2017-08-15

R E M I S S V A R

Justitiedepartementet
103 33 Stockholm

ju.I4@regeringskansliet.se

FI Dnr 17-8769
(Anges alltid vid svar)

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

Remissvar – Betänkandet SOU 2017:36 Informationssäkerhet för samhällsviktiga och digitala tjänster (Ju2017/03997/L4)

Sammanfattning

Finansinspektionen (FI) tillstyrker i huvudsak utredningens förslag.

FI vill dock uppmärksamma regeringen på att utredningens förslag till krav om incidentrapportering tillsammans med andra närliggande krav, som exempelvis förslaget till ny säkerhetsskyddslag (SOU 2015:25) och dataskyddsförordningen, kan medföra parallell rapportering till flera myndigheter med varierande innehåll och responstid om samma händelse. En bristande harmonisering av kraven kan enligt FI komma att medföra en risk för att vissa leverantörer väljer att inte rapportera alla relevanta incidenter och att lagstiftarens syfte med reglerna därmed undermineras.

Vidare anser FI att det finns väsentliga effektivitetsvinster för tillsynen av de finansiella företagens arbete med informationssäkerhet om befintlig sektorreglering i så stor utsträckning som möjligt beaktas. I det sammanhanget vill FI påpeka att verksamhet som drivs i Sverige genom filialer till banker i andra EES-länder inte omfattas av de svenska reglerna utan av de som gäller i bankens hemland. Det är viktigt att ta hänsyn till detta vid utformningen av reglerna.

FI föreslår även att
- begreppet autenticitet stryks från definitionen av begreppet säkerhet i nätverk och informationssystem (avsnitt 1.1),
- benämningen av begreppet säkerhetsprinciper ändras till säkerhetsregler och att definitionen av begreppet justeras (avsnitt 1.1),
- under den fortsatta beredningen av utredningens förslag det klargörs vad som avses med begreppet annan författning i 5 § andra stycket lagen (avsnitt 5.4),
- de nya föreskrifter som Myndigheten för samhällsskydd och beredskap (MSB) föreslås ta fram om systematiskt arbete med informationssäkerhet blir principbaserade till sin utformning (avsnitt 7.3.1), och att

- begreppet auktoriserad revisor ändras till begreppet kvalificerad oberoende granskare (avsnitt 8.5.3).

Allmänt

Den avsnittsnumrering som används nedan i detta remissvar avser motsvarande avsnitt i utredningsbetänkandet.

1.1 Definitioner i lagen (7 §)

Säkerhet i nätverk och informationssystem
FI föreslår att begreppet *autenticitet* stryks från definitionen av begreppet *säkerhet i nätverk och informationssystem.*

Genom att ta bort begreppet autenticitet likställs definitionen med den i Sverige mer etablerade definitionen bestående av begreppen *konfidentialitet, riktighet* och *tillgänglighet.* Det minskar risken för att ett ökat fokus oavsiktligt läggs på säkerställandet av informationens autenticitet. En sådan definition skulle också ge en ökad harmonisering med befintliga legaldefinitioner på nationell nivå och inte minst allmänt etablerad praxis inom exempelvis sektorerna för bankverksamhet och finansmarknadsinfrastruktur.

Enligt FI:s bedömning ryms egenskapen/skyddsmålet autenticitet redan inom begreppet riktighet, varför en sådan ändring inte innebär någon förändring i sak.

Säkerhetsprinciper
FI föreslår att benämningen av begreppet *säkerhetsprinciper* ändras till *säkerhetsregler* och att definitionen av begreppet utvidgas till:

”… styrande dokument, till exempel föreskrifter och interna riktlinjer genom vilka en leverantör styr sitt säkerhetsarbete.”

Av författningskommentaren (s. 288) till 7 § lagen framgår det att ”uppräkningen av styrande dokument är inte uttömmande men visar på att det ska vara *en viss nivå* [FI:s kursivering] på dokumenten”. FI uppfattar att det är utredningens avsikt att definitionen ska förstås såsom dokument som är centrala och övergripande till sin karaktär och/eller styrdokument som är beslutade högt upp i en leverantörs beslutshierarki.

Den indikerade inriktningen på begreppet *säkerhetsprinciper* innebörd riskerar emellertid enligt FI medföra att mycket fokus läggs på de styrdokument som har det som i författningskommentaren benämns *en viss nivå*. En mer öppen utformning är enligt FI att föredra då det tydligare öppnar upp för ett riskbaserat angreppsätt där även en leverantörs styrande dokument för

exempelvis hantering av brandväggar eller backup och andra reservlösningar inkluderas.

Enligt FI bör det centrala i begreppet vara att dokumenten är formellt fastställda. FI har i direktivet inte kunnat utläsa någon begränsning av begreppet säkerhetsprinciper (eng. security policies) som visar att det nödvändigtvis endast är dokument med *en viss nivå* som avses.

Utredningens tolkning är visserligen rimlig utifrån den svenska språkversionens användning av *säkerhetsprinciper* som motsvarighet till det engelska begreppet *security policies*. Den svenska versionen framstår dock inte som helt tillfredställande korrekt på denna punkt. Av den engelska termen *policy,* såsom den används på engelska avseende it- och informationssäkerhetsfrågor, följer inte automatiskt att det är styrdokument på *en viss nivå* som avses. Detta i kontrast mot hur begreppet policy ofta används i Sverige - informationssäkerhetspolicy, kontinuitetspolicy etc. Enligt FI:s uppfattning bör *säkerhetsprinciper* i detta fall tolkas som att det har en vidare betydelse än den som utredningen föreslagit.

5.4 Den nya lagens tillämpningsområde

Uttryckliga undantag m.m.

Den nya lagens bestämmelser om krav på leverantörerna ska inte tillämpas om det i annan lag finns bestämmelser som minst motsvarar bestämmelserna i den nya lagen

FI anser att det är viktigt att under den fortsatta beredningen av utredningens förslag det klargörs vad som avses med begreppet *annan författning* i 5 § andra stycket lagen.

De relevanta författningarna för banksektorn består huvudsakligen av myndighetsföreskrifter. Dessa föreskrifterna utvecklar allmänt hållna lagbestämmelser om att kreditinstituten ska hantera sina operativa risker.

Av 5 § andra stycket i den föreslagna lagen framgår det att om sådana bestämmelser som framgår av första stycket finns i *annan författning* ska de bestämmelserna tillämpas om kraven minst motsvarar verkan av skyldigheterna i den föreslagna lagen. FI instämmer i att så bör vara fallet. I författningskommentaren för bestämmelserna i 5 § andra stycket (s. 286) samt i utredningens resonemang om den nya lagens tillämpningsområde (s. 97-98) används emellertid endast det snävare begreppet *nationell lag*.

7.3.1 Säkerhetsåtgärder

Tekniska och organisatoriska åtgärder
Genom harmonisering på EU-rättslig nivå har filialer till kreditinstitut med säte i ett annat EES-land rätt att bedriva verksamhet i Sverige direkt utifrån tillståndet i sitt hemland. Exempelvis bedriver Danske Bank (Sveriges femte största bank) och DNB huvudsakligen sin svenska verksamhet i denna form. FI:s befintliga föreskrifter och allmänna råd om informationssäkerhet gäller alltså idag inte för denna verksamhet. Den omfattas istället av motsvarande sektorreglering i hemlandet och den tillsyn som FI genomför på informationssäkerhetsområdet idag sker i nära samarbete med tillsynsmyndigheten i hemlandet.

Sådan verksamhet som bedrivs i Sverige från en filial omfattas emellertid inte av undantagen om avvikande bestämmelser i annan författning i 5 § i den föreslagna lagen. I det fall att en sådan verksamhet omfattas av kraven som en leverantör av banktjänster enligt förslagen skulle således MSB:s kommande föreskrifter om systematiskt arbete med informationssäkerhet bli tillämpliga. Detta får till följd att FI:s tillsyn avsektorn för banktjänster avseende leverantörernas arbete med informationssäkerhet skulle ske utifrån två parallella och kanske olika utformade regelverk.

FI anser följaktligen att det är viktigt att de nya föreskrifter som MSB föreslås ta fram om systematiskt arbete med informationssäkerhet blir principbaserade till sin utformning snarare än detaljreglerande. Detta så att förutsättningar skapas för tillsynsmyndigheter med befintlig sektorreglering för informationssäkerhet att i möjligaste mån kunna bygga vidare på dess struktur och redan etablerad tillsyns- och branschpraxis.

Flertalet av leverantörerna inom de sektorer som FI föreslås bli tillsynsmyndighet för omfattas redan idag av Finansinspektionens föreskrifter och allmänna råd (FFFS 2014:5) om informationssäkerhet, it-verksamhet och insättningssystem. Dessa föreskrifter har sin utgångspunkt i den slags godkänd nationell och internationell standard som utredningen (s. 133) föreslår att MSB bör utgå från i sitt föreskriftsarbete.

7.3.2 Incidentrapportering

En bristande harmonisering av de föreslagna kraven och närliggande krav om incidentrapportering kan enligt FI komma att medföra en risk för att vissa leverantörer väljer att inte rapportera inträffade incidenter och att lagstiftarens syfte därmed undermineras.

FI vill i sammanhanget uppmärksamma regeringen på att företagen inom sektorerna bankverksamhet och finansmarknadsinfrastuktur redan idag omfattas av krav om att rapportera väsentliga händelser, inklusive sådana som avser informationssäkerhet, till FI. Genomförandet av det andra

betaltjänstdirektivet (PSD 2) kommer även att medföra särskilda krav på att kreditinstitut rapporterar väsentliga händelser relaterade till betaltjänster till FI. Kreditinstituten kommer likt leverantörer inom övriga sektorer även att omfattas av krav på incidentrapportering i personuppgiftsförordningen och viss verksamhet kan även komma att omfattas av rapportering enligt förslaget om en ny säkerhetsskyddslag.

Ett företag inom banksektorn som drabbas av en allvarlig säkerhetsincident som påverkar flera delar av företagets verksamhet kan följaktligen i vissa fall bli skyldigt att separat rapportera om incidenten till såväl FI, MSB, Datainspektionen samt till den myndighet som utses som säkerhetsskyddstödjande myndighet avseende föreslaget till ny säkerhetsskyddslag. Det är högst angeläget att de krav som ställs från olika håll samordnas, inte minst när det gäller incidentrapporteringens innehåll och responstid.

8.5.3 Tillsyn m.m.

FI föreslår att ordet *dokumenterade* i 26 § första stycket första punkten i lagen stryks eftersom, det av definitionen till begreppet säkerhetsprinciper framgår att det rör sig om dokument. Detsamma gäller för 27 § i lagen.

I 26 § första stycket andra punkten i lagen föreslår FI att begreppet *auktoriserad revisor* byts ut mot begreppet *kvalificerad oberoende granskare.* I den engelska versionen av direktivet används begreppet *qualified auditor.* Detta begrepp motsvaras enligt FI inte av den i Sverige förekommande titeln *auktoriserad revisor*. Någon liknande översättning går inte heller att utläsa av exempelvis den danska eller tyska versionen av direktivet.

Begreppet *revisor* är inom sektorerna för bankverksamhet och finansmarknadsinfrastruktur i hög utsträckning förknippat med den funktion som utför den årliga externa revisionen av ett företags finansiella rapportering respektive den oberoende internrevisionsfunktion som finansiella företag är skyldiga att ha. Vidare har kombinationen *kvalificerad revisor* redan en etablerad och i sammanhanget problematiskt innebörd avseende den externa revisionen av företags finansiella rapportering.

Enligt FI är det centralt att en säkerhetsgranskning utförs av någon som är oberoende från den verksamhet som granskas. För företag inom sektorerna bankverksamhet och finansmarknadsinfrastruktur utförs sådan granskning normalt av den oberoende funktion för internrevision.

Då det enligt FI inte är uppenbart att samtliga leverantörer som omfattas av lagen är skyldliga att ha en oberoende internrevisionsfunktion föreslår FI att begreppet *kvalificerad oberoende granskare* används. Detta för att särskilt betona att säkerhetsgranskningen behöver utföras av en oberoende funktion för att de ska kunna anses ha någon slags bevisvärde i ett tillsynssammanhang.

Konsekvenser

Förslagen innebär utökade uppgifter för FI. Omfattningen på de tillkommande uppgifterna beror på antalet identifierade leverantörer inom sektorerna bankverksamhet och finansmarknadsinfrastruktur, behovet av att ta fram nya eller uppdaterade föreskrifter, samt på hur tillsynen slutligen utformas. Med reservation för dessa osäkerheter har FI begärt ett löpande tillskott om 20 miljoner kronor för ändamålet i myndighetens budgetunderlag. För att de uppgifter som följer av den nya lagstiftningen inte ska tränga ut andra delar av FI:s verksamhet är det av stor vikt att anslaget utökas i proportion med förväntningarna på ökad tillsyn.

Beslut i detta ärende har tagits av generaldirektören Erik Thedéen med seniora riskexperten Anders Lindgren som föredragande.

FINANSINSPEKTIONEN

Erik Thedéen
Generaldirektör

Anders Lindgren
Senior riskexpert