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 informationsöverväganden 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 kapitaltäcknings-direktivet 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

D E L G I V N I N G S K V I T T O

FI Dnr 15-9258
Delgivning nr 1

**Finansinspektionen**
Box 7821
SE-103 97 Stockholm
[Brunnsgatan 3]
Tel +46 8 787 80 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

## Anmärkning och sanktionsavgift

### Handling:

Beslut avseende anmärkning och sanktionsavgift till Nasdaq Clearing Aktiebolag meddelat **den 13 december 2016**

Jag har denna dag tagit del av handlingen.

DATUM

NAMNTECKNING

NAMNFÖRTYDLIGANDE

EV. NY ADRESS

Detta kvitto ska sändas tillbaka till Finansinspektionen **omgående**. Om kvittot inte skickas tillbaka kan delgivning ske på annat sätt, t.ex. genom stämningsman.

Om du använder det bifogade kuvertet är återsändandet gratis.

Glöm inte att **ange datum** för mottagandet.

**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.

***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.