P R O M E M O R I A

Datum **2018-03-15** FI Dnr 18-5393

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

Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer

Sammanfattning

Ett ökat användande av molntjänster kan ha positiva effekter för enskilda finansiella företag och för finansmarknaden och samhället i stort. Molntjänsterna kan bidra till att sänka inträdesbarriärerna till finanssektorn, möjliggöra konkurrens, i vissa fall skapa stabilare it-miljöer och i slutändan medverka till bättre och billigare finansiella tjänster för konsumenter. Men molntjänster innebär också risker som måste hanteras. De krav som finns på finansiella företags förmåga att hantera sina risker, gäller därför också när de använder molntjänster. Ett företag som vill använda sig av molntjänster måste säkerställa att företaget, dess revisorer och FI får tillgång till relevant information och lämpliga lokaler – så kallad revisionsrätt – för att vid behov kunna kontrollera och på plats inspektera den utlagda verksamheten hos molntjänstleverantören.

Om en molntjänstleverantör av legitima skäl vill begränsa tillgången till exempelvis datahallen, och en obegränsad tillgång inte är nödvändig för att kontrollera den utlagda verksamheten, behöver en sådan begränsning enligt FI inte nödvändigtvis hindra företaget från att ingå avtal. Ett företag som ingår avtal med begränsningar i revisionsrätten måste emellertid ha gjort en grundlig riskanalys och kunna motivera för FI varför begränsningarna inte påverkar företagets kontrollmöjligheter. Det är enligt FI inget självändamål att företag säkerställer tillgång till information eller lokaler som inte är nödvändiga för att på ett relevant sätt kunna kontrollera eller inspektera den utlagda verksamheten.

Användande av molntjänster regleras normalt av standardavtal. Det ligger i sakens natur att standardavtal sällan tar hänsyn till det enskilda företagets förhållanden, som till exempel hur kritisk den utlagda verksamheten är för företaget. Även om revisionsrätten kan utformas olika beroende på vilken typ av verksamhet det är fråga om, borde det ligga i allas intresse att standardavtalen utformas så att de kan användas i de flesta situationer utan risk för att de inte ska erbjuda en tillräcklig revisionsrätt. FI vill därför uppmuntra finansiella företag och molntjänstleverantörer till fortsatt diskussion med FI om

revisionsrättens innebörd, och om utformningen av revisionsrätten i praktiken och i det enskilda fallet.

Bakgrund

Den 1 december 2017 lämnade FI en rapport till regeringen om myndighetens roll när det gäller finansiella innovationer. Rapporten är ett resultat av uppdraget att utreda hur FI kan möta de frågor och behov som kan uppstå när nya innovativa finansiella tjänster etableras på marknaden. Enligt rapporten är användningen av molntjänster den största utmaningen för innovativa finansiella tjänster. Det framgår av samtal som FI har fört med företag under tillsyn. Mindre företag lyfter fram molntjänster som det enda alternativet för sin verksamhet och större företag ser det som ett attraktivt alternativ till egna driftslösningar, eftersom molntjänster medger en skalbarhet som är svår att uppnå i egen regi.

Gemensamt för företagen är att de är osäkra på FI:s syn på molntjänster och att de har fått intrycket att FI inte tillåter användning av molntjänster. Företagen ber därför om tydliga besked från FI och betonar att det är viktigt att FI förstår hur central den här frågan är för dem. De är särskilt angelägna om att få veta hur FI ser på revisionsrätten. Vissa företag uppger att delade meningar om innebörden av revisionsrätten har varit det största hindret för många bolag att använda sig av molntjänster.

Vad säger regelverken?

Regelverken för utläggning av verksamhet och molntjänster är utformade med utgångspunkt från lagens övergripande krav på finansiella företags förmåga att hantera och kontrollera sina risker. Revisionsrätt innebär att företag under FI:s tillsyn, som ingår avtal med uppdragstagare, måste säkerställa att avtalet ger företaget, dess revisorer och FI tillgång till uppgifter om den utlagda verksamheten samt tillträde till uppdragstagarens lokaler. Syftet med revisionsrätt är att möjliggöra såväl företagets egen kontroll av den utlagda verksamheten som FI:s möjlighet att fortsatt utöva en effektiv tillsyn över företaget. Krav på revisionsrätt kan uttryckas på olika sätt i de regler om utläggning av verksamhet som gäller för företag under FI:s tillsyn, men de övergripande principerna och syftet med krav på revisionsrätt är i allt väsentligt desamma.

Regelverken för utläggning av verksamhet är under utveckling. Europeiska bankmyndigheten (EBA) håller på att se över riktlinjerna om utläggning, som är från 2006[1]. I december 2017 beslutade EBA om rekommendationer för användning av molntjänster, som börjar gälla den 1 juli 2018.[2] När det gäller

[1] Riktlinjerna gavs ut av EBA:s föregångare, Europeiska banktillsynskommittén (CEBS).

[2] http://www.eba.europa.eu/documents/10180/1712868/Final+draft+Recommendations+on+Cloud+Outsourcing+%28EBA-Rec-2017-03%29.pdf

revisionsrätten framgår det av rekommendationerna att företagen, dess revisorer och FI bör ha full tillgång till molntjänstleverantörens lokaler samt obegränsade möjligheter att granska, och på plats inspektera, den utlagda verksamheten.

EBA:s riktlinjer och rekommendationer riktar sig visserligen endast till kreditinstitut och värdepappersbolag, men motsvarande regler om utläggning för andra företag under tillsyn, är som sagt baserade på samma övergripande principer och söker uppnå samma syfte. FI betraktar revisionsrätten på samma sätt oavsett regelverk, men utgår i den här promemorian från EBA:s rekommendationer.

Det bör i detta sammanhang nämnas att Europeiska kommissionen har tagit initiativ för ökad tydlighet kring hur företag och tillsynsmyndigheter bör förhålla sig till molntjänster. I den nyligen antagna handlingsplanen för FinTech[3], föreslår kommissionen t.ex. att de europeiska tillsynsmyndigheterna EBA, Eiopa och Esma utreder behovet av riktlinjer för användning av molntjänster och att finansiella företag och molntjänstleverantörer utarbetar standardklausuler för avtal om molntjänster avseende bl.a. revisionsrätten.

Därutöver ska kommissionen under andra kvartalet 2018 etablera ett ”FinTech Lab” som ska erbjuda utbildning och kunskapsutbyte för tillsynsmyndigheter i frågor kring teknikbaserade finansiella innovationer. Det första tillfället för labbet kommer att ägnas åt just molntjänster och utläggning av verksamhet.

Varför behövs revisionsrätten?

Oavsett formen för utläggning av verksamhet – molntjänster eller inte – så grundar sig revisionsrätten på den övergripande principen att det är företaget som ansvarar för att uppdragstagaren hanterar riskerna i den utlagda verksamheten på ett adekvat sätt. Det ansvaret kan inte läggas ut på en uppdragstagare. Företaget behöver därför analysera vilka risker – inte minst för informationssäkerheten – som en utläggning av verksamheten innebär. Företaget måste också säkerställa att molntjänstleverantören har förmåga att hantera de risker som den utlagda verksamheten är förenad med. Ett företag kan inte säkerställa att molntjänstleverantören har en adekvat riskhantering med mindre än att det gör regelbundna kontroller av den utlagda verksamheten.

Företagets kontroll av den utlagda verksamheten bör i normalfallet vara riskbaserad. Här ger EBA:s rekommendationer utrymme för alternativa sätt att utföra kontroller. Det är till exempel vanligt, och kan ofta vara tillräckligt, att företaget begär information från molntjänstleverantören i form av så kallade oberoende revisionsrapporter och certifieringar. Ett företag måste emellertid säkerställa att det har möjlighet att självständigt, på plats, kontrollera att molntjänstleverantörens hantering av riskerna i den utlagda verksamheten är tillräcklig. Det fordrar att företaget har tillgång till relevant information och,

[3] https://ec.europa.eu/info/sites/info/files/180308-action-plan-fintech_en.pdf

vid behov, direkt tillgång till molntjänstleverantören i lokalerna där den utlagda verksamheten drivs. Även vid incidenter, exempelvis dataintrång, kan företaget eller FI snabbt behöva få tillgång till den utlagda verksamheten för att utreda händelsens omfattning och orsak.

Syftet med FI:s revisionsrätt skiljer sig något från syftet med företagens revisionsrätt. FI utövar tillsyn över företag och inte molntjänstleverantörer, vilket innebär att FI i första hand vänder sig till företaget för att få den information som behövs för tillsynen. Det är främst i de fall FI inte kan få tillräcklig information från företaget som myndigheten måste kunna begära information direkt från molntjänstleverantören eller göra inspektioner på plats. Företagen måste därför säkerställa att avtalet inte begränsar FI:s möjlighet att få fullständig information eller göra kontroller på plats om det skulle behövas.

Anser FI att revisionsrätten alltid måste vara obegränsad?

Revisionsrätten och de regler som den grundas på är principbaserade. Det innebär att syftet med reglerna ska uppnås, det vill säga man ska kunna säkerställa en tillräcklig riskhantering och kontroll. En ovillkorlig revisionsrätt, eller ”obegränsad” revisionsrätt som EBA uttrycker det i sina rekommendationer, är alltså inget självändamål. Därför kan exempelvis tillgången till vissa av molntjänstleverantörens lokaler begränsas om det är uppenbart att det inte försämrar företagets möjligheter till adekvat kontroll eller FI:s möjligheter att utöva en effektiv tillsyn.

Vilka eventuella begränsningar i revisionsrätten som ett företag kan tänkas acceptera är svårt att precisera i förväg, eftersom det ytterst beror på riskerna med utläggningen, omfattningen av den utlagda verksamheten och hur kritisk den är för företaget. Om en molntjänstleverantör av legitima skäl vill införa begränsningar i tillgången till exempelvis datahallen, och en obegränsad tillgång inte är nödvändig för att kunna utföra kontroller av den utlagda verksamheten, behöver en sådan begränsning enligt FI inte hindra företaget från att ingå avtal. Här behöver man dock gå tillbaka till den riskanalys som företaget måste göra innan avtal om molntjänster ingås. Ett företag som accepterar sådana begränsningar måste ha gjort en grundlig riskanalys, och måste kunna motivera för FI varför eventuella begränsningar inte påverkar företagets möjligheter till kontroll. I slutändan är det företagets förmåga att kontrollera sina risker som FI kommer att behöva bedöma.

FI:s erfarenheter av standardavtal

Beroende på vilken typ av företag och utlagd verksamhet det är fråga om ställs det krav på att företaget ska anmäla utläggningen samt skicka in uppdragsavtalet till FI. Det finns flera skäl till en sådan ordning. FI behöver kunna skapa sig en bild av hur omfattande företagens utlagda verksamhet är och vilka risker den kan medföra. Det innebär emellertid inte att FI alltid granskar inkomna avtal i sin helhet när det gäller företagens riskhantering, det

är företagens ansvar. Det bör i detta sammanhang påpekas att FI inte heller formellt godkänner avtal.

Molntjänstleverantörernas tjänster är i regel standardiserade och omfattas av standardavtal. Ofta åtföljs standardavtalen av en bilaga med villkor som gäller särskilt för finansiella företag under tillsyn. Standardavtal tar oftast inte hänsyn till företagens specifika förhållanden, utan är i stället utformade för att kunna användas av alla finansiella företag oberoende av hur kritisk verksamheten är för det enskilda företaget. Eftersom flera av de avtal som FI tagit del av har gällt verksamheter som av olika anledningar anses kritiska eller särskilt riskfyllda, till exempel hanering av kunduppgifter, har det funnits väldigt lite utrymme för annat än mindre begränsningar i avtalen. FI har därför behövt ställa krav på företagen att omförhandla avtalen, så att de erbjuder tillräckliga möjligheter för kontroll och tillsyn.

Begränsningar som inte innebär att FI är förhindrade att utöva en effektiv tillsyn, är till exempel att FI ska utöva sin revisionsrätt endast om det är nödvändigt och i proportion till rättsliga krav samt arten och omfattningen av den utlagda verksamheten.

FI har också träffat molntjänstleverantörer för att diskutera revisionsrätten och varför den är viktig för företagens riskkontroll och FI:s tillsyn. FI har också påtalat att en helt obegränsad revisionsrätt inte innebär att vare sig företag eller FI kommer att göra fler eller mer omfattande kontroller. Sannolikheten för att FI kommer att behöva utöva sin revisionsrätt är egentligen inte särskilt stor, men om det skulle behövas är det viktigt att FI har möjlighet att granska den utlagda verksamheten som om den drevs i företagets egen regi.

En positiv effekt av att FI ställt krav på standardavtalen är att de utformas på ett likartat sätt, så att de kan användas av alla företag oberoende av vilken tjänst som molntjänstleverantören tillhandahåller. Ett uppdragsavtal reglerar dock endast förutsättningarna för en tillräcklig revisionsrätt. Skulle det visa sig att avtalet i praktiken inte ger företaget, dess revisorer eller FI möjlighet att utföra adekvata kontroller måste företaget omförhandla eller häva avtalet.

Avslutande kommentarer

Tillgången till molntjänster har visat sig vara viktig för såväl små, nystartade företag som för stora, väletablerade aktörer. En utveckling av molntjänsterna kan få positiva effekter för enskilda företag, men också för samhället i stort om utvecklingen kan bidra till att sänka inträdesbarriärerna till finanssektorn, möjliggöra konkurrens, skapa stabilare it-miljöer och i slutändan bättre och billigare finansiella tjänster för företag och konsumenter. Men en sådan utveckling innebär också att väsentliga risker för såväl enskilda företag och deras kunder som det finansiella systemet i stort hanteras av företag som inte står under tillsyn. En i grunden positiv utveckling av finanssektorn får inte ske på bekostnad av tillräcklig kontroll, tillsyn eller finansiell stabilitet.

Det är också viktigt att det inte bara är företag med resurser att driva igenom villkorsändringar i avtalen, som får möjlighet att använda molntjänster. Här fyller molntjänstleverantörernas standardavtal en viktig funktion. FI:s förhoppning är att alla företag ska kunna ingå avtal med molntjänstleverantörer utan risk för att avtalen begränsar företagens möjligheter att leva upp till regelverkets krav. De diskussioner som FI har haft med företag och molntjänstleverantörer om standardavtalens utformning tyder på att utvecklingen går i den riktningen. I detta avseende välkomnar FI också Europeiska kommissionens initiativ till att finansiella företag och molntjänstleverantörer gemensamt utarbetar standardiserade avtalsskrivningar.

Även om EBA:s rekommendationer besvarar många frågor om hur företag och tillsynsmyndigheter bör förhålla sig till användningen av molntjänster finns det, som Europeiska kommissionen också uppmärksammat, fortfarande ett behov av ökad tydlighet om inte minst tillsynsmyndigheternas förväntningar. FI avser därför att i nära dialog med branschen fortsätta utveckla och förtydliga praxis på detta område.

Som ett led i detta arbete kommer FI inom kort att bjuda in till diskussion kring användning av molntjänster och ge finansiella företag och molntjänstleverantörer möjlighet att ställa frågor till FI.