

Remissvar



Finansdepartementet
fi.remissvar@regeringskansliet.se

Finansinspektionen
Box 7821
103 97 Stockholm
Tel +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

2024-04-12

FI dnr 24-2093
(Anges alltid vid svar)

Digital operativ motståndskraft för finanssektorn

Ert dnr: Fi2024/00073

Sammanfattning

Finansinspektionen tillstyrker i stora delar de förslag som lämnas i promemorian, men efterfrågar i några avseenden ett antal förtydliganden. Finansinspektionen delar dock inte bedömningen i promemorian att effekten på kostnaderna för Finansinspektionen till följd av Dora-förordningen är begränsade, utan anser tvärtom att de är omfattande.

Flera av de finansiella entiteter som omfattas av Dora-förordningen¹ bedriver säkerhetskänslig verksamhet, och omfattas i den delen av säkerhetskyddslagen (2018:585). Eftersom EU inte har kompetens inom området nationell säkerhet, efterfrågar Finansinspektionen förtydliganden när det gäller hur de båda författningarna förhåller sig till varandra.

Såvitt gäller ansvaret för de hotbildsstyrda penetrationstesterna anser Finansinspektionen att det behöver tydliggöras vilka beslut enligt Dora-förordningen som ska fattas av Riksbanken.

När det gäller tillsyn och ingripanden bör vissa av de föreslagna bestämmelserna förtydligas eller anpassas till hur motsvarande reglering är ut-

¹ Europaparlamentet och Rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011

formad i olika rörelselagar på det finansiella området, för att det inte ska bli någon skillnad mellan de finansiella entiteter som lyder under en av de rörelselagarna och de som inte gör det.

Finansinspektionen utvecklar nedan närmare sina synpunkter på promemorian.

Dora-förordningens förhållande till regler om nationell säkerhet

I princip alla företag som står under Finansinspektionens (FI) tillsyn omfattas av Dora-förordningen. Vissa av dessa företag omfattas även av säkerhetsskyddslagen (2018:585), nedan SSL.

I artikel 1.3 i Dora-förordningen anges att förordningen inte påverkar medlemsstaternas ansvar vad gäller statliga funktioner inom bland annat området nationell säkerhet. I promemorian förtydligas att detta för svensk del i första hand berör SSL, men vad det innebär för de finansiella företag som bedriver säkerhetskänslig verksamhet förklaras inte. Inte heller i övrigt ger promemorian någon ledning i frågan om hur de två författningarna förhåller sig till varandra. Enligt FI:s mening bör regeringen i det fortsatta lagstiftningsarbetet tydliggöra detta. Annars riskerar regleringen att få en sådan utformning att säkerhetsskyddsklassificerade uppgifter kan hanteras felaktigt eller hamna i orätta händer.

Det har satts i fråga om artikel 1.3 i Dora-förordningen innebär att förordningen över huvud taget inte ska tillämpas på säkerhetskänslig verksamhet, det vill säga att de företag som bedriver säkerhetskänslig verksamhet ska tillämpa Dora-förordningen på de delar av verksamheten som inte är säkerhetskänsliga men inte på den säkerhetskänsliga verksamheten. En sådan tolkning framstår dock som mindre ändamålsenlig då den skulle medföra att Dora-förordningens krav inte kommer att gälla för de verksamheter som är mest skyddsvärda och där kraven bäst behövs. Tolkningen skulle dessutom medföra svårigheter vid genomförandet av den hotbildsstyrda penetrationstestningen, eftersom testningen inte alltid kan avgränsas så att den enbart träffar de delar som inte är säkerhetskänsliga. Därutöver skulle det inte finnas författningsstöd för att genomföra hotbildsstyrda penetrations-tester på säkerhetskänslig verksamhet.

I det fall regeringen är av uppfattningen att förordningen inte kan tillämpas på verksamhet som omfattas av SSL skulle det därför behöva övervägas att i

den nu aktuella kompletteringslagen (KomplL) utsträcka Dora-förordningens tillämpningsområde – eller i vart fall kraven på hotbildsstyrda penetrationstester – till att omfatta även säkerhetskänslig verksamhet.

En annan och mer rimlig tolkning av artikel 1.3 i Dora-förordningen är att förordningen ska tillämpas även på säkerhetskänslig verksamhet, men att avsteg från förordningens krav ska eller kan göras när det krävs på grund av säkerhetsskyddslagstiftningen.

FI förordar en sådan tolkning, men även i detta fall behövs ett antal ställningstaganden i det fortsatta lagstiftningsarbetet för att säkerställa en ändamålsenlig reglering.

För det första behövs sådana ställningstaganden i fråga om kravet på hotbildsstyrd penetrationstestning. När penetrationstestningen omfattar säkerhetskänslig verksamhet exponeras den säkerhetskänsliga verksamheten för såväl Riksbanken som för de leverantörer som ska genomföra testningen. Utgångspunkten är därför att företagen i förekommande fall behöver teckna säkerhetsskyddsavtal enligt 4 kap. 1 § SSL inför förfarandet (prop. 2020/21:194 s. 30 f.). Dessförinnan behöver företagen göra en särskild säkerhetsskyddsbedömning och lämplighetsprövning samt i vissa fall samråda med tillsynsmyndigheten, 4 kap. 7–9 §§ SSL.

Något krav på säkerhetsskyddsavtal bör rimligen inte uppställas i förhållande till Riksbanken. Det finns enligt FI:s uppfattning goda skäl för att jämställa Riksbankens roll i penetrationstesterna med en tillsynsmyndighets (jfr. prop 2020/21:194, s. 32 och 128). FI anser att detta bör komma till klart uttryck i det fortsatta lagstiftningsarbetet, eftersom det rör sig om ett avsteg från utgångspunkten att det är risken för exponering snarare än anledningen till exponeringen som är avgörande för om förfarandet omfattas av krav på säkerhetsskyddsavtal.

Det är FI:s uppfattning att företagen i förhållande till leverantörerna ska följa kraven på säkerhetsskyddsavtal, särskild säkerhetsskyddsbedömning och lämplighetsprövning samt samråd. Bedömningen, prövningen och samrådet bör emellertid inte ta sikte på frågan om förfarandet – testningen – ska genomföras eller inte, eftersom FI i dessa fall redan har beslutat att så ska ske, utan vara begränsad till formerna för genomförandet. FI anser att även detta bör förtydligas under den fortsatta beredningen.

För det andra behövs ställningstaganden i fråga om uppgiftsskyldighet i förhållande till tystnadsplikt. I 8 kap. 1 och 2 §§ SSL finns bestämmelser om tystnadsplikt, samtidigt som det i Dora-förordningen finns en uppgiftsskyldighet för finansiella entiteter gentemot tillsynsmyndigheterna. För säkerhetskänslig verksamhet är det inte uteslutet att dessa bestämmelser kan överlappa varandra, det vill säga det kan finnas en uppgiftsskyldighet enligt Dora-förordningen samtidigt som det föreligger en tystnadsplikt enligt SSL.

Enligt skäl 17 till Dora-förordningen omfattar Dora-förordningen inte tillhandahållande av information om tillhandahållandet står i strid med skyddet av den nationella säkerheten. Av detta borde enligt FI:s uppfattning följa att uppgiftsskyldigheten enligt Dora-förordningen inte omfattar säkerhetskvalificerade uppgifter enligt SSL eller, med andra ord, att tystnadsplikten enligt SSL har företräde framför uppgiftsskyldigheten enligt Dora-förordningen. Detta bör förtydligas av lagstiftaren och en bestämmelse med den innebörden bör införas i KomplL, förslagsvis enligt följande.

Skyldigheten att lämna uppgifter enligt Dora-förordningen omfattar inte uppgifter som är säkerhetskvalificerade enligt säkerhetskvalificeringslagen (2018:585).

Om regeringen anser att ett förbud mot att lämna säkerhetskvalificerade uppgifter redan följer av artikel 1.3 i Dora-förordningen, är det FI:s uppfattning att den föreslagna bestämmelsen ändå bör införas i KomplL, men då utformad som en upplysningsbestämmelse.

Möjligheten att bedriva en effektiv tillsyn för FI påverkas emellertid om myndigheten inte får ta del av all relevant information. Det är därför nödvändigt att skyldigheten att lämna sådana uppgifter som avses i Dora-förordningen till FI har företräde framför tystnadsplikten i SSL och att ett sådant uppgiftslämnande inte ska ses som ett obehörigt röjande enligt 8 kap. SSL. Detsamma bör gälla för uppgifter som lämnas till Riksbanken och berörda leverantörer inom ramen för förfarandet med de hotbildsstyrda penetrationstesterna. I KomplL bör det därför införas en skyldighet att lämna sådana uppgifter som avses i Dora-förordningen till FI, Riksbanken och berörda leverantörer, även om uppgifterna är säkerhetskvalificerade enligt SSL. Denna uppgiftsskyldighet skulle komplettera den uppgiftsskyldighet som följer av Dora-förordningen, och följa helt av nationell rätt.

För det tredje behövs ställningstaganden i fråga om incidentrapportering. I såväl Dora-förordningen som säkerhetsskyddsförordningen (2021:955), nedan SSF, finns bestämmelser om incidentrapportering. Incidenter i säkerhetskänslig verksamhet ska således rapporteras enligt såväl Dora-förordningen som SSF.

Trots vad som sagts ovan om att uppgiftsskyldigheten enligt Dora-förordningen i förhållande till FI bör ha företräde framför tystnadsplikten i SSL, är det av största vikt att incidentrapporteringen enligt Dora-förordningen inte innehåller säkerhetsskyddsklassificerade uppgifter. Det finns nämligen en skyldighet för FI att vidarerapportera incidenter till bland annat de europeiska tillsynsmyndigheterna och i vissa fall till ECB. Därtill kommer att FI:s system för mottagandet av rapporterna är inte anpassat för att hantera säkerhetsskyddsklassificerad information. Ytterst kan det därför uppkomma ett hot mot nationell säkerhet om säkerhetsskyddsklassificerade uppgifter tillåts ingå i incidentrapporteringen enligt Dora-förordningen. FI föreslår mot den bakgrunden att det i KomplL införs en bestämmelse med innebörd att incidentrapporteringen enligt Dora-förordningen inte får omfatta säkerhetsskyddsklassificerade uppgifter.

Som nämnts ovan berörs ett flertal företag av såväl Dora-förordningen som SSL. Det är FI:s uppfattning att det inte bör överlämnas till varje berört företag att själv ta ställning till hur artikel 1.3 i Dora-förordningen ska förstås och inte heller att bedöma vilka eventuella avsteg från Dora-förordningens krav som ska göras. Förhållandet mellan de två lagstiftningarna behöver därför förtydligas från lagstiftarens sida. En avsaknad av ett sådant förtydligande riskerar att leda till att företagen tolkar författningarna olika och att effektiv tillsyn inte kan bedrivas, eftersom det i brist på ledning finns utrymme för olika tolkningar. Den allvarligaste konsekvensen är emellertid risken för att säkerhetsskyddsklassificerade uppgifter hanteras felaktigt eller hamnar i orätta händer, vilket ytterst är ett hot mot Sveriges säkerhet.

FI ser mot den bakgrunden ett behov av att regeringen i det fortsatta lagstiftningsarbetet tydliggör förhållandet mellan de båda regelverken. Dels i frågan om Dora-förordningen ska tillämpas av verksamhetsutövare enligt säkerhetsskyddslagstiftningen, och då även på de säkerhetskänsliga delarna av deras verksamheter, dels om avsteg från Dora-förordningen ska göras med stöd av förordningens artikel 1.3 när förordningens krav står i strid med säkerhetsskyddslagstiftningen, och om det i sådana fall är upp till varje enskild aktör att själv bedöma om sådana avsteg ska göras.

Hotbildsstyrda penetrationstester (avsnitt 6)

FI tillstyrker att Riksbanken får ansvaret för att övervaka och samordna de hotbildsstyrda penetrationstesterna, efter att FI har fattat beslut om vilka enheter som ska genomgå sådana tester och hur ofta. FI anser däremot att 2 kap. 1 och 2 §§ KomplL är otydliga när det gäller vilka delar av artikel 26 i Dora-förordningen som FI respektive Riksbanken ansvarar för. Det bör därför tydliggöras i de nämnda bestämmelserna enligt vilka punkter i artikeln som FI respektive Riksbanken ska fatta beslut.

Både artikel 26 och 27 anger, i olika delar, vilka beslut och andra godkännanden som ska fattas av *behörig myndighet* (dvs. FI). Eftersom det i Dora-förordningen finns en utpekad myndighet som, om inte annat beslutas på nationell nivå, ska ha hela ansvaret för de hotbildsstyrda penetrations-testerna, är det särskilt angeläget att lagstiftaren är tydlig i fråga om när det är som en annan myndighet (i det här fallet Riksbanken) får ansvar för att fatta vissa beslut. Det är också viktigt att begreppet *behörig myndighet* används konsekvent och i enlighet med förordningen och de tekniska standarderna. För att undvika missförstånd, kan begreppet *TLPT²-myndighet* användas för Riksbanken. Det begreppet används i [förslaget till] regulatorisk teknisk standard i den här delen och kan vara ett lämpligt sätt att tydliggöra att ansvaret ligger på olika myndigheter. De uppgifter som anges i den regulatoriska tekniska standarden är sådana som bör ligga på Riksbanken att fatta beslut om, givet att FI har förstått uppdelningen av ansvar mellan myndigheterna på ett korrekt sätt. Även detta kan vara lämpligt att förtydliga i det fortsatta lagstiftningsarbetet.

Beslut om att en finansiell entitet ska genomföra hotbildsstyrda penetrationstester är ett beslut av sådant slag att det bör kunna gälla omedelbart om FI finner att det finns skäl till det. Ett tillägg bör därför göras i 5 kap. 3 § KomplL av den innebörden att även sådana beslut omfattas av bestämmelsen. En överklagandeprocess kan ta flera år, vilket skulle kunna leda till stor skada om en finansiell entitet genom att överklaga Finansinspektionens beslut kan förskjuta testningen under lång tid. Om ett beslut gäller omedelbart, har den finansiella entiteten alltid möjlighet att begära inhibition vid ett eventuellt överklagande.

FI bedömer att det är av särskild betydelse att hotbildsstyrda penetrations-tester kan genomföras utan fördröjning och med det intervall som FI be-

² TLPT är en förkortning av Threat-Led Penetration Testing.

slutar om, eftersom det annars riskerar att sårbarheter hos de finansiella entiteterna inte upptäcks i tid. Den möjlighet som FI har att med stöd av 35 § förvaltningslagen (2017:900) bestämma att ett beslut ska gälla omedelbart, bedöms inte vara tillräcklig. De kriterier som gäller enligt den bestämmelsen, till exempel på att ett väsentligt allmänt eller enskilt intresse kräver omedelbar verkställighet, är utformade med andra situationer i åtanke än de som är aktuella vid hotbildsstyrda penetrationstester. Ett beslut om att ett företag ska genomgå hotbildsstyrda penetrationstester är snarare att jämföras med ett beslut om föreläggande, en kategori beslut för vilken FI föreslås få möjlighet att bestämma om omedelbar verkställighet.

Tillsyn och ingripanden (avsnitt 7 och 8)

Omfattningen av FI:s tillsyn

I ett flertal artiklar i Dora-förordningen ges kommissionen befogenhet att anta tekniska standarder, i vilka förordningens krav närmare specificeras. De tekniska standarderna är, precis som förordningen, direkt tillämpliga. Eftersom det är i de tekniska standarderna som de närmare kraven på de finansiella entiteterna anges, behöver det vara tydligt att även efterlevnaden av dessa författningar är något som FI utövar tillsyn över. Ett tillägg bör därför göras i 3 kap. 1 § och i 4 kap. 1 och 2 §§ KomplL att även efterlevnaden av ”andra författningar som reglerar verksamheten” ska omfattas av FI:s tillsynsansvar. Detta är i likhet med hur det uttrycks i andra lagar på finansmarknadsområdet.

Platsundersökning

Av 3 kap. 3 § förslag till KomplL framgår att FI får genomföra undersökningar *i verksamhetslokalerna hos en finansiell entitet*. I författningskommentaren anges att bestämmelsen är utformad efter förebild av bland annat 23 kap. 4 § lagen (2007:528) om värdepappersmarknaden (LV).

Av 23 kap. 4 § LV framgår emellertid att FI får göra undersökningar *hos ett värdepappersinstitut* (eller annan aktör som omfattas av bestämmelsen). Motsvarande lydelse för kreditinstitut finns i 13 kap. 4 § lagen (2004:297) om bank- och finansieringsrörelse, nedan LBF. I båda dessa fall anges dessutom att undersökning får ske hos ett företag som fått i uppdrag av ett värdepappersinstitut eller ett kreditinstitut att utföra visst arbete eller vissa funktioner.

FI anser att begreppet *i verksamhetslokalerna* i den föreslagna lydelsen av 3 kap. 3 § KomplL, utgör en begränsning och innebär ett snävare tillämpningsområde än vad gäller i vissa rörelselagar. Lydelsen av 3 kap. 3 § KomplL bör därför justeras dels genom att begreppet ”i verksamhetslokalerna” stryks, dels genom att FI även ges möjlighet att genomföra undersökningar hos en uppdragstagare på samma sätt som för värdepappersinstitut och kreditinstitut. Justeringen behöver ske i KomplL för att på så sätt ge samma förutsättningar för tillsyn enligt Dora-förordningen för alla finansiella entiteter, oavsett vilken formulering som finns i olika rörelselagar på det finansiella området.

Svenska skeppshypotekskassan

FI ska ingripa mot en fysisk företrädare för Svenska skeppshypotekskassan genom beslut om förbud att utöva ledningsuppdrag, beslut om sanktionsavgift eller en kombination av de två enligt 4 kap. 9 § KomplL. Däremot ges FI inte möjlighet att besluta om sanktionsavgift mot den juridiska personen Svenska skeppshypotekskassan enligt 4 kap. 7 §, eftersom kassan inte omfattas av 4 eller 5 §§ som bestämmelsen hänvisar till.

Att det vid en juridisk persons överträdelse är möjligt att ingripa med sanktionsavgift mot en fysisk företrädare men inte mot den juridiska personen avviker från annan lagstiftning på finansmarknadsområdet. Se t.ex. 15 kap. 7 § LBF.

För FI är det inte klart om det finns några sakliga skäl för en sådan ordning. På s. 84 i Remisspromemorian anges att ingripandebefogenheterna som utgångspunkt bör vara desamma i kompletteringslagen som i de olika rörelselagarna. Varken lagen (1980:1097) om Svenska skeppshypotekskassan, lagen (2014:968) om särskild tillsyn över kreditinstitut och värdepappersbolag eller lagen (2014:966) om kapitalbuffertar innehåller någon möjlighet att besluta om sanktionsavgift mot vare sig kassan eller dess fysiska företrädare, vilket talar för att möjligheten att ingripa mot Svenska skeppshypotekskassans fysiska företrädare bör tas bort.

Ingripanden mot finansiella entiteter med dubbla tillstånd

När det gäller finansiella entiteter med dubbla tillstånd, till exempel ett kreditinstitut som även har tillstånd att bedriva gräsrotsfinansieringstjänster eller ett värdepappersinstitut som har tillstånd att bedriva kryptotillgångstjänster, kan det bli aktuellt för FI att ingripa enligt både KomplL och rörelselag. Det bör förtydligas i det fortsatta lagstiftningsarbetet hur

ingripandebestämmelserna i KomplL respektive rörelselagarna förhåller sig till varandra. I ett sådant fall bör FI få göra en självständig prövning av vilket förfarande som framstår som mest effektivt i den aktuella situationen. Detta ligger i linje med hur regeringen i vissa tidigare lagstiftningsärenden har resonerat när FI har haft möjlighet att ingripa enligt flera regelverk (se prop. 2016/17:22 s. 205).

Övrigt

Även leverantörer av kryptotillgångstjänster bör omfattas av 4 kap. 15 § i KomplL, eftersom sådana finansiella entiteter omfattas av motsvarande försiktighetskrav³ som leverantörer av gräsrotsfinansieringstjänster. Ett tillägg om detta bör därför göras i den bestämmelsen. När det gäller sista meningen i 4 kap. 15 § KomplL bör det förtydligas i promemorian vilka andra bestämmelser om soliditet och likviditet som avses.

Konsekvensanalys (avsnitt 19)

FI delar inte bedömningen i promemorian att effekten på FI:s kostnader för FI till följd av Dora-förordningen är begränsade, utan anser att de är omfattande. FI bedömer att det kommer att behövas betydande informationsinsatser och en betydande ökning av tillsynen, eftersom Dora-förordningen omfattar ett stort antal institut med skärpta regler jämfört med de regler och riktlinjer som gäller idag. FI kommer även att behöva samla in, upprätthålla och vidarerapportera informationsregister om IKT-tredjepartsleverantörer samt delta i arbetet med de gemensamma undersökningsgrupperna (JET), vilket kommer att kräva betydande resurser. FI kommer dessutom att behöva ta fram systemstöd för incidentrapportering och informationsregister. Att ta fram systemstöd innebär inte bara initiala kostnader för att ta fram systemet, utan även löpande kostnader för underhåll.

FI har äskat ytterligare medel för de omfattande merkostnader som Dora-förordningen innebär för myndigheten.

Ändringar i olika rörelselagar

I förslagen till 2 kap. 17 § lagen (2004:46) om värdepappersfonder (LVF) och 8 kap. 2 § lagen (2013:561) om förvaltare av alternativa investerings-

³ Artikel 11 i gräsrotsförordningen (EU) 2020/1503 jämfört med art 67 i MiCA-förordningen (EU) 2023/1114

fonder (LAIF) bör det förtydligas i det fortsatta lagstiftningsarbetet att fondbolag och AIF-förvaltares rutiner för drift och förvaltning av sina informationssystem även omfattar *nätverkssystem*. I artikel 1 och 3 i ändringsdirektivet anges att såväl fondbolag som AIF-förvaltare ska ha nätverks- och informationssystem som inrättas och förvaltas i enlighet med EU-förordningen. I förslagen till 2 kap. 17 § LVF och 8 kap. 2 § LAIF anges endast att fondbolag och AIF-förvaltares rutiner för drift och förvaltning av informationssystem ska uppfylla kraven i EU-förordningen. I förslagen till 6 kap. 2 § LBF, 10 kap. 3 § försäkringsrörelselagen (2010:2043) och 9 kap. 2 § lagen (2019:742) om tjänstepensionsföretag anges att dessa aktörer ska ha nätverks- och informationssystem som uppfyller kraven i EU-förordningen. Med hänsyn till att samtliga aktörer som omfattas av EU-förordningen ska ha nätverks- och informationssystem som uppfyller kraven i EU-förordningen, bör det i det fortsatta lagstiftningsarbetet förtydligas att samma krav gäller även för fondbolag och AIF-förvaltare.

I förslaget till lag om ändring i lagen (2010:751) om betaltjänster (LBT) föreslås ett nytt sista stycke i 5 kap. 3 §. I promemorian anges att artikel 96.7 i betaltjänstdirektivet, i lydelsen enligt artikel 7.5 i ändringsdirektivet genomförs genom denna ändring. Av artikel 26 i Dora-förordningen framgår att de krav som fastställs i Dora-förordningen om hantering av, klassificering av och rapportering om IKT-relaterade incidenter även ska tillämpas på betalningsrelaterade operativa incidenter eller säkerhetsincidenter och på allvariga betalningsrelaterade operativa incidenter eller säkerhetsincidenter, om de gäller kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar. Skäl 23 respektive skäl 54 till Dora-förordningen förtydligar att detta gäller oavsett om sådana incidenter är IKT-relaterade eller inte. I och med att den rapporteringsskyldighet som tidigare framgick av betaltjänstdirektivet nu omfattas i sin helhet av rapporteringsskyldigheten enligt Dora för kreditinstitut, betalningsinstitut, leverantörer av kontoinformationstjänster och institut för elektroniska pengar, bör det tydliggöras i det fortsatta lagstiftningsarbetet vilka institutstyper som återstår som rapporteringsskyldiga enligt 3 § första och andra stycket LBT.

I förslaget till 14 kap. 1 b § LAIF anges att FI ska ingripa mot AIF-förvaltarens *ledning* eller styrelse eller förvaltarens verkställande direktör eller motsvarande, eller ersättare för någon av dem, om förvaltaren har åsidosatt sina skyldigheter enligt EU-förordningen. I 12 kap. 1 a § LVF, 15 kap. 1 a § LBF, 25 kap. 1 a, i och j §§ LV och 8 kap. 8 b § LBT anges endast att FI ska

ingripa mot någon som ingår i ett företags styrelse eller är dess verkställande direktör, eller ersättare för någon av dem. Vidare anges i promemorian att ingripanden bör kunna ske mot den som ingår i styrelsen för en finansiell entitet eller är dess verkställande direktör, eller ersättare för någon av dem. Det bör tydliggöras i det fortsatta lagstiftningsarbetet vilka andra än styrelse och verkställande direktör som kan ingå i ledningen och varför FI just kan ingripa mot en AIF-förvaltares ledning. Att FI skulle kunna ingripa mot en AIF-förvaltares ledning utgör en stor skillnad jämfört med vilka ingripandemöjligheter som finns i andra rörelselagar på det finansiella området.

Övrigt

Enligt artikel 2 a) i Dora-förordningen omfattas "kreditinstitut" av förordningens tillämpningsområde. Kreditinstitut definieras som "ett företag vars verksamhet är att ta emot insättningar eller andra återbetalbara medel från allmänheten och att bevilja krediter för egen räkning". Bostadskreditinstitut och konsumentkreditinstitut, som inte får finansieras av medel från allmänheten, omfattas därmed inte av Dora-förordningen. I avsnitt 4.3 i promemorian (s. 57) behandlas flertalet institut av varierande storlek som omfattas av eller undantas från Dora-förordningens tillämpningsområde. Finansinspektionen efterfrågar ett förtydligande i promemorian avseende institutstyperna bostadskreditinstitut och konsumentkreditinstitut, för att det inte ska råda några tveksamheter om de omfattas eller inte av förordningen.

FI efterfrågar ett bemyndigande från regeringen för att kunna föreskriva om vilket format som inrapportering enligt Dora-förordningen ska ske och vid vilken tidpunkt den ska lämnas. Rapporteringen behöver ske i ett format som kan läsas in i FI:s rapporteringssystem, för att sedan kunna användas både för analys och för vidare rapportering till de europeiska tillsynsmyndigheterna.

FINANSINSPEKTIONEN

Daniel Barr
Generaldirektör

Agneta Blomquist
Rådgivare

I detta ärende har generaldirektören Daniel Barr beslutat. Rådgivaren Agneta Blomquist har varit föredragande. I den slutliga handläggningen har också chefsjuristen Eric Leijonram och enhetschefen Halszka Onoszko deltagit.

Kopia till anna.stenberg@regeringskansliet.se