2019-04-01

R E M I S S V A R

Justitiedepartementet
103 33 Stockholm

FI Dnr 19-31

Finansinspektionen
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

Betänkande SOU 2018:82 Kompletteringar till den nya säkerhetsskyddslagen (Dnr Ju2018/0592/L4)

Sammanfattning

Finansinspektionen (FI) tillstyrker i stort utredningens förslag, men vill uppmärksamma följande:

- Detaljreglering av säkerhetsskyddschefens organisatoriska placering är olämplig. Säkerhetsskyddschefen behöver ha en eller flera biträdande säkerhetsskyddschefer för att inte det ska uppstå luckor i säkerhetsskyddet vid dennes frånvaro.
- FI anser också att det inte är tydligt om ny särskild säkerhetsbedömning, lämplighetsprövning och samråd behöver genomföras vid större revideringar av säkerhetskyddsavtal. Därtill är det oklart om och när en omfattande revidering av säkerhetsskyddsavtalet har förändrat förutsättningarna för det bör anses som ett nytt avtal.
- Frågan om i vilken utsträckning tillsynsmyndigheterna kan lämna sekretessbelagda uppgifter, t.ex. rörande ett enskilt tillsynsobjekt, till samordningsmyndigheten bör belysas ytterligare i den fortsatta beredningen.
- Maximibeloppet för sanktionsavgifterna bör höjas och bestämmas i proportion till företagets omsättning för att vara effektiva, proportionerliga och avskräckande. Förslaget i betänkandet med ett maxbelopp på 10 miljoner kronor är lågt sett till att storleken på de företag inom den finansiella sektorn som kommer att omfattas av reglerna. FI bedömer att högre maxbelopp bör övervägas för att sanktionerna ska vara avskräckande.

FI:s synpunkter

FI ordnar sina synpunkter enligt betänkandets disposition. Underrubrikerna nedan avser avsnitt i betänkandet.

5.4 Skyldigheten att ingå säkerhetskyddsavtal bör utvidgas

FI stödjer en utvidgad skyldighet för det allmänna och enskilda att ingå säkerhetsskyddsavtal, samt att tillgång till säkerhetsskyddsklassificerade uppgifter eller säkerhetsskyddad verksamhet ska vara avgörande. FI delar även utredningens syn att det finns ett stort behov att säkra säkerhetsskyddsklassificerade uppgifter i andra situationer än vid upphandlingar.

FI tolkar det som att olika bolag inom samma koncern anses som utomstående parter i förhållande till varandra, eftersom de är skilda juridiska personer (se avsnitt 5.4.2). Det kan skapa komplikationer för berörda företag. I den finansiella sektorn förekommer att moderkoncerner lägger ut IT-driften på dotterbolag alternativt centraliserar IT-driften hos moderkoncernen. Det skulle därför krävas ett stort antal koncerninterna avtal, vilket riskerar att bli kostsamt sett i relation till fördelarna. I förlängningen ser FI en risk att detta ger upphov till en stor volym ärenden gällande bland annat samrådsförfaranden. Det skulle kräva stora tillsynsresurser inom ett område där riskerna kan kontrolleras med andra medel.

Mot denna bakgrund anser FI att det vore önskvärt i den fortsatta beredningen överväga en lösning som innebär att moderbolag/koncerner tillsammans med sina dotterbolag i lagen hanteras som en enhet. FI ser en möjlig lösning i att moderbolag/koncerner tillsammans med sina dotterbolag i lagen behandlas som en enhet.

6.6 Säkerhetsskyddschefens roll i organisationen bör stärkas

FI stödjer förslaget att säkerhetsskyddschefens roll och uppdrag tydligt framgår i lag. Det är vidare positivt att funktionens ansvar inte får delegeras. Det bör dock poängteras att ansvaret kan behöva delas med en eller flera biträdande säkerhetsskyddschefer, då en enskild person inte ständigt kan vara närvarande eller i tjänst. Ansvaret bör dock aldrig rutinmässigt delegeras.

FI ser inga problem med formuleringen ”säkerhetskyddschefen ska vara direkt underställd den person som är ansvarig för verksamhetsutövarens verksamhet”. FI anser dock att det är olämpligt att detaljreglera säkerhetsskyddschefens organisatoriska placering. Säkerhetsskyddschefen och säkerhetsskyddsfrågorna torde kunna få komma till tals frekvent i t.ex. en ledningsgrupp utan att säkerhetsskyddschefens organisatoriska placering anges i lag. Ansvaret för att säkerhetsskyddschefen får adekvat utrymme i ett sådant forum åligger den

person som är ansvarig för verksamhetsutövarens verksamhet. Hur detta ska ske kan regleras i interna styrdokument för verksamheten.

FI vill också påpeka tvetydighet i skrivningar. Under avsnitt 6.6 på s. 200 står det att ”säkerhetsskyddschefen *bör* rapportera till organisationens högsta chef…”. Under avsnitt 6.7.1 på s. 204 framgår det att ”säkerhetsskyddschefen *ska* leda… samt rapportera till organisationens högsta chef*”*. I 6 c § anges inget krav om rapportering alls. FI förstår det som att kravet på rapportering ligger implicit i att säkerhetsskyddschefen ska vara direkt underställd den person som är ansvarig för verksamhetsutövarens verksamhet, men detta förhållande bör beskrivas enhetligt i motivtexten.

Givet utredningens förslag i avsnitt 5.4 tolkar FI det som att samtliga dotterbolag som bedriver säkerhetskänslig verksamhet, i exempelvis en koncern, ska ha en egen säkerhetsskyddschef. FI ser dock fördelar i att moderbolag och dotterbolag behandlas som en enhet även i fråga om säkerhetsskyddschef. Det skulle underlätta för vissa företagsgrupper, där mycket av riskhanteringen sköts från central nivå och där den lokala organisationen har små resurser. FI ser att ett krav på en särskild säkerhetsskyddschef för varje eget dotterbolag innebära en betydande kostnad.

Alldeles oavsett om den fortsatta beredningen behandlar moderbolag och dotterbolag som en enhet eller ej, så FI föreslår att det i den fortsatta beredningen förtydligas om/att uppgiften som säkerhetsskyddschef kan kombineras med en annan roll i verksamheten.

6.11 Uppföljning av avtal under avtalstiden och ändrade förhållanden.

FI ser positivt på att säkerhetsskyddsavtal ska följas upp. FI menar att även frekvens och omfattning bör anges i lag eller förskrifter. Det ansluter till kravet på att verksamhetsutövare ska uppdatera sin säkerhetsskyddsanalys årligen, enligt förslaget i 2 kap. 1 §. Vidare rekommenderas i avsnitt 8.16 att frekvens för tillsynen över säkerhetsskyddet hos tillsynsobjekten skrivs in i samordningsmyndigheternas föreskrifter.

FI föreslår mot den bakgrunden att det även anges i författning hur ofta en verksamhetsutövare ska följa upp sina säkerhetsskyddsavtal. FI förstår att det kan bli resurskrävande för verksamhetsutövare med många säkerhetsskyddsavtal. FI anser dock att kravet är motiverat. Uppföljningen innebär kontroll av skyddet för säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre, eller att en utomstående fått tillgång till säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet, såsom anges under avsnitt 3.4.6.

6.11.3 Revidering av säkerhetsskyddsavtal efter ändrade förhållanden
FI bedömer att det är rimligt att en revidering av säkerhetskyddsavtal sker vid ändrade förutsättningar. Det skulle exempelvis kunna bero på en aggregering av konfidentiella uppgifter i ett datasystem, såsom nämns i avsnitt 5.4.7. Det

kan leda till att datasystemet behöver vara anpassat för att hantera information av säkerhetsskyddsklassen hemlig, och således behöver omgärdas av ett annat paket av säkerhetsskyddsåtgärder, vilket kommer att medföra ökade kostnader.

Därtill framgår det inte tydligt om en revidering av säkerhetsskyddsavtalet, enligt vad som beskrevs ovan i exemplet med datasystem, innebär att ny särskild säkerhetsbedömning, lämplighetsprövning och samråd behöver genomföras. FI anser att detta bör specificeras, då verksamhetsutövares lämplighet att hantera säkerhetsskyddsklassificerade uppgifter kan vara beroende av vilken säkerhetsskyddsklass som omfattas.

FI ser ett behov av att regler och förutsättningar för att revidera ingångna säkerhetsskyddsavtal belyses ytterligare i den fortsatta beredningen.

8.10.3 Verksamhetsutövarens uppgiftsskyldighet

Frågan om sekretessbrytande bestämmelser (10 kap. 17 § OSL) när en myndighet som står under tillsyn ska lämna uppgifter till tillsynsmyndigheten berörs i avsnittet. Däremot behandlas inte frågan om i vilken utsträckning tillsynsmyndigheterna kan lämna sekretessbelagda uppgifter, t.ex. rörande ett enskilt tillsynsobjekt, till samordningsmyndigheten med stöd av samma bestämmelse. Detta bör belysas ytterligare i den fortsatta beredningen.

8.15 Systematisk kartläggning och dokumentation av tillsynsobjekt

FI stöder utredningens förslag att tillsynsmyndigheten ska identifiera och systematiskt kartlägga de verksamheter inom tillsynsmyndighetens ansvarsområde som omfattas av säkerhetsskyddslagen. En sådan kartläggning förutsätter dock att det är tydligt vilka typer av verksamheter och vilken information som omfattas av lagen.

I sammanhanget noterar FI att för vissa fall kan säkerhetskänsliga verksamhetsutövare falla utanför en tillsynsmyndighets ansvarsområde samtidigt som det inte är uppenbart för annan tillsynsmyndighet att leverantören ingår i dennes tillsynsområde. Anta exempelvis att utkontraktering görs av flera aktörer, som har olika tillsynsmyndigheter för deras säkerhetsskydd, till en och samma leverantör och att aktörernas egna verksamheter eller uppgifter inte faller inom ramen kravet på säkerhetsskyddsavtal i säkerhetsskyddslagen. Då kan det uppstå aggregering av information samt koncentrationsrisker hos leverantören. Koncentrationsrisken hos en sådan leverantör skulle kunna innebära att verksamheten som sådan eller dennes aggregerade information skulle kunna falla innanför ramen för säkerhetsskyddslagen. En sådan omständighet kan vara helt okänd för berörda tillsynsmyndigheter.

Ett mer specifikt exempel är Finansiell ID-teknik, bolaget bakom mobilt Bank-ID. Denna tjänst är en förutsättning för vissa betalningslösningar, men faller utanför FI:s föreslagna tillsynsområde. Bank-ID används samtidigt på en rad

områden utanför den finansiella sektorn. Sammantaget bedömer FI att det kan finnas ett behov av samordning mellan tillsynsmyndigheter för att sådana verksamhetsutövare ska kunna identifieras och därmed ingå i den kartläggning som berörd tillsynsmyndighet ska upprätta. FI anser att ett krav på sådan samordning bör framgå i författning eller vägledning.

9.11 Sanktionsavgiftens storlek

Utredningen har gett förslag om sanktionsavgifter ”som ska bestämmas till lägst 5 000 kronor och högst 10 miljoner kronor”. Mot bakgrund av betydelsen för Sveriges säkerhet att lagen upprätthålls och den skada som överträdelser kan orsakas bör sanktionsavgiften vara avskräckande, vilket också utredningen föreslår under avsnitt 9.11 ”för att sanktionsavgifterna ska vara effektiva, proportionerliga och avskräckande bör intervallet för sanktionsavgiften vara förhållandevis stort. Tillsynsmyndigheten får då möjlighet att göra en nyanserad bedömning när avgiftens storlek ska bestämmas.”

FI vill uppmärksamma att sanktionsavgifterna är betydligt högre i andra lagar inom FI:s tillsynsområde. Som exempel kan nämnas lag (2004:297) om bank- och finansieringsrörelse, i vilken en överträdelse till exempel kan leda till en sanktionsavgift för en storbank med årsomsättning på 70 miljarder kronor som högst fastställas till 7 miljarder kronor. Även inom andra sektorer är det i många fall stora företag som berörs av reglerna.

FI ser en risk i att relativt låga sanktionsavgifter i säkerhetsskyddslagen kan leda till att arbete för att leva upp till kraven i lagen inte kommer prioriteras tillräcklig högt.

Lagen tillämpas på ett flertal olika branscher med företag av olika storlek. FI uppmärksammar således ett behov av att taket är anpassat till detta för att sanktionsavgiften ska vara effektiv, proportionerlig och avskräckande även för företag inom det föreslagna tillsynsområdet för FI. Att koppla sanktionsavgiften till ett mått på företagets omsättning är en lösning som bör övervägas.

11.4.1 Ekonomiska konsekvenser för det allmänna

FI delar utredningens mening i avsnitt 8.4.7 om att tillsynskompetensen måste öka, samt att tillsynen över säkerhetsskydd inte kan fortsätta bedrivas i sådan begränsad omfattning som av utredningen anges under avsnitt 8.4.6 samt att tillsynen bör ha en kvalitativ inriktning såsom anges i avsnitt 8.3.

FI har tidigare angett, i begäran från utredningen om uppgifter från föreslagna tillsynsmyndigheter, bland annat att det idag finns åtta verksamhetsutövare inom det föreslagna tillsynsområdet, och att det inte kan uteslutas att ytterligare några aktörer bedriver säkerhetskänslig verksamhet, t.ex. de mellanstora bankerna. FI uppskattade då ett permanent behov av tio årsarbetskrafter för detta ändamål.

Utredningen bedömer att det av FI uppskattade resursbehovet framstår som mycket högt i förhållande till antalet tillsynsobjekt för andra föreslagna tillsynsmyndigheter, även med beaktande av verksamheternas komplexitet. Utredningen anser även att det borde vägas in att flera av tillsynsobjekten ifråga står under annan typ av tillsyn från FI.

FI anser dock att antalet tillsynsobjekt förvisso är färre än för vissa andra föreslagna tillsynsmyndigheter, men storleken och komplexiteten (strukturer, ägarförhållande, verksamheter som spänner över nationsgränserna) hos företagen, mängden leverantörer företagen använder sig av samt beroende av internationella aktörer inom det område som FI förslås utöva tillsyn över, kommer innebära en väsentligt ökad arbetsbelastning.

Enligt förslaget under avsnitt 8.7.3 skrivs det att ”vi föreslår därför att tillsynsområdet definieras som finansiella företag och motsvarande utländska företag som är etablerade i Sverige”. FI vill poängtera att den tillsyn FI bedriver idag skiljer sig från tillsynen över säkerhetsskyddet. Även om samordningsfördelar finns inom tillsynen kan de tillkommande uppgifterna inte utföras med befintlig kompetens och nuvarande resurser inom FI.

Mot den bakgrunden understryker FI att myndighetens behov för att utöva adekvat tillsyn inom det föreslagna tillsynsområdet uppgår till tio permanenta årsarbetskrafter, utöver de sju till nio föreslagna årsresurserna för de tillkommande säkerhetsprövningarna.

Allmänna reflektioner kring utredningens förslag

FI vill påtala ett behov av tydlig vägledning och metodik för verksamhetsutövare men också tillsynsmyndigheter på flertalet punkter.

Inom den finansiella sektorn finns ett stort internationellt beroende, bland annat till europeiska centrala betalningsinfrastrukturer (t.ex. EU Target2, T2S, TIPS), tjänster som levereras av moderbolag i koncerner inom och utanför EU, tjänsterna som levereras av verksamhetsutövarens egen filial verksamhet eller dotterbolag inom EU, vissa tjänster förses av etablerade globala tjänsteleverantörer för betalningar, t.ex. kortföretag, samt datahallar, IT-system samt utvecklingen av IT-system som finns utanför Sveriges gränser.

Den finansiella sektorn är beroende av IT och det finansiella systemet är i hög grad digitaliserad, komplext och sammanlänkad. Detta försvårar identifieringen för verksamhetsutövare under tillsyn, men också tillsynsmyndigheternas tillsyn. Vissa IT-system är troligtvis att anse som säkerhetskänsliga. Processen att identifiera dem kommer troligtvis inte vara helt enkel, men nödvändig för att inte tillämpa kostnadsdrivande säkerhetsskyddsåtgärder på hela IT-system eller IT-avdelningar.

Det behöver finnas tydlig vägledning i självidentifieringsprocessen, med kriterier, men också motsvarande vägledning för tillsynsmyndigheterna som i sin tur ska ge vägledning, samt identifiera ej anmälda tillsynsobjekt.

Av samma anledning ser FI ett tydligt behov av vägledning med tydliga kriterier, för tillsynsmyndigheterna att kunna ge vägledning, utöva tillsyn över säkerhetsskyddet såsom säkerhetsskyddsanalyser och säkerhetsskyddsavtal samt vid samråd vid säkerhetsskyddsavtal och överlåtelser i avsnitten 6.8-6.9 och 7.10. Motsvarande vägledning behöver finnas för verksamhetsutövarna under tillsyn för bland annat särskild säkerhetsbedömning och lämplighetsbedömning med riskparametrar och kriterier, vid säkerhetsskyddsavtal och överlåtelser, samt tillgängliga listor över länder som Sverige har en överenskommelse med om säkerhetsskydd.

Några specifika frågor som kan kräva vägledning med kriterier är exempelvis hur verksamhetsutövaren i lämplighetsprövningen bör beakta användningen av kryptografiska funktioner i lösningar, om data och servrar finns i Sverige eller utanför landets gränser? Bör lämplighetsbedömningen utgå ifrån specifika IT-system eller verksamheten i sig eller bör den även omfatta miljöerna och data hallar som IT-system finns i? Spelar kriticitet av leverantör roll i omfattningen av lämplighetsprövning? Bör samma kriterier tillämpas för en mindre leverantör som för den centrala leverantören?

FI önskar därmed att regeringen ger samordningsmyndigheterna i uppdrag att ta fram tydliga vägledningar för tillsynsmyndigheter och verksamhetsutövare.

11.4.5 Kompetensförsörjning och behov av utbildning

FI instämmer i utredningens resonemang kring kompetensförsörjning inom området och vill understryka vikten av att resurser och kompetens inom säkerhetsskydd finns tillgängliga vid ikraftträdande. Resurser och kompetensförsörjningen inom området är förutsättningen för implementeringen av förslagen i utredningen. Kompetensförsörjningen inom området bör vara prioriterat, i synnerhet då efterfrågan sannolikt kommer öka markant i samband med att den nya säkerhetsskyddslagen träder ikraft. FI ser således ett tydligt behov av utbildningsinsatser från exempelvis samordningsmyndigheterna innan ikraftträdandet 2021.

FINANSINSPEKTIONEN

Erik Thedéen
Generaldirektör

Stefan Jonasson
Säkerhetssamordnare
08-408 980 00