RAPPORT

Handlingsplan om att stärka kontrollen över de finansiella företagens utlagda verksamhet

28 februari 2023

Dnr 22-18123

Innehåll

Finansinspektionen
Box 7821, 103 97 Stockholm
Besöksadress Brunnsgatan 3
Telefon +46 8 408 980 00
finansinspektionen@fi.se
www.fi.se

Förord

Finansinspektionen (FI) fick den 22 juni 2022 i uppdrag att ta fram en handlingsplan om att stärka kontrollen över de finansiella företagens utlagda verksamhet. I uppdraget ingick även att göra en analys av vilka regeländringar som behövs för att uppnå bättre kontroll över de finansiella företagens utlagda verksamhet. FI ska även lämna nödvändiga författningsförslag.

Vi redovisar resultatet av uppdraget i form av denna rapport.

Stockholm den 28 februari 2023

Susanna Grufman

Vikarierande generaldirektör

Sammanfattning

För att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet bedömer FI att det krävs en ökad tydlighet och enhetlighet i reglerna för finansiella företags utkontrakterade verksamhet. Skälen till denna bedömning är att kraven idag återspeglas i en mängd olika regler och att dessa i delar är allmänt hållna samt skiljer sig åt mellan olika sektorer av den svenska finansiella sektorn. FI bedömer att Europarlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (Dora-förordningen) kommer att innebära en tydlig kvalitetshöjning när det gäller de krav som ställs på de finansiella företagens kontroll över utkontrakterad verksamhet. De skärpta och enhetliga kraven ger också tillsynsmyndigheterna bättre verktyg.

FI noterar däremot att företag som bedriver clearing och avveckling av betalningar, såsom Bankgirot, inte kommer att omfattas av Dora-förordningens bestämmelser. Eftersom denna typ av företag har en central betydelse på finansmarknaden anser FI att de behöver omfattas av en reglering som åtminstone motsvarar de regler som framgår av Dora-förordningen. FI ser positivt på de förslag som lämnas i promemorian Ökad motståndskraft i betalningssystemet[1] för dessa typer av företag eftersom förslagen innebär att tydligare krav ställs på clearingbolagen och möjliggör en mer effektiv tillsyn från FI:s sida. Detta är angeläget i och med att det rör sig om systemviktig verksamhet och bolag som fyller en viktig samhällsfunktion.

FI bedömer att det inte är effektivt eller ändamålsenligt att i dagsläget lämna närmare förslag på förändringar i gällande svenska författningar för att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet. Även om Dora-förordningen är beslutad bedömer FI att förslag till regeländringar kräver en analys av de tekniska standarder[2] som ska utarbetas under förordningen och det är i dagsläget oklart vilket närmare innehåll dessa standarder kommer att få. Beträffande clearingbolag har det vidare föreslagits att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka åtgärder ett clearingbolag ska vidta för att uppfylla krav som är relevanta för clearingbolags utkontraktering. Om nya regler utformas idag finns det alltså en risk för att dessa kan komma att behöva justeras eller upphävas när andra redan pågående regelverksförändringar träder i kraft. Mot denna bakgrund framstår det inte som effektivt att lämna närmare förslag på författningsändringar i dagsläget och FI

[1] Promemoria Ökad motståndskraft i betalningssystemet, Fi2022/02529.
[2] Tekniska standarder tas fram av de europeiska tillsynsmyndigheterna och beslutas av EU-kommissionen i form av förordningar, och de gäller därmed som lagar.

bedömer att sådana ändringar bör övervägas först när de nu pågående lagstiftningsinitiativen på såväl nationell som EU-nivå har kommit längre.

I enlighet med uppdraget från regeringen har FI tagit fram en handlingsplan som avser att ytterligare förstärka arbetet med att stärka kontrollen över de finansiella företagens utlagda verksamhet. Handlingsplanen kompletterar FI:s befintliga arbete med utkontraktering och tredjepartsleverantörer.

Bakgrund

Finansiella företag väljer att i allt högre grad sluta avtal med en leverantör om att utföra (helt eller delvis) en process, tjänst eller annan aktivitet som företaget i annat fall själv skulle utföra (utkontraktering eller utlagd verksamhet). Inte sällan är det fråga om utkontraktering av kritisk verksamhet, särskilt inom it-området, vilket exempelvis omfattar drift eller utveckling av verksamhetskritiska system. Tjänsteleverantörerna – även kallade tredjepartsleverantörer – är ofta icke-finansiella företag som utför olika it-relaterade tjänster åt ett finansiellt företag. Detta kan vara både kvalitetssäkrande och mer resurseffektivt när företaget inte på egen hand kan skaffa sig tillräcklig kompetens för att hantera en viss verksamhet. Företaget måste dock alltid ha tillräcklig förmåga och kompetens att kunna styra över den utkontrakterade verksamheten. Ett företag har lika stort ansvar för att verksamhet som är utkontrakterad drivs enligt gällande reglering som det har över verksamhet som företaget självt svarar för.

Allvarliga it-incidenter i finansiella företag, inklusive incidenter kopplade till utkontrakterad verksamhet, kan ha en negativ inverkan på den finansiella stabiliteten oavsett incidentens typ och dess eventuella syfte. Såväl rena driftsstörningar som cyberangrepp kan påverka vitala funktioner i det finansiella systemet, såsom förmågan att göra betalningar. Under ogynnsamma förutsättningar kan skadan få bredare spridning och drabba samhället i stort. Saken förvärras av att incidenten kan undergräva allmänhetens förtroende för drabbade finansinstitut eller det finansiella systemet som helhet. I de fall det är fråga om utkontraktering av säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) kan it-incidenter vidare ha en negativ inverkan på Sveriges säkerhet. Ett viktigt verktyg i tillsynen över de finansiella företagen är därför tillsynen över utkontrakterade verksamheter hos tredjepartsleverantörer av information och kommunikationstekniktjänster (IKT-tjänster).

FI utövar idag tillsyn över hur företagen hanterar sina it-risker. I rapporten Förstärkt digital motståndskraft hos företag i den finansiella sektorn[3], som FI tog fram i maj 2022 på uppdrag av regeringen, konstaterade FI att det finns ett behov av en mer omfattande kontroll och bättre tillsyn över de finansiella företagens utlagda verksamhet. I rapporten beskrivs också olika tillvägagångssätt för att stärka denna tillsyn.

Sedan den rapporten publicerades har Dora-förordningen beslutats. Dora-förordningen ska tillämpas från den 17 januari 2025. Syftet med Dora-förordningen är att ge ett enhetligt regelverk för digital operativ motståndskraft, där hela den

[3] FI dnr 22-10015, publicerad den 9 maj 2022.

finansiella sektorn kan stå emot alla typer av IKT-relaterade störningar och hot för att förebygga och minska cyberhot. Förordningen är alltså tillämplig på de allra flesta typer av finansiella företag.

I denna rapport redogör FI för sin syn på behovet av regeländringar som i dagsläget behövs för att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet. Därutöver presenteras en handlingsplan för hur en mer omfattande kontroll och bättre tillsyn över finansiella företags utkontrakterade verksamhet ska åstadkommas.

Behov av regeländringar

I uppdraget ingår att göra en analys av vilka regeländringar som behövs för att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet. Vid analysen ska relevanta EU-rättsliga regelverk beaktas. I detta avsnitt redogörs för FI:s analys i detta avseende.

Nuvarande reglering

De flesta finansiella företag som står under FI:s tillsyn är redan i dag skyldiga att följa vissa krav när det utkontraktering av verksamhet. Företag som väljer att lägga ut verksamhet på andra aktörer behöver ha tillräcklig kunskap och utöva god styrning och kontroll över den utlagda verksamheten. När ett företag för första gången ansöker om verksamhetstillstånd kan FI avslå ansökan om det finns brister i företagets planerade utkontraktering av verksamhet.

För finansiella företag som har tillstånd och som därmed redan står under FI:s tillsyn gäller också oftast ett krav på att företaget ska anmäla uppdragsavtal till FI.[4] Anmälningsskyldigheten för uppdragsavtal är viktig eftersom FI får information om planerad eller genomförd utkontraktering. När det gäller sådana finansiella företag som bedriver säkerhetskänslig verksamhet kan FI, med stöd av säkerhetsskyddslagstiftningen, också motsätta sig att ett sådant företag ingår ett uppdragsavtal. Det förutsätter dock att såväl företaget som den aktuella verksamheten omfattas av denna lagstiftning.

Därutöver gäller att de finansiella företagen vid var tid behöver följa reglerna för utkontrakterad verksamhet och löpande hantera de risker som utkontrakteringen innebär. FI kan ingripa mot ett finansiellt företag om risker relaterade till utkontraktering inte hanteras och om utkontrakteringen av den anledningen inte lever upp till kraven som finns i rörelsereglerna.

Det finns alltså regler som tar sikte på finansiella företags hantering av utkontrakterad verksamhet och som ger FI verktyg att utöva tillsyn och ingripa mot de företag som är under tillsyn. Dessa regler återspeglas däremot för närvarande i en mängd olika svenska lagar och förordningar, gällande föreskrifter och allmänna råd från FI samt olika EU-regler. I stora delar är reglerna också allmänt hållna. Även om reglerna tar sikte på samma risker kan de vara uttryckta på olika sätt och dessutom skilja sig åt mellan olika sektorer av den svenska finansiella sektorn.[5] På EU-nivå har det exempelvis utfärdats separata riktlinjer av de europeiska

[4] Se bl.a. 6 kap. 7 § lagen (2004:297) om bank- och finansieringsrörelse, 8 kap. 22 § lagen (2007:528) om värdepappersmarknaden, 3 kap. 28 § lagen (2010:751) om betaltjänster och 10 kap. 19-22 §§ försäkringsrörelselagen (2010:2043).
[5] Se även de slutsatser som FI redovisade beträffande regelverken kring cyberrisker i promemorian Cyberhot och finansiell stabilitet – FI:s roll och uppgifter, FI Dnr 20-3685.

tillsynsmyndigheterna Europeiska bankmyndigheten (Eba), Europeiska försäkrings- och tjänstepensionsmyndigheten (Eiopa) och Europeiska värdepappers- och marknadsmyndigheten (Esma) som var för sig ställer upp olika rekommendationer kring utkontrakterad verksamhet.[6]

Förutom att skapa otydlighet för de aktörer som ska tillämpa reglerna kan dessa omständigheter försvåra FI:s möjligheter att bedriva en effektiv tillsyn över finansiella företags utlagda verksamhet. För att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet bedömer FI att det krävs en ökad tydlighet och enhetlighet i reglerna för finansiella företags utkontrakterade verksamhet.

Kommande reglering

FI konstaterar att det genom Dora-förordningen introduceras en helt ny tillsynsram för finansiella företags utläggning av IKT-tjänster och tredjepartsleverantörer av IKT-tjänster.[7] Ett av Dora-förordningens kärnområden är just utkontrakterad verksamhet. Den mest påtagliga förändringen avseende utkontrakterad verksamhet som Dora-förordningen medför är att kraven skärps på ett antal områden, bland genom att det som idag är riktlinjer blir rättsligt bindande krav men även att områden som inte regleras alls i dagsläget nu regleras. Kraven på avtal, utvärdering och uppföljning av tredjepartsleverantören blir tydligare. Det blir även enklare för de finansiella företagen att ställa krav på tredjepartsleverantörer när krav framgår av förordningen. De europiska tillsynsmyndigheterna har också fått i uppdrag att ta fram ett antal tekniska standarder för att ytterligare specificera detaljerna som framgår av artiklarna relaterade till tredjepartsrisk,[8] bland annat detaljerade bestämmelser för den strategi för IKT-tredjepartsrisk som finansiella företag är skyldiga att anta enligt artikel 28.2.

Förslagen till tekniska standarder ska överlämnas till Kommissionen senast den 17 januari 2024 och i vissa fall senast den 17 juni 2024. Det är i dagsläget inte klart hur de tekniska standarderna till Dora-förordningen kommer att utformas, men FI bedömer det som sannolikt att det kommer att finnas ett behov av nationella verkställighetsföreskrifter i vissa delar. Någon närmare redogörelse för detta behov lämnas inte inom ramen för denna rapport, men det skulle exempelvis kunna gälla formerna för viss inrapportering eller tidpunkt för vissa anmälningsskyldigheter enligt EU-förordningen.

[6] Se ESMA50-157-2403 Riktlinjer för utkontraktering till molntjänstleverantörer, EBA/GL/2019/02 Riktlinjer för utkontraktering och EIOPA-BoS-20-002 Riktlinjer om uppdragsavtal med molntjänstleverantörer.
[7] Skäl 20.
[8] Artikel 30.

FI bedömer att Dora-förordningen kommer att innebära en tydlig kvalitetshöjning när det gäller de krav som ställs på de finansiella företagens kontroll över utkontrakterad verksamhet. De skärpta och enhetliga kraven ger också tillsynsmyndigheterna bättre verktyg.

FI noterar däremot att företag som bedriver clearing och avveckling av betalningar, såsom Bankgirot, inte kommer att omfattas av EU-förordningens bestämmelser. Eftersom dessa typer företag har en central betydelse på finansmarknaden anser FI att de behöver omfattas av en reglering som åtminstone motsvarar de regler som framgår av Dora-förordningen.

FI konstaterar att det i promemorian Ökad motståndskraft i betalningssystemet[9] har lämnats förslag som innebär ökade krav på dessa typer av företag, bland annat gällande riskhantering och krav vid utkontraktering av verksamhet i dessa företag. Som framgår av FI:s remissvar[10] ser FI positivt på de förslag som lämnas i promemorian eftersom förslagen innebär att tydligare krav ställs på clearingbolagen. FI noterar också att det föreslås att Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka åtgärder ett clearingbolag ska vidta för att uppfylla kraven på bland annat riskhantering, informations-, it- och cybersäkerhet, uppdragsavtal och styrning verksamheten. Den föreslagna regleringen möjliggör en mer effektiv tillsyn från FI:s sida. Detta är särskilt angeläget i och med att det rör sig om systemviktig verksamhet och bolag som fyller en viktig samhällsfunktion.

Slutsatser i fråga om behov av regeländringar

Som framgår ovan gör FI bedömningen att det krävs en ökad tydlighet och enhetlighet i reglerna för finansiella företags utkontrakterade verksamhet. Skälen till denna bedömning är att kraven idag återspeglas i en mängd olika regler och att dessa i delar är allmänt hållna samt skiljer sig åt mellan olika sektorer av den svenska finansiella sektorn.

FI bedömer dock att det inte är effektivt eller ändamålsenligt att i dagsläget lämna närmare förslag på förändringar i gällande svenska författningar för att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet. Även om Dora-förordningen är beslutad bedömer FI att förslag till regeländringar kräver en analys av de tekniska standarder som ska utarbetas under förordningen och det är i dagsläget oklart vilket närmare innehåll dessa standarder kommer att få. Beträffande clearingbolag har det, som framgår ovan, vidare föreslagits att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka åtgärder ett clearingbolag ska vidta för att uppfylla krav som är relevanta för clearingbolags utkontraktering. Om nya regler utformas idag föreligger det

[9] Promemoria Ökad motståndskraft i betalningssystemet, Fi2022/02529.
[10] Remissvar, FI dnr 22-23532.

alltså en risk för att dessa kan komma att behöva justeras eller upphävas när andra redan pågående regelverksförändringar träder i kraft. Mot denna bakgrund framstår det inte som effektivt att lämna närmare förslag på författningsändringar i dagsläget och FI bedömer att sådana ändringar bör övervägas först när de nu pågående lagstiftningsinitiativen på såväl nationell som EU-nivå har kommit längre.

Handlingsplan

I uppdraget ingår att ta fram en handlingsplan om att stärka kontrollen över de finansiella företagens utlagda verksamhet. Nedan redogörs för FI:s handlingsplan i detta avseende. Handlingsplanen kompletterar FI:s befintliga arbete med utkontraktering och tredjepartsleverantörer.

Aktivt arbete med såväl nationell som EU-rättslig regelgivning

Som framgår ovan bedömer FI att det inte är effektivt eller ändamålsenligt att i dagsläget lämna närmare förslag på förändringar i gällande svenska författningar för att uppnå en bättre kontroll över de finansiella företagens utlagda verksamhet. Detta innebär däremot inte att det finns hinder mot att påbörja en analys och inventering av befintlig lagstiftning och övriga regelverk som har koppling till eller påverkar arbetet med tredjepartsrisker till följd av utkontrakterad verksamhet. Ett sådant arbete har redan påbörjats av FI och myndigheten ska fortsatt lägga resurser på detta arbete. Det handlar exempelvis om en behovsanalys av nationella anpassningar av lagar, förordningar och föreskrifter till följd av Dora-förordningens bestämmelser. Framöver kan det också handla om att bidra till arbetet med att ta fram verkställighetsföreskrifter till en ny clearinglag i enlighet med förslagen i promemorian Ökad motståndskraft i betalningssystemet.[11]

En annan del av detta arbete består av aktivt bidragande i framtagandet av tekniska standarder under Dora-förordningen. Även om Dora-förordningen har antagits återstår fortfarande arbetet med att ta fram tekniska standarder under EU-förordningen, inklusive krav kopplat till utkontrakterad verksamhet. FI kommer att bidra aktivt i det europeiska arbetet genom att delta i den kommittee[12] som ska utforma de aktuella tekniska standarderna. I kommitteen ska samtliga utkast på regleringar diskuteras innan de går vidare ut på remiss för att sedan beslutas. Genom att delta i detta arbete bidrar FI inte bara till den gemensamma regelutvecklingen utan kan också ta tillvara alla EU-länders samlade kompetens vilket kommer att påverka och stärka den nationella tillsynen. Med utgångspunkt i de kommande tekniska standarderna kommer FI också analysera behovet av verkställighetsföreskrifter på nationell nivå.

Fortsatt förhöjt fokus på tredjepartsrisker i tillsynen

FI har sedan ett par år tillbaka haft särskilt fokus på tredjepartrisker i den löpande tillsynen med anledning av den ökade risken på området. Med anledning av

[11] Se Promemorian Ökad motståndskraft i betalningssystemet, Fi2022/02529.
[12] Joint Committee Sub-committee on Digital Operational Resilience.

omvärldsläget har vi under det senaste året behövt ändra inriktning på tillsynen – något vi tidigare har rapporterat om – men myndigheten kommer fortsatt att ha tredjepartsrisker som en prioriterad risk.[13]

En central del av detta arbete handlar om fortsatt täta dialoger med de finansiella företagen. Detta innefattar bland annat fortlöpande analys av riskbilden kopplat till utkontraktering med utgångspunkt i ett tydligt definierat nuläge. En annan viktig fråga inom ramen för dessa dialoger handlar om de finansiella företagens förberedelser och eventuella utmaningar inför Dora-förordningens tillämpning. Dialogen kommer att ske bland annat genom att träffa flera företag samtidigt men även enskilda företag i samband med löpande tillsyn.

Med utgångspunkt i de kommande tekniska standarderna under Dora-förordningen och eventuell ny lagstiftning för clearingorganisationer kommer FI också att utforma tillsynsmetoder för att på ett effektivt sätt granska företagens hantering av tredjepartsrisker. Exempelvis kommer de register som ska föras enligt Dora-förordningen ge FI en uppfattning om koncentrationsrisker inom företaget och en uppfattning om hur företaget följer upp den utkontrakterade verksamheten.

Utveckla systemstöd

Det krav på register över utkontrakterad verksamhet som finansiella företag är skyldiga att upprätta enligt artikel 28.3 i Dora-förordningen föranleder ett behov av att utveckla systemstöd för att ta hand om inrapporteringen på ett effektivt sätt.[14]

Detaljerade mallar avseende registerföring kommer att tas fram i en teknisk standard. Det är i dagsläget oklart om det är fråga om en centraliserad rapportering på EU-nivå och om den praktiska insamlingen av informationen om utkontrakterad verksamhet ska ske i ett standardiserat tekniskt format som de europeiska tillsynsmyndigheterna bestämt, eller om den praktiska insamlingen ska utformas av de enskilda nationella myndigheterna. Om de nationella tillsynsmyndigheterna själva ska utforma systemet kommer FI behöva ställa krav på format och utformning av rapporteringen för att få in informationen på ett sätt som gör den hanterbar och möjlig att analysera på det sätt vi anser lämpligt. Frågorna kopplat till den praktiska hanteringen av register över utkontrakterad verksamhet behöver klarläggas innan FI påbörjar utvecklingen av egna system.

FI bedömer det dock som sannolikt att myndigheten under alla omständigheter till de europiska tillsynsmyndigheterna kommer att behöva återrapportera den nationella koncentrationsrisken och vilka motparter svenska finansiella företag har lagt ut verksamhet till. Detta innebär att FI kommer behöva utveckla ett systemstöd oavsett om den praktiska hanteringen av register över utkontrakterad verksamhet

[13] Delredovisning över tillsynsuppdraget av it-risker FI dnr 22-25815.
[14] Se även FI dnr 22-10015, publicerad den 9 maj 2022.

kommer tas fram centralt av de europeiska tillsynsmyndigheterna eller på nationell nivå.