Stockholm den 28 juni 2018

Datainspektionen
Box 8114
104 20 Stockholm

Hemställan om klargörande avseende tillämpningen av artikel 10 i EU:s dataskyddsförordning alternativt meddelande av föreskrift eller undantag enligt 3 kap 9 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning

Säkerhets- och Försvarsföretagen (fortsättningsvis SOFF) hemställer härmed om att Datainspektionen klargör att SOFF:s medlemmars behov av att genomföra kontroller mot vissa amerikanska spärr- och sanktionslistor är förenlig med EU:s dataskyddsförordning.

Om så inte skulle bedömas vara fallet hemställer SOFF:s medlemmar att Datainspektionen:

- i första hand genom tillägg till Datainspektionens föreskrift DIFS 2018:02 meddelar undantag från förbudet i artikel 10 för andra än myndigheter att behandla uppgifter som rör lagöverträdelser i enlighet med vad som föreslås under rubriken *Förslag till utformning av föreskrift.*

- i andra hand – med verkan från och med den 25 maj 2018 – meddelar undantag för SOFF:s medlemmar från förbudet i artikel 10 för andra än myndigheter att behandla uppgifter som rör lagöverträdelser.

Bakgrund till hemställan

Efter att SOFF och andra företag i samband med remissyttrande över lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (fortsättningsvis Dataskyddslagen) framfört synpunkter avseende tillämpningen av artikel 10 i EU:s dataskyddsförordning (fortsättningsvis artikel 10) har regeringen i propositionen 2017:39 Ny dataskyddslag, s 100-101, anfört att

”... Det är regeringens uppfattning att svenska företag inte ska ges sämre möjligheter att behandla uppgifter som rör lagöverträdelser än företag i andra länder. Regeringen kan också konstatera att det typiskt sett bör vara möjligt för svenska exportföretag att få tillstånd att behandla sådana uppgifter i den mån detta krävs för sådan kontroll mot sanktions- och spärrlistor som är nödvändig för export till vissa länder. Detta bör i vart fall gälla om dessa listor är fastställda i demokratisk ordning och allmänt tillgängliga. Några remissinstanser pekar på att systemet med särskilda beslut i enskilda fall är betungande för både tillsynsmyndigheten och företagen, varför föreskrifter som tillåter nödvändig behandling är att föredra. Med anledning av denna synpunkt vill regeringen understryka att det, t.ex. i fråga om vissa viktigare spärr- och sanktionslistor, kan finnas anledning för tillsynsmyndigheten

att använda möjligheten att meddela föreskrifter. Detta kan minska den administrativa bördan både för företagen och för tillsynsmyndigheten själv….”

SOFF har uppfattat denna skrivning som att regeringens inställning varit att Datainspektionen ska meddela föreskrift med innehåll som skulle göra det möjligt för svenska företag att behandla uppgifter som rör lagöverträdelse i den mån det krävs för att genomföra en sådan kontroll mot sanktions- och spärrlistor som amerikanska regelverk ställer krav på för att tillåta handhavandet av viss amerikansk materiel och att en sådan föreskrift skulle träda i kraft från och med 25:e maj 2018.

Datainspektionen har i den föreskrift som meddelar undantag från förbudet för andra än myndigheter att behandla uppgifter som rör lagöverträdelse, DIFS 2018:02, inte tagit med någon skrivning som innefattar dylikt undantag.

Omständigheter

Allmänt

SOFF:s medlemsföretag tillverkar, underhåller och säljer krigsmateriel och produkter med dubbla användningsområden[1]. Företagen är i stor omfattning i behov av internationellt samarbete för att utveckla avancerade plattformar, system och produkter som efterfrågas på försvarsmarknaden. Detta innebär att företagen även måste kunna få tillgång till försvarsteknik som utvecklats i andra länder.

Sverige har ett mycket omfattande försvarstekniskt samarbete med USA, som 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, mjukvaror och produkter som tillverkas i Sverige innehåller därför amerikanska delkomponenter. Sverige är härigenom starkt beroende av tillgång till amerikansk högteknologi. Det skulle idag vara omöjligt för svenska företag att producera och exportera flera av de större militära systemen utan godkännande från USA.

Av säkerhetspolitiska skäl finns det i USA sedan länge omfattande restriktioner avseende vilken teknik som får exporteras till andra länder samt även hur tekniken 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 spärr- och sanktionslistor inte får ges tillgång till

[1] Med produkter med dubbla användningsområden menas; produkter, inbegripet programvara och teknik, som kan användas för både civila och militära ändamål, samt alla varor som kan användas både för icke-explosiva ändamål och för att på något sätt bidra vid tillverkning av kärnvapen eller andra kärnladdningar

amerikansk försvarsteknik. Spärrlistornas syfte är att bekämpa terrorism och andra allvarliga brott och oegentligheter.

De amerikanska spärr- och sanktionslistorna är som huvudregel tillämpliga på samtliga företag, både amerikanska och utländska, som handlar med amerikanskt kontrollerade produkter och teknologi.

Då export och andra typer av tillgängliggöranden 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 – bl.a. anställda, arbetssökande, leverantörer, kunder, samarbetspartners – gentemot spärrlistorna (s.k. screening). 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.

Svenska företag måste även göra screening av mottagare och leverantörer mot EU:s och FN:s sanktionslistor för att uppfylla sina skyldigheter att säkerställa att brott mot dessa inte förekommer. Även dessa sanktioner vänder sig ofta mot en specifik vara (t.ex. vapen, produkter med dubbla användningsområden, diamanter eller mineraler), ett lands ledarskap, en organisation eller en individ (t.ex. finansiella restriktioner såsom frysning av tillgångar och andra ekonomiska resurser), i stället för generellt mot ett land. Denna screening är idag tillåten och grundar sig på Sveriges folkrättsliga förpliktelser (FN) och direkt tillämpliga EU förordningar.[2]

Listor som svenska företag enligt amerikansk lag måste screena mot, listornas bakgrund och innehåll

De amerikanska spärr- och sanktionslistorna är offentliga och innehåller uppgifter om både företag, organisationer, enskilda individer m.m. Uppgifterna ska beaktas i samband med internationella affärer, till exempel orderhantering och betalning, och företag, myndigheter och enskilda åläggs olika skyldigheter som till exempel anmälningsskyldighet eller förbud mot att handla med på listorna angivna personer, organisationer och företag.

Det amerikanska exportkontrollsystemet är omfattande, men det är särskilt två amerikanska exportkontrollregelverk och listor som är kopplade till dessa som berör

[2] Se regeringens hemsida https://www.regeringen.se/regeringens-politik/utrikes--och-sakerhetspolitik/sanktioner/

svenska företag som importerar och säljer amerikanska produkter eller teknologier: International Traffic in Arms Regulations (ITAR) och Export Administration Regulation (EAR).

ITAR-regelverket hanteras *av US Department of State, Directorate of Defense Trade Controls (US DoS/DDTC)* och dessa regler tar främst sikte på amerikansk utrikespolitik och intern säkerhet i USA. Produkterna som omfattas anges i US Munitions List, dvs. försvarsrelaterade produkter.

US DoS/DDTC administrerar följande listor: List of Administratively Debarred Parties och List of Statutorily Debarred Parties.

EAR-regelverket hanteras av *U.S. Department of Commerce (US DoC), Bureau of Industry and Security (BIS)*. Dessa regler har som mål att tillgodose USA:s ekonomiska intressen. Produkterna som omfattas anges i 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 hamna i orätta händer, såsom till exempel terrorister, organiserade brottslingar eller icke önskvärda länder.

BIS administrerar följande listor: Denied-Persons-listan, Entity-listan och Unverified List-listan.

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- och handelssanktioner. Dessa sanktioner kan avse alla typer av produkter, dvs. inte bara sådana som har strategisk betydelse och sanktionerna gäller även transaktioner som genomförs i amerikansk dollar (USD).

OFAC administrerar följande listor: Specially Designated Nationals-listan och Consolidated Sanctions-listan.

Ytterligare ett regelverk som omfattar en lista hanteras av *Department of State – Bureau of International Security and Nonproliferation (ISN).* Denna lista inbegriper utländska individer, juridiska personer och stater som ägnar sig åt spridningsverksamhet av massförstörelsevapen mot vilka USA har uppställt rättsliga restriktioner enligt olika amerikanska rättsliga källor. Restriktionerna innebär att samtliga transaktioner mellan en part som finns upptagen på listan och amerikanska rättssubjekt är förbjudna, samt att eventuella tillgångar som en sådan part besitter och som är föremål för amerikansk jurisdiktion ska frysas. ISN administrerar följande lista: List of Nonproliferation Sanctions. Ytterligare detaljer kring listorna och deras innehåll finns i Bilaga A.

Genomförande av screening – olika tillvägagångssätt

Företag kan använda olika metoder för att genomföra screening i syfte att säkerställa att reexport av amerikansk teknologi eller produkter inte sker till personer eller företag som finns upptagna på spärr- och sanktionslistor. Detta kan ske enligt samma metoder som används för idag tillåtna kontrollåtgärderna gentemot FN- och EU:s sanktionslistor, t.ex. på något av följande sätt:

1. Företag abonnerar på listor som integreras in i företagets egna databehandlingsapplikationer och listorna databehandlas mot de data som finns i företagens interna system varje gång listan uppdateras. Denna databehandling kan göras mot både kund- och leverantörsdatabaserna samt mot listan av anställda. Träffar måste sen hanteras enligt bolagets egna rutiner och utredas vidare om det är falska positiva träffar[3].

2. Företagen skickar ut sina kund- och leverantörsregister samt personalregister till en tredje part (t.ex. en advokatbyrå eller 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 tredje part 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.

4. Ett sista alternativ är att screening inte utförs automatiserat utan manuellt genom att en person kontrollerar personuppgifter inom företaget mot befintliga listor.

I samtliga fall kommer företagen att behöva hantera kunder, leverantörer eller anställda som ger, eller bedöms som, positiva utslag gentemot listorna. Positiva träffar hanteras olika beroende på vilken lista som genererat det positiva utslaget. I vissa fall måste kontakt tas med ansvarig amerikansk myndighet för riktlinjer och i andra fall framgår av listan i sig att personen är föremål för en viss typ av sanktion som innebär t.ex. krav på viss licens vid

[3] Med utredning av falskt positiva träffar menas att företaget utreder om den person som är föremål för träffen endast har samma eller liknande namn eller andra uppgifter som delvis stämmer med namnet i listan för att kunna sortera bort oriktiga träffar.

export eller liknande. I inget fall vid ett positivt utslag sker ytterligare sökningar som innefattar behandling av personuppgifter.

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 efterlever den amerikanska lagstiftningen 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 USD 1,000,000 i böter per förseelse och brott mot EAR innebär upp till USD 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 företaget 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.

Behandlingar enligt artikel 10 och 3 kap 9 § lag Dataskyddslagen

SOFF:s inställning

Den screening som genomförs mot amerikanska spärr- och sanktionslistor är förenlig med dataskyddsförordningen och innefattar inte en behandling av den typ av personuppgifter som omfattas av artikel 10. Behandlingen kräver inte något undantag enligt 3 kap 9 § Dataskyddslagen.

I första hand görs gällande att behandling av personuppgifter som rör misstankar om brott enbart omfattas av kravet på undantag enligt artikel 10 och 3 kap 9 § Dataskyddslagen om misstanken har kvalificerats till att avse ett visst, konkret brott.

I andra hand görs gällande att behandling av personuppgifter som rör misstankar om brott inte ska omfattas av kravet på undantag enligt artikel 10 och 3 kap 9 § Dataskyddslagen.

Bakgrund – tidigare tillämpning av 21 § Personuppgiftslagen (PuL)

När det gäller den tidigare tillämpningen av 21 § PuL framgår av kommentaren till denna paragraf (Öman, Lindblom, Personuppgiftslagen – en kommentar, 2011, s. 330) att varje överträdelse av förhållningsregler i lag inte ska omfattas av 21 §, utan straff måste vara föreskrivet för överträdelsen. Uppgifter om överträdelser som är osanktionerade eller som bara för med sig administrativa sanktioner, t.ex. oriktigt uppgiftslämnande på skatteområde, otillåtet byggande eller felaktigheter vid miljöfarlig verksamhet, omfattas inte.

Avseende begreppet ”misstankar om brott” framgår av kommentaren till 21 § PuL (s. 331) att en uppgift om att någon har eller *kan ha begått ett visst brott* utgör en uppgift om lagöverträdelser, även om det inte finns någon dom eller motsvarande beträffande brottet. Dock framfördes i det utredningsbetänkande som föregick propositionen till PuL (SOU 1997:39 s. 380) att en uppgift om att någon har eller kan ha begått ett visst brott utgör en uppgift om lagöverträdelse, även om det inte finns någon dom eller motsvarande beträffande brottet, *om uppgiften har kvalificerats till att avse något visst brott*.

Datainspektionen har i tidigare beslut avseende tillämpningen av 21 § PuL ansett att bland annat uppgifter som förekommer på USA:s lista över personer med blockerade eller frysta tillgångar (beslut 2006-02-24, dnr 1344-2005 och beslut 2010-09-16, dnr 589-2010) och uppgifter om personer som förekommer på FN:s s.k. terrorlista (samrådsyttrande 2007-11-20, dnr 886-2007) utgör personuppgifter om lagöverträdelser och att screening mot dessa listor utgör behandling som krävde undantag enligt 21 § PuL. Detta var även Kammarrättens slutsats avseende behandling av personuppgifter genom kontroller mot bl.a. den av OFAC utfärdade Special Designated and Blocked Persons-listan (Kammarrätten i Stockholm mål nr 3946-15, 2015-03-18).

I den dom som meddelades av Kammarrätten framgår i bedömningen, tredje stycket, att ”... omständigheterna under vilka sanktionslistorna och t.ex. Bolagens personalregister

sambearbetas för kontrolländamål liknas vid en form av misstankeregister…". Även Datainspektionen anförde att "När sanktionslistan och Bolagens personalregister sambearbetas för detta kontrolländamål uppkommer momentant ett misstankeregister". Det framgår dock inte av detta avgörande och inte heller av de beslut som Datainspektionen meddelat, vilka brottsmisstankar detta "misstankeregister" skulle innehålla och hur misstankarna kan anses ha kvalificerats till att avse ett visst eller vissa brott.

Artikel 10 omfattar enbart misstankar om brott om brottsmisstanken har kvalificerats till att avse något visst, konkret brott

När det gäller den kommande tillämpningen av artikel 10 kan först konstateras att av texten i artikel 10 framgår att artikeln omfattar behandling av personuppgifter som rör *fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder.* Enligt propositionen till Dataskyddslagen (proposition 2017:39 Ny dataskyddslag, s 98) ska ordet "överträdelser" tolkas som "lagöverträdelser som innefattar brott". Där har det även lagts till att begreppet "säkerhetsåtgärder" ska bedömas likvärdigt med "straffprocessuella tvångsmedel", det vill säga bland annat häktning, kvarstad och beslag. Dock omfattas inte administrativa sanktioner och avgöranden i tvistemål.

Avseende frågan om "misstankar om brott" även fortsättningsvis ska innefattas i begreppet "lagöverträdelser som innefattar brott" har regeringen i propositionen 2017:39 Ny dataskyddslag, s 99, framfört att det inte är säkert att den praxis som finns sedan tidigare enligt personuppgiftslagen kring vilka uppgifter som omfattas av regleringen om personuppgifter fortfarande är aktuellt (se vidare nedan).

Även om begreppet "misstankar om brott" i huvudsak skulle anses ha samma innebörd som enligt 21 § PuL, kan konstateras – i enlighet med vad som framförts ovan – att det redan i det utredningsbetänkande som föregick propositionen till PuL framgick att en uppgift om att någon har eller kan ha begått ett visst brott utgör en uppgift om lagöverträdelse, även om det inte finns någon dom eller motsvarande beträffande brottet, *om uppgiften har kvalificerats till att avse något visst brott*. Detta innebär att en misstanke om brott måste ha kvalificerats på visst sätt för att kunna anses utgöra en uppgift om lagöverträdelse.

Tolkningen av vad som ska avses med begreppet "visst brott" bör vara detsamma som reglerar när förundersökning ska inledas och när straffprocessuella tvångsmedel får användas. Detta framgår av rättegångsbalken 23:1 och här stadgas att förundersökning ska inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats.

Av kommentaren till denna paragraf (se Fitger, Rättegångsbalken, s. 23:6) kan utläsas att det krävs misstanke om ett konkret brott; det räcker inte att det finns anledning att anta att någon ägnar sig åt brottslig verksamhet, t.ex. att införa större mängder narkotikapartier till Sverige och att här försälja densamma, såvida man inte känner till något konkret fall härav. En sådan verksamhet är något som kan "utövas" men inte "förövas". Om det inte föreligger en misstanke om ett konkret brott, finns det ingen möjlighet att bedriva en förundersökning och ingen möjlighet att använda RB:s regler om tvångsmedel.

Det framgår även (se Bring, Diesen, Förundersökning, 2009, s. 219) att det vid inledning av förundersökning ska finnas bevisning om en ”konkret brottslig gärning”, d.v.s. någon omständighet som kan ingå i den gärningsbeskrivning som åklagaren sedan ska formulera, t.ex. tid, plats, tillvägagångssätt eller målsägande. Om en misstanke inte är konkretiserad till en viss gärning brukar uttrycket ”brottslig verksamhet” användas och med detta avses att en persons livsföring och levnadsomständigheter kan tyda på en ”brottslig verksamhet”.

Om det finns anledning att anta att ett brott begåtts och förundersökning ska inledas enligt RB 23:1 föreligger den lägsta misstankegraden enligt svenska straffprocessuella regler. Rimligen kan de lagöverträdelser som avser misstankar om brott och som eventuellt ska omfattas av artikel 10 inte innefatta misstankar om brott som innebär en lägre misstankegrad än vad som tillämpas inom straffprocessrätten. Detta innebär att det måste finnas en misstanke om ett visst, konkret brott även vid tillämpningen av artikel 10.

SOFF:s uppfattning är att det i samband med screening mot de listor som finns i Bilaga A inte framkommer några uppgifter om en person som innebär att denna kan anses misstänkt för ett visst, konkret brott. Det finns inga uppgifter om preciserade gärningar som anger t.ex. tid, plats eller tillvägagångssätt vid förövandet av en misstänkt brottslig gärning.

Det företagen kan erhålla information om vid en träff mot någon av listorna (se Bilaga A) är:

- den förvaltnings- och/eller civilrättsliga processen som lett fram till att en person har påförts administrativa böter eller ålagts sanktioner för att denne t.ex. inte efterföljt exportkontrollagstiftning eller

- vilket sanktionsprogram en person är föremål för med hänvisning till relevant lag.

Den enda listan som kan sägas innehålla personer som dömts för brott mot exportkontrollagstiftningen (i detta fall Arms Export Control Act, AECA) är List of Statutorily Debarred Parties. Listan innehåller personer som är föremål för ”statutory debarment” och listans syfte är att redovisa dessa personer så att interaktion med dessa förhindras. Vid en träff mot listan erhålls en referens (länk) till Federal Register Notice. I Federal Register Notice finns uppgifter om att personen som finns på listan dömts för brott mot AECA, datum för domen, målnummer och domsaga. Men det saknas uppgift om vilket konkret brott som kan ha legat till grund för domen och för att erhålla dessa uppgifter skulle krävas att företag vänder sig till en amerikansk domstol och begär ut domen. Företag har vidare ingen anledning att inhämta vare sig uppgifter ur Federal Register Notice eller domar då det följer av lagstiftning i sig (ITAR section 127.7. (b)) att varje person som finns med på listan är ”…prohibited from participating directly or indirectly in any activities that are subject to the ITAR.” Detta innebär att företagen vet direkt vid en träff mot denna lista hur de har att förehålla sig gentemot personen i fråga.

Sammanfattningsvis kan konstateras att de uppgifter som företagen kan ta del av vid en träff mot en lista i första hand innehåller uppgifter om att en person varit föremål för en förvaltnings- och/eller civilrättslig process och att denne påförts administrativa böter eller ålagts sanktioner. I enlighet med vad som ovan anförts framgår av propositionen till Dataskyddslagen att administrativa sanktioner och avgöranden i tvistemål inte omfattas av

artikel 10. Förekomsten på listorna skulle möjligen kunna anses tyda på att en person sysslar med ”brottslig verksamhet”, men det kan inte leda till några slutsatser om att personen gjort sig skyldig till eller är misstänkt för ett visst, konkret brott. Något undantag från artikel 10 kan därför inte behövas i samband med att företag genomför screening mot de aktuella listorna då behandlingen inte innefattar någon av de personuppgifter som omfattas av denna artikel.

Dataskyddsförordningen bör innebära en ny tolkning av begreppet ”Misstankar om brott” och att detta inte omfattas av artikel 10

Avseende frågan om ”misstankar om brott” även fortsättningsvis ska innefattas i begreppet "lagöverträdelser som innefattar brott" har regeringen i propositionen 2017:39 Ny dataskyddslag, s 99, framfört att ett av de huvudsakliga syftena med dataskyddsförordningen är att åstadkomma en harmonisering av dataskyddsregleringen inom EU och att det därför är angeläget att artikel 10 inte tolkas på ett mer extensivt sätt i Sverige än i andra medlemsstater. Regeringen konstaterar härvid att artikel 10 har en annan utformning än motsvarande reglering i dataskyddsdirektivet och personuppgiftslagen och att det därför inte är säkert att den praxis enligt personuppgiftslagen kring vilka uppgifter som omfattas av regleringen om personuppgifter fortfarande är aktuell.

Vid beaktande av att de flesta andra EU-länders dataskyddsmyndigheter inte synes göra tolkningen att misstankar om brott innefattas i artikel 10 och mot bakgrund av regeringens bedömning att artikel 10 inte ska tolkas på ett mer extensivt sätt i Sverige, måste slutsatsen vara att behandling av personuppgifter som enbart rör misstankar om brott inte omfattas kravet på undantag enligt 3 kap 9 § Dataskyddslagen.

Om ”misstankar om brott” exkluderas ur begreppet "lagöverträdelser som innefattar brott" krävs inget undantag från artikel 10 för företag som genomför screening mot listorna i Bilaga A. Detta då ingen av de listor som redovisas i Bilaga A kan anses innehålla uppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande straffprocessuella tvångsmedel.

Förslag till utformning av föreskrift

För det fall att Datainspektionen inte skulle dela SOFF:s bedömning enligt ovan bör Datainspektionen, i enlighet med regeringens riktlinjer i propositionen 2017:39 Ny dataskyddslag, s 100-101, meddela undantag i föreskriftsform från artikel 10 i EU:s dataskyddsförordning avseende viktigare spärr- och sanktionslistor.

Av vad som redovisats ovan och av vad som framgår av uppgifterna i Bilaga A kan konstateras att samtliga listor i Bilaga A är fastställda i demokratisk ordning och de finns allmänt tillgängliga. Mot bakgrund av det syfte som de uppräknande listorna ska tillgodose – bl.a. att förhindra illegal vapenexport, terrorhandlingar, finansiering av terrorism och spridning av massförstörelsevapen - måste de anses utgöra viktigare spärr- och sanktionslistor.

Föreskriften bör utformas enligt följande:

”Personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning får behandlas av andra än myndigheter om

5. uppgifterna avser en person som i sin anställning eller i sitt samröre med svenska företag kan komma i kontakt med teknologi, produkter eller ekonomisk och finansiella transaktioner som omfattas av sanktions- eller spärrlistor som har sin grund i de amerikanska exportkontrollregelverken International Traffic in Arms Regulations, Export Administration Regulations, Office of Foreign Assets Controls eller liknande författning och vars syfte är att kontrollera och förhindra illegal spridning av amerikansk teknologi eller produkter. Syftet med behandlingen ska vara att utesluta att personen är inblandad i illegal vapenexport, terrorhandlingar, finansiering av terrorism, spridning av massförstörelsevapen och teknologi kopplat till missiler eller är föremål för andra sanktionsåtgärder.

   Alternativt:

6. uppgifterna avser personer som i sin anställning eller i sitt samröre med svenska företag kan komma i kontakt med teknologi, produkter eller ekonomiska och finansiella transaktioner som omfattas av sanktions- eller spärrlistor vilka syftar till att förhindra att personer namngivna på sådana listor deltar i illegal vapenexport, terrorhandlingar, finansiering av terrorism, spridning av massförstörelsevapen och teknologi kopplad till missiler eller är föremål för andra sanktionsåtgärder. Sådana sanktions- eller spärrlistor ska vara allmänt tillgängliga, ha tillkommit i demokratisk ordning och kan ha nationellt eller internationellt ursprung.

Meddelande av undantag för SOFF:s medlemmar från förbudet i artikel 10 för andra än myndigheter att behandla uppgifter som rör lagöverträdelser

I sista hand hemställer SOFF:s medlemmar att Datainspektionen meddelar undantag för SOFF:s medlemmar från förbudet i artikel 10 för andra än myndigheter att behandla uppgifter som rör lagöverträdelser.

När det gäller bakgrunden till att undantag ska meddelas hänvisas i huvudsak till vad som anförts ovan.

Här ska särskilt framhållas att bolagen har ett berättigat intresse att följa tillämpliga amerikanska regler som, i likhet med de regler och sanktioner som införts av FN och EU, har till syfte att förhindra illegal spridning vapenteknologi, massförstörelsevapen och finansiering av terrorism.

Det potentiella intrång som kontrollerna skulle kunna innebära för enskilda är begränsat, särskilt genom att företagen har utvecklade metoder för att förhindra sammanblandning av personer som finns med på listan och andra personer med samma eller liknande namn (äkta respektive falska träffar).

När det gäller intrånget för den enskilde måste även beaktas att det är först vid en ”äkta träff” som personuppgifter som relaterar till lagöverträdelser överhuvudtaget kommer att behandlas av företagen. Detta innebär att det är ett mycket litet antal behandlingar som undantaget faktiskt skulle komma att omfatta.

Även att listorna publicerats av amerikanska myndigheter på internet och är allmänt tillgängliga måste anses innebära att integritetsintresset för de individer som finns på listorna är begränsat. Det går t.ex. inte att jämställa med det integritetsintresse som finns för en individ som misstänks eller dömts för brott i Sverige där dessa uppgifter enbart finns tillgängliga i domar och brotts- och misstankeregister, som inte är allmänt tillgängliga. Integritetsintresset hos individer som finns med på listorna bör istället jämställas med t.ex. fall när svensk massmedia publicerat personuppgifter avseende publika personer vid brott och/eller brottsmisstankar.

Sammantaget överväger företagens berättigade intresse det potentiella intrånget för enskilda och därmed föreligger skäl för att meddela undantag.

Behandlingen kommer i övrigt att ske i enlighet med de krav som Dataskyddsförordningen och dess kompletterande bestämmelser uppställer. Detta innebär bland annat att enskilda kommer att informeras om att deras personuppgifter kommer att behandlas genom att screening genomförs och att det finns rutiner för arkivering och radering.

Undantag ska beviljas avseende kontroller mot listor uppräknade i Bilaga A av:

- potentiella kunder, leverantörer, samarbetspartners, förmedlare (broker/agent)
- befintliga kunder,
- arbetssökande, arbetstagare och uppdragstagare, besökare
- potentiella leverantörer, tjänsteleverantörer, samarbetspartners samt
- ställföreträdare, firmatecknare, ägare, verkliga huvudmän och borgensmän för de angivna personerna.

För Säkerhets- och försvarsföretagen,

Robert Limmergård

Generalsekreterare

Bilaga A - US Screening lists

Bilaga B - SOFF:s medlemsförteckning

Bilaga A

Authority	List	Content	Personal Information which could be exposed when screening	Is information relating to criminal convictions and offences or related security measures exposed when screening?
Department of Commerce – Bureau of Industry and Security (BIS)	Denied Persons List https://www.bis.doc.gov/index.php/the-denied-persons-list	Names of persons who have violated US export regulations and against whom the Bureau of Industry and Security has therefore issued a denial order. Usually there is a violation of the law and usually if there is, it is a criminal violation in order for it to reach the level of being placed on the denied persons list. However, criminal charges or convictions are not required, see EAR 763(a) which provides for being placed on the list as a civil penalty. The listed persons have been denied all exporting privileges, meaning that no US goods can be provided to or purchased from them. Businesses that violate such a denial order are in violation of US export regulations and risk being listed on the DPL themselves.	Name, address	NO Reference to Appropriate Federal register, eg. Appropriate Federal Register Citations: 68 F.R. 38290 6/27/03, 80 F.R 57572 9/24/15. To receive information about the reasons why a persons is on the list, you need to search the Federal Register
	Entity List (Supplement No. 4 to Part 744) https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=9ae4a21068f2bd41d4a5aee843b63ef1&ty=HTML&h=L&n=15y2.1.3.4.28&r=PART	Names of persons whose presence in a transaction can trigger a license requirement supplemental to those elsewhere in the Export Administration Regulations (EAR). The list specifies the license requirements and policy that apply to each listed party. This does not require a criminal conviction or a criminal charge. BIS has stated "BIS first published the Entity List in February 1997 as part of its efforts to inform the public of entities who have engaged in activities that could result in an increased risk of the diversion of exported, reexported and transferred (in-country) items to weapons of mass destruction (WMD) programs. Since its initial publication, grounds for inclusion on the Entity List have expanded to activities sanctioned by the State Department and activities contrary to U.S. national security and/or foreign policy interests.	Name, address	NO Specifies the license requirements that it imposes on each listed person (eg. For all items subject to EAR). Reference to Federal Register (eg. 76 FR 71869, 11/21/11). To receive information about the reasons why a persons is on the list, you need to search the Federal Register

	Unverified List (Supplement No. 6 to Part 744) https://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=15:2.1.3.4.28#ap15.2.744_122.6	Names of persons that are ineligible to receive items subject to the Export Administration Regulations (EAR) by means of a license exception. In addition, exporters must file an Automated Export System record for all exports to parties listed on the UVL and obtain a statement from such parties prior to exporting, reexporting, or transferring to such parties any item subject to the EAR which is not subject to a license requirement. Restrictions on exports, reexports and transfers (in-country) to persons listed on the UVL are set forth in Section 744.15 of the EAR. This does not require a criminal conviction or even a criminal charge, see 744.15. The List is a Supplement ti EAR Part 744 and is also called Supplement No. 6	Name, address	NO Reference to Federal Register citation, eg. 82 FR 16732, April 6, 2017. To receive information about the reasons why a persons is on the list, you need to search the Federal Register

Department of the Treasury – Office of Foreign Assets Controls (OFAC)	Specially Designated Nationals List https://www.treasury.gov/ofac/downloads/sdnlist.pdf	Names of all persons, groups, and entities worldwide implicated by American authorities as involved in terrorist activities threatening US security. Includes Parties who may be prohibited from export transactions based on OFAC's regulations. The EAR require a license for exports or reexports to any party in any entry on this list that contains any of the suffixes "SDGT", "SDT", "FTO", "IRAQ2" or "NPWMD". The OFAC Specially Designated Nationals List includes the following active sanctions programs: North Korea Sanctions Regulations, Iranian Financial Sanctions Regulations, Libyan Sanctions, Global Terrorism Sanctions Regulations, Narcotics Trafficking Sanctions Regulations, Transnational Criminal Organizations Sanctions Regulations The individuals and entities located throughout the world are blocked pursuant to the various sanctions programs administered by OFAC. SDNs can be front companies, parastatal entities, or individuals determined to be owned or controlled by, or acting for or on behalf of, targeted countries or groups. They also can be specially identified individuals such as terrorists or narcotics traffickers. U.S. persons are prohibited from engaging in any transactions with SDNs and must block any property in their possession or under their control in which an SDN has an interest. SDNs are designated primarily under the statutory authority of the Trading With the Enemy Act, the International Emergency Economic Powers Act, the Anti-Terrorism and Effective Death Penalty Act and the Foreign Narcotics Kingpin Designation Act. Implementing regulations can be found in Chapter V, Title 31 of the U.S. Code of Federal Regulations. Placement on the list does not require a criminal charge or conviction.	Name, Place of Birth, Nationality, Passport (country) info, National ID no., Residency Number (country of residence), Address, Gender, E-mail address, Membership of organization, Employment	NO Information about which Sanction Program subject to with law ref. (eg. Iranian Transactions and Sanctions Regulations, 31 CFR part 560, Blocked Pending Investigation, Patriot Act, Foreign Sanctions Evaders Executive Order 13608 Syria)

	Consolidated Sanctions List (OFAC) https://sanctionssearch.ofac.treas.gov/	A consolidated list of all persons and entities of OFACs non-SDN sanctions programs. All new non-SDN sanctions programs will be added to this consolidated list in the future. The OFAC Consolidated Sanctions List includes the following sanctions lists, for example: **Foreign Sanctions Evaders (FSE) List** - Foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Syria or Iran, as well as foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. Sanctions. Transactions by U.S. persons or within the United States involving Foreign Sanctions Evaders (FSEs) are prohibited. These are persons who are not subject to US laws and thus would in general not have criminal charges or convictions. Instead they are people that the US government has found would have violated the law had they been subject to US laws and thus it does not want companies to do business with them **Sectoral Sanctions Identifications (SSI) List** - Individuals operating in sectors of the Russian economy with whom U.S. persons are prohibited from transacting in, providing financing for, or dealing in debt with a maturity of longer than 90 days. These are economic sanctions that do not require criminal charges or convictions. **Palestinian Legislative Council (NS-PLC) list-** Individuals of the PLC who were elected on the party slate of Hamas, or any other Foreign Terrorist Organization (FTO), Specially Designed Terrorist (SDT), or Specially Designated Global Terrorist (SDGT). This does not require a criminal charge or conviction. Placement on the list is a matter of being an elected individual. **The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List) –** The Part 561 List includes the names of foreign financial Institutions that are subject to sanctions, certain prohibitions, or strict conditions before a U.S. company may do business with them. This does not require criminal charges or conviction.	Name, Place of Birth, Nationality, Passport (country) info, National ID no., Residency Number (country of residence), Address, Gender, E-mail address, Membership of organization, Employment	NO Information about which List subject to with law ref. (eg. Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560)

		Non-SDN Iranian Sanctions Act (NS-ISA) List –The ISA List includes persons determined to have made certain investments in Iran's energy sector or to have engaged in certain activities relating to Iran's refined petroleum sector. Their names do not appear on the Specially Designated Nationals or Blocked Persons (SDN) List, and their property and/or interests in property are not blocked, pursuant to this action. This is an economic sanction and being placed on this list means the person has made investments in the energy section or participated in the petroleum sector. List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List)		
Department of State – Directorate of Defence Trade Controls (DDTC)	List of Administratively Debarred Parties https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=8a89528adb3cd30044f9ff621f961931	Includes persons who have been subject of an administrative procedure in accordance with part 128 ITAR and are administratively debarred pursuant to ITAR section 127.7 (a). Thus, these persons are prohibited from participating directly or indirectly in any activities that are subject to ITAR. Only three persons on the list.	Name, date of birth	NO Information about Federal Register Notice (eg. 83 FR 18112), link to Federal Register with information about persons administratively debarred and information about administrative procedures. In two cases attached Charging Letter – administrative procedures are constituted by means of a charging letter ag. Respondent for the purpose of obtaining an Order imposing civil administrative sanctions.

	List of Statutorily Debarred Parties https://www.pmddtc.state.gov/?id=ddtc_kb_article_page&sys_id=7188dac6db3cd30044f9ff621f961914	Entities and individuals prohibited from participating directly or indirectly in any activities that are subject to ITAR. Pursuant to the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), the List includes persons convicted of violating the AECA or of conspiracy to violate the AECA and who are subject to "statutory debarment" pursuant to §38(g)(4) of the AECA and §127.7 of the International Traffic in Arms Regulations (ITAR). The first criteria is a criminal action. However, the administrative debarment is not criminal and would not result in a criminal record.	Name	NO Information about Federal Register Notice (eg. 78 FR 72745) link to Federal Register – information about persons under statutory debarment - name of persons convicted in a U.S. District Court - Name; Date of Judgment; Judicial District; Case No.; Month/Year
Department of State – Bureau of International Security and Nonproliferation	List of Nonproliferation Sanctions https://www.state.gov/documents/organization/273924.pdf	The United States imposes sanctions under various legal authorities (eg. Nuclear Proliferation Prevention Act, Export Import Bank Act, Executive Orders) against foreign individuals, private entities, and governments that engage in proliferation activities. These are individuals and entities which have been found to be a threat to non-proliferation. Placement on the list does not require criminal changes or convictions	Name, Country	NO Information about Federal Register Notice (eg Vol. 83, No 91, May 10, 2018.) link to Federal Register with information about what act/regulation violated (eg. Nuclear Proliferation Prevention Act) and what sanctions are in place (eg. The United States shall not procure, or enter into any contract for the procurement of, any goods or services from these persons)

Bilaga 2 – Medlemmar i Säkerhets- och försvarsföretagen

2Secure AB
4C Strategies AB
Aimpoint AB
AirContact Group Sverige
AVL MTC Motortestcenter
BAE Systems Hägglunds AB
Borderlight
CBJ Tech AB
CGI Sverige AB
CNC Quality AB
Comex Electronics AB
CRD Protection AB
CybAero AB
Dockstavarvet AB
Eltel Networks Infranet AB
Eurenco Bofors AB
FLIR Systems AB
GKN Aerospace Sweden AB
GomSpace Group
Habia Cable AB
Hilleberg Tentmaker AB
Kitron AB
Kriisa Consulting AB
Marine Jet Power AB
Mildef AB
MIPS AB
Nammo Sweden AB
Nixu AB
Partnertech
Pitch Technologies AB
Poseidon Diving Systems AB
Recotech AB
Rote Consulting AB
Saab AB
Scama AB
Scania CV AB
Secana AB
Sepson AB
SnigelDesign AB
System Engineering Solution 37 AB
3M Svenska AB (Peltor)
Acker Enterprises AB
Air Target Sweden
Armstech International Defence Group AB
BAE Systems Bofors AB
Bofors Test Center AB
Carmenta AB
Cervino Consulting
CLP Systems AB
Combitech AB
Condesign AB
Crypto International Group
Datapath International AB
Ekelöw/PWC
Esri Sverige AB
Expisoft
Foreseeti AB
GlenAir Nordic
Granqvist Sportartiklar AB
Hammar Maskin AB
IBM Svenska AB
Knowit Dataunit AB
Lidan Marine AB
Mekanotjänst
Military Work AB
MSE Engineering AB
Ninac Holding AB
Outmeals AB
Patria Helicopters AB
Polyamp AB
Qinetiq Sweden AB
Rolls-Royce AB
RSG Connexion
SAS Institute AB
Scandinavian Risk Solutions AB
Scienta Sensor Systems AB
Sensec AB
Skyddsprodukter i Sverige AB
St Hunna
Swede Ship Marine AB

Svekon – Svensk Konstruktionstjänst AB
Systecon AB
Taiga AB
Teleanalys AB
T-Kartor Sweden AB
W-5 Systems AB
Vibratec Akustikprodukter
Woolpower Östersund AB
Vricon Systems AB
ÅF Solutions AB
Syntell AB
Systematic Sweden AB
TD Fiberoptik AB
Tempest Security AB
Tutus Data AB
Venatio AB
Volvo Defense AB
WorkCon AB
ÅAC Microtec AB
Åkers Krutbruk Protection