Säkerhets- och försvarsföretagen, SOFF
ombud för 2 Secure AB
samt 99 bolag enligt bilaga

Beslut om tillstånd att behandla personuppgifter om lagöverträdelser

Datainspektionens beslut

Bolaget får tillstånd att behandla personuppgifter om lagöverträdelser som innefattar brott genom kontroller av Bolagets befintliga och potentiella kunder, befintliga och potentiella leverantörer, samarbetspartners, förmedlare, arbetstagare, arbetssökande, uppdragstagare och besökare samt ställföreträdare, firmatecknare, ägare, verkliga huvudmän och borgensmän för de angivna juridiska personerna i den mån det är nödvändigt för att uppfylla krav inom ramen för de amerikanska regelverken International Traffic in Arms Regulations (ITAR) och Export Administration Regulation (EAR) och de sanktionsprogram som administreras av Office of Foreign Assets Control (OFAC) och Bureau of International Security and Nonproliferation som svenska bolag måste följa för att inte enligt amerikansk lagstiftning riskera böter och förlora sina exportlicenser och olika andra typer av tillstånd mot följande sanktionslistor:

De av Department of State – Directorate of Defence Trade Controls (DDTC) utfärdade listorna:

- List of Administratively Debarred Parties
- List of Statutorily Debarred Parties

De av Department of Commerce – Bureau of Industry and Security (BIS) utfärdade listorna:

- Denied Persons List

- Entity List
- Unverified List

De av Department of the Treasury - Office of Foreign Assets Control (OFAC) utfärdade listorna:

- Specially Designated Nationals and Blocked Persons (SDN-listan)
- Consolidated Sanctions List ("CSL-listan"), som för närvarande omfattar listorna:

  - Sectorial Sanctions Identifications List ("SSI-listan")
  - Foreign Sanctions Evaders List ("FSE-listan")
  - Non-SDN Iranian Sanctions Act List ("NS-ISA-listan")
  - Palestinian Legislative Council List ("NS-PLC-listan")
  - List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions ("CAPTA-listan")
  - The List of Foreign Financial Institutions Subjekt to Part 561 (the Part 561 List)

Den av Department of State – Bureau of International Security and Nonproliferation (ISN) utfärdade listan:

- List of Nonproliferation Sanctions

CSL-listan är en dynamisk och konsoliderad sanktionslista, varför Datainspektionen kan komma att ändra eller återkalla beslutet i denna del för det fall CSL-listan utökas med ytterligare sanktionslistor.

Beslutet gäller tills vidare men kan återkallas om Bolaget behandlar eller kan komma att behandla personuppgifter på ett sätt som strider mot förutsättningarna i detta beslut.

Ansökan

Bolaget (se bilaga) är medlem i branschorganisationen Säkerhets- och försvarsföretagen (SOFF). Bolaget har genom sitt ombud SOFF ansökt om tillstånd att behandla personuppgifter om lagöverträdelser. Av ansökan framgår bl.a. följande.

SOFF:s medlemsföretag tillverkar, underhåller och säljer krigsmateriel och produkter med dubbla användningsområden. 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. 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 utvecklas 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 försvars- och säkerhetsprodukter. 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 i dag 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 dubbla användningsområden. De amerikanska exportrestriktionerna innebär bl.a. att personer som finns med på vissa spärr- och sanktionslistor inte får gens tillgång till 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 enskilda – befintliga och potentiella kunder, befintliga och potentiella leverantörer, samarbetspartners, förmedlare, arbetstagare, arbetssökande, uppdragstagare och besökare samt ställföreträdare, firmatecknare, ägare, verkliga huvudmän och borgensmän

för de angivna juridiska personerna – gentemot spärrlistorna. 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.

De amerikanska spärr- och sanktionslistor som svenska företag enligt amerikansk lag måste screena mot är offentliga och innehåller uppgifter om både företag, organisationer och enskilda individer. Uppgifterna ska beaktas i samband med internationella affärer, t.ex. orderhantering och betalning. Företag, myndigheter och enskilda åläggs olika skyldigheter som t.ex. anmälningsskyldighet eller förbud mot att handla med de på listorna angivna personerna, organisationerna eller företagen.

Det amerikanska exportkontrollsystemet är omfattande, men det är särskilt två amerikanska exportkontrollregelverk och listor som är kopplade till dessa som berör svenska företag som importerar och säljer amerikanska produkter och teknologier: International Traffic in Arms Regulations (ITAR) och Export Administration Regulation (EAR)

ITAR-regelverket hanteras av Department of State – Directorate of Defence Trade Controls (DDTC). Dessa regler tar främst sikte på amerikansk utrikespolitik och intern säkerhet. DDTC adminstrerar List of Administratively Debarred Parties och List of Statutorily Debarred Parties.

EAR-regelverket hanteras av Department of Commerce – Bureau of Industry and Security (BIS). Dessa regler har som mål att tillgodose USA:s ekonomiska intressen. BIS administrerar Denied Persons List, Entity List och Unverified List.

Ytterligare regelverk som måste efterlevas är det av Department of the Treasury - Office of Foreign Assets Control (OFAC) administrerade regelverk som syftar till att upprätthålla ekonomiska sanktioner och handelssanktioner. OFAC administrerar Specially Designated Nationals and Blocked Persons (SDN-listan) och Consolidated Sanctions List (“CSL-listan”). CSL-listan är en konsoliderad lista som för närvarande omfattar listorna Sectorial Sanctions Identifications List (“SSI-listan”), Foreign Sanctions Evaders List (“FSE-listan”), Non-SDN Iranian Sanctions Act List (“NS-ISA-listan”), Palestinian Legislative Council List (”NS-PLC-listan”), List of Foreign

Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (“CAPTA-listan”) och The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)..

Vidare administrerar Department of State – Bureau of International Security and Nonproliferation (ISN) det regelverk som syftar till att motverka förbjuden spridning av massförstörelsevapen. ISN administrerar List of Nonproliferation Sanctions.

Vid överträdelser av den amerikanska lagstiftningen 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 själva 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 skulle kunna innebära t.ex. uteblivna leveranser till det svenska försvaret och att svenska staten inte längre kan säkerställa sin materielförsäljning, särskilt där staten har ett systemberoende.

Bolaget har mot denna bakgrund ett berättigat intresse att behandla de aktuella uppgifterna. Det potentiella intrånget i integritet för den registrerade är begränsat. Listorna är publicerade av amerikanska myndigheter på Internet och är allmänt tillgängliga. SOFF:s medlemsföretag har utvecklade metoder för att förhindra sammanblandning av personer som finns med på listorna och andra personer med samma eller liknande namn (äkta respektive falska träffar). Behandlingen kommer i övrigt att ske i enlighet med tillämplig dataskyddslagstiftning, t.ex. att den registrerade kommer att informeras på förhand om att dennes personuppgifter kommer behandlas genom screening mot sanktionslistor och att det finns rutiner för arkivering och radering.

Skäl för beslutet

Av artikel 10 dataskyddsförordning (2016/679) framgår att behandling av personuppgifter som rör fällande domar i brottmål och lagöverträdelser som innefattar brott eller därmed sammanhängande säkerhetsåtgärder får utföras

endast under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

Datainspektionen har med stöd av 3 kap. 9 § lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och 6 § andra stycket förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning möjlighet att i enskilda fall besluta att andra än myndigheter får behandla personuppgifter som avses i artikel 10 i EU:s dataskyddsförordning. Ett beslut får förenas med villkor.

Datainspektionen har i flera fall tidigare beviljat enskilda undantag från förbudet i 21 § personuppgiftslagen (1998:204) för bolag som bedrivit sådan verksamhet som krävt kontroll av sina kunder mot SDN-listan. Med ledning av förarbetsuttalandena till den numera upphävda personuppgiftslagen drog Datainspektionen dock slutsatsen att möjligheten att meddela undantag från förbudet att behandla uppgifter om lagöverträdelser skulle utnyttjas restriktivt. Denna restriktiva tolkning slogs även fast av Högsta förvaltningsdomstolen i HFD 2016 ref 8.

Av förarbetena till lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning framgår att utrymmet för att tillåta behandling av personuppgifter som rör lagöverträdelser är större genom EU:s dataskyddsförordning eftersom det inte längre finns något principiellt förbud mot att andra än myndigheter behandlar personuppgifter om lagöverträdelser, (se prop. 2017/18:105, s. 99 ff.). Vidare följer av förarbetena att regeringen bedömde att kravet på lämpliga skyddsåtgärder i artikel 10 i EU:s dataskyddsförordning i princip kan vara uppfyllt genom den tillstånds-prövning som föregår sådana beslut som Datainspektionen kan meddela andra än myndigheter i enskilda fall. Det tilläggs att besluten vid behov även kan förenas med villkor såsom återkallelseförbehåll, tidsbegränsningar eller krav på återrapportering samt krav på att den personuppgiftsansvarige ska vidta vissa åtgärder till skydd för de registrerades rättigheter och friheter. Mot bakgrund av det anförda konstaterade regeringen att Datainspektionens utrymme att avslå en begäran om tillstånd i princip torde vara begränsat till de fall där behandlingen skulle vara oförenlig med EU:s dataskyddsförordning i övrigt, i synnerhet principerna i artikel 5 och kravet på rättslig grund i artikel 6. I annat fall bör tillstånd beviljas, men vid behov

förenas med krav på lämpliga skyddsåtgärder för de registrerades rättigheter och friheter. Regeringen konstaterade särskilt avseende möjligheten för svenska bolag att få tillstånd i den mån detta krävs för kontroll mot sanktions- och spärrlistor, t.ex. för export till vissa länder, att detta bör vara möjligt, i vart fall om dessa listor är fastställda i demokratisk ordning och allmänt tillgängliga. Vidare är regeringens uppfattning att svenska företag inte ska ges sämre möjligheter att behandla sådana uppgifter än företag i andra länder.

Datainspektionen konstaterar att företag som tillverkar, underhåller och säljer krigsmateriel och produkter med dubbla användningsområden, för att leva upp till krav inom ramen för regelverk inom den amerikanska exportlagstiftningen som ett svenskt bolag måste följa för att inte riskera att påföras höga böter och förlora sina exportlicenser och olika andra typer av tillstånd samt att självt hamna på spärrlistan, måste vidta åtgärder som effektivt motverkar att amerikansk försvarsteknik kommer i orätta händer, vilket bland annat kan innefatta kontroller mot sanktionslistor.

Behovet av att kunna utföra kontroller mot en sanktionslista måste dock vägas mot risken för att de personer som kontrolleras kan komma att uppleva att kontrollerna innebär ett intrång i deras personliga integritet. Det kan också finnas risk för att en person felaktigt kan komma att förknippas med en person som förekommer på listan som har samma namn som den kontrollerade personen.

Datainspektionen anser att behovet av att behandla personuppgifter om de aktuella kategorierna personer för att leva upp till krav inom ramen för olika regelverk inom den amerikanska exportlagstiftningen är berättigade ändamål och har stöd i en intresseavvägning enligt dataskyddsförordningens artikel 6 1 f.

Datainspektionen bedömer att de aktuella listorna får anses vara fastställda i demokratisk ordning och är allmänt tillgänglig på amerikanska myndigheters webbplatser.

Datainspektionen konstaterar att Bolaget har infört rutiner för att skilja på s.k. äkta och falska träffar vid kontroller mot sanktionslistor, för att på så sätt

undvika felaktiga utpekanden av personer och en felaktig personuppgiftsbehandling.

Vid en sammantagen bedömning anser Datainspektionen att det finns förutsättningar att meddela tillstånd för Bolaget att behandla personuppgifter om lagöverträdelser vid kontroller av ovan angivna kategorier av personer mot de aktuella listorna.

Beslutet förutsätter att Bolaget i övrigt behandlar personuppgifter i enlighet med bestämmelserna i EU:s dataskyddsförordning.

Beslutet kan komma att återkallas om det visar sig att Bolaget behandlar eller kan komma att behandla personuppgifter på ett sätt som strider mot förutsättningarna i detta beslut.

Hur man överklagar

Om ni vill överklaga beslutet ska ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Förutsatt att överklagandet inte innehåller några integritetskänsliga personuppgifter eller uppgift som kan omfattas av sekretess, kan ni e-posta överklagandet till datainspektionen@datainspektionen.se.

Detta beslut har fattats av enhetschefen Catharina Fernquist efter föredragning av avdelningsdirektören Hans Kärnlöf.

Catharina Fernquist, 2019-09-12 (Det här är en elektronisk signatur)

SOFF
Säkerhets- och försvarsföretagen

Bilaga – 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

SOFF
Säkerhets- och försvarsföretagen

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