I

(Beslutninger og resolutioner, henstillinger og udtalelser)

HENSTILLINGER

DET EUROPÆISKE UDVALG FOR SYSTEMISKE RISICI

DET EUROPÆISKE UDVALG FOR SYSTEMISKE RISICIS HENSTILLING

af 2. december 2021

om en paneuropæisk ramme for relevante myndigheders koordinering i tilfælde af systemiske cyberhændelser

(ESRB/2021/17)

(2022/C 134/01)

DET ALMINDELIGE RÅD FOR DET EUROPÆISKE UDVALG FOR SYSTEMISKE RISICI HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til aftalen om Det Europæiske Økonomiske Samarbejdsområde ([1]), særlig bilag IX,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) nr. 1092/2010 af 24. november 2010 om makrotilsyn på EU-plan med det finansielle system og om oprettelse af et europæisk udvalg for systemiske risici ([2]), særlig artikel 3, stk. 2, litra b), og d) og artikel 16 og 18,

under henvisning til Det Europæiske Udvalg for Systemiske Risicis afgørelse ESRB/2011/1 af 20. januar 2011 om vedtagelse af forretningsordenen for Det Europæiske Udvalg for Systemiske Risici ([3]), særlig artikel 18 til 20, og

ud fra følgende betragtninger:

(1) Som det fremgår af fjerde betragtning til Det Europæiske Udvalg for Systemiske Risicis henstilling ESRB/2013/1 ([4]), er det endelige mål med den makroprudentielle politik at bidrage til at sikre hele det finansielle systems stabilitet, herunder ved at styrke det finansielle systems modstandsdygtighed og mindske opbygningen af systemiske risici, for herved at sikre, at den finansielle sektor yder et holdbart bidrag til den økonomiske vækst. Det Europæiske Udvalg for Systemiske Risici (ESRB) har ansvaret for makrotilsynet med det finansielle system i EU. ESRB bør ved opfyldelsen af sit mandat bidrage til at forebygge og reducere systemiske risici for den finansielle stabilitet, herunder risici i forbindelse med cyberhændelser, og fremsætte forslag til, hvorledes disse risici kan begrænses.

(2) Større cyberhændelser kan udgøre en systemisk risiko for det finansielle system som følge af deres potentiale til at forstyrre kritiske finansielle tjenester og operationer. Et første stød vil kunne blive forstærket gennem afsmittende operationelle eller finansielle effekter eller ved, at tilliden til det finansielle system undermineres. Er det finansielle system ikke i stand til at absorbere disse stød, vil den finansielle stabilitet være i fare, og en sådan situation vil kunne medføre en systemisk cyberkrise ([5]).

([1]) EFT L 1 af 3.1.1994, s. 3.
([2]) EUT L 331 af 15.12.2010, s. 1.
([3]) EUT C 58 af 24.2.2011, s. 4.
([4]) Det Europæiske Udvalg for Systemiske Risicis henstilling ESRB/2013/1 af 4. april 2013 om delmål og instrumenter for den makroprudentielle politik (EUT C 170 af 15.6.2013, s. 1).
([5]) Se publikationen Systemic cyber risk, ESRB, februar 2020, som findes på ESRB's websted www.esrb.europa.eu

(3) De stadig mere avancerede cybertrusler og den seneste tids stigning i antallet af større cyberhændelser er tegn på større risici for den finansielle stabilitet i Unionen. Covid-19-pandemien har understreget, hvor vigtig en rolle teknologien spiller i driften af det finansielle system. Myndigheder og institutioner har været nødt til at tilpasse deres tekniske infrastruktur og risikostyringsrammer til en pludselig stigning i antallet af medarbejdere, der arbejdede hjemmefra, hvilket har øget det finansielle systems samlede eksponering mod cybertrusler og givet kriminelle mulighed for både at udtænke nye fremgangsmåder og at tilpasse sig til de eksisterende for at udnytte situationen ([6]). På den baggrund steg antallet af cyberhændelser, som blev indberettet til ECB Banktilsyn i 2020, med 54 % set i forhold til 2019 ([7]).

(4) Omfanget og den hastighed, hvormed en større cyberhændelse kan forplante sig, kræver en effektiv indsats fra de relevante myndigheder for at afbøde de potentielle negative effekter for den finansielle stabilitet. Hurtig koordinering og kommunikation mellem relevante myndigheder på EU-plan vil kunne bidrage til at vurdere en større cyberhændelses indvirkning på den finansielle stabilitet på et tidligt tidspunkt, bevare tilliden til det finansielle system og begrænse de afsmittende effekter på andre finansielle institutioner og dermed bidrage til at forhindre, at en større cyberhændelse kommer til at udgøre en risiko for den finansielle stabilitet.

(5) Det underliggende stød har sine rødder i en ny type situation, som adskiller sig fra de traditionelle finans- og likviditetskriser, som myndighederne normalt står over for. Ud over de finansielle aspekter skal den overordnede risikovurdering omfatte driftsforstyrrelsernes omfang og indvirkning, da disse faktorer kan have betydning for valget af makroprudentielle værktøjer. På samme måde kan den finansielle stabilitet også påvirke cybereksperternes valg af foranstaltninger til modvirkning af driftsforstyrrelserne. Dette kræver en tæt og hurtig koordination samt åben kommunikation for bl.a. at øge situationsbevidstheden.

(6) Risikoen for manglende koordination blandt myndighederne er til stede og kræver handling. Det er nødvendigt, at relevante myndigheder i Unionen koordinerer indbyrdes og med andre myndigheder såsom Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) (tidligere Den Europæiske Unions Agentur for Net- og Informationssikkerhed), som de normalt måske ikke samarbejder med. Da et betydeligt antal finansielle institutioner i Unionen har aktiviteter på globalt plan, vil en større cyberhændelse sandsynligvis ikke begrænse sig til Unionen, eller den kan blive udløst uden for Unionen og kræve en globalt koordineret indsats.

(7) Det er nødvendigt, at myndighederne er forberedt på et sådant samarbejde. Ellers kan de risikere at træffe inkonsekvente foranstaltninger, der er i modstrid med eller bringer andre myndigheders reaktioner i fare. En sådan mangel på koordination vil kunne forstærke stødet for det finansielle system, idet det kan underminere tilliden til det finansielle systems funktion, hvilket – i værste fald – vil kunne udgøre en risiko for den finansielle stabilitet ([8]). Det er derfor påkrævet at træffe de nødvendige foranstaltninger for at imødegå den risiko, som manglende koordinering vil kunne medføre for den finansielle stabilitet i tilfælde af en større cyberhændelse.

(8) ESRB's rapport fra 2021 *Mitigating systemic cyber risk* ([9]) fastslår, at der er behov for at fastlægge en paneuropæisk ramme for relevante myndigheder i EU's koordinering i tilfælde af systemiske cyberhændelser (herefter »EU-SCICF«). Målet med rammen vil være at øge de relevante myndigheders beredskabsniveau for at fremme en koordineret reaktion på en potentiel større cyberhændelse. ESRB's rapport fra 2021 *Mitigating systemic cyber risk* indeholder ESRB's vurdering af, hvorledes rammen skal se ud – prima facie – for at imødegå risikoen for manglende koordinering.

(9) Hovedformålet med denne henstilling er at bygge videre på en af de roller, som de europæiske tilsynsmyndigheder (European Supervisory Authorities, ESA) tillægges i forslaget til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor ([10]) (herefter »DORA-forordningen«), og som tager sigte på gradvist at muliggøre en effektiv koordineret indsats på EU-plan i tilfælde af en større grænseoverskridende informations- og kommunikationsteknologirelateret hændelse (herefter »IKT-relateret hændelse«) eller dermed forbundet trussel, som har systemiske virkninger for Unionens finansielle sektor som helhed. Denne proces vil føre til, at der skabes en paneuropæisk ramme for relevante myndigheders koordinering i tilfælde af systemiske cyberhændelser (EU-SCICF).

([6]) Se Internet Organised Crime Threat Assessment, Europol, 2020, som findes på Europols websted www.europol.europa.eu
([7]) Se IT and cyber risk: a constant challenge, ECB, 2021, som findes på ECB Banktilsyns websted www.bankingsupervision.europa.eu
([8]) Se publikationen Systemic cyber risk, ESRB, februar 2020, som findes på ESRB's websted www.esrb.europa.eu
([9]) Se Mitigating systemic cyber risk, ESRB, 2021, (kommer snart).
([10]) COM(2020) 595 final.

(10) Hensigten med EU-SCICF er ikke, at den skal erstatte de eksisterende rammer, men bygge bro over koordinations- og kommunikationshuller indbyrdes mellem de relevante myndigheder og i forhold til andre myndigheder i Unionen og andre centrale aktører på internationalt plan. I den forbindelse bør det overvejes, hvor i landskabet af de eksisterende rammer til håndtering af finansielle kriser og cyberhændelser i Unionen den nye koordineringsramme skal placeres. Hvad angår koordineringen indbyrdes mellem de relevante myndigheder, bør der tages hensyn til faktorer som, men ikke begrænset til, de roller og aktiviteter, som samarbejdsgruppen inden for net- og informationssystemer (Network and Information Systems (NIS) Cooperation Group for financial entities) (herefter »NIS-samarbejdsgruppen«) tillægges i henhold til Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 ([11]) og de koordineringsmekanismer, der forventes oprettet gennem etableringen af den fælles cyberenhed sideløbende med inddragelsen af ENISA.

(11) Navnlig har forslaget om at iværksætte forberedelserne til EU-SCICF til formål at understøtte den potentielle rolle, som ESA'erne tillægges i henhold til DORA-forslaget. I henhold til forslaget til DORA-forordningen kan »ESA'erne [...] via det fælles Udvalg og i samarbejde med de kompetente myndigheder, ECB og ESRB indføre mekanismer, der gør det muligt at udveksle effektive fremgangsmåder på tværs af finansielle sektorer for at forbedre situationskendskabet og identificere fælles cybersårbarheder og risici på tværs af sektorer« og »udvikle simuleringsøvelser for krisestyring og beredskab, der omfatter cyberangrebsscenarier, med henblik på at udvikle kommunikationskanaler og gradvist muliggøre en effektiv koordineret indsats på EU-plan i tilfælde af en større grænseoverskridende IKT-relateret hændelse eller dermed forbundet trussel, som har systemiske virkninger for Unionens finansielle sektor som helhed« ([12]). En paneuropæisk koordineringsramme som EU-SCICF findes endnu ikke og bør etableres og udvikles inden for rammerne af DORA.

(12) I lyset af den risiko, som cyberrisici udgør for den finansielle stabilitet i Unionen, bør det forberedende arbejde til en gradvis etablering af EU-SCICF påbegyndes allerede nu, i det omfang det er muligt, før de nødvendige retlige og politiske rammer for etableringen af den er fuldt ud fastlagt. Den retlige og politiske ramme vil være fuldt ud fastlagt og vedtaget, så snart de relevante bestemmelser i DORA-forordningen og dens delegerede retsakter finder anvendelse.

(13) Effektiv kommunikation bidrager til at skabe situationsbevidsthed blandt relevante myndigheder og er således en absolut nødvendig forudsætning for koordination på EU-plan under større cyberhændelser. I den forbindelse bør kommunikationsinfrastrukturen, som er nødvendig for at koordinere reaktionen på en større cyberhændelse, defineres. Dette omfatter bl.a. at specificere typen af informationer, der skal deles, hvilke kanaler der skal anvendes til at dele sådanne informationer, og de kontaktpunkter, som informationerne skal deles med. Udvekslingen af informationer skal respektere de eksisterende lovkrav. Endvidere kan det være nødvendigt, at de relevante myndigheder fastsætter en klar handlingsplan og de protokoller, der skal følges, for at sikre en korrekt koordinering mellem de myndigheder, der deltager i planlægningen af en koordineret indsats som reaktion på en større cyberhændelse.

(14) En systemisk cyberhændelse vil kræve, at der iværksættes et fuldt samarbejde på nationalt plan og EU-plan. Det kan derfor være nyttigt at udpege kontaktpunkterne for ESA'erne, ECB og de enkelte medlemsstater blandt deres relevante nationale myndigheder, som ESA'erne skal informeres om, for at fastlægge de primære samtalepartnere i koordineringsordningen under EU-SCICF, som skal informeres i tilfælde af en større cyberhændelse. Behovet for at udpege kontaktpunkter bør vurderes under udviklingen af EU-SCICF under hensyntagen til det centrale kontaktpunkt, som medlemsstaterne har udpeget for sikkerheden i net- og informationssystemer i henhold til direktiv (EU) 2016/1148 for at sikre et grænseoverskridende samarbejde med andre medlemsstater og NIS-samarbejdsgruppen ([13]).

(15) Afholdelsen af simuleringsøvelser for krisestyring og beredskab vil kunne fremme gennemførelsen af EU-SCICF og gøre det muligt for myndighederne at vurdere deres parathed og beredskab i tilfælde af en systemisk cyberkrise på EU-plan. Sådanne øvelser vil give myndighederne et erfaringsgrundlag og gøre det muligt løbende at forbedre og udvikle EU-SCICF.

([11]) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

([12]) Jf. udkastet til artikel 43 i forslaget til DORA-forordningen.

([13]) Se Europa-Kommissionen, NIS-samarbejdsgruppen, som findes på Europa-Kommissionens websted ec.europa.eu

(16) For at udvikle EU-SCICF er det af afgørende vigtighed, at ESA'erne i fællesskab udfører relevant forberedende arbejde med henblik på at vurdere, hvilke vigtige elementer rammen skal indeholde og hvilke ressourcer og behov, der er nødvendige for at videreudvikle den. Herefter kunne ESA'erne foretage en foreløbig analyse af, om der er eventuelle hindringer for, at ESA'erne og de relevante myndigheder kan oprette en sådan ramme og dele relevante informationer gennem kommunikationskanaler i tilfælde af en større cyberhændelse. En sådan analyse vil være et vigtigt skridt som informationsgrundlag for yderligere foranstaltninger, det være sig af lovgivningsmæssig karakter eller andre støtteinitiativer, som Europa-Kommissionen måtte iværksætte, efter at DORA-forordningen er blevet gennemført —

VEDTAGET DENNE HENSTILLING:

AFSNIT 1

HENSTILLINGER

Henstilling A – Oprettelse af en paneuropæisk ramme for koordinering i tilfælde af systemiske cyberhændelser (EU-SCICF)

1. I overensstemmelse med Kommissionens forslag til Europarlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor (herefter »DORA«) henstilles det, at de europæiske tilsynsmyndigheder (ESA'erne) i fællesskab via Det Fælles Udvalg og i samarbejde med Den Europæiske Centralbank (ECB), Det Europæiske Udvalg for Systemiske Risici (ESRB) og relevante nationale myndigheder begynder at forberede sig på den gradvise udvikling af en effektiv koordineret indsats på EU-plan i tilfælde af en større grænseoverskridende cyberhændelse eller dermed forbundet trussel, som kan have systemiske virkninger for Unionens finansielle sektor. Det forberedende arbejde hen imod en koordineret indsats på EU-plan bør omfatte den gradvise udvikling af en paneuropæisk ramme for koordinering i tilfælde af systemiske cyberhændelser (EU-SCICF) for ESA'erne, ECB, ESRB og relevante nationale myndigheder. Arbejdet bør også omfatte en vurdering af, hvilke ressourcer der kræves for at kunne udvikle EU-SCICF effektivt.

2. Det henstilles, at ESA'erne i lyset af delhenstilling A(1) og i samråd med ECB og ESRB kortlægger og efterfølgende analyserer, hvilke aktuelle hindringer og hvilke retlige og andre operationelle barrierer der er for en effektiv udvikling af EU-SCICF.

Henstilling B – Udpegning af kontaktpunkter i EU-SCICF

Det henstilles, at ESA'erne, ECB og de enkelte medlemsstater blandt deres relevante nationale myndigheder udpeger et primært kontaktpunkt og informerer ESA'erne om dette. Denne liste over kontaktpunkter vil gøre det nemmere at udvikle rammen, og på det tidspunkt hvor EU-SCICF er på plads, er det disse kontaktpunkter og ESRB, der skal informeres i tilfælde af en større cyberhændelse. Der bør også ske en koordinering mellem EU-SCICF og det centrale kontaktpunkt, som medlemsstaterne har udpeget for sikkerheden i net- og informationssystemer i henhold til direktiv (EU) 2016/1148 for at sikre et grænseoverskridende samarbejde med andre medlemsstater og NIS-samarbejdsgruppen.

Henstilling C – Passende foranstaltninger på EU-plan

Det henstilles, at Kommissionen på grundlag af resultaterne af den analyse, der foretages i overensstemmelse med henstilling A, vurderer, hvilke foranstaltninger der er nødvendige for at sikre en effektiv koordineret indsats i tilfælde af systemiske cyberhændelser.

AFSNIT 2

GENNEMFØRELSE

1. **Definitioner**

I denne henstilling gælder følgende definitioner:

a) »cyber«: vedrørende, i eller gennem et medie i form af den indbyrdes forbundne informationsinfrastruktur af interaktioner mellem mennesker, processer, data og informationssystemer ([14])

([14]) Se Cyber Lexicon, FSB, 12. november 2018, som findes på FSB's websted www.fsb.org

b) »større cyberhændelse«: en IKT-relateret hændelse med en potentielt stor negativ indvirkning på net- og informationssystemer, som understøtter kritiske funktioner i finansielle enheder ([15])

c) »systemisk cyberkrise«: en større cyberhændelse, der forårsager så omfattende en forstyrrelse i Unionens finansielle system, at den kan have alvorlige negative konsekvenser for det indre markeds smidige funktion og realøkonomiens funktion. En sådan krise kan opstå som følge af en større cyberhændelse, der forårsager stød i en række kanaler, herunder operationelle, tillidsmæssige og finansielle

d) »de europæiske tilsynsmyndigheder« (European Supervisory Authorities) eller »ESA'erne«: Den Europæiske Banktilsynsmyndighed (European Banking Authority), som blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 ([16]), sammen med Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger (European Insurance and Occupational Pensions Authority), som blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 ([17]) og Den Europæiske Værdipapir- og Markedstilsynsmyndighed (European Securities and Markets Authority), som blev oprettet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 ([18])

e) »Det Fælles Udvalg« (Joint Committee): Det Fælles Udvalg af Europæiske Tilsynsmyndigheder, som blev nedsat ved artikel 54 i forordning (EU) nr. 1093/2010, forordning (EU) nr. 1094/2010 og forordning (EU) nr. 1095/2010

f) »relevant national myndighed«:

1. en kompetent myndighed eller tilsynsmyndighed i en medlemsstat som omhandlet i de EU-retsakter, hvortil der henvises i artikel 1, stk. 2, i forordning (EU) nr. 1093/2010, forordning (EU) nr. 1094/2010 og forordning (EU) nr. 1095/2010, og alle andre kompetente nationale myndigheder som omhandlet i EU-retsakter, der overdrager opgaver til ESA'erne

2. en kompetent myndighed i en medlemsstat udpeget i overensstemmelse med:

i. Artikel 4 i Europa-Parlamentets og Rådets direktiv 2013/36/EU ([19]) uden at berøre de specifikke opgaver, der er overdraget til ECB i henhold til Rådets forordning (EU) nr. 1024/2013 ([20])

ii. Artikel 22 i Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 ([21])

iii. Artikel 37 i Europa-Parlamentets og Rådets direktiv 2009/110/EF ([22])

iv. Artikel 4 i Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 ([23])

([15]) Jf. udkastet til artikel 3, punkt 7, i forslaget til DORA-forordningen.

([16]) Europa-Parlamentets og Rådets forordning (EU) nr. 1093/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Banktilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/78/EF (EUT L 331 af 15.12.2010, s. 12).

([17]) Europa-Parlamentets og Rådets forordning (EU) nr. 1094/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Tilsynsmyndighed for Forsikrings- og Arbejdsmarkedspensionsordninger), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/79/EF (EUT L 331 af 15.12.2010, s. 48).

([18]) Europa-Parlamentets og Rådets forordning (EU) nr. 1095/2010 af 24. november 2010 om oprettelse af en europæisk tilsynsmyndighed (Den Europæiske Værdipapir- og Markedstilsynsmyndighed), om ændring af afgørelse nr. 716/2009/EF og om ophævelse af Kommissionens afgørelse 2009/77/EF (EUT L 331 af 15.12.2010, s. 84).

([19]) Europa-Parlamentets og Rådets direktiv 2013/36/EU af 26. juni 2013 om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF (EUT L 176 af 27.6.2013, s. 338).

([20]) Rådets forordning (EU) nr. 1024/2013 af 15. oktober 2013 om overdragelse af specifikke opgaver til Den Europæiske Centralbank i forbindelse med politikker vedrørende tilsyn med kreditinstitutter (EUT L 287 af 29.10.2013, s. 63).

([21]) Europa-Parlamentets og Rådets direktiv (EU) 2015/2366 af 25. november 2015 om betalingstjenester i det indre marked, og om ændring af direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om ophævelse af direktiv 2007/64/EF (EUT L 337 af 23.12.2015, s. 35).

([22]) Europa-Parlamentet og Rådets direktiv 2009/110/EF af 16. september 2009 om adgang til at optage og udøve virksomhed som udsteder af elektroniske penge og tilsyn med en sådan virksomhed, ændring af direktiv 2005/60/EF og 2006/48/EF og ophævelse af direktiv 2000/46/EF (EUT L 267 af 10.10.2009, s. 7).

([23]) Europa-Parlamentets og Rådets direktiv (EU) 2019/2034 af 27. november 2019 om tilsyn med investeringsselskaber og om ændring af direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU (EUT L 314 af 5.12.2019, s. 64).

v. Artikel 3, stk. 1, litra ee), første led, i forslaget til Europa-Parlamentets og Rådets forordning om markeder for kryptoaktiver og om ændring af direktiv (EU) 2019/1937 ([24])

vi. Artikel 11 i Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 ([25])

vii. Artikel 22 i Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 ([26])

viii. artikel 67 i Europa-Parlamentets og Rådets direktiv 2014/65/EU ([27])

ix. Artikel 22 i forordning (EU) nr. 648/2012

x. Artikel 44 i Europa-Parlamentets og Rådets direktiv 2011/61/EU ([28])

xi. Artikel 97 i Europa-Parlamentets og Rådets direktiv 2009/65/EF ([29])

xii. Artikel 30 i Europa-Parlamentets og Rådets direktiv 2009/138/EF ([30])

xiii. Artikel 12 i Europa-Parlamentets og Rådets direktiv (EU) 2016/97 ([31])

xiv. Artikel 47 i Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 ([32])

xv. Artikel 22 i Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 ([33])

xvi. Artikel 3, stk. 2, og artikel 32 i Europa-Parlamentets og Rådets direktiv 2006/43/EF ([34])

xvii. Artikel 40 i Europa-Parlamentets og Rådets forordning (EU) nr. 2016/1011 ([35])

xviii. Artikel 29 i Europa-Parlamentets og Rådets forordning (EU) nr. 2020/1503 ([36])

([24]) COM/2020/593 final.

([25]) Europa-Parlamentets og Rådets forordning (EU) nr. 909/2014 af 23. juli 2014 om forbedring af værdipapirafviklingen i Den Europæiske Union og om værdipapircentraler samt om ændring af direktiv 98/26/EF og 2014/65/EU samt forordning (EU) nr. 236/2012 (EUT L 257 af 28.8.2014, s. 1).

([26]) Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 af 4. juli 2012 om OTC-derivater, centrale modparter og transaktionsregistre (EUT L 201 af 27.7.2012, s. 1).

([27]) Europa-Parlamentets og Rådets direktiv 2014/65/EU af 15. maj 2014 om markeder for finansielle instrumenter og om ændring af direktiv 2002/92/EF og direktiv 2011/61 (EUT L 173 af 12.6.2014, s. 349).

([28]) Europa-Parlamentets og Rådets direktiv 2011/61/EU af 8. juni 2011 om forvaltere af alternative investeringsfonde og om ændring af direktiv 2003/41/EF og 2009/65/EF samt forordning (EF) nr.1060/2009 og (EU) nr. 1095/2010 (EUT L 174 af 1.7.2011, s. 1).

([29]) Europa-Parlamentets og Rådets direktiv 2009/65/EF af 13. juli 2009 om samordning af love og administrative bestemmelser om visse institutter for kollektiv investering i værdipapirer (investeringsinstitutter) (EFT L 302 af 17.11.2009, s. 32).

([30]) Europa-Parlamentets og Rådets direktiv 2009/138/EF af 25. november 2009 om adgang til og udøvelse af forsikrings- og genforsikringsvirksomhed (Solvens II) (EUT L 335 af 17.12.2009, s. 1).

([31]) Europa-Parlamentets og Rådets direktiv (EU) 2016/97 af 20. januar 2016 om forsikringsdistribution (EUT L 26 af 2.2.2016, s. 19).

([32]) Europa-Parlamentets og Rådets direktiv (EU) 2016/2341 af 14. december 2016 om arbejdsmarkedsrelaterede pensionskassers (IORP'ers) aktiviteter og tilsynet hermed (EUT L 354 af 23.12.2016, s. 37).

([33]) Europa-Parlamentets og Rådets forordning (EF) nr. 1060/2009 af 16. september 2009 om kreditvurderingsbureauer (EUT L 302 af 17.11.2009, s. 1).).

([34]) Europa-Parlamentets og Rådets direktiv 2006/43/EF af 17. maj 2006 om lovpligtig revision af årsregnskaber og konsoliderede regnskaber, om ændring af Rådets direktiv 78/660/EØF og 83/349/EØF og om ophævelse af Rådets direktiv 84/253/EØF (EUT L 157 af 9.6.2006, s. 87).

([35]) Europa-Parlamentets og Rådets forordning (EU) 2016/1011 af 8. juni 2016 om indeks, der bruges som benchmarks i finansielle instrumenter og finansielle kontrakter eller med henblik på at måle investeringsfondes økonomiske resultater, og om ændring af direktiv 2008/48/EF og 2014/17/EU samt forordning (EU) nr. 596/2014 (EUT L 171 af 29.6.2016, s. 1).

([36]) Europa-Parlamentets og Rådets forordning (EU) 2020/1503 af 7. oktober 2020 om europæiske crowdfundingtjenesteudbydere for erhvervslivet og om ændring af forordning (EU) 2017/1129 og direktiv (EU) 2019/1937 (EUT L 347 af 20.10.2020, s. 1).

3. en myndighed, der har til opgave at vedtage og/eller aktivere makroprudentielle politiske foranstaltninger eller andre opgaver med hensyn til finansiel stabilitet såsom opgaver vedrørende understøttende analyser, herunder, men ikke begrænset til, følgende:

   i. en udpeget myndighed i henhold til kapitel 4, afsnit VII, i direktiv 2013/36/EU eller artikel 458, stk. 1, i forordning (EU) nr. 575/2013 Europa-Parlamentets og Rådets ([37])

   ii. en makroprudentiel myndighed med de mål, ordninger, beføjelser, instrumenter, ansvarlighedskrav og andre egenskaber, som er fastsat i Det Europæiske Udvalg for Systemiske Risicis henstilling ESRB/2011/3 ([38])

g) »relevant myndighed«:

   1. en ESA

   2. ECB, for så vidt angår de opgaver, som er overdraget til ECB i henhold til artikel 4, stk. 1 og 2, og artikel 5, stk. 2, i forordning (EU) nr. 1024/2013

   3. en relevant national myndighed.

2. **Kriterier for gennemførelse**

Følgende kriterier gælder for gennemførelsen af denne henstilling:

a) der bør tages behørigt hensyn til nødvendighedsprincippet og proportionalitetsprincippet henset til målet og indholdet af hver enkelt henstilling

b) de specifikke overholdelseskriterier, der er fastsat i bilaget hvad angår hver enkelt henstilling, bør opfyldes.

3. **Tidsfrister for opfølgning**

I henhold til artikel 17, stk. 1, i forordning (EU) nr. 1092/2010 skal adressaterne meddele Europa-Parlamentet, Rådet, Kommissionen og ESRB hvilke handlinger, de har foretaget som svar på denne henstilling, eller begrunde eventuel manglende handling. Adressaterne skal fremsende disse oplysninger i overensstemmelse med følgende tidsfrister:

1. Henstilling A

   a) Senest 30. juni 2023, men tidligst seks måneder efter DORA-forordningens ikrafttrædelse, skal ESA'erne fremlægge en midtvejsrapport om gennemførelsen af delhenstilling A(1) for Europa-Parlamentet, Rådet, Kommissionen og ESRB.

   b) Senest 30. juni 2024, men tidligst 18 måneder efter DORA-forordningens ikrafttrædelse, skal ESA'erne fremlægge en endelig rapport om gennemførelsen af delhenstilling A(1) for Europa-Parlamentet, Rådet, Kommissionen og ESRB.

   c) Senest 30. juni 2025, men tidligst 30 måneder efter DORA-forordningens ikrafttrædelse, skal ESA'erne fremlægge en rapport om gennemførelsen af delhenstilling A(2) for Europa-Parlamentet, Rådet, Kommissionen og ESRB.

2. Henstilling B

   Senest 30. juni 2023, men tidligst seks måneder efter DORA-forordningens ikrafttrædelse, skal ESA'erne, ECB og medlemsstaterne fremlægge en rapport om gennemførelsen af henstilling B for Europa-Parlamentet, Rådet, Kommissionen og ESRB.

3. Henstilling C

   a) Senest 31. december 2023, men tidligst 12 måneder efter DORA-forordningens ikrafttrædelse, skal Kommissionen fremlægge en rapport om gennemførelsen af henstilling C i lyset af ESA'ernes midtvejsrapport i overensstemmelse med delhenstilling A(1) for Europa-Parlamentet, Rådet og ESRB.

([37]) Europa-Parlamentets og Rådets forordning (EU) nr. 575/2013 af 26. juni 2013 om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012 (EUT L 176 af 27.6.2013, s. 1).

([38]) Det Europæiske Udvalg for Systemiske Risicis henstilling ESRB/2011/3 af 22. december 2011 om de nationale myndigheders makroprudentielle mandat (EUT C 41 af 14.2.2012, s. 1).

b) Senest 31. december 2025, men tidligst 36 måneder efter DORA-forordningens ikrafttrædelse, skal Kommissionen fremlægge en rapport om gennemførelsen af henstilling C i lyset af ESA'ernes rapport i overensstemmelse med henstilling A for Europa-Parlamentet, Rådet og ESRB.

4. **Overvågning og vurdering**

1. ESRB's sekretariat:

a) bistår adressaterne ved at fremme en koordineret rapportering, udarbejde relevante skemaer og, om nødvendigt, ved at give en detaljeret beskrivelse af procedurerne og tidsfristerne for opfølgning,

b) kontrollerer adressaternes opfølgning, bistår dem på anmodning og aflægger rapport om opfølgningen til Det Almindelige Råd. Vurderingerne vil blive foretaget som følger:

i) inden for 12 måneder efter DORA-forordningens ikrafttrædelse for så vidt angår gennemførelsen af henstilling A og B

ii) inden for 18 måneder efter DORA-forordningens ikrafttrædelse for så vidt angår gennemførelsen af henstilling C

iii) inden for 24 måneder efter DORA-forordningens ikrafttrædelse for så vidt angår gennemførelsen af henstilling A

iv) inden for 36 måneder efter DORA-forordningens ikrafttrædelse for så vidt angår gennemførelsen af henstilling A

v) inden for 42 måneder efter DORA-forordningens ikrafttrædelse for så vidt angår gennemførelsen af henstilling C.

2. Det Almindelige Råd vurderer de foranstaltninger og begrundelser, som adressaterne har meddelt, og træffer, i givet fald, afgørelse med hensyn til, om denne henstilling ikke er blevet fulgt, og om en adressat ikke har givet en tilfredsstillende begrundelse for at have undladt at gennemføre foranstaltninger.

Udfærdiget i Frankfurt am Main, den 2. december 2021.

Leder af ESRB's sekretariat,
på vegne af ESRB's Almindelige Råd
Francesco MAZZAFERRO

BILAG

PRÆCISERING AF DE OVERHOLDELSESKRITERIER, DER GÆLDER FOR HENSTILLINGERNE

Henstilling A – Oprettelse af en paneuropæisk ramme for koordinering i tilfælde af systemiske cyberhændelser (EU-SCICF)

For delhenstilling A(1) gælder følgende overholdelseskriterier.

1. I forbindelse med forberedelsen af en effektiv koordineret indsats på EU-plan, som bør omfatte den gradvise udvikling af EU-SCICF ved at udøve de beføjelser, som forventes at følge af Europa-Parlamentets og Rådets fremtidige forordning om digital operationel modstandsdygtighed i den finansielle sektor (herefter »DORA«), bør de europæiske tilsynsmyndigheder (ESA'erne), der handler via Det Fælles Udvalg, og i samarbejde med Den Europæiske Centralbank (ECB), Det Europæiske Udvalg for Systemiske Risici (ESRB) og relevante nationale myndigheder og i samråd med Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) (tidligere Den Europæiske Unions Agentur for Net- og Informationssikkerhed) og Kommissionen, hvis det anses for nødvendigt, som minimum overveje at inddrage følgende aspekter i forberedelsen af EU-SCICF:

   a. foretage en analyse af, hvilke ressourcer der kræves for at kunne udvikle EU-SCICF effektivt

   b. udvikle simuleringsøvelser for krisestyring og beredskab, der omfatter cyberangrebsscenarier, med henblik på at udvikle kommunikationskanaler

   c. udvikle et fælles glossar

   d. udvikle en logisk sammenhængende klassifikation af cyberhændelser

   e. oprette sikre og pålidelige kanaler til informationsudveksling, herunder backupsystemer

   f. oprette kontaktpunkter

   g. adressere fortrolighedsspørgsmål i forbindelse med informationsudveksling

   h. tage initiativer til samarbejde og informationsudveksling med cyber-efterretningstjenester i den finansielle sektor

   i. udvikle effektive aktiverings- og eskaleringsprocesser gennem situationsbevidsthed

   j. præcisere, hvilket ansvar der påhviler deltagerne i rammen

   k. udvikle grænseflader til koordinering på tværs af sektorer og, hvor det er relevant, med tredjelande

   l. sikre, at de relevante myndigheder kommunikerer med offentligheden på en sammenhængende måde for at bevare tilliden

   m. oprette forud fastlagte kommunikationslinjer for at sikre rettidig kommunikation

   n. gennemføre passende test af rammen, herunder test på tværs af jurisdiktioner og koordinering med tredjelande, og foretage vurderinger, der kan danne erfaringsgrundlag og bidrage til at udvikle rammen

   o. sikre effektiv kommunikation og modforanstaltninger i tilfælde af misinformation.

Henstilling B – Udpegning af kontaktpunkter i EU-SCICF

For henstilling B gælder følgende overholdelseskriterier.

1. ESA'erne, ECB og de enkelte medlemsstater blandt deres relevante national myndigheder bør indgå en aftale om en fælles tilgang til deling og opdatering af listen over udpegede kontaktpunkter i EU-SCICF.

2. Udpegningen af kontaktpunktet bør vurderes under hensyntagen til det centrale kontaktpunkt, som medlemsstaterne har udpeget for sikkerheden i net- og informationssystemer i henhold til direktiv (EU) 2016/1148 for at sikre et grænseoverskridende samarbejde med andre medlemsstater og NIS-samarbejdsgruppen.

Henstilling C – Ændringer af EU's retlige ramme

For henstilling C gælder følgende overholdelseskriterier.

Kommissionen bør overveje, hvorvidt der er behov for foranstaltninger, herunder ændringer af den relevante EU-lovgivning, som konsekvens af den analyse, der er udført i overensstemmelse med henstilling A, for at sikre, at ESA'erne, via Det Fælles Udvalg og sammen med ECB, ESRB og relevante nationale myndigheder, kan udvikle EU-SCICF i overensstemmelse med delhenstilling A(1), og for at sikre, at ESA'erne, ECB, ESRB og de relevante myndigheder, såvel som andre myndigheder, kan deltage i koordinerende tiltag og udveksle informationer, der er tilstrækkeligt detaljerede og konsistente til at støtte en effektiv koordineringsramme (EU-SCICF).