FÖRVALTNINGSRÄTTEN I STOCKHOLM

Avdelning 30

DOM
2020-08-25
Meddelad i Stockholm

Mål nr
25438-19

KLAGANDE
Nasdaq Clearing AB, 556383-9058

Ombud: Advokaterna Mattias Göransson och Fredrik Sjövall samt biträdande juristen Fredrika Bladh
Mannheimer Swartling Advokatbyrå AB
Box 1711
111 87 Stockholm

MOTPART
Finansinspektionen
Box 7821
103 97 Stockholm

ÖVERKLAGAT BESLUT
Finansinspektionens beslut den 12 december 2016, se Bilaga 1

SAKEN
Anmärkning och sanktionsavgift enligt lagen (2007:528) om värdepappersmarknaden – LV

FÖRVALTNINGSRÄTTENS AVGÖRANDE

Förvaltningsrätten avslår yrkandet om muntlig förhandling.

Förvaltningsrätten bifaller överklagandet och upphäver det överklagade beslutet.

Postadress	Besöksadress	Telefon	Telefax	Expeditionstid
	Tegeluddsvägen 1	08-561 680 00	-	måndag–fredag
115 76 Stockholm		**E-post**: avd30.fst@dom.se		08:00–16:00
		www.domstol.se/forvaltningsratt		

BAKGRUND

1. Finansinspektionen beslutade den 12 december 2016 att ge Nasdaq Clearing AB (fortsättningsvis Nasdaq Clearing) en anmärkning samt en sanktionsavgift om 25 miljoner kronor. De närmare detaljerna kring samt skälen för beslutet framgår av Bilaga 1.

2. Nasdaq Clearing överklagar beslutet och yrkar i första hand att det ska undanröjas och i andra hand att sanktionsavgiften ska sättas ned. Bolaget yrkar vidare att det ska hållas muntlig förhandling i målet. Som grund för sin talan anför bolaget att Finansinspektionen saknat stöd i tillämplig lagstiftning för beslutet och att det skulle strida mot legalitets- och proportionalitetsprincipen att meddela en sanktion.

3. Finansinspektionen bestrider bifall till överklagandet.

VAD PARTERNA ANFÖR

Nasdaq Clearing

4. Nasdaq Clearing har erhållit information avseende informationssäkerhetsrelaterade ämnen. Bolaget delar därför inte Finansinspektionens uppfattning att bolaget inte skulle ha haft tillgång till information eller inte följt upp tjänsteleveransen. Efter en större översyn antog styrelsen vidare en reviderad informationssäkerhetspolicy den 23 september 2015. Styrelsen har uppdragit åt InfoSec[1] att utföra arbetet i enlighet med denna policy, underordnade policys, standarder och riktlinjer. Utöver den rapportering som faktiskt har skett, har bolaget enligt outsourcingavtalet haft en rätt att ta del av all information (inklusive dokumentation, data, filer och utdrag från informationssystem) som skäligen kan begäras för att övervaka och försäkra

[1] Nasdaqkoncernens informationssäkerhetsavdelning

att outsourcingavtalet efterlevs och för att kunna fullgöra bolagets regulatoriska skyldigheter. Genom den rapportering som har skett och genom bestämmelser i outsourcingavtalet har bolaget haft tillgång till relevant information och även haft möjlighet att kontinuerligt få nödvändig information för att övervaka och utvärdera kvaliteten på de outsourcade tjänsterna. Även om rapporteringen rent formellt hade kunnat organiseras och uppföljningen formaliseras och dokumenteras på ett annat sätt än vad som skett anser bolaget inte att det har delegerat sitt ansvar eller underlåtit att övervaka outsourcingen i strid med kraven i EMIR[2]. Genom bolagets CTO[3] har bolaget även haft kompetens att utvärdera och övervaka de outsourcade funktionerna. Det finns inte heller något krav på dokumentation gällande uppföljningen av utkontrakteringen enligt regelverket.

5. Det har funnits utförligare beskrivningar av tjänstenivåer, s.k. Service Level Agreement (SLA) avseende outsourcingen av IT-leveranser. I outsourcingavtalet avseende IT-leveranser finns SLA med parametrar som är direkt relevanta för hanteringen av cyberrisker, exempelvis krav på produktionssystemets tillgänglighet, responstid, incidenthantering m.m., med avtalade krav på rapportering avseende utförandet av tjänsterna, inklusive orsaker till eventuella avbrott eller driftstopp. Informationssäkerhet har således varit en integrerad del av IT-leveransen och det har där skett en regelbunden rapportering av exempelvis tillgänglighet och incidenter.

6. Sedan i vart fall september 2015 har informationssäkerhetsrelaterade ämnen rapporterats till styrelsen. Dessutom har information avseende informationssäkerhet kvartalsvis rapporterats till Nasdaq Clearings lokala

[2] Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (the European Market Infrastructure Regulation)
[3] Chief Technology Officer (ansvarar för att övervaka Nasdaq Clearings outsourcing)

riskhanteringsforum LRMF[4]. Därutöver har incidentrapportering avseende IT-leveransen skett dagligen, veckovis eller vid behov. Vad gäller hotbildsinformation relaterad till Sverige och Norden har InfoSec haft informella kontakter med relevanta intressenter. InfoSec och bolaget har härigenom tillsett att ha tillgång till ett lokalt och regionalt riskperspektiv.

7. Vad gäller det lokala riskperspektivet har, som framgått ovan, LRMF haft kvartalsvisa möten. Om LRMF har identifierat några risker, har bolagets VD rapporterat detta till styrelsen. Bolaget har även haft tillgång till information från det koncerngemensamma Technology Risk Committee på förfrågan. Bolaget har även utfört självutvärderingar avseende risk för att identifiera lokala risker, som därefter har överlämnats till bolagets styrelse via LRMF. Bolaget har även utfört självutvärderingar avseende risk för att identifiera lokala risker, som därefter har överlämnats till bolagets styrelse via LRMF. Bolaget har alltså sett till att ha tillgång till ett lokalt riskperspektiv.

8. Att riskhanteringsverktyget BWISE inte användes vid tidpunkten för undersökningen har inte inneburit att det inte genomförts någon riskrapportering. Istället för att använda BWISE, rapporterades och följdes riskerna upp i Excel inom respektive funktion i organisationen. Det har således alltid funnits ett register i vilket risker har registrerats.

9. Vid tiden för Finansinspektionens undersökning hade Nasdaq Clearing antagit toleransnivåer för bl.a. systemavbrott och återhämtningstid, vilka i högsta grad har bäring på cyberrisker. Toleransnivåerna är medvetet antagna utan hänsyn till orsakerna till störningarna, delvis för att inte begränsa tillämpligheten till cyberrisker som orsak. Bolaget har svårt att se att påståendet om att det skulle ha förelegat en risk för att Bolaget inte skulle ha ekonomisk beredskap för att hantera risker eftersom bolaget inte

[4] Local Risk Management Forum

haft en process för att koppla risktoleransnivå och risktålighet till sina finansiella överväganden skulle vara relevant för ett bolag i en koncern där tjänsterna tillhandahålls på gruppnivå.

10. Det är riktigt att det, såvitt avser andra parter än leverantörer, inte har funnits någon formaliserad rutin för insyn i partens cybersäkerhet, eller något formaliserat informationsutbyte avseende just cyberrisker. I sammanhanget bör det emellertid noteras att artikel 4.2 i tillämpningsförordningen föreskriver att en central motpart *i möjligaste mån* ska ha en samlad och heltäckande syn avseende relevanta risker som de utsätts för av andra än clearingmedlemmar.

11. Vid tidpunkten för Finansinspektionens undersökning innefattades cyberriskrelaterade scenarier i bolagets allmänna och scenarioneutrala kontinuitetstestplaner. Nasdaq Clearings kontinuitetsplanering har tidigare inte utgått från orsaken till att en riskhändelse inträffar, utan har varit neutral i förhållande till denna. Istället har alternativa planer upprättats utifrån vilken resurs som drabbats. Bolaget har utformat sin kontinuitetshantering på ett sätt som är vanligt i branschen.

12. Det stämmer att Nasdaq Clearing i sin ansökan om auktorisation enligt EMIR har identifierat cyberrisker, även om begreppet som sådant inte använts. Det förhållandet att dessa risker har identifierats innebär dock inte att bolaget också måste ha de rutiner för uppföljning och rapportering i förhållande till den utkontrakterade verksamheten som Finansinspektionen hävdar, i stället för de rutiner som bolaget faktiskt haft för att följa upp bl.a. cyberrisker. Tillståndsansökan kan vidare varken utvidga eller i övrigt påverka området för sanktioner som sådant. De krav som regelverket uppställer måste fastställas objektivt.

Finansinspektionen

13. Finansinspektionen anser inte att möjligheten att ta del av den nödvändiga informationen räcker. Det räcker inte heller att informationen tillhandahålls. För att företaget ska kunna anses ha tagit emot kontinuerlig information som ger en samlad bild av leveransen måste det också finnas praktiska arrangemang med rutiner för att ta hand om informationen. Finansinspektionen har gjort bedömningen att oavsett om företaget har haft möjlighet att skaffa sig tillgång till kontinuerlig information om de utkontrakterade tjänsterna, så har det inte funnits några processer för att ta hand om informotionen och säkerställa att den kan användas för att övervaka verksamheten och ställa krav på leverantören. Dokumentation torde även vara helt nödvändigt för att informationen ska kunna användas för att övervaka och följa upp leveransen och ställa krav på leverantören. Dokumentationen är också nödvändig för att Finansinspektionen ska kunna följa företagets regelefterlevnad.

14. Finansinspektionen anser inte att regelverket ställer något uttryckligt krav på SLA. Däremot kräver artikel 35.1 g i EMIR att företaget övervakar de utkontrakterade verksamheterna. Finansinspektionens uppfattning är att en effektiv övervakning av de utkontrakterade verksamheterna åtminstone förutsätter en regelbunden uppföljning av tjänsteleveransen och av avtalet. En sådan regelbunden uppföljning är enligt Finansinspektionens bedömning bara möjlig om avtalet innehåller detaljerade överenskommelser om servicenivåer. Bolaget har inte aktivt uppfyllt skyldigheterna och inte utnyttjat de möjligheter som finns i avtalen för att faktiskt leva upp till kraven på uppföljning av den utkontrakterade verksamheten och eventuellt vidta nödvändiga åtgärder. Avgörande är inte om det krävs några rapporter i riktlinjer, dokumentation och avtal utan vilka åtgärder som faktiskt vidtagits. Avsaknaden av dokumentation kring övervakning och riskhantering visade att det fanns brister i hur denna hanteras.

15. När det gäller bristen på information om hotbild, personalsituation m.m. tar Finansinspektionens iakttagelse sikte på att Nasdaq Clearings styrelse och ledning inte har haft tillräckligt underlag för att hantera de risker som utkontrakteringen av informationssäkerheten har medfört. Iakttagelserna handlar om att Nasdaq Clearings styrelse, i samband med utkontrakteringen av tjänster till InfoSec, inte har haft kontroll på de risker som denna utkontraktering har varit förenad med.

16. Finansinspektionen har vidare gjort bedömningen att InfoSec har saknat information om lokala riskförhållanden i sitt arbete med informationssäkerhet och att det därmed har funnits en risk för att koncernens informationssäkerhetsarbete inte har varit anpassat för svenska förhållanden. Som exempel kan nämnas att även om cyberrisker till sin natur är gränslösa, så kan hotbilden mot ett svenskt infrastrukturföretag vara olik den mot ett amerikanskt, exempelvis med avseende på vem som skulle kunna vilja angripa företaget.

17. Det alternativa verktyg som användes under den tid då riskhanteringsverktyget BWISE var ur bruk har inte kunnat ge en samlad bild av riskerna i organisationen.

18. Nasdaq Clearing hade vid tiden för undersökningen inte hade tagit ställning till cyberrisker och dokumenterat sina ställningstaganden på ett sådant sätt att det framgick i vilken utsträckning sådana risker kunde tolereras, hur företagets beredskap för att möta riskerna såg ut, vilka förändringar och investeringar som var nödvändiga för att beredskapen skulle motsvara den risktoleransnivå som styrelsen fastställt, samt hur förändringar i omvärlden skulle kunna påverka riskbilden och därmed investeringsbehovet. Enligt Finansinspektionen krävs att alla dessa led har tagits om hand i riskarbetet för att företagets riskhantering och riskkontroll ska

kunna anses tillfredsställande.

19. När det gäller Nasdaq Clearings kontinuitetsplanering framgår det av kompletteringsförordningen att företaget ska ha en scenariobaserad riskanalys, samt arrangemang för att säkra kontinuitet, grundade på olika scenarier. Detta har Nasdaq Clearing inte haft. Enligt Finansinspektionen måste orsaken till en händelse beaktas för att kontinuitetsplaneringen ska kunna fungera. Scenariot som helhet kan nämligen ha stor betydelse för vilka åtgärder som bör, respektive inte bör, vidtas pga. en händelse.

20. Nasdaq Clearing har redan i sin ansökan om auktorisation enligt EMIR tydligt förklarat att cyberrisker utgör en central del av de aktuella bestämmelserna. Trots denna insikt kännetecknas företagets argumentation i målet av en begränsning till ordalydelsen i de aktuella bestämmelserna. Nasdaq Clearing har i ansökan identifierat externa hot mot IT-systemen som en av de konkreta riskerna mot den kontinuerliga verksamheten. Av ansökan framgår vidare att företaget anser att det system[5] som clearingverksamheten bedrivs i inte bara omfattas av artikel 26.6 i EMIR utan även bidrar till att uppfylla sundhetskraven i artikel 26.1 i EMIR och artikel 4 i tillämpningsförordningen. Detta torde i sig kräva att företagets ledning definierar, skattar och dokumenterar risktoleransnivå och risktålighet specifikt i förhållande till cyberrisker inklusive externa intrång. Med tanke på den centrala punkt som systemet för clearingverksamheten har för företagets verksamhet är det vidare naturligt att IT-systemet ses som en kritisk funktion i den mening som avses i bestämmelserna om kontinuerlig verksamhet.

[5] Genium INET Clearing-systemet

SKÄLEN FÖR AVGÖRANDET

Inledning

21. Finansinspektionen har med stöd av 25 kap. 1 § LV beslutat att ge Nasdaq Clearing en anmärkning och med stöd av 25 kap. 8 § samma lag beslutat att bolaget ska betala en sanktionsavgift. Av 25 kap. 1 § LV följer bl.a. att om ett svenskt värdepappersinstitut, en börs, en svensk leverantör av datarapporteringstjänster eller en svensk clearingorganisation har åsidosatt sina skyldigheter enligt denna lag, andra författningar som reglerar företagets verksamhet, företagets bolagsordning, stadgar eller reglemente eller interna instruktioner som har sin grund i en författning som reglerar företagets verksamhet, ska Finansinspektionen ingripa.

22. Finansinspektionen har i beslutet ansett att Nasdaq Clearing åsidosatt sina skyldigheter enligt föreskrifter som främst återfinns i EMIR och Kommissionens delegerade förordning (EU) nr 153/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 med avseende på tekniska tillsynsstandarder för krav på centrala motparter (tillämpningsförordningen). Finansinspektionen har också gjort gällande att bolaget har åsidosatt skyldigheter enligt sin egen policy.

23. Förvaltningsrätten har i första hand att ta ställning till om bolaget har åsidosatt de av Finansinspektionen angivna bestämmelserna och, för det fall svaret på den frågan är jakande, om Finansinspektionen därmed har haft rätt att påföra en sanktionsavgift.

24. Eftersom det är fråga om ett ingripande från det allmännas sida är det Finansinspektionen som har bevisbördan för att förutsättningarna att påföra sanktionsavgiften är uppfyllda (jfr Kammarrätten i Stockholms dom den 9 november 2016 i mål nr 315-16 och SOU 2010:29 s. 407). Av rättspraxis följer vidare att beviskravet av rättssäkerhetsskäl bör ställas högt när det gäller sådana ingripanden, men att beviskravet inte kan ställas lika högt som för en fällande dom i ett brottmål eftersom det även måste beaktas att syftet med sanktionsavgiften är att bevaka allmänna intressen (jfr Högsta förvaltningsdomstolens refererade avgöranden RÅ 2006 ref. 7 och RÅ 1994 ref. 88). Förvaltningsrätten kommer fortsättningsvis att använda värdeordet *klarlagt* som riktmärke för frågan huruvida Finansinspektionen har uppfyllt sin bevisbörda.

25. Parternas argumentation har till stor del handlat om på vilket sätt vissa av reglerna ska uttolkas och vilket underlag som ska användas vid denna tolkning. Förvaltningsrätten konstaterar i sammanhanget att Finansinspektionen, gällande valet av ingripande, har anfört att ett föreläggande om rättelse – eventuellt med vite – i praktiken inte skulle kunna uppfylla kraven på tydlighet och rättssäkerhet, eftersom det rör sig om specifika frågor hur verksamheten bedrivs och hur de befintliga ramverken ska tillämpas. Finansinspektionen har också konstaterat att det antagligen finns mer än ett sätt för Nasdaq Clearing att rätta till de konstaterade bristerna. Finansinspektionen har gjort gällande att bestämmelserna bör tolkas i ljuset av vad bolaget angett i sin ansökan om auktorisation enligt EMIR. Förvaltningsrätten delar inte denna sist nämnda uppfattning.

26. Högsta förvaltningsdomstolen har i ett avgörande den 28 maj 2020, mål nr 1593-19, klargjort vad som krävs för att ett vitesföreläggande ska anses vara tillräckligt precist utformat för att ett vite ska kunna dömas ut. Beslut om anmärkning och sanktionsavgift till följd av bristande regelefterlevnad är ett betungande ingripande från det allmännas sida och det är

här fråga om tolkning av regler som aktörer på marknaden har en skyldighet att rätta sig efter. Vid prövningen om Nasdaq Clearing har brutit mot gällande regelverk bör därför samma principiella krav på förutsägbarhet och tydighet ställas som när ett vitesföreläggande endast upprepar en viss reglerings lydelse. För att tillgodose kravet fordras enligt nämnda avgörande från HFD därför att de bestämmelser som Nasdaq Clearing ska ha överträtt är så precisa att det inte kan råda något tvivel om vilka åtgärder som ska vidtas eller underlåtas. De uppställda kraven måste därför tydligt kunna utläsas redan av regelverket.

Utkontraktering

27. Av handlingarna i målet framgår följande. Nasdaq Clearing har lagt ut funktionen för informationssäkerhet till det amerikanska moderbolaget Nasdaq Inc. och dess informationssäkerhetsavdelning InfoSec. Utkontrakteringen har skett genom ett outsourcingavtal[6]. Nasdaq Clearing har även utkontrakterat sina IT-leveranser till ett bolag inom Nasdaq-koncernen, Nasdaq Exchange and Clearing Services AB. Den utkontrakteringen regleras i ett separat avtal mellan dessa parter.

Direkt tillgång till relevanta uppgifter m.m.

28. Finansinspektionen har gjort gällande att Nasdaq Clearing inte har uppfyllt kraven i 35.1 h EMIR. Finansinspektionen har i denna del anfört att det inte finns något underlag som visar att någon faktisk genomförd rapportering har skett från tiden före undersökningen eller att styrelsen på något annat sätt har försäkrat sig om att företaget löpande har haft direkt tillgång till relevanta uppgifter om de utkontrakterade verksamheterna.

[6] Master Administrative Service Agreement

29. Nasdaq Clearing har i förvaltningsrätten bl.a. anfört att bolaget, i enlighet med ordalydelsen av outsourcingavtalet, har haft rätt att ta del av all information (inklusive dokumentation, data, filer och utdrag från informationssystem) som skäligen kan begäras för att övervaka och försäkra att avtalet efterlevs och för att kunna fullgöra bolagets regulatoriska skyldigheter. Detta har inte ifrågasatts av Finansinspektionen. Finansinspektionen anför dock att möjligheten att ta del av den nödvändiga informationen inte är tillräcklig. Inspektionen gör gällande att det också måste finnas praktiska arrangemang med rutiner för att ta hand om informationen för att företaget ska kunna anses ha tagit emot kontinuerlig information som ger en samlad bild av leveransen.

30. Av bestämmelsen följer att den centrala motparten ska ha direkt tillgång till relevanta uppgifter om de utkontrakterade verksamheterna. Det kan, enligt förvaltningsrättens bedömning, inte utläsas av bestämmelsen att rapportering ska ske eller att bolaget ska visa att det finns praktiska arrangemang för att ta hand om informationen, på det sätt som Finansinspektionen gör gällande. Mot bakgrund av att bolaget har haft rätt att ta del av uppgifter avseende outsourcingen enligt avtalet görs bedömningen att Finansinspektionen inte har klarlagt att bolaget har åsidosatt sina skyldigheter enligt artikel 35.1 h EMIR.

Uppföljning

31. Finansinspektionen har gjort gällande att bolaget i praktiken saknat möjlighet till utförlig uppföljning eftersom outsourcingavtalet SLA. Finansinspektionen har i förvaltningsrätten vidare utvecklat att Nasdaq Clearing inte aktivt har uppfyllt sina skyldigheter som finns i avtalen för att faktiskt leva upp till kravet på uppföljning. Avgörande är inte om det krävs rapporter i riktlinjer, dokumentation och avtal utan vilka åtgärder

som faktiskt har vidtagits. Avsaknaden av dokumentation kring övervakning och riskhantering visade att det fanns brister i hur denna hanteras.

32. Det är mellan parterna ostridigt att outsourcingavtalet mellan Nasdaq Clearing och Nasdaq Inc., vid den i målet aktuella tidpunkten, inte innehöll någon SLA. Nasdaq Clearing har däremot gjort gällande att outsourcingavtalet för IT-leveransen hela tiden haft SLA med relevanta parametrar för hanteringen av cyberrisker.

33. Av utredningen i målet framgår vidare att avtalet relaterat till IT-tjänsterna innehåller beskrivningar av de tjänster som utkontrakterats av Nasdaq Clearing. Avtalet innehåller bl.a. beskrivningar av IT-systemets tillgänglighet, tidsramar avseende när hantering av olika incidenter ska ske samt skyldigheter gällande både incidentrapportering och övrig löpande rapportering. Avtalet hanterar incidenter oavsett orsaken till dessa och, även om det inte är uttryckligen angett, bedöms avtalet även vara tillämpligt på incidenter orsakade av cybersäkerhetsrelaterade händelser. Mot bakgrund av innehållet i nämnda avtal görs bedömningen att Finansinspektionen inte har klarlagt att avsaknaden av SLA i outsourcingavtalet innebär att bolaget har överträtt bestämmelsen i 35.1 g EMIR, i fråga om riskhantering och övervakning beträffande utkontraktering av tjänster hänförliga till cybersäkerhet.

34. Vad gäller den faktiska uppföljningen konstaterar förvaltningsrätten att Nasdaq Clearing redogjort för hur det tagit emot information medan Finansinspektionen i denna del i huvudsak grundar sitt ställningstagande på att det inte finns någon dokumentation avseende detta. Av artikel 35.1 g EMIR följer att den centrala motparten löpande ska övervaka de utkontrakterade verksamheterna och hantera dessa risker. Förvaltningsrätten konstaterar att det förvisso inte framgår av artikel 35.1 g EMIR att det finns ett dokumentationskrav men att avsaknaden av dokumentation

i och för sig kan tala för att någon uppföljning inte har skett. Som konstaterats i avsnittet ovan har Nasdaq Clearing enligt outsourcingavtalet haft rätt att ta del av uppgifter om outsourcingen och det framgår även av bolagets outsourcingpolicy att uppföljning ska ske. Finansinspektionen har inte ifrågasatt bolagets uppgifter om att styrelsen har uppdragit åt InfoSec att utföra arbetet i enlighet med denna policy. Av utredningen framgår även att avtalet relaterat till IT-tjänsterna anger att Nasdaq Clearing är skyldig att övervaka de tjänsterna på en lämplig och effektiv nivå. Förvaltningsrätten bedömer mot den bakgrunden, samt med beaktande av innehållet i avtalet gällande IT-leveransen som redogjorts för ovan, att Finansinspektionen inte har klarlagt att det skett en överträdelse av aktuell bestämmelse i EMIR i detta avseende.

35. Givet det anförda i denna del bedöms Finansinspektionen vidare inte ha klarlagt att Nasdaq Clearing skulle ha delegerat sitt ansvar i strid med artikel 35.1 a i EMIR eller att Nasdaq inte har följt artikel 4.4 i tillämpningsförordningen.

36. Finansinspektionen har vidare gjort gällande att Nasdaq Clearing brutit mot sin egen policy genom att inte inkludera SLA i outsourcingavtalet. En förutsättning för detta är enligt 25 kap. 1 § LV att den interna instruktionen har sin grund i en författning som reglerar bolagets verksamhet. Enligt förvaltningsrättens mening har Finansinspektionen inte klarlagt att så skulle vara fallet.

Information om hotbild och risker m.m. i samband med utkontraktering

37. Finansinspektionen har i beslutet gjort gällande att Nasdaq Clearings styrelse inte har haft förutsättningar att hantera de risker som utkontrakteringen innebär eftersom styrelsen saknat information om hotbild och risker i samband med utkontrakteringen. Förvaltningsrätten konstaterar

att parterna i denna del har olika uppfattningar om vilken information styrelsen har haft tillgång till. Enligt förvaltningsrättens mening kan det dock inte utläsas av varken EMIR eller tillämpningsförordningen att styrelsen ska ges tillgång till sådan information på det sätt Finansinspektionen gör gällande. Givet det anförda bedöms Finansinspektionen inte ha klarlagt att Nasdaq Clearing brutit mot bestämmelsen i 35.1 g EMIR.

Riskhantering

Brister i riskhanteringen

38. Finansinspektionen har i beslutet gjort gällande att bolaget inte fullt ut har uppfyllt kravet på effektiva metoder för att identifiera, hantera, övervaka och rapportera risker enligt artikel 26.1 EMIR. Finansinspektionen menar att bolaget inte heller har haft ett sunt system för att hantera alla väsentliga risker i enlighet med artikel 4.1 i tillämpningsförordningen samt att bolaget saknat en samlad och heltäckande syn på cyberrisker och inte heller har haft något lämpligt riskhanteringsverktyg för att kunna hantera och rapportera dessa risker. Vidare anser Finansinspektionen att bolaget inte i tillräcklig utsträckning tagit hänsyn till koncernens påverkan på företagets organisationsstyrning. Finansinspektionen bedömer därför att bolaget inte heller har uppfyllt kraven i artiklarna 3.4, 4.2 och 4.3 i tillämpningsförordningen.

39. Finansinspektionen har i denna del gjort gällande att Nasdaq Clearing inte försäkrat sig om att företagets lokala riskperspektiv beaktas på området för cybersäkerhet. Nasdaq Clearings uppfattning är att det lokala riskperspektivet har beaktats och har i inlagor till domstolen redogjort för detta. Finansinspektionen har inte utvecklat varför de av bolaget redogjorda åtgärderna inte skulle vara tillräckliga för att bevaka det lokala riskperspektivet. Finansinspektionen har inte heller närmare preciserat i

vilket avseende den påstådda avsaknaden av ett lokalt riskperspektiv gällande cybersäkerhet skulle utgöra en överträdelse av EMIR eller tillämpningsförordningen. Enligt förvaltningsrättens mening kan det heller inte utläsas av reglerna att det finns ett sådant krav. Givet det anförda görs bedömningen att Finansinspektionen inte har klarlagt att Nasdaq Clearing åsidosatt sina åtaganden i denna del.

40. Finansinspektionen gör i denna del vidare gällande att Nasdaq Clearing saknat ett lämpligt riskhanteringsverktyg för cyberrisker som kunnat ge företaget en samlad och heltäckande bild för bedömning av riskerna. Enligt Finansinspektionen har inte det alternativa system för rapportering av risk som använts under den tid då riskhanteringsverktyget BWISE var ur bruk kunnat ge en samlad bild av riskerna i organisationen. Förvaltningsrätten konstaterar att det av artikel 4.3 tillämpningsförordningen framgår att centrala motparter ska utveckla lämpliga riskhanteringsverktyg för att kunna hantera och rapportera relevanta risker. Närmare reglering om utformningen av ett sådant verktyg finns däremot inte, varför det i sig inte bedöms utgöra en brist att använda ett alternativt riskhanteringssystem på det sätt som Nasdaq Clearing har gjort. Av artikel 4.2 i tillämpningsförordningen följer dock att centrala motparter ska ha en samlad och heltäckande syn på alla relevanta risker. I bestämmelsen beskrivs det emellertid inte närmare på vilket sätt detta ska ske. Det konstateras att Nasdaq Clearing beskrivit det alternativa riskhanteringsverktyget och i anslutning till detta angett att det alltid funnits ett register i vilket risker har registrerats. Finansinspektionen har inte bemött detta och närmare redogjort för på vilket sätt det alternativa systemet för riskrapportering inte skulle vara tillräckligt för att ge en samlad bild av riskerna i organisationen. Mot bakgrund av det anförda görs bedömningen att Finansinspektionen inte klarlagt att Nasdaq Clearing har åsidosatt sina åtaganden i denna del.

41. Utredningen ger vidare inte stöd för att bolaget inte i tillräcklig utsträckning tagit hänsyn till koncernens påverkan på företagets organisationsstyrning. Sammantaget görs därmed bedömningen att Finansinspektionen inte har klarlagt att Nasdaq Clearing inte skulle ha uppfyllt kraven i artikel 26.1 i EMIR eller artiklarna 3.4, 4.1, 4.2 och 4.3 i tillämpningsförordningen.

Brister i styrelsens fastställande av risktolerans och risktålighet i fråga om cyberrisker

42. Finansinspektionen har gjort gällande att bolagets styrelse inte har haft tillgång till någon kontinuerlig rapportering om cybersäkerhet från tjänsteproducenten. Finansinspektionen har inte utvecklat eller närmare preciserat på vilket sätt det skulle utgöra en överträdelse av artikel 4.1 eller 4.4 i tillämpningsförordningen. Finansinspektionen bedöms därmed genom enbart påståendet inte ha klarlagt att Nasdaq Clearing har åsidosatt sina skyldigheter.

43. Finansinspektionen gör vidare gällande att Nasdaq Clearing inte haft någon process för att koppla risktoleransnivå och risktålighet till sina finansiella överväganden. Enligt Finansinspektionen har cyberrisker därför inte omfattats av ett sunt system för riskhantering enligt artikel 4.1 i tillämpningsförordningen. Av den aktuella bestämmelsen framgår att centrala motparter ska ha ett sunt system för att hantera alla väsentliga risker som de är eller kan bli exponerade mot. Enligt förvaltningsrätten mening kan det dock inte utläsas av nämnda artikel att det finns ett specifikt krav på att centrala motparter ska koppla risktoleransnivå och risktålighet till sina finansiella överväganden. Finansinspektionen bedöms därmed inte ha klarlagt att Nasdaq Clearing har överträtt artikel 4.1 i tillämpningsförordningen.

44. Finansinspektionen har vidare gjort gällande att Nasdaq Clearing vid tiden för undersökningen inte hade definierat, skattat och dokumenterat den centrala motpartens lämpliga risktoleransnivå och risktålighet i förhållande till cyberrisker. Enligt Finansinspektionen har bolaget därmed åsidosatt sina skyldigheter enligt 4.4 i tillämpningsförordningen. Under domstolsprocessen har Finansinspektionen utvecklat sin uppfattning och anfört att Nasdaq Clearing vid tiden för undersökningen inte hade tagit ställning till cyberrisker och dokumenterat sina ställningstaganden på ett sådant sätt att det framgick i vilken utsträckning sådana risker kunde tolereras, hur företagets beredskap för att möta riskerna såg ut, vilka förändringar och investeringar som var nödvändiga för att beredskapen skulle motsvara den risktoleransnivå som styrelsen fastställt, samt hur förändringar i omvärlden skulle kunna påverka riskbilden och därmed investeringsbehovet.

45. Av artikel 4.4 i tillämpningsförordningen framgår att en styrelse ska definiera, skatta och dokumentera den centrala motpartens lämpliga risktoleransnivå. Även om cyberrisker är en av de risker som får anses omfattas av tillämpningsområdet så kan bestämmelsen enligt förvaltningsrättens mening inte tolkas som att det också finns ett krav på att specifikt ange cyberrisker som orsak till en störning. Det kan därför inte utläsas av bestämmelsen att cyberrisker måste tas upp särskilt på det sätt som Finansinspektionen gör gällande i det överklagade beslutet. Det bedöms inte heller följa av bestämmelsen att en styrelse åläggs ett så långtgående ansvar att ta ställning till och dokumentera cyberrisker som Finansinspektionen gjort gällande under domstolsprocessen. Det har inte ifrågasatts av Finansinspektionen att Nasdaq Clearing, vid tiden för Finansinspektionens undersökning, antagit toleransnivåer för bl.a. systemavbrott och återhämtningstid och att dessa var tillämpliga även till händelser relaterade till cyberrisker. Det förhållandet att toleransnivåerna inte specifikt utformats för cyberrisker innebär inte att Finansinspektionen har

klarlagt att Nasdaq Clearing åsidosatt sina skyldigheter enligt artikel 4.4 i tillämpningsförordningen.

Brister i riskhanteringen som innebär tekniska kontakter

46. Finansinspektionen har i det överklagade beslutet anfört att Nasdaq Clearing inte uppfyller kraven i artikel 4.2 i tillämpningsförordningen eftersom det inte funnits något utbyte av information om relevanta cyberrisker mellan Nasdaq Clearing och andra parter, utöver leverantörer, som företaget har teknisk kontakt med. Enligt Finansinspektionen saknar Nasdaq Clearing därmed en samlad och heltäckande syn på relevanta risker.

47. Av bestämmelsen följer att centrala motparter ska ha en samlad och heltäckande syn på alla relevanta risker. I bestämmelsen beskrivs det dock inte närmare på vilket sätt detta ska ske. Givet detta görs bedömningen att Finansinspektionen inte har klarlagt att Nasdaq Clearing har åsidosatt sina skyldigheter enligt bestämmelsen genom att inte ha någon formaliserad rutin för insyn i cybersäkerhet, eller något formaliserat informationsutbyte avseende just cyberrisker, med andra parter som bolaget har kontakt med.

Kontinuerlig verksamhet

48. Finansinspektionen har gjort gällande att scenarier relaterade till cyberattacker inte inkluderats i bolagets scenariobaserade riskanalys som ska användas enligt artikel 18.2 i tillämpningsförordningen, eller bland de katastrofscenarier som legat till grund för arrangemang för kontinuitet enligt artikel 19.1 i tillämpningsförordningen. Det har enligt inspektionen därmed funnits en risk att bolaget inte skulle ha den beredskap som

anges i kontinuitetsriktlinjerna, i enlighet med kraven i artikel 17.6 i tillämpningsförordningen. Bolaget har inte gjort någon analys av den mest lämpade strategin för återställning i fråga om cyberrelaterade scenarier enligt artikel 17.5. Det har enligt Finansinspektionen vid tiden för undersökningen inte funnits tillräcklig beredskap för cyberattacker eller bristande dataintegritet i företagets beredskapsplanering. Bolaget har enligt finansinspektionen överträtt kraven i artiklarna 17.4–17.6, 18.2 och 19.1 i tillämpningsförordningen.

49. Förvaltningsrätten konstaterar att en central motpart har en skyldighet enligt artikel 18.2 i tillämpningsförordningen att använda en scenariobaserad riskanalys i sin verksamhetsanalys och enligt artikel 19.1 en skyldighet att på grundval av olika katastrofscenarier ha arrangemang för att säkra kritiska funktioners kontinuitet.

50. Det bedöms som utrett att Nasdaq Clearing inte har inkluderat scenarier hänförliga till cyberattacker i den scenariobaserade riskanalys som bolaget ska göra enligt artikel 18.2 i tillämpningsförordningen samt att bolaget inte inkluderat cyberattacker som ett sådant katastrofscenario som nämns i artikel 19.1. Enligt förvaltningsrättens mening kan det dock inte utläsas av bestämmelserna att det skulle utgöra ett specifikt krav att inkludera scenarier relaterade till just cyberattacker i de sammanhangen. Finansinspektionen bedöms därmed inte ha klarlagt att Nasdaq Clearing överträtt artiklarna 18.2 och 19.1 i tillämpningsförordningen på det sätt som Finansinspektionen gör gällande.

51. Beträffande artiklarna 17.4, 17.5 och 17.6 i tillämpningsförordningen görs bedömningen att artiklarna inte innehåller krav på att cyberrelaterade scenarier måste anges specifikt. Finansinspektionen har därmed inte klarlagt att Nasdaq Clearing har åsidosatt sina skyldigheter i denna del.

Sammanfattning

52. Sammanfattningsvis bedöms Finansinspektionen inte i något avseende ha klarlagt att Nasdaq Clearing har överträtt någon av bestämmelserna i EMIR eller tillämpningsförordningen eller i någon annan författning som, inom ramen för det överklagade beslutets tillämpningsområde, reglerar Nasdaq Clearings verksamhet. Det har därmed saknats laglig grund för Finansinspektionen att med stöd av enligt 25 kap. 1 och 8 §§ LV ingripa mot Nasdaq Clearing. Det överklagande beslutet upphävs därmed.

Muntlig förhandling

53. Vid denna utgång saknas det anledning att hålla muntlig förhandling i målet. Yrkandet härom avslås därmed.

HUR MAN ÖVERKLAGAR

54. Detta avgörande kan överklagas. Information om hur man överklagar finns i Bilaga 2 (FR-03).

Lars-Åke Johansson
Chefsrådman

Johan Gefvert
Rådman

Nämndemännen Håkan Lindberg, Marie Sjölund och Lena Törner har också deltagit i avgörandet.

Förvaltningsrättsfiskalen Jennie Åsberg har föredragit målet.

Bilaga 1

2016-12-12

B E S L U T

Nasdaq Clearing Aktiebolag
genom styrelsens ordförande
105 78 Stockholm

FI Dnr 15-9258
Delgivning nr 1

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

Anmärkning och sanktionsavgift

Finansinspektionens beslut (att meddelas den 13 december 2016 kl. 08.00)

1. Finansinspektionen ger Nasdaq Clearing Aktiebolag (556383-9058) en anmärkning.

   (25 kap. 1 § lagen [2007:528] om värdepappersmarknaden)

2. Nasdaq Clearing Aktiebolag ska betala en sanktionsavgift på 25 000 000 kronor.

   (25 kap. 8 § lagen om värdepappersmarknaden)

Hur man överklagar, se *bilaga 1*.

Sammanfattning

Nasdaq Clearing Aktiebolag (Nasdaq Clearing eller företaget) är ett svenskt aktiebolag som har tillstånd att tillhandahålla clearingtjänster som central motpart enligt bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (Emir).

Finansinspektionen har undersökt hur Nasdaq Clearing har följt vissa grundläggande krav på en central motpart enligt bestämmelserna i Emir.

Undersökningen har fokuserat på hur företaget hanterar cyberrisker. Eftersom bland annat funktionen för informationssäkerhet är utkontrakterad till koncernens moderbolag Nasdaq, Inc., har frågor om företagets självständighet och oberoende granskats i undersökningen. Finansinspektionen finner att Nasdaq Clearing inte har försett sig med den information som behövs för att bedöma de levererade tjänsternas kvalitet och ställa tillräckliga krav på leverantören. Undersökningen visar också att Nasdaq Clearing i sin riskhantering inte har haft tillräckliga underlag för de beslut som fattats och att

hänsyn inte har tagits till lokala förhållanden. Finansinspektionen konstaterar slutligen att företagets kontinuitetsriktlinjer och katastrofplan har tagits fram utan hänsyn till ett scenario som behandlar risken för cyberattacker.

Eftersom centrala motparter har en systemviktig funktion i det finansiella systemet är kraven på intern styrning och kontroll, riskhantering och informationssäkerhet för ett sådant företag mycket höga. Finansinspektionens undersökning visar att Nasdaq Clearing inte i alla delar har uppfyllt dessa krav. Bristerna har varit sådana att Finansinspektionen bedömer att det finns skäl att ingripa mot Nasdaq Clearing. Företagets överträdelser har dock inte varit så allvarliga att det är aktuellt att återkalla företagets tillstånd. Finansinspektionen ger därför företaget en anmärkning, som förenas med en sanktionsavgift på 25 miljoner kronor.

1 Bakgrund

1.1 Företagets verksamhet

Nasdaq Clearing Aktiebolag (Nasdaq Clearing eller företaget) har tillstånd att tillhandahålla clearingtjänster som central motpart enligt bestämmelserna i Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (Emir). Företaget omfattas av Finansinspektionens tillsyn enligt 23 kap. 1 § första och andra styckena lagen (2007:528) om värdepappersmarknaden (LV). Nasdaq Clearing hade under 2015 en årsomsättning på cirka 637 miljoner kronor och 66 anställda.

Nasdaq Clearing ingår i Nasdaqkoncernen, som är en internationell koncern med verksamhet i bland annat USA, Norden och Baltikum. Verksamheten består till stor del i att driva handelsplatser för finansiella instrument.

De nordiska dotterbolagen i Nasdaqkoncernen, däribland Nasdaq Clearing, har utkontrakterat en stor del av sina funktioner till moderbolaget Nasdaq, Inc. Till de tjänster som moderbolaget levererar till Nasdaq Clearing hör bland annat informationssäkerhet.

1.2 Ärendet

Som ett led i tillsynen av Nasdaq Clearing inledde Finansinspektionen i juni 2015 en undersökning av företaget. Finansinspektionen har även gjort en motsvarande undersökning rörande systerföretaget Nasdaq Stockholm Aktiebolag, som driver den reglerade marknaden Nasdaq Stockholm.

Undersökningen har inriktats mot hur företaget hanterar cyberrisker, det vill säga risken för att företaget utsätts för cyberattacker. Med cyberattack menas i detta beslut ett elektroniskt angrepp mot informationssystem, teknisk infrastruktur, datornätverk eller persondatorer. En cyberattack syftar vanligen till att få tillgång till, manipulera eller förstöra viss information, eller till att

åstadkomma ett driftstopp. Arbetet med att förebygga cyberattacker benämns i detta beslut cybersäkerhet. I de riskanalyser som Finansinspektionen har genomfört de senaste åren har cyberattacker mot de finansiella infrastrukturföretagen identifierats som en betydande risk, dels för att sannolikheten för attacker är hög, dels för att sådana attacker kan orsaka stor skada. En framgångsrik cyberattack mot ett infrastrukturföretag kan exempelvis leda till att handeln störs, manipuleras eller avbryts under en längre eller kortare tid. En sådan händelse skulle kunna medföra att förtroendet för de finansiella marknaderna skadas allvarligt. Syftet med undersökningen har därför varit att granska företagets riskhantering, styrning och kontroll på området.

Finansinspektionen har genomfört en skrivbordsundersökning där information har hämtats in genom frågeformulär och efterföljande begäran om ytterligare information. Denna informationsinsamling har kompletterats med två platsbesök. Det första platsbesöket fokuserade på företagets tekniska kontroller, medan det andra inriktades mot att undersöka företagets riskhantering samt styrning och kontroll.

Den 25 januari 2016 skickade Finansinspektionen en avstämningsskrivelse till Nasdaq Clearing. I skrivelsen redogjorde Finansinspektionen närmare för sina iakttagelser i undersökningen. Den 16 februari 2016 lämnade företaget ett svar på avstämningsskrivelsen.

Nasdaq Clearing har fått möjlighet att yttra sig över Finansinspektionens preliminära bedömningar om att företaget har åsidosatt sina skyldigheter. Den 7 juli 2016 kom Nasdaq Clearing in med ett yttrande till Finansinspektionen. Den 26 augusti besökte Nasdaq Clearing Finansinspektionen och lämnade uppgifter muntligen.

2 Tillämpliga bestämmelser

Centrala motparter fyller en systemviktig funktion i det finansiella systemet och därför är de organisatoriska krav som ställs på en central motpart särskilt höga. De grundläggande kraven på verksamheten framgår av Emir. Utöver det finns mer detaljerade krav i kommissionens delegerade förordning (EU) nr 153/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 med avseende på tekniska tillsynsstandarder för krav på centrala motparter (kommissionens förordning (EU) nr 153/2013). Den delegerade förordningen innehåller regler om bland annat organisationsstyrning, riskhantering, it-system och kontinuerlig verksamhet.

Genom olika bestämmelser i regelverket framgår vikten av centrala motparters självständighet och oberoende i förhållande till exempelvis tjänsteleverantörer och företag i samma koncern. I Emir finns bland annat regler om att en central motpart vid utkontraktering ska förbli fullt ansvarig för att fullgöra sina skyldigheter enligt förordningen och att utkontraktering inte får innebära

delegering av ansvar. Det finns också bestämmelser om minsta antal oberoende styrelseledamöter och om förfaranden för att se till att clearingmedlemmarnas och kundernas intressen inte åsidosätts. I kommissionens förordning (EU) nr 153/2013 finns bland annat regler om en central motparts självständighet i förhållande till en koncern som den ingår i. Centrala motparter som ingår i en koncern ska ta hänsyn till koncernens eventuella påverkan på dess organisationsstyrning, till exempel om den är tillräckligt oberoende för att kunna fullgöra sina lagstadgade skyldigheter som en separat juridisk person och om dess oberoende kan äventyras av koncernstrukturen.

För en redogörelse för tillämpliga bestämmelser, se *bilaga 2*.

3 Finansinspektionens bedömning

I detta avsnitt redogör Finansinspektionen för sina iakttagelser och bedömningar när det gäller hur Nasdaq Clearing följer vissa bestämmelser som reglerar verksamheten för centrala motparter. Det rör sig om brister i fråga om företagets utkontraktering av tjänster samt i fråga om riskhantering och planer för kontinuerlig verksamhet.

3.1 Utkontraktering

Det är tillåtet för centrala motparter att utkontraktera verksamhet, det vill säga avtala om att någon annan ska sköta en viss verksamhet, men utkontrakteringen är noggrant reglerad för att inte äventyra den centrala motpartens oberoende och systemviktiga funktion på finansmarknaden.

Av artikel 35.1 i Emir framgår det att om en central motpart utkontrakterar operativa funktioner, tjänster eller verksamheter, ska den förbli fullt ansvarig för att fullgöra samtliga skyldigheter enligt Emir. Enligt artikel 35.1 a i Emir ska den centrala motparten säkerställa att utkontrakteringen inte innebär en delegering av ansvar. Av artikel 35.1 g i Emir framgår också att den centrala motparten vid utkontraktering ska bibehålla den sakkunskap och de resurser som krävs dels för att kunna bedöma de tillhandahållna tjänsternas kvalitet samt tjänsteproducentens organisatoriska kompetens och kapitaltäckning, dels för att effektivt kunna övervaka de utkontrakterade verksamheterna och hantera de risker som utkontrakteringen är förenad med. Den centrala motparten ska också löpande övervaka dessa verksamheter och hantera dessa risker. Enligt artikel 35.1 h ska den centrala motparten ha direkt tillgång till relevanta uppgifter om de utkontrakterade verksamheterna.

I artikel 4.4 i kommissionens förordning (EU) nr 153/2013 föreskrivs att organisationsstyrningen ska garantera att en central motparts styrelse har det yttersta ansvaret och kan ställas till svars för hanteringen av den centrala motpartens risker. Styrelsen ska definiera, skatta och dokumentera den centrala motpartens lämpliga risktoleransnivå och risktålighet. Styrelsen och den högsta ledningen ska se till att den centrala motpartens riktlinjer, förfaranden och

kontroller är förenliga med dess risktolerans och risktålighet och att de anger hur den ska klarlägga, rapportera, övervaka och hantera risker.

Nasdaq Clearing har, som tidigare nämnts, utkontrakterat ett antal tjänster till koncernens moderbolag Nasdaq, Inc. Bland de utkontrakterade tjänsterna finns informationssäkerhet, inklusive cybersäkerheten.

Vid tiden för undersökningen gällde ett allmänt huvudavtal mellan parterna för samtliga tjänster som Nasdaq Clearing hade utkontrakterat till koncernens moderbolag. Avtalet innehöll dock inga utförliga beskrivningar av de aktuella tjänsterna eller fastställda överenskommelser om servicenivå, så kallade Service Level Agreements (SLA). Det fanns visserligen bilagor till huvudavtalet med kortfattade beskrivningar av tjänsterna, men inga detaljerade kvalitetsmått. Detta trots att det framgår av företagets egen policy för utkontraktering att de exakta kraven ska preciseras i SLA.[1]

Nasdaq Clearing har inte tagit emot någon kontinuerlig information eller uppföljningsstatistik som ger en samlad bild av tjänsteleveransen. Vid tiden för undersökningen gjordes inte någon löpande uppföljning av avtalet och leveransen.

Vidare har företaget inte haft tillgång till information om hotbild, personalsituation, incidenthantering, pågående projekt eller utbildning i cybersäkerhet. Det har inte heller funnits någon hotbildsinformation relaterad till Sverige eller Norden.

Av Nasdaq Clearings yttrande framgår att företaget anser att huvudavtalet redan vid tiden för undersökningen uppfyllde de legala och affärsmässiga krav som kan ställas på ett sådant avtal, förutom att en överenskommelse om servicenivå (SLA) saknades. Företaget uppger också att huvudavtalet numera har kompletterats med SLA. Vidare uppger Nasdaq Clearing att företagets tekniska chef (CTO) är ansvarig för all utkontraktering av teknologi, inklusive översyn av avtalen och uppföljning av tjänsteleveransen. Den tekniska chefen förser företagets styrelse med rapporter inom sitt ansvarsområde.

Nasdaq Clearing förklarar i sitt yttrande att företaget anser att såväl rollen som teknisk chef, som de personer som har haft rollen i företaget, har uppfyllt de krav som Emir ställer på beställarkompetens. Enligt företaget finns det därmed tillräcklig kompetens för att utvärdera de levererade tjänsterna. I sitt yttrande anger Nasdaq Clearing också att såväl företagets ledning som viktiga forum, exempelvis det så kallade Local Risk Management Forum, har fått regelbundna rapporter om uppföljning av tjänsteleveransen. Detta har gett företaget direkt tillgång till relevant information om de utkontrakterade funktionerna, anser Nasdaq Clearing. Företaget påpekar vidare att företagsledningen och styrelsen

[1] "...the precise requirements concerning the performance of the service provider should be specified and documented by a service level agreement, taking account of the objective of the outsourcing solution."

har fått uppföljande rapportering genom den årliga översynen av bland annat huvudavtalet. Nasdaq Clearing anför också i sitt yttrande att incidentrelaterad rapportering genomförs veckovis, dagligen eller när en incident inträffar, utifrån en bestämd struktur. Om incidenterna är av kritisk natur träder kontinuitets- och katastrofåterställningsplanerna i kraft och relevanta intressenter informeras.

Finansinspektionen konstaterar att Nasdaq Clearing visserligen uppger att regelbunden rapportering har skett, och att företaget för att visa detta har lämnat in en översikt över rapporteringsrutiner upprättad av företagets tekniska chef. Bland de underlag som företaget bifogat till sitt yttrande finns det emellertid inga protokoll eller annan dokumentation som visar någon faktiskt genomförd rapportering från tiden före undersökningen. Det finns inte heller något underlag som visar att styrelsen på något annat sätt har försäkrat sig om att företaget löpande har haft direkt tillgång till relevanta uppgifter om de utkontrakterade verksamheterna. Finansinspektionens bedömer därför att Nasdaq Clearing inte har uppfyllt kraven i artikel 35.1 h i Emir.

Bland de underlag som Nasdaq Clearing har bifogat till sitt yttrande finns det inte heller något som visar att företaget har genomfört dokumenterade uppföljningar av de levererade tjänsterna. Företaget har visserligen hänvisat till en presentation och ett mötesprotokoll gällande en översyn av huvudavtalet, men den översynen ägde rum efter att undersökningen inleddes. Dessutom innehåller dessa dokument inte någon egentlig uppföljning av leveransen av informationssäkerhetstjänster, utan bara en kortfattad beskrivning av tjänsterna och några nyheter i punktform från tjänsteproducenten.

Eftersom avtalet har saknat SLA för informationssäkerhetstjänsterna har det i praktiken inte heller varit möjligt för företaget att göra någon utförlig uppföljning. Finansinspektionens uppfattning är att en effektiv övervakning av de utkontrakterade verksamheterna åtminstone förutsätter regelbunden uppföljning av leveransen och av avtalet.

Undersökningen visar också att styrelsen inte har haft tillgång till någon information om hotbild och risker i samband med utkontrakteringen. Styrelsen har även i övrigt saknat tillräckliga underlag för att hantera de risker som utkontrakteringen av informationssäkerheten har medfört. Därmed har styrelsen inte heller haft förutsättningar att hantera de risker som utkontrakteringen innebär.

För att kunna bedöma de tillhandahållna tjänsternas kvalitet och övervaka de utkontrakterade verksamheterna måste den centrala motparten ha de resurser och den kompetens som krävs. Nasdaq Clearing har inte dokumenterat någon uppföljning av leveransen. Detta innebär att Nasdaq Clearing inte haft möjlighet att löpande övervaka de utkontrakterade verksamheterna eller hantera de risker som utkontrakteringen innebär. Nasdaq Clearing har därför inte uppfyllt kraven för utkontraktering i artikel 35.1 g i Emir.

De ovan nämnda bristerna, tillsammans med det faktum att företaget inte har sett till att det har funnits SLA för att möjliggöra en kritisk utvärdering av leveransen, visar enligt Finansinspektionens uppfattning att företaget i stor utsträckning har förlitat sig på tjänsteproducentens sakkunskap och kompetens.

Finansinspektionen bedömer därför att Nasdaq Clearing, vad gäller cybersäkerhet, i praktiken har delegerat sitt ansvar till tjänsteproducenten och att utläggningen därför inte har skett i enlighet med artikel 35.1 a i Emir. Företagets styrelse har därmed inte heller tagit ansvaret för hanteringen av företagets risker. Utkontrakteringen har därför även medfört att Nasdaq Clearing inte har följt artikel 4.4 i kommissionens förordning (EU) nr 153/2013.

3.2 Riskhantering

Ett av de grundläggande krav som ställs på en central motpart är att den ska ha effektiva metoder för att identifiera, hantera, övervaka och rapportera de risker som den är eller kan bli utsatt för. Detta krav framgår av artikel 26.1 i Emir.

Kravet på riskhantering preciseras i artikel 4 i kommissionens förordning (EU) nr 153/2013. Enligt artikel 4.1 ska centrala motparter ha ett sunt system för att hantera alla väsentliga risker som de är eller kan bli exponerade för. De ska fastställa dokumenterade riktlinjer, förfaranden och system för att kartlägga, mäta, övervaka och hantera sådana risker. I artikel 4.2 anges att centrala motparter ska ha en samlad och heltäckande syn på alla relevanta risker, bland annat risker som de utsätter clearingmedlemmar för eller vice versa, i möjligaste mån även kunder och andra enheter. Av artikel 4.3 framgår bland annat att den centrala motparten ska utveckla lämpliga riskhanteringsverktyg för att kunna hantera och rapportera alla relevanta risker.

Enligt artikel 4.4 ska organisationsstyrningen garantera att en central motparts styrelse har det yttersta ansvaret och kan ställas till svars för hanteringen av den centrala motpartens risker. Styrelsen ska definiera, skatta och dokumentera den centrala motpartens lämpliga risktoleransnivå och risktålighet. Styrelsen och den högsta ledningen ska se till att den centrala motpartens riktlinjer, förfaranden och kontroller är förenliga med dess risktolerans och risktålighet och att riktlinjerna anger hur den ska klarlägga, rapportera, övervaka och hantera risker.

I artikel 35.1 e i Emir anges att en utkontraktering inte får innebära att den centrala motparten berövas sina nödvändiga riskhanteringssystem och riskhanteringskontroller. I det fall en central motpart ingår i en koncern anger artikel 3.4 i kommissionens förordning (EU) nr 153/2013 att företaget ska ta hänsyn till koncernens eventuella påverkan på dess organisationsstyrning, och anger som exempel om den är tillräckligt oberoende för att kunna fullgöra sina lagstadgade skyldigheter som en separat juridisk person.

3.2.1 Brister i riskhanteringen

Som beskrivits tidigare är stora delar av verksamheten utkontrakterade inom koncernen och beslut om cybersäkerhet fattas i stor utsträckning av moderbolaget, tillika tjänsteproducenten, med informationsövervägande gjorda av globala riskhanteringsorgan. Mot den bakgrunden är det viktigt att ett lokalt riskperspektiv omhändertas och att de globala organen förses med information som är relevant både från ett lokalt perspektiv och från företagets perspektiv. Av den information som företaget lämnat i fråga om beslutsprocessen på området för cybersäkerhet framgår att det vid tiden för undersökningen inte förekom någon rapportering mellan det lokala riskhanteringsforumet och moderbolagets riskhanteringsorgan Technology Risk Committee. Därmed har det lokala riskperspektivet saknats.

Finansinspektionen konstaterar vidare att företaget har saknat ett risk-hanteringsverktyg för cyberrisker som kunnat ge företaget en samlad bild för bedömning av riskerna. Vid tiden för undersökningen fanns visserligen ett verktyg för hantering av risker, men detta omfattade inte cyberrisker. Delar av riskinformationen har funnits tillgänglig hos olika enheter inom moderbolaget. Det har dock inte funnits någon samlad bild av risker relaterade till cyber-säkerhet, sårbarheter och problem som informationssäkerhetsavdelningen och eventuellt andra enheter har kunnat ta del av.

Av Nasdaq Clearings yttrande framgår att det riskhanteringsverktyg som tidigare användes (under 2013 och 2014) tillfälligt togs ur bruk i processen för självutvärdering av risker. Enligt företaget innebar detta dock inte att riskrapportering saknades. Rapporteringen och uppföljningen gjordes i stället i kalkylprogrammet Excel inom de olika funktionerna i organisationen. Enligt företaget kommer riskhanteringsverktyget åter att tas i bruk och användas för självutvärdering av informationssäkerhetsrisker.

Det framgår av Finansinspektionens undersökning att Nasdaq Clearing inte har försäkrat sig om att företagets lokala riskperspektiv beaktas på området för cybersäkerhet. Nasdaq Clearing har inte haft en samlad hotbild för detta område och har inte haft möjlighet att producera en relevant hotbild, varken för Sverige eller Norden. Undersökningen visar också att företaget har saknat ett ändamålsenligt verktyg för att hantera och rapportera om cyberrisker. Undersökningen visar visserligen att det finns ett riskhanteringsverktyg, men det framgår också av undersökningen att detta verktyg hittills inte har använts för att hantera cyberrisker.

Finansinspektionen bedömer att företaget inte fullt ut har uppfyllt kravet på effektiva metoder för att identifiera, hantera, övervaka och rapportera risker enligt artikel 26.1 i Emir. Nasdaq Clearing har inte heller haft ett sunt system för att hantera alla väsentliga risker i enlighet med artikel 4.1 i kommissionens förordning (EU) nr 153/2013. Vidare har företaget saknat en samlad och heltäckande syn på cyberrisker och det har inte heller haft något lämpligt riskhanteringsverktyg för att kunna hantera och rapportera dessa risker. Nasdaq

Clearing har inte heller i tillräcklig utsträckning tagit hänsyn till koncernens påverkan på företagets organisationsstyrning. Det kan därför ifrågasättas om företaget är tillräckligt oberoende för att kunna fullgöra sina lagstadgade skyldigheter i fråga om riskhantering, som en separat juridisk person. Finansinspektionen bedömer att Nasdaq Clearing därmed inte heller har uppfyllt kraven i artiklarna 3.4, 4.2 och 4.3 i kommissionens förordning (EU) nr 153/2013.

3.2.2 Brister i styrelsens fastställande av risktolerans och risktålighet i fråga om cyberrisker

Det framgår av undersökningen att Nasdaq Clearings styrelse inte fattat något självständigt beslut om risktoleransnivå och risktålighet för företaget i fråga om cyberrisker. Styrelsen har inte heller haft tillgång till någon kontinuerlig rapportering om cybersäkerhet från tjänsteproducenten. Styrelsen har inte heller haft tillgång till någon egen information som har kunnat utgöra underlag för sådana beslut. Av den information som Nasdaq Clearing har lämnat framgår visserligen att styrelsen har godkänt den policy för informationssäkerhet som moderbolaget, tillika tjänsteproducenten, har upprättat för koncernen. Denna policy har enligt företaget legat till grund för en nivå på risktolerans när det gäller informationssäkerhet som godkändes av moderbolagets revisionsutskott i augusti 2015. Det har dock inte framgått att Nasdaq Clearing vid tiden för undersökningen hade fattat några självständiga beslut i fråga om risktoleransnivå och risktålighet.

Finansinspektionen kan också konstatera att Nasdaq Clearing inte har haft någon process för att koppla risktoleransnivå och risktålighet till sina finansiella överväganden.

Nasdaq Clearing uppger i sitt yttrande att företagets styrelse i maj 2016 fattade beslut om riskaptit och risktolerans.

Finansinspektionen konstaterar att styrelsen i Nasdaq Clearing vid tiden för undersökningen inte hade definierat, skattat och dokumenterat den centrala motpartens lämpliga risktoleransnivå och risktålighet i förhållande till cyberrisker. Styrelsen och den högsta ledningen har därför inte kunnat se till att företagets riktlinjer, förfaranden och kontroller är förenliga med dess risktolerans och risktålighet. Finansinspektionen bedömer därför att Nasdaq Clearing inte har uppfyllt kraven i artikel 4.4 i kommissionens förordning (EU) nr 153/2013.

En viktig del av riskkontrollen är att uppskatta vilka ekonomiska konsekvenser som följer av olika ställningstaganden i fråga om risktoleransnivå och risktålighet. Av undersökningen framgår dock att Nasdaq Clearing inte har haft någon process som kopplar beslut om risktoleransnivå och risktålighet till finansiella överväganden. Det har därför inte funnits klara regler för hur en förändrad hotbild påverkar vilka investeringar i cybersäkerhet som behövs. Koncernens riskhanteringsstrategier har därmed saknat förankring i företagets

finansiella planer, vilket kan leda till att Nasdaq Clearing inte har ekonomisk beredskap att hantera riskerna. Finansinspektionen bedömer därför att cyberrisker inte har omfattats av ett sunt system för riskhantering enligt artikel 4.1 i kommissionens förordning (EU) nr 153/2013.

3.2.3 Brister i riskhanteringen i samarbeten som innebär tekniska kontakter

Nasdaq Clearing har teknisk kontakt med ett antal parter utöver moderbolaget. Med teknisk kontakt menas sådan kontakt som innebär att företagets it-system i något avseende interagerar med den andra partens it-system, eller som på något annat sätt ger den andra parten tillträde till företagets egna it-system. Finansinspektionen noterar att det endast gentemot leverantörer har funnits krav på att inkludera villkor relaterade till cybersäkerhet i avtal. När det gäller samarbeten med andra parter som företaget har teknisk kontakt med har företaget inte haft någon insyn i cybersäkerheten och det har inte heller funnits något informationsutbyte om hot och incidenter mellan företaget och dessa parter.

Av Nasdaq Clearings yttrande framgår att koncernen arbetar för att etablera en global process för att hantera motpartsrisker relaterade till informationssäkerhet.

Finansinspektionen bedömer att avsaknaden av insyn i cybersäkerheten hos de parter som Nasdaq Clearing har teknisk kontakt med kan leda till att de risker som dessa tekniska kontakter medför inte beaktas och hanteras på ett tillfredsställande sätt. Risken finns också att företaget blir mer sårbart i förhållande till sina samarbetspartner då man inte försäkrar sig om att dessa har en fastställd standard för att hantera cyberrisker. Dessutom kan Nasdaq Clearing gå miste om värdefull hotbildsinformation.

Eftersom det inte har funnits något utbyte av information om relevanta cyberrisker mellan Nasdaq Clearing och andra parter som företaget har teknisk kontakt med, bedömer Finansinspektionen att Nasdaq Clearing i detta avseende saknar en samlad och heltäckande syn på relevanta risker och att företaget därmed inte uppfyller kraven i artikel 4.2 i kommissionens förordning (EU) nr 153/2013.

3.3 Kontinuerlig verksamhet

Av artikel 34.1 i Emir framgår att en central motpart ska etablera, genomföra och upprätthålla lämpliga riktlinjer för kontinuerlig verksamhet och en lämplig katastrofplan för att trygga verksamheten, snabbt återuppta den och fullgöra den centrala motpartens skyldigheter. En sådan plan ska åtminstone göra det möjligt att återställa alla transaktioner som de var vid tidpunkten för störningen, så att den centrala motpartens verksamhet är fortsatt säker och så att den centrala motparten kan fullfölja avvecklingen vid fastställt datum.

Enligt artikel 17.4 i kommissionens förordning (EU) nr 153/2013 ska kontinuitetsriktlinjerna och katastrofplanen säkerställa en lägsta servicenivå för kritiska funktioner. Vidare ska katastrofplanen, enligt artikel 17.5 i samma förordning, innehålla mål för återställningspunkt och återställningstid för kritiska funktioner, samt den mest lämpade återställningsstrategin för var och en av dessa funktioner. Vidare följer av artikel 17.6 att kontinuitetsriktlinjerna ska ange hur länge kritiska funktioner och system maximalt får vara ur funktion. Den maximala återställningstiden för kritiska funktioner som ska anges i riktlinjerna får inte vara längre än två timmar.

I samband med den verksamhetsanalys som ska utföras enligt artikel 18 i kommissionens förordning (EU) nr 153/2013 ska de centrala motparterna, enligt artikel 18.2, analysera hur olika scenarier påverkar riskerna för dess kritiska affärsfunktioner.

När det gäller katastrofåterställning ska centrala motparter, enligt artikel 19.1 i kommissionens förordning (EU) nr 153/2013, på grundval av olika katastrofscenarier ha arrangemang för att säkra kontinuiteten för sina kritiska funktioner. Arrangemangen ska åtminstone beröra tillgång till tillräcklig personal, maximal längd för avbrott i kritiska funktioner, omkoppling och återställning till reservplats.

Enligt vad Nasdaq Clearing har upplyst hade cyberattacker inte inkluderats i företagets scenariobaserade riskanalys vid tiden för undersökningen och företaget hade därför inte fastställt hur dessa scenarier specifikt påverkar riskerna för dess kritiska affärsfunktioner eller it-system. Det fanns inte heller några förberedelser för alternativa arrangemang eller dokumentation av testade scenarier för att säkerställa att Nasdaq Clearing skulle kunna återuppta kritiska funktioner eller it-system inom rimlig tid.

Nasdaq Clearing har inte kunnat ange hur man kommer att kunna hantera händelser som innebär att it-system har blivit attackerade eller att information har blivit manipulerad eller förvanskad. Nasdaq Clearing uppger i sitt yttrande att scenarier som inkluderar cyberattacker har varit underförstådda i företagets kontinuitetsplaner, men att inga uttalade sådana scenarier har funnits med. Nu arbetar företaget med att inkludera sådana scenarier i sina kontinuitetsplaner.

Enligt Finansinspektionens uppfattning kan scenariobaserade analyser och arrangemang inte fungera för underförstådda scenarier, eftersom varje scenario kan kräva en unik serie av åtgärder. Ett katastrofscenario som innebär att data blivit manipulerad eller förvanskad på grund av en cyberattack kan inte med säkerhet hanteras med samma arrangemang som andra katastrofscenarier.

Scenarier relaterade till cyberattacker har inte tagits med i den scenariobaserade riskanalys som ska användas enligt artikel 18.2, eller bland de katastrofscenarier som legat till grund för arrangemang för kontinuitet enligt artikel 19.1 i kommissionens förordning (EU) nr 153/2013. Nasdaq Clearing har därför saknat en tillräcklig analys och planerade åtgärder för att kunna

behålla dataautenticitet och skydda dataintegritet i situationer då informationen har blivit manipulerad eller förvanskad.

Det har därmed funnits en risk att Nasdaq Clearing inte skulle ha beredskap för att kunna återuppta kritiska funktioner inom den tid som anges i kontinuitetsriktlinjerna, i enlighet med kraven i artikel 17.6 i förordningen. Nasdaq Clearing har inte gjort någon analys av den mest lämpade strategin för återställning i fråga om cyberrelaterade scenarier så som föreskrivs i artikel 17.5 i förordningen. Sammanfattningsvis fanns det vid tiden för undersökningen inte tillräcklig beredskap för cyberattacker eller bristande dataintegritet i företagets beredskapsplanering. Finansinspektionens bedömer därför att Nasdaq Clearing inte uppfyller kraven i artiklarna 17.4–17.6, 18.2 och 19.1 i kommissionens förordning (EU) nr 153/2013.

4 Överväganden om ingripande

4.1 Tillämpliga bestämmelser

Av 1 kap. 1 § tredje stycket LV framgår vilka regler i den lagen som ska tillämpas på centrala motparters clearingverksamhet. Hit hör bland annat bestämmelserna i 25 kap. 1, 2, 6 och 8–10 §§ om ingripanden.

Enligt 25 kap. 1 § första stycket LV ska Finansinspektionen ingripa bland annat om en svensk clearingorganisation har åsidosatt sina skyldigheter enligt den lagen, andra författningar som reglerar företagets verksamhet, företagets bolagsordning, stadgar eller reglemente eller interna instruktioner som har sin grund i en författning som reglerar företagets verksamhet.

Enligt paragrafens andra stycke ska Finansinspektionen då utfärda ett föreläggande att inom en viss tid begränsa eller minska riskerna i rörelsen i något avseende, begränsa eller helt underlåta utdelning eller räntebetalningar eller vidta någon annan åtgärd för att komma till rätta med situationen, meddela ett förbud att verkställa beslut eller göra en anmärkning. Om överträdelsen är allvarlig, ska företagets tillstånd återkallas eller, om det är tillräckligt, varning meddelas.

Av 25 kap. 1 b § första stycket LV framgår att Finansinspektionen vid valet av sanktion ska ta hänsyn till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som uppstått och graden av ansvar.

Enligt 25 kap. 1 c § första stycket LV ska, utöver det som anges i 1 b §, i försvårande riktning beaktas om företaget tidigare har begått en överträdelse. Vid denna bedömning bör särskild vikt fästas vid om överträdelserna är likartade och den tid som har förflutit mellan de olika överträdelserna. Enligt andra stycket i samma paragraf ska i förmildrande riktning beaktas om

1. företaget i väsentlig mån genom ett aktivt samarbete har underlättat Finansinspektionens utredning, och
2. företaget snabbt upphört med överträdelsen, sedan den anmälts till eller påtalats av Finansinspektionen.

Enligt 25 kap. 2 § LV får Finansinspektionen avstå från ingripande enligt 1 § om en överträdelse är ringa eller ursäktlig, om företaget gör rättelse eller om något annat organ har vidtagit åtgärder mot företaget som bedöms tillräckliga.

Av 25 kap. 8 § första stycket LV framgår att om ett svenskt värdepappers-institut, en börs eller en svensk clearingorganisation har meddelats beslut om bland annat anmärkning eller varning enligt 1 § samma kapitel får Finansinspektionen besluta att företaget ska betala en sanktionsavgift.

Enligt 25 kap. 9 § första stycket LV ska sanktionsavgiften för ett svenskt värdepappersinstitut, en börs eller en svensk clearingorganisation fastställas till högst

1. tio procent av företagets omsättning närmast föregående räkenskapsår,
2. två gånger den vinst som företaget erhållit till följd av regelöverträdelsen, om beloppet går att fastställa, eller
3. två gånger de kostnader som företaget undvikit till följd av regel-överträdelsen, om beloppet går att fastställa.

Av förarbetena till bestämmelsen framgår att det är det högsta beloppet enligt de alternativa beräkningarna som utgör ett avgiftstak (prop. 2013/14:228 s. 235).

Av andra stycket samma paragraf framgår att sanktionsavgiften inte får bestämmas till ett lägre belopp än 5 000 kronor.

När sanktionsavgiftens storlek fastställs, ska enligt 25 kap. 10 § LV särskild hänsyn tas till sådana omständigheter som anges i 1 b och 1 c §§, samt till företagets finansiella ställning och, om det går att fastställa, den vinst som företaget erhållit till följd av regelöverträdelsen eller de kostnader som undvikits.

4.2 Företagets svar

I sitt yttrande anför Nasdaq Clearing bland annat följande i fråga om ett möjligt ingripande från Finansinspektionen.

Nasdaq Clearing anser att de brister som Finansinspektionen tar upp i undersökningen, betraktade mot bakgrund av Nasdaq Clearings säkerhetsnivå som helhet, komplexiteten och de snabba förändringarna på området samt den generella bristen på tydlig vägledning i lagar, föreskrifter och rekommendationer, inte har medfört betydande risker eller kan ses som systemkritiska.

Nasdaq Clearing framhåller vidare att företaget konsekvent har genomfört förbättringar för att rätta till brister. Från det att Finansinspektionen inledde sin undersökning har Nasdaq Clearing tagit myndighetens observationer och preliminära bedömningar på stort allvar, och företaget inledde omedelbart sitt arbete med att stärka och förbättra cybersäkerheten. Sedan i februari 2016 har Nasdaq Clearing arbetat utifrån en åtgärdsplan för att förbättra cybersäkerheten inom organisationen. Åtgärdsplanen är kopplad till de iakttagelser som Finansinspektionen har gjort i sin undersökning och innehåller bland annat status för varje åtgärdspunkt. Den kommer att godkännas av styrelsen och behandlas kvartalsvis i styrelsen framöver. Nasdaq Clearing påpekar också att förbättringsarbetet även omfattar områden där företaget i och för sig anser sig uppfylla de legala kraven, eftersom företaget strävar efter att uppfylla de krav som Finansinspektionen anser gäller.

Vidare påpekar Nasdaq Clearing att företaget har samarbetat med Finansinspektionen till exempel genom att ledningen har deltagit i möten med kort varsel, genom att frågor har besvarats snabbt och genom att platsbesök med personal från Nasdaq, Inc. närvarande har ordnats på begäran. Företaget menar att det på så vis har underlättat Finansinspektionens utredning.

Företaget uppger också att det har strävat efter att följa reglerna fullt ut inom ett område som är komplext på ett legalt plan, med ett regelverk som vilar på generella bestämmelser. Bristen på detaljerade bestämmelser har gjort att en av företagets utmaningar har varit risken att feltolka tillämpliga regler. Dessutom ändras själva definitionen av cybersäkerhet kontinuerligt. Företaget ber därför Finansinspektionen ta hänsyn till att reglerna om cybersäkerhet, som företaget ser det, är ”ett rörligt mål” inom ett område i snabb förändring. De brister som myndigheten har funnit bör tolkas i ljuset av denna utveckling, anser Nasdaq Clearing och tillägger att det inte har varit helt förutsebart för företaget hur de aktuella reglerna ska tillämpas och tolkas eller vilken måttstock som ska gälla.

Slutligen påpekar Nasdaq Clearing att bristerna inte har orsakat någon skada på företagets egna system, dess verksamhet eller några andra parter och att de inte heller har medfört någon risk för effekter på det finansiella systemet.

4.3 Bedömning av överträdelserna och val av ingripande

Bristande insyn i handeln med OTC-derivat och förekomsten av stora motpartsrisker som inte hade åtgärdats med tillräckliga säkerheter, i kombination med en stor koncentration av risker, anses ha bidragit till att förstärka finanskrisen under hösten 2008. Genom införandet av Emir reglerades handeln med derivat bland annat på så sätt att alla standardiserade OTC-derivat ska clearas via en central motpart. Den centrala motpartens uppgift är att träda in mellan parter som tecknar ett OTC-kontrakt och vara ”köpare till varje säljare och säljare till varje köpare” och därmed garantera villkoren i affären även om en av de ursprungliga avtalsparterna inte uppfyller sina åtaganden. Den centrala motparten minskar därmed bland annat de

operativa, legala och marknadsmässiga riskerna för avtalsparterna i affären. Syftet med regleringen har varit att öka transparensen och kontrollen av risker med handeln med derivatkontrakt.

Bestämmelserna i Emir syftar bland annat till att samla, överblicka och kontrollera motpartsrisker, och därför är också de krav som ställs på en central motparts hantering och kontroll av risker mycket höga. Eftersom det finns lagkrav på central motpartsclearing för OTC-derivat fyller den centrala motparten också en kritisk funktion för de finansiella marknaderna. Den centrala motparten anses därför vara ett systemviktigt företag.

Detta innebär att de organisatoriska krav som ställs på en central motpart är särskilt höga. Genom ett antal olika bestämmelser i regelverket framgår vikten av centrala motparters självständighet och oberoende i förhållande till exempelvis leverantörer och ägare. Den rika förekomsten av regler som syftar till att säkerställa centrala motparters självständighet och oberoende visar att kraven på en central motparts oberoende i förhållande till exempelvis en koncern som den ingår i är mycket höga. Det är med denna utgångspunkt som Finansinspektionen har gjort sin bedömning av överträdelserna i det här ärendet.

Finansinspektionens undersökning visar att Nasdaq Clearing inte i alla delar har uppfyllt de krav som ställs på en central motpart enligt Emir och enligt kommissionens förordning (EU) nr 153/2013.

Vid utkontrakteringen av tjänster har företaget inte försäkrat sig om den styrning och kontroll, och inte heller haft tillgång till den information, som krävs för att företagets styrelse ska kunna ta fullt ansvar för verksamheten. Styrning, kontroll och ansvar har i stället till stor del i praktiken överlåtits till företagets moderbolag, Nasdaq, Inc. När det gäller Nasdaq Clearing anser Finansinspektionen att det inte har varit företagets styrelse som har utövat den egentliga styrningen och kontrollen i företaget. Finansinspektionen bedömer att detta är en betydande brist. Dessutom fanns det vid tiden för undersökningen brister i Nasdaq Clearings riskhantering och riskkontroll.

Bristerna har varit sådana att Finansinspektionen bedömer att det finns skäl att ingripa mot Nasdaq Clearing, i enlighet med 25 kap. 1 § LV. Företagets överträdelser kan inte betraktas som ringa och det har inte heller framkommit några skäl för att överträdelserna ska anses som ursäktliga. Bristerna har dock inte varit så allvarliga att det är aktuellt att återkalla företagets tillstånd. Finansinspektionen ger därför Nasdaq Clearing en anmärkning.

När ett företag har fått en anmärkning får Finansinspektionen, enligt 25 kap. 8 § LV, besluta att företaget också ska betala en sanktionsavgift. Finansinspektionen bedömer att Nasdaq Clearings överträdelser har varit sådana att anmärkningen ska förenas med en sanktionsavgift.

Finansinspektionen konstaterar att det inte går att fastställa i vilken mån företaget har gjort någon vinst eller undvikit någon kostnad till följd av överträdelserna. Avgiften som Nasdaq Clearing ska betala ska därför bestämmas till högst tio procent av företagets omsättning närmast föregående räkenskapsår, i enlighet med 25 kap. 9 § första stycket 1 LV. Nasdaq Clearings omsättning närmast föregående år uppgick till cirka 637 miljoner kronor och Finansinspektionen kan därför bestämma sanktionsavgiften till högst 63,7 miljoner kronor. Sanktionsavgiften får inte bestämmas till ett lägre belopp än 5 000 kronor.

Bestämmelsen om hur hög sanktionsavgiften får vara fick sin nuvarande utformning i samband med att kapitaltäckningsdirektivet[2] genomfördes i svensk rätt (se prop. 2013/14:228 s. 235 ff.). Av skäl 36 till kapitaltäckningsdirektivet framgår att sanktionsavgifterna ska kunna uppnå en nivå som är stor nog att balansera eventuella fördelar som en överträdelse genererat och vara stora nog att avskräcka även större institut från att begå överträdelser.

Sanktionsavgiften ska ses som en gradering av överträdelserna. Med hänsyn till innehållet i skäl 36 till kapitaltäckningsdirektivet anser Finansinspektionen att en utgångspunkt för denna gradering bör vara hur stor den högsta möjliga sanktionsavgiften kan vara, snarare än till vilket belopp denna avgift bestäms. Detta innebär att sanktionsavgifterna för två företag som har överträtt regelverket på likartade sätt inte behöver bestämmas till samma belopp, om taket för sanktionsavgifterna skiljer sig åt, till exempel på grund av att företagen har olika stora omsättningar.

När sanktionsavgiftens storlek fastställs ska hänsyn tas till hur allvarlig överträdelsen är och hur länge den har pågått. Särskild hänsyn ska tas till överträdelsens art, överträdelsens konkreta och potentiella effekter på det finansiella systemet, skador som har uppstått och graden av ansvar. Finansinspektionen konstaterar att överträdelserna inte har gett upphov till några skador eller konkreta effekter, men bedömer att de potentiella effekterna på det finansiella systemet och på förtroendet för finansmarknaden har varit omfattande. Centrala motparters kritiska betydelse för handeln med derivat har betydelse när sanktionsavgiftens storlek ska bestämmas. Detta beror på de stora potentiella effekter som överträdelser av det aktuella slaget kan ha på det finansiella systemet. Å andra sidan ska Finansinspektionen i förmildrande riktning beakta om företaget i väsentlig mån, genom ett aktivt samarbete, har underlättat Finansinspektionens utredning, och om företaget snabbt har upphört med överträdelsen sedan den anmälts till eller påtalats av Finansinspektionen.

Nasdaq Clearing har presenterat en omfattande plan för att åtgärda många av de brister som har identifierats. Finansinspektionen bedömer att denna åtgärdsplan, tillsammans med förbättringar som företaget redan har genomfört,

[2] Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG.

gör att förutsättningarna är goda för att företaget ska kunna avhjälpa de identifierade bristerna i kontinuitetsplaneringen och flera av bristerna i företagets riskarbete. Detta bör i viss utsträckning beaktas som en förmildrande omständighet. Däremot bedömer Finansinspektionen att Nasdaq Clearings förändringsarbete inte i tillräcklig utsträckning har inriktats på att tydliggöra företagets oberoende i förhållande till koncernen.

Nasdaq Clearing har i sitt yttrande också anfört att företaget har underlättat undersökningen genom att samarbeta med Finansinspektionen. Som framgått ska Finansinspektionen i förmildrande riktning beakta om företaget i väsentlig mån, genom ett aktivt samarbete, har underlättat utredningen. Enligt förarbetena (prop. 2013/14:228 s. 241) förutsätter detta att företaget självmant för fram viktig information som Finansinspektionen inte själv redan förfogar över eller med lätthet kan få fram. Enligt Finansinspektionens uppfattning har företagets samarbete emellertid inte varit mer aktivt än vad som rimligen förväntas av ett företag under tillsyn. Det bör därför inte ses som en förmildrande omständighet.

Efter en samlad bedömning av de omständigheter som Finansinspektionen ska ta hänsyn till när sanktionsavgiften fastställs, beslutar Finansinspektionen att Nasdaq Clearing ska betala en sanktionsavgift på 25 miljoner kronor.

Sanktionsavgiften tillfaller staten och faktureras av Finansinspektionen när beslutet har vunnit laga kraft.

FINANSINSPEKTIONEN

Sven-Erik Österberg
Styrelseordförande

Carl Sehlin
Jurist

Beslut i detta ärende har fattats av Finansinspektionens styrelse (Sven-Erik Österberg, ordförande, Maria Bredberg Pettersson, Sonja Daltung, Marianne Eliason, Anders Kvist, Astri Muren, Hans Nyman och Gustaf Sjöberg) efter föredragning av juristen Carl Sehlin. I den slutliga handläggningen har också den seniora rådgivaren Per Håkansson, områdeschefen Sophie Degenne, avdelningschefen Marie Jesperson, enhetschefen Charlotta Tajthy samt den seniora juristen Denny Sternad deltagit.

Bilagor
Bilaga 1 – Hur man överklagar
Bilaga 2 – Tillämpliga bestämmelser

Kopia: Nasdaq Clearing Aktiebolags verkställande direktör

Bilaga 1

Hur man överklagar

Om ni anser att beslutet är felaktigt kan ni överklaga det genom att skriva till förvaltningsrätten. Ställ överklagandet till Förvaltningsrätten i Stockholm, men skicka eller lämna det till Finansinspektionen, Box 7821, 103 97 Stockholm.

Ange följande i överklagandet:

- Namn och adress
- Vilket beslut ni överklagar och ärendets nummer
- Varför ni anser att beslutet är felaktigt
- Vilken ändring ni vill ha och varför ni anser att beslutet ska ändras.

Kom ihåg att underteckna skrivelsen.

Överklagandet ska ha kommit in till Finansinspektionen inom tre veckor från den dag ni fått ta del av beslutet.

Finansinspektionen skickar överklagandet vidare till Förvaltningsrätten i Stockholm, om det kommit in i tid och Finansinspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Bilaga 2

Tillämpliga bestämmelser

Europaparlaments och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (Emir)

Organisatoriska krav

Enligt artikel 26.1 i Emir ska en central motpart ha stabila styrformer som omfattar en tydlig organisationsstruktur med en väldefinierad, transparent och konsekvent ansvarsfördelning, effektiva metoder för att identifiera, hantera, övervaka och rapportera de risker som denna motpart är eller kan bli utsatt för samt ha tillfredsställande rutiner för intern kontroll, däribland sunda förfaranden för administration och redovisning.

Kontinuerlig verksamhet

Av artikel 34.1 framgår att en central motpart ska etablera, genomföra och upprätthålla lämpliga riktlinjer för kontinuerlig verksamhet och en lämplig katastrofplan för att trygga verksamheten, snabbt återuppta den och fullgöra den centrala motpartens skyldigheter. En sådan plan ska åtminstone göra det möjligt att återställa alla transaktioner som de var vid tidpunkten för störningen, så att den centrala motpartens verksamhet är fortsatt säker och den kan fullfölja avvecklingen vid fastställt datum.

Utkontraktering

Av artikel 35.1 framgår bland annat att om en central motpart utkontrakterar operativa funktioner, tjänster eller verksamheter, ska den förbli fullt ansvarig för fullgörandet av samtliga skyldigheter enligt Emir.

Enligt artikel 35.1 a får utkontraktering inte innebära delegering av ansvar.

Av artikel 35.1 g framgår att den centrala motparten vid utkontraktering ska säkerställa att den bibehåller den sakkunskap och de resurser som krävs för att kunna bedöma tillhandahållna tjänsters kvalitet, tjänsteproducentens organisatoriska kompetens och kapitaltäckning och för att effektivt kunna övervaka de utkontrakterade verksamheterna och hantera de risker som utkontrakteringen är förenad med samt löpande övervaka dessa verksamheter och hantera dessa risker.

Enligt artikel 35.1 h ska den centrala motparten ha direkt tillgång till relevanta uppgifter om de utkontrakterade verksamheterna.

Bilaga 2

Kommissionens delegerade förordning (EU) nr 153/2013 av den 19 december 2012 om komplettering av Europaparlamentets och rådets förordning (EU) nr 648/2012 med avseende på tekniska tillsynsstandarder för krav på centrala motparter (kommissionens förordning nr (EU) nr 153/2013)

Organisationsstyrning

Enligt artikel 3.4 kommissionens förordning (EU) nr 153/2013 ska centrala motparter som ingår i en koncern ta hänsyn till koncernens eventuella påverkan på dess organisationsstyrning, till exempel om den är tillräckligt oberoende för att kunna fullgöra sina lagstadgade skyldigheter som en separat juridisk person och om dess oberoende kan äventyras av koncernstrukturen och av att styrelseledamöter även sitter i styrelsen för andra enheter inom samma koncern. Sådana centrala motparter ska framför allt överväga att införa särskilda förfaranden för att förhindra och hantera intressekonflikter, till exempel i samband med utkontraktering.

Riskhantering och interna kontrollmekanismer

Av artikel 4.1 framgår att centrala motparter ska ha ett sunt system för att hantera alla väsentliga risker som de är eller kan bli exponerade mot. Centrala motparter ska fastställa dokumenterade riktlinjer, förfaranden och system för att kartlägga, mäta, övervaka och hantera sådana risker. När centrala motparter fastställer riktlinjer, förfaranden och system för riskhantering, ska de utformas så att clearingmedlemmar hanterar och begränsar de risker som de utgör för dessa centrala motparter på rätt sätt.

I artikel 4.2 anges att centrala motparter ska ha en samlad och heltäckande syn på alla relevanta risker. Det handlar om risker som de utsätter clearingmedlemmar för eller vice versa, i möjligaste mån även kunder och andra enheter, till exempel men inte bara centrala motparter med vilka det finns en samverkansöverenskommelse, värdepappersavvecklings- och betalningssystem, avvecklingsbanker, likviditetsförsörjare, värdepapperscentraler, handelsplatser som används av den centrala motparten och andra kritiska tjänsteleverantörer.

Av artikel 4.3 kommissionens förordning (EU) nr 153/2013 framgår bland annat att den centrala motparten ska utveckla lämpliga riskhanteringsverktyg för att kunna hantera och rapportera alla relevanta risker.

Enligt artikel 4.4 ska organisationsstyrningen garantera att en central motparts styrelse har det yttersta ansvaret och kan ställas till svars för hanteringen av den centrala motpartens risker. Styrelsen ska definiera, skatta och dokumentera den centrala motpartens lämpliga risktoleransnivå och risktålighet. Styrelsen och den högsta ledningen ska se till att den centrala motpartens riktlinjer, förfaranden och kontroller är förenliga med dess risktolerans och risktålighet och att de anger hur den ska klarlägga, rapportera, övervaka och hantera risker.

Kontinuerlig verksamhet

Enligt artikel 17.4 ska kontinuitetsriktlinjerna och katastrofplanen säkerställa en lägsta servicenivå för kritiska funktioner.

I artikel 17.5 anges att katastrofplanen ska innehålla mål för återställningspunkt och återställningstid för kritiska funktioner, samt den mest lämpade återställningsstrategin för var och en av dessa funktioner. Dessa arrangemang ska syfta till att kritiska funktioner i extrema scenarier kan slutföras i tid och på ett sätt som uppnår avtalad servicenivå.

Av artikel 17.6 framgår att kontinuitetsriktlinjerna ska ange hur länge kritiska funktioner och system maximalt får vara ur funktion. Den maximala återställningstiden för kritiska funktioner som ska anges i riktlinjerna får inte vara längre än två timmar. Förfaranden och betalningar vid dagens slut ska under alla omständigheter fullföljas på utsatt tid och dag.

Enligt artikel 18.2 ska centrala motparter använda en scenariobaserad riskanalys som syftar till att fastställa hur olika scenarier påverkar riskerna för dess kritiska affärsfunktioner.

Av artikel 19.1 framgår att centrala motparter på grundval av olika katastrofscenarier ska ha arrangemang för att säkra deras kritiska funktioners kontinuitet. Arrangemangen ska åtminstone beröra tillgång till tillräcklig personal, maximal längd för avbrott i kritiska funktioner, omkoppling och återställning till reservplats.

SVERIGES DOMSTOLAR

Hur man överklagar

FR-03

Vill du att beslutet ska ändras i någon del kan du överklaga. Här får du veta hur det går till.

Överklaga skriftligt inom 3 veckor

Tiden räknas oftast från den dag som du fick del av det skriftliga beslutet. I vissa fall räknas tiden i stället från beslutets datum. Det gäller om beslutet avkunnades vid en muntlig förhandling, eller om rätten vid förhandlingen gav besked om datum för beslutet.

För en part som företräder det allmänna (till exempel myndigheter) räknas tiden alltid från den dag domstolen meddelade beslutet.

Observera att överklagandet måste ha kommit in till domstolen när tiden går ut.

Vilken dag går tiden ut?
Sista dagen för överklagande är samma veckodag som tiden börjar räknas. Om du exempelvis fick del av beslutet måndagen den 2 mars går tiden ut måndagen den 23 mars.

Om sista dagen infaller på en lördag, söndag eller helgdag, midsommarafton, julafton eller nyårsafton, räcker det att överklagandet kommer in nästa vardag.

Så här gör du

1. Skriv förvaltningsrättens namn och målnummer.
2. Förklara varför du tycker att beslutet ska ändras. Tala om vilken ändring du vill ha och varför du tycker att kammarrätten ska ta upp ditt överklagande (läs mer om prövningstillstånd längre ner).
3. Tala om vilka bevis du vill hänvisa till. Förklara vad du vill visa med varje bevis. Skicka med skriftliga bevis som inte redan finns i målet.
4. Lämna namn och personnummer eller organisationsnummer.

   Lämna aktuella och fullständiga uppgifter om var domstolen kan nå dig: postadresser, e-postadresser och telefonnummer.

   Om du har ett ombud, lämna också ombudets kontaktuppgifter.
5. Skicka eller lämna in överklagandet till förvaltningsrätten. Du hittar adressen i beslutet.

Vad händer sedan?

Förvaltningsrätten kontrollerar att överklagandet kommit in i rätt tid. Har det kommit in för sent avvisar domstolen överklagandet. Det innebär att beslutet gäller.

Om överklagandet kommit in i tid, skickar förvaltningsrätten överklagandet och alla handlingar i målet vidare till kammarrätten.

Har du tidigare fått brev genom förenklad delgivning kan även kammarrätten skicka brev på detta sätt.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05

Prövningstillstånd i kammarrätten

När överklagandet kommer in till kammarrätten tar domstolen först ställning till om målet ska tas upp till prövning.

Kammarrätten ger prövningstillstånd i fyra olika fall.

- Domstolen bedömer att det finns anledning att tvivla på att förvaltningsrätten dömt rätt.
- Domstolen anser att det inte går att bedöma om förvaltningsrätten dömt rätt utan att ta upp målet.
- Domstolen behöver ta upp målet för att ge andra domstolar vägledning i rättstillämpningen.
- Domstolen bedömer att det finns synnerliga skäl att ta upp målet av någon annan anledning.

Om du *inte* får prövningstillstånd gäller det överklagade beslutet. Därför är det viktigt att i överklagandet ta med allt du vill föra fram.

Vill du veta mer?

Ta kontakt med förvaltningsrätten om du har frågor. Adress och telefonnummer hittar du på första sidan i beslutet.

Mer information finns på www.domstol.se.

Anvisningar för överklagande **FR-03 – Överklagandetid 3 v - PT** • Producerat av Domstolsverket, Avd. för domstolsutveckling • 2020-05