skydda framför allt sådan information om den personuppgiftsansvariges eller biträdets affärs- och driftsförhållanden som dataskyddsombudet kan komma att få tillgång till vid utövandet av sitt uppdrag. Det kan dock inte uteslutas att avsikten också har varit att skydda anmälares namn eller andra uppgifter om enskildas personliga förhållanden".

Tystnadsplikten avser att skydda enskildas personliga och ekonomiska förhållanden, enligt 1 kap 6 § 1 stycket i författningsförslaget. Det vore önskvärt att paragrafens lydelse innehöll formulering som avspeglade behovet av att skydda information om den personuppgiftsansvariges eller biträdets affärs- och driftsförhållanden då det inte är givet att lagen om skydd av företagshemligheter omfattar dataskyddsombudets hela uppdrag.

I SOU 2017:39 s. 263 framhålls att tystnadsplikten för dataskyddsombud bör utformas på liknande sätt som för revisorer eller skyddsombud. Svenskt Näringsliv instämmer i detta och föreslår en motsvarande reglering som i revisorslagen, se nedan.

Revisorslagen 26 §, om tystnadsplikt:
En revisor får inte, till fördel för sig själv eller till skada eller nytta för någon annan, använda uppgifter som revisorn har fått i sin yrkesutövning. Revisorn får inte heller obehörigen röja sådana uppgifter. Revisorn ska se till att biträde till honom eller henne iakttar dessa föreskrifter

Personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott, artikel 10 dataskyddsförordningen

3 kapitlet 9 §
Under kontroll av myndighet
Den svenska tolkningen att "under kontroll av myndighet" innebär att det endast är myndigheter som får behandla särskilt känsliga personuppgifter medför problem för företagen. Att få behandla personuppgifter om brott och lagöverträdelser är avgörande för företags dokumentation och bevisföring vid brott, brottsmisstankar och möjlighet att fullfölja tredje lands regler för stävjande och finansiering av grov brottslighet.

Misstankar om brott
Svenskt Näringsliv anser att misstankar om brott inte ska utgöra otillåten behandling av personuppgifter. Näringslivet behöver liksom det offentliga stärka det brottsförebyggande arbetet genom till exempel ökad IT-säkerhet och kameraövervakning.

I SOU 2017:39 s. 193 bedömer utredningen att misstankar om brott ska anses vara otillåten behandling i avvaktan på EU-rättslig praxis. Svenskt Näringsliv ifrågasätter detta eftersom misstankar om brott inte omfattas av begreppet överträdelser i förordningen. Den praxis som tillkommit under personuppgiftslagen har orsakat svårigheter för företag bland annat i arbetsgivarrollen och i säkerhetsarbetet och därför anser vi inte att denna till synes extensiva tolkning ska gälla efter 25 maj 2018. Harmonisering av regelverket på EU-nivå är önskvärt så långt möjligt.

3 kapitlet 10 §
Den svenska restriktiva tolkningen att endast tillstånd kan ges i enskilda fall gör rättsläget osäkert för företag med internationella affärer.

I sammanhanget vill vi understryka att svensk ekonomi och arbetsmarknad är starkt beroende av export och utrikeshandel. Till att börja med svarar exporten för 45 procent av Sveriges BNP. 2016 uppgick det totala exportvärdet till nära 2000 miljarder. [1] Ungefär en fjärdedel av Sveriges totala sysselsättning beror på näringslivets produktion av exportprodukter, dvs. export av både varor och tjänster och ofta en mix av båda. Utöver ren export är betydelsen av utrikeshandel central för många svenska företag, inte minst när det gäller näringslivets ökade beroende av deras globala värdekedjor. Med andra ord har företagens beroende av att importera insatsvaror och tjänster för sin produktion ökat i takt med ökad specialisering av produktionen utmed globala värdekedjor. [2]

Mot denna bakgrund uppmanar Svenskt Näringsliv regeringen att föreslå ett regelverk som ger företag rätt att behandla personuppgifter på de sätt som krävs för att kunna följa de utländska regelverken och därmed möjliggöra den för Sverige så viktiga handeln med USA och övriga världen. Att söka tillstånd hos Datainspektionen för enstaka fall fungerar inte för de svenska exportföretagen. De företag som eventuellt får avslag på sin tillståndsansökan kommer hamna på spärrlistor och därmed förlora sina internationella affärsmöjligheter, skrivelse till Justitiedepartementet den 5 april 2017, bilaga 1.

Medlemsstaterna har rätt att införa nationella regler som gör behandling av domar i brottmål och lagöverträdelser tillåten. I detta fall bör en intresseavvägning göras där näringslivets intressen bättre tillgodoses än i SOU 2017:39.

Sanktionsavgifter för olovlig behandling som rör fällande domar i brottmål samt lagöverträdelser
Svenskt Näringsliv avstyrker förslaget att sanktionsavgift för brott mot 10 § i dataskyddsförordningen ska utdömas.

I betänkandet SOU 2017:39 föreslås att sanktionsavgift ska kunna tas ut vid brott mot artikel 10 i dataskyddsförordningen (kompletteringslagens 3 kapitlet 9 §). Sanktionsavgift för detta brott kan införas av medlemsstaterna genom nationell lag. Har övriga EU-medlemsstater gjort detta tillägg? Näringslivet har ett stort intresse av harmonisering för att kunna konkurrera på lika villkor. I betänkandet SOU 2017:39 s. 295 framförs att det inte framstår "som osannolikt att artikel 10 skulle omfattas av regleringen om sanktionsavgifter". Som framförs ovan och i bilaga 1 är screening av personuppgifter mot sanktionslistor för att förhindra grov brottslighet otroligt viktig för internationell handel. Det är förödande om svenska företag hamnar i en situation där den svenska kompletterande lagen klart hämmar export och möjlighet till global handel.

Preskriptionstid
Svenskt Näringsliv anser att författningsförslagets 7 kapitlet 3 § föreslagna femåriga preskriptionstiden för beslut om administrativa sanktionsavgifter bör sänkas till tre år.

Dataskyddsförordningen anger inte någon preskriptionstid för överträdelser. I SOU 2017:39 s. 315 konstateras att administrativa sanktionsavgifter är en särskilt ingripande åtgärd.

Svenskt Näringsliv anser att författningsförslagets 7 kapitlet 3 § föreslagna femåriga preskriptionstiden för beslut om administrativa sanktionsavgifter bör sänkas till tre år från överträdelsen. För detta talar utrednings- och allmänna rättssäkerhetsskäl. Om en viss momentan behandling av personuppgift skett bör tillsynsmyndigheten rimligen inom tre år kunna ta ställning till om behandlingen är tillåten eller ej och fatta beslut om eventuell sanktionsavgift, låt vara att kännedom om behandlingen kanske erhålls något senare. Utredningen hänvisar till de regler om preskriptionstid som gäller för beslut om sanktionsavgifter enligt miljöbalken respektive arbetsmiljölagen. Det kan dock antas att utredningar om överträdelser av dessa författningar typiskt sett är mer komplicerade och kan motivera en längre preskriptionstid för beslut om sanktionsavgift.

En kortare preskriptionstid kan dessutom ge den personuppgiftsansvarige ett starkare incitament att gallra behandlade personuppgifter när syftet med behandlingen upphört. Underlåten gallring kan ju medföra att preskriptionstid annars inte börjar löpa.

DEL 2: Kommentarer ur ett arbetsrättsligt perspektiv

Denna del av remissyttrande har tagits fram av en arbetsrättslig sektorgrupp inom Svenskt Näringsliv där representanter från samtliga sektorer inom Svenskt Näringsliv deltagit.

Sammanfattning

- Utnyttja möjligheten i Dataskyddsförordningen art 88 för att bibehålla möjligheten att exkludera ostrukturerat material och behålla missbruksregeln i dagens 5 § Personuppgiftlagen.
- Utlämnade av personuppgifter enligt 3 kap 2 § inom arbetsrätten är inte tillräckligt belyst av utredningen.
- Dataskyddslagen, eller i varje fall dess förarbeten, bör tydligt förbjuda överlämnade av personuppgifter till arbetstagarorganisationer avseende personuppgifter om andra än den mottagande arbetstagarorganisationens egna medlemmar. En fackförening ska alltså bara kunna få del av personuppgifter avseende de egna medlemmarna.
- Betänkandet redogör inte för den situationen att en personuppgiftsansvarig överlämnar personuppgifter till en facklig förtroendeman, anställd av den personuppgiftsansvarige. Enligt Svenskt Näringsliv är den fackliga förtroendemannen att betrakta som "tredje part".
- Dataskyddslagen bör innehålla ett tydligt undantag för en arbetsgivare att, inom arbetsrättens område, hantera personuppgifter innehållande lagöverträdelser, såväl konstaterade som misstänkta.

En förändring och ur våra medlemsföretags perspektiv och en av de stora försämringarna med Dataskyddsförordning, är att det framdeles inte kommer vara möjligt att hantera ostrukturerat material "utanför" Dataskyddsförordningen. Detta har hitintills underlättat företagens hantering av personuppgifter och vi beklagar att denna möjlighet kommer att försvinna. Vi utgår från att regeringen har gjort och även framdeles kommer göra vad som är möjligt för att bevara den nuvarande ordningen och vill i det sammanhanget lyfta fram artikel

88 som synes öppna för möjligheten att ha kvar den svenska nuvarande regleringen rörande ostrukturerat material inom arbetsrätten.

Av författningsförslaget 3 kap 2 § krävs det att det finns en "skyldighet" att lämna ut personuppgifter till tredje part eller den registrerades uttryckliga samtycke till utlämnandet. En arbetsgivare har ofta ett behov av att kunna lämna ut personuppgifter till en tredje part. Inte sällan rör det känsliga personuppgifter. Ett exempel på en situation där överlämnade till tredje part kan aktualiseras är i samband med en utredning inför en förestående uppsägning eller avsked, eller i samband med att arbetsgivaren utför sin skyldighet att genomföra rehabiliteringsåtgärder.

Vid rådgivning i arbetsrättsliga tvister är det regelmässigt så att arbetsgivaren behöver överlämna information till tredje part, det kan vara fråga om arbetsgivarens arbetsgivareorganisation, lönekonsulter, eller extern juridisk eller ekonomisk expertis i komplicerade uppsägningsärenden, som t.ex. advokatbyrå.

Det är inte alltid det föreligger en explicit "skyldighet" att överlämna dessa personuppgifter till tredje part. Inte desto mindre är det av avgörande betydelse för en arbetsgivare att kunna göra detta, precis som det för en enskild arbetstagare är viktigt att kunna konsultera sin fackförening eller t.ex. en advokat i händelse av en tvist. Det hade varit förtjänstfullt att det av betänkandet framgick att Dataskyddslagen inte lägger några hinder i vägen för detta och kanske belyst detta, för arbetsmarknadens parter, mycket viktiga förhållande.

Det förekommer att arbetsgivarorganisationer är organiserade i olika juridiska personer. Vissa anställda vid en arbetsgivarorganisation är anställda av en juridisk person och andra av en annan juridisk person, men arbetar med exakt samma frågor, i samma lokaler och under samma ledning. Anledningen är att verksamheten ofta är uppdelad mellan den ideella organisationen (själva förbundet) och dels ett servicebolag. Dessa behöver dela personuppgifter mellan sig eftersom personalen som hanterar arbetsrättsliga tvister och rådgivning arbetar med samma frågor, oavsett juridisk arbetsgivare. Det är för Svenskt Näringsliv och övriga förbund som står bakom detta remissyttrande, oklart om den beskrivna situationen verkligen är ett överlämnade till tredje part eftersom definitionen av tredje part på sidan 365 (kommentaren till 3 kap 2 §) i betänkandet inte är helt klar. Det hade varit bra om det av betänkandet hade framgått tydligt att den beskriva situationen inte är att betrakta som ett överlämnade till tredje part eftersom den personal som hanterar personuppgifterna "... står under den personuppgiftsansvariges eller personuppgiftsbiträdets direkta ansvar...".

På sid 365 i kommentaren står det att "en arbetsgivarens utlämnande till facklig organisation omfattas av regleringen". Svenskt Näringsliv vill här erinra om att en förutsättning för detta är att det föreligger en skyldighet att överlämna personuppgifter till en facklig organisation. Omfattningen av en sådan skyldighet kan framgå av kollektivavtal.

Det hade varit önskvärt att betänkandet tydligt markerade att en skyldighet i ett kollektivavtal att överlämna personuppgifter till en arbetstagarorganisation bara kan avse den organisationens egna medlemmar – inga andra. Om en arbetstagarorganisation skulle ha rätt att få del av personuppgifter avseende de arbetstagare som valt att inte vara medlemmar i den organisationen, eller valt att vara oorganiserade kan det utgöra ett brott mot arbetstagarnas personliga integritet och ett möjligt brott mot art 8 i Europeiska konventionen av den 4 nov. 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

Som utredningen beskriver på sidan 169 så innebär exempelvis en arbetsgivares utlämnande till en facklig organisation ett utlämnande till tredje part. Svenskt Näringsliv utgår från att detta även gäller en facklig företrädare som är anställd hos den personuppgiftsansvarige. Ett motsatt synsätt skulle få den konsekvensen att den personuppgiftsansvarige hålls ansvarig för en behandling av personuppgifter hos en motpart hos vilken den personuppgiftsansvarige inte kan kontrollera behandlingen.

Som exempel kan nämnas känsliga uppgifter i samband med en uppsägningssituation. Denna fackliga förtroendeman är förvisso anställd av den personuppgiftsansvarige men erhåller personuppgifterna i sin egenskap av facklig företrädare på arbetsplatsen och förväntas även kunna dela med sig av informationen till sin fackliga organisation. Enligt Svenskt Näringsliv är denne facklige förtroendeman att betrakta som "tredje part", varvid den personuppgiftsansvarige måste ha rättsligt stöd i Dataskyddsförordningen för utlämnandet.

Ytterligare en typ av personuppgifter av känslig natur som en arbetsgivare hanterar är lagöverträdelser. Det sker vid de tillfällen som en arbetstagare har begått ett brott och detta ska läggas till grund för en utredning om det ska vidtas någon form av arbetsrättslig åtgärd som erinran, varning, uppsägning eller avsked.

Behandling av personuppgifter som rör fällande domar i brott mot samt överträdelser regleras i art 10. Artikeln reglerar således endast "fällande" domar och gäller inte andra domar än brottmål.

Huvudregeln är att sådan hantering bara får ske av myndighet. Det finns möjlighet för resp. land att göra särskild reglering gällande lagöverträdelser, om vissa villkor är uppfyllda enligt art. 10.

Som framgår av betänkande sid 195 föreslår utredningen att undantag från förbudet att hantera personuppgifter som gäller lagöverträdelser ska kunna ges av "regeringen eller den myndighet som regeringen bestämmer". Det får antas att det är Datainspektionen som avses.

Av Datainspektionens författningssamling (DIFS 2010:1 med ändring av DIFS 1998:3) framgår att det är tillåtet att hantera personuppgifter innehållande lagöverträdelser om "behandlingen avser endast enstaka uppgift som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall". Möjligheten att hantera personuppgifter innehållande lagöverträdelser är av central betydelse för företag och arbetsgivarorganisationer. Det är absolut nödvändigt att denna möjlighet inte på något sätt inskränks framdeles. Enligt Svenskt Näringsliv bör regleringen avseende detta framgå direkt av Dataskyddslagen och inte av Datainspektionens författningssamling.

Svenskt Näringsliv utgår från att hantering av personuppgift innehållande *misstanke* om lagöverträdelse är möjlig att hantera med stöd av artikel 9 p. 2b men att det vore bra om även detta kunde klart framgå av Dataskyddslagen, eller i varje fall av dess förarbeten. Det är vanligare att en arbetsgivare hanterar personuppgifter relaterade till en *misstanke* om lagöverträdelse än en *konstaterad* lagöverträdelse.

Det förekommer att företag har sin HR-avdelning i ett moderbolag, som har ett ansvar för alla HR-frågor inom koncernen. Denna HR-funktion kan vara förlagd utomlands, ibland även

utanför Europeiska unionen. Det blir då nödvändigt att personuppgifter förs mellan olika juridiska personer inom koncernen och ibland även till utlandet. Det är, enligt Svenskt Näringsliv, viktigt att Dataskyddslagen inte lägger hinder i vägen för denna "företagsinterna" hantering av personuppgifter.

Oavsiktlig överimplementering i Dataskyddslagen

I avsnitt 18.4.2 (sid 279-280) i betänkandet redogör utredningen för att Dataskyddsförordningen art 83 saknar en hänvisning till art 10 och därför inte omfattas av regleringen om sanktionsavgifter. Utredningen spekulerar i att detta möjligen må bero på ett förbiseende. Det må så vara och i så fall ankommer det på EU att rätta till detta misstag. Till dess så skett ska inte Dataskyddslagen innehålla någon bestämmelse av det slaget då detta är en överimplementering av Dataskyddsförordningen.

SVENSKT NÄRINGSLIV

Caroline af Ugglas
Vice VD

Carolina Brånby

Ola Brinnen

Bilaga 1.

SOFF Säkerhets- och försvarsföretagen

Teknikföretagen

SVENSKT NÄRINGSLIV

5 april 2017

Skrivelse till Justitiedepartementet

Begäran om undantag från dataskyddsförordningen gällande personuppgiftsbehandling mot sanktionslistor

Bakgrund

Den nya dataskyddsförordningen ska tillämpas inom EU från den 25 maj 2018. Den ersätter då den i Sverige gällande personuppgiftslagen. Denna skrivelse rör frågan om dataskydd i relation till de krav som ställs för behandling av särskilt känsliga personuppgifter.

En rad olika organisationer, nationella som internationella, offentliggör så kallade spärrlistor som åtgärd för att bekämpa terrorism och andra allvarliga brott och oegentligheter. Företag och enskilda åläggs skyldigheter som till exempel anmälningsskyldighet eller förbud mot att handla med på listan angivna personer.

Regelverken och spärrlistorna

Spärrlistor finns av flera olika slag. EU publicerar till exempel spärrlistor som bilagor till EU-förordningar då sanktioner beslutats inom ramen för EU. I denna skrivelse behandlas problematiken som uppstår då svenska företag måste efterleva utländska spärrlistor i samband med svensk export och andra ekonomiska förbindelser.

De amerikanska spärrlistorna är offentliga och innehåller uppgifter om både företag och enskilda individer, namn, adressuppgifter och organisationsanknytning. Dessa uppgifter ska beaktas i samband med internationella affärer, till exempel orderhantering och betalning.

USA tillämpar extraterritoriell jurisdiktion vilket bland annat påverkar svenska företag som hanterar produkter samt teknik med amerikanskt ursprung. Problematiken kan dock uppkomma även avseende spärrlistor som härrör från andra länder eller organisationer.

Särskilt två regelverk berör svenska företag som importerar och säljer amerikanska produkter eller teknologier: International Traffic in Arms Regulations (ITAR) under U.S. Department of State, Directorate of Defense Trade Controls (US DoS) respektive Export Administration Regulation (EAR) under U.S. Department of Commerce (US DoC), Bureau of Industry and Security (BIS).

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 bl.a. 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 även länder som hanterar amerikanska produkter och teknik.

Ett annat regelverk omfattar listor administrerade 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 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. Special Designated Nationals and Blocked Persons (SDN) ska blockeras eller frysas. Detsamma gäller tillgångar som tillhör en SDN.

BIS Denied-Persons-listan, administreras av BIS 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.

Vidare finns också BIS Entity-listan och ISN Nonproliferation listan bestående av både företag och enskilda personer.

ITAR listan 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.

Tillvägagångssätt

För att kunna svara upp mot de amerikanska reglerna måste företag säkerställa att reexport av amerikansk teknologi eller produkter inte sker till personer eller företag på spärrlistorna. För att göra detta kan företag exempelvis databehandla på något av följande sätt:

1. Företag abonnerar på listor som integreras in i företagets egna databehandlingsapplikationer och listorna databehandlas mot den data som finns i företagens interna system varje gång listan uppdateras. Denna databehandling kan göras mot både kund-, leverantörsdatabaserna samt mot listan av anställda. Träffar måste sen hanteras enligt bolagets egna rutiner och utredas vidare om det är falskt positiva träffar.

2. Företagen skickar ut sina kund- och leverantörsregister samt personalregister till en utomstående byrå eller till ett annat företag inom samma koncern som gör databehandlingen och genererar en rapport till företaget. I denna situation kan ytterligare information om kunder, leverantörer eller anställda behöva delges för att utreda om det är falskt positiva träffar mot listorna.

3. Företagen skapar ett IT-gränssnitt mellan sina interna kund- och leverantörsregister samt personalregister till en extern databas för databehandling och resultaten rapporteras systemmässigt direkt till företaget som sedan gör sin bedömning angående falskt positiva träffar.

I samtliga tre fall kommer företagen att behöva hantera kunder, leverantörer eller anställda som ger, eller som bedöms ge, positiva utslag gentemot listorna. Alternativ 2 och 3 innebär att känslig information, både företagshemliga uppgifter likväl som personuppgifter, kommer att på något vis att vara tillgängliga för personer utanför företaget. Dessa alternativ kan även innebära överföring av uppgifter till ett tredje land.

Konsekvenser

Den nu gällande 21 § i personuppgiftslagen förbjuder andra än myndigheter att behandla så kallade särskilt känsliga personuppgifter som innehåller uppgifter om brott och lagöverträdelser. Dataskyddsförordningen, artikel 10, förbjuder personuppgiftsbehandling som omfattar domar i brottmål och lagöverträdelser i annat fall än under kontroll av myndighet. Svenska exportföretag riskerar därmed att hamna mellan två konkurrerande regler: svensk/EU lagstiftning och USA:s regelverk.

Dataskyddsförordningen innebär avsevärt strängare lagstiftning än personuppgiftslagen genom de höga sanktionsavgifter som kan utdömas direkt av Datainspektionen om företag bryter emot regelverket.

Ännu större konsekvenser, inte minst ekonomiskt, innebär det att bryta mot USA:s regler.

Direkta konsekvenser

Att bryta mot ITAR medför $ 1 000 000 i böter per förseelse och brott mot EAR innebär upp till $ 284 582 per förseelse. I bägge fallen riskerar man också åtal, att förlora sin exportlicens och olika typer av tillstånd samt att företaget själv hamnar på spärrlistan. Dessutom innebär det stora kostnader att påvisa att man vidtagit åtgärder för att i framtiden säkra efterlevnaden. Ett ärende kan i sig bestå av hundratals exporter och då adderas förseelserna till skillnad från i Sverige där de kan kumuleras. Bötesbeloppen kan vara både så kallade "Civil- or criminal penalty" och dömas ut av både justitiedepartementet (US DoJ) och av utrikesdepartementet (US DoS för ITAR) eller handelsdepartementet (US DoC för EAR).

När det gäller databehandling och brott mot OFAC:s regelverk finns två olika sätt att utdöma böter och beloppen varierar på mellan $ 125 000 - 250 000 per förseelse. Ett och samma ärende kan uppgå till flera tusen förseelser. Beloppen kan bli ännu högre beroende på omständigheterna.

Mer info: https://www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf

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. Särskilt allvarligt är det för ett företag att själv hamna på spärrlistor som i sin tur screenas av företagets kunder som då enligt amerikanska regler är förhindrade att handla med svartlistade företag.

Mer info: https://www.justice.gov/opa/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions-sending

Särskilt svårt blir det för företag som säljer produkter med dubbla användningsområden. Eftersom USA har en catch-all klassificering i form av EAR99 så gäller det samtliga produkter som svenska företag köper från USA och som säljs till sanktionerade länder.

Indirekta konsekvenser

Förutom ovannämnda direkta konsekvenser, kan det även bli stora indirekta konsekvenser för företag. Att hamna på sanktionslistor kan även innebära att företagens kunder och leverantörer drabbas. Detta kan få följdkonsekvenser som till exempel att svenska staten inte längre kan säkerställa sin materielförsörjning, särskilt där staten har ett systemberoende. Vidare kan det även omöjliggöra försvarssamarbeten med stater som Sverige ingått avtal med.

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.

Undantag från regelverket

Undantag att hantera särskilt känsliga personuppgifter enligt 21 § PUL kan formellt sökas hos Datainspektionen men Högsta Förvaltningsdomstolen (HFD) har gjort bedömningen att sådana möjligheter till undantag ska utnyttjas med restriktivitet (HFD 2016 ref. 8). Detta tydliggörs även i en dom från Kammarrätten (2016-04-13 i mål nr 3946-15 m.fl.) där GE Capital, GE Healthcare, International General Electric etc. ansökt om tillstånd för att kunna genomföra personuppgiftsbehandling mot USA:s OFAC SDN-list, BIS Denied-Persons-list, BIS Entity-list and ISN Nonproliferation list. Detta avslogs med hänsyn till vikten av den personliga integriteten. Däremot beviljades företagets finansiella verksamhet – bankverksamhet – undantag. Datainspektionen har beviljat banksektorn i Sverige som enda bransch ett generellt undantag.

Begäran:

Om svenska företag ska kunna handla med amerikanska produkter och teknologier måste det finnas rimliga möjligheter att leva upp till de krav som ställs i ovannämnda regelverk och sanktionslistor.

Mot bakgrund av detta vill undertecknade organisationer föreslå att det införs regler som ger företag möjlighet att behandla de personuppgifter som krävs för att kunna följa de utländska regelverken och därmed möjliggöra den för Sverige så viktiga handeln med USA och övriga världen.

Stockholm den 5 april 2017

Klas Wåhlberg,
VD, Teknikföretagen

Robert Limmergård
Generalsekreterare SOFF

Carola Lemne
Svenskt Näringsliv