DEN EUROPÆISKE CENTRALBANKS UDTALELSE

af 11. april 2022

om forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Indledning og retsgrundlag

Den 16. december 2020 vedtog Europa-Kommissionen et forslag til Europa-Parlamentets og Rådets direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148 ([1]) (herefter »direktivforslaget«). Den 3. december 2021 nåede Rådet for Den Europæiske Union til enighed om den generelle indstilling til direktivforslaget ([2]). Den Europæiske Centralbanks (ECB) kompetence til at afgive udtalelsen er baseret på artikel 127, stk. 4, andet underafsnit, i traktaten om Den Europæiske Unions funktionsmåde, da direktivforslaget indeholder bestemmelser, som henhører under ECB's kompetenceområder, navnlig fremme af betalingssystemernes smidige funktion, bidrag til en smidig gennemførelse af de kompetente myndigheders politikker vedrørende det finansielle markedssystems stabilitet og ECB's opgaver vedrørende tilsyn med kreditinstitutter i henhold til traktatens artikel 127, stk. 2, fjerde led, artikel 127, stk. 5, og artikel 127, stk. 6. I overensstemmelse med artikel 17.5, første punktum, i forretningsordenen for Den Europæiske Centralbank er denne udtalelse vedtaget af ECB's Styrelsesråd.

Generelle bemærkninger

ECB støtter kraftigt målene i direktivforslaget om at øge cyberrobustheden på tværs af alle relevante sektorer, mindske uoverensstemmelser på tværs af det indre marked og forbedre situationsbevidstheden og den kollektive kapacitet til at forberede sig og reagere ved at sikre et effektivt samarbejde i Unionen.

ECB anerkender betydningen af at opretholde stærke forbindelser mellem direktivforslaget og den finansielle sektor, som fortsat bør være en del af økosystemet for net- og informationssystemer (NIS) for at fremme en konsekvent vurdering af risici i forbindelse med informations- og kommunikationsteknologi (IKT) i hele Unionen og fremme effektiv tværsektoriel informationsudveksling og tværsektorielt samarbejde i forbindelse med håndtering af cybertrusler. Med henblik herpå bør det være muligt for de kompetente myndigheder i henhold til forslaget til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor ([3]) (herefter »DORA«) at deltage i de strategiske politiske drøftelser og det tekniske arbejde i NIS-samarbejdsgruppen samt at udveksle oplysninger og samarbejde yderligere med de centrale kontaktpunkter og de nationale enheder, der håndterer it-sikkerhedshændelser (computersikkherhedsberedskabsteams), som der henvises til i direktivforslaget ([4]).

1. Direktivforslagets anvendelsesområde

1.1 ECB forstår det således, at DORA, for så vidt angår enheder i den finansielle sektor, vil blive betragtet som sektorspecifik lovgivning, som indfører krav til styring af cybersikkerhedsrisici og indberetning af hændelser, der som minimum har samme virkning som dem, der er fastsat i det direktivforslaget ([5]). Derfor vil direktivforslagets bestemmelser, der vedrører risikostyring i forbindelse med cybersikkerhed, indberetningsforpligtelser, informationsudveksling samt tilsyn og håndhævelse, ikke finde anvendelse på finansielle enheder, som er omfattet af DORA ([6]). Som præciseret i direktivforslagets betragtninger bør de bestemmelser i DORA, der vedrører IKT-risikostyringsforan-

([1]) COM(2020) 823 final.
([2]) Findes på Rådets websted www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Se bemærkning 1.5 i Den Europæiske Centralbanks udtalelse af 4. juni 2021 om et forslag til Europa-Parlamentets og Rådets forordning om digital operationel modstandsdygtighed i den finansielle sektor (CON/2021/20) (EUT C 343 af 26.8.2021, s. 1). Alle ECB's udtalelser er offentliggjort i EUR-Lex. Artikel 17, stk. 5, og artikel 42 i DORA, artikel 11 i direktivforslaget.
([5]) Artikel 2, stk. 6, i direktivforslaget.
([6]) Betragtning 13 og artikel 2, stk. 6), i direktivforslaget.

staltninger, håndtering af IKT-relaterede hændelser og indberetning af hændelser, afprøvning af digital operationel modstandsdygtighed, informationsudvekslingsordninger og IKT-tredjepartsrisici, finde anvendelse i stedet for direktivforslagets bestemmelser ([7]).

1.2 ECB bemærker også, at Rådet i sin generelle indstilling til direktivforslaget fremsætter en ændring for at udelukke »enheder, der udøver aktiviteter inden for retsvæsenet, parlamenter eller centralbanker« ([8]), fra direktivforslagets anvendelsesområde. ECB forstår det således, at den forslåede ændring vil omfatte alle Det Europæiske System af Centralbankers (ESCB) grundlæggende opgaver og kompetencer, jf. traktatens artikel 127, stk. 2, og artikel 3.1 i statutten for Det Europæiske System af Centralbanker og Den Europæiske Centralbank (herefter »ESCB-statutten«), såsom fremme af betalingssystemernes smidige funktion. I den forbindelse anses Eurosystem-ejede og -drevne finansielle markedsinfrastrukturer såsom TARGET2 og TARGET2-Securities for at være omfattet af Rådets forslag om at udelukke centralbanker fra direktivforslagets anvendelsesområde.

2. **ESCB's og Eurosystemets overvågningskompetencer**

2.1 Parallelt med ESCB's primære mål om at fastholde prisstabilitet og i overensstemmelse med traktatens artikel 127, stk. 2, er en af de grundlæggende opgaver, der skal udføres gennem ESCB, at fremme betalingssystemernes smidige funktion ([9]). Med henblik på at sikre effektive og pålidelige clearing- og betalingssystemer inden for Unionen og over for tredjelande kan ECB og de nationale centralbanker tilbyde faciliteter, og ECB kan udstede forordninger, for at udføre denne grundlæggende opgave ([10]). Under udøvelse af overvågningsrollen vedtog ECB forordning (EU) nr. 795/2014 (ECB/2014/28) ([11]) (herefter »forordningen om systemisk vigtige betalingssystemer«), som omsætter CPSS-IOSCO-principperne for finansielle markedsinfrastrukturer ([12]) til umiddelbart gældende lovgivning. Forordningen om systemisk vigtige betalingssystemer fastsætter krav til både betalingssystemer for store betalinger og detailbetalingssystemer af systemisk betydning, uanset om de er offentlige eller privatejede. Kravene i forordningen om systemisk vigtige betalingssystemer omfatter allerede bl.a. operationel risikostyring og etablering af en ramme for cyberrobusthed ([13]).

2.2 Ud over systemisk vigtige betalingssystemer dækker Eurosystemets overvågning ikke-systemisk vigtige betalingssystemer, elektroniske betalingsinstrumenter, -ordninger og -arrangementer samt andre infrastrukturer og kritiske tjenesteudbydere, som dette er fastsat i Eurosystemets overvågningsrammer ([14]). Betalingssystemer og andre ordninger, der er underlagt Eurosystemets overvågning, er ikke udtrykkeligt omfattet af direktivforslagets anvendelsesområde ([15]). Da direktivforslaget er et instrument til minimumsharmonisering ([16]), kan medlemsstaternes gennemførelse af lovgivning dog med tiden overlappe Eurosystemets overvågningskompetence. For at undgå dette bør ESCB's beføjelser i henhold til traktaten og ESCB-statutten samt Eurosystemets kompetencer i henhold til forordningen om systemisk vigtige betalingssystemer og generelt inden for rammerne af Eurosystemets overvågningsrammer udtrykkeligt anerkendes i direktivforslagets betragtninger.

([7]) Betragtning 13 til direktivforslaget.
([8]) Artikel 2, stk. 3a, første underafsnit, litra b), i Rådets generelle indstilling til direktivforslaget.
([9]) Traktaten om Den Europæiske Unions funktionsmåde, artikel 127, stk. 2, som afspejlet i ESCB-statuttens artikel 3.1.
([10]) ESCB-statuttens artikel 22.
([11]) Den Europæiske Centralbanks forordning (EU) nr. 795/2014 af 3. juli 2014 om overvågningskrav for systemisk vigtige betalingssystemer (ECB/2014/28) (EUT L 217 af 23.7.2014, s. 16).
([12]) Jf. komitéen for betalings- og afviklingssystemer (CPSS) og Den Internationale Børstilsynsorganisations (IOSCO) Tekniske Komités anbefalinger »Principles for Financial Market Infrastructures« af april 2012, som findes på Den Internationale Betalingsbanks websted www.bis.org. Af Responsibility D deraf fremgår det, at »alle CPSS-medlemmer og IOSCO-medlemmer forventes at anvende principperne på de relevante finansielle markedsinfrastrukturer i deres jurisdiktion i det omfang, det er tilladt i henhold til de retlige rammer i deres jurisdiktion«.
([13]) Artikel 15 i forordning (EU) nr. 795/2014 (ECB/2014/28).
([14]) Eurosystemets overvågningsramme, revideret udgave (juli 2016), som findes på ECB's websted www.ecb.europa.eu
([15]) Artikel 2 samt bilag I og II i direktivforslaget.
([16]) Artikel 3 i direktivforslaget.

3. **IKT-tredjepartsrisiko, håndtering af væsentlige hændelser og kriser, informationsudveksling og national cybersikkerhedsstrategi**

3.1 *Styring af IKT-tredjepartsrisiko*

3.1.1 Når de kompetente myndigheder udøver deres håndhævelsesbeføjelser i forhold til væsentlige enheder, giver direktivforslaget giver dem beføjelse til at udstede bindende instrukser eller et påbud om, at disse enheder skal afhjælpe de konstaterede mangler eller afhjælpe overtrædelserne af direktivforslagets forpligtelser ([17]). Samtidig kan den »ledende tilsynsførende«, der er udpeget i henhold til DORA, rette henstillinger til kritiske tredjepartsudbydere af IKT-tjenester med henblik på at styre de potentielle systemiske risici, der er forbundet med anvendelse af outsourcing og IKT-tredjepartskoncentration ([18]).

3.1.2 I betragtning af at en væsentlig enhed i henhold til det foreslåede direktiv også kan udpeges som en kritisk tredjepartsudbyder af IKT-tjenester i henhold til DORA, understreger ECB ([19]), at det bør undgås at udstede modstridende henstillinger og bindende instrukser. I den forbindelse hilser ECB Rådets generelle indstilling til direktivforslaget velkommen. Ifølge indstillingen skal de kompetente myndigheder underrette det »tilsynsforum«, der er oprettet i henhold til DORA, når de udøver deres tilsyns- og håndhævelsesbeføjelser over for en væsentlig enhed, der er udpeget som værende en kritisk tredjepartsudbyder af IKT-tjenester i henhold til DORA ([20]).

3.2 *Håndtering af væsentlige hændelser og kriser*

3.2.1 I overensstemmelse med direktivforslaget ([21]) skal medlemsstaterne udpege en eller flere kompetente myndigheder med ansvar for håndtering af væsentlige hændelser og kriser. Som det præciseres i direktivforslagets betragtninger, bør en væsentlig hændelse forstås som en hændelse med en betydelig indvirkning på mindst to medlemsstater, eller hvis afbrydelse overstiger en medlemsstats kapacitet til at reagere på den. Væsentlige hændelser kan blive til fuldgyldige kriser, hvilket forstyrrer det indre markeds funktion ([22]).

3.2.2 Selvom de kompetente myndigheder, der er udpeget i henhold til DORA, fortsat er ansvarlige for håndteringen af cybersikkerhedshændelser vedrørende finansielle enheder, vil samarbejde med de strukturer og myndigheder, der er oprettet i henhold til direktivforslaget, være afgørende for at sikre en koordineret indsats i hele Unionen. Med henblik herpå ser ECB gerne, at de kompetente myndigheder, der er udpeget i henhold til DORA, herunder ECB, deltager i European Cyber Crises Liaison Organization Network (EU-CyCLONe) ([23]), når væsentlige cybersikkerhedshændelser og -kriser påvirker den finansielle sektor.

3.3 *Informationsudveksling*

3.3.1 Som anført ovenfor støtter ECB kraftigt samarbejdet mellem de kompetente myndigheder, der er udpeget i henhold til DORA, med de strukturer og myndigheder, der er oprettet i henhold til direktivforslaget. Informationsudveksling mellem myndigheder kan navnlig muliggøre tværsektoriel læring, bidrage til forebyggelse og effektiv håndtering af cyberangreb samt fremme en konsekvent vurdering af IKT-relaterede risici i hele Unionen. Ikke desto mindre understreger ECB, at informationsudveksling bør finde sted, hvor der er klart fastlagte klassificerings- og informationsudvekslingsmekanismer kombineret med passende sikkerhedsforanstaltninger til at sikre fortrolighed ([24]). ECB glæder sig over Rådets generelle indstilling til direktivforslaget, som fremlægger regelmæssig udveksling af relevante

([17]) Artikel 29, stk. 4, litra b, i direktivforslaget.
([18]) Artikel 31 i DORA.
([19]) Afsnit 1.2 i udtalelse CON/2021/20.
([20]) Artikel 29, stk. 10, i Rådets generelle indstilling til direktivforslaget.
([21]) Artikel 7, stk. 1, i direktivforslaget.
([22]) Betragtning 27 til direktivforslaget.
([23]) Artikel 14 i direktivforslaget.
([24]) Afsnit 1.5 i udtalelse CON/2021/20.

information mellem myndigheder ([25]), etablering af samarbejdsordninger, der præciserer en mekanisme til informationsudveksling ([26]), og automatisk og direkte fremsendelse af anmeldelse af hændelser ([27]). I den forbindelse bør det sikres, at oplysninger, der er fortrolige jævnfør bestemmelserne om tavshedspligt i henhold til DORA ([28]) eller den relevante sektorspecifikke lovgivning ([29]) kun kan udveksles med de kompetente myndigheder, der henvises til i direktivforslaget, hvis denne udveksling er nødvendig for, at de kompetente myndigheder kan anvende direktivforslagets bestemmelser ([30]).

3.4 *National cybersikkerhedsstrategi*

3.4.1 I henhold til direktivforslaget skal medlemsstaterne vedtage nationale cybersikkerhedsstrategier for at definere de strategiske mål og passende politiske og reguleringsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau ([31]). Som præciseret i direktivforslagets betragtninger bør medlemsstaterne fortsat medtage den finansielle sektor i deres respektive cybersikkerhedsstrategier ([32]). Vejledende bør medlemsstaterne som led i deres nationale cybersikkerhedsstrategier vedtage politikker vedrørende cybersikkerhed i forsyningskæden for IKT-produkter og -tjenester, der anvendes af enheder til levering af deres tjenester. For så vidt angår den finansielle sektor, bør de nationale cybersikkerhedsstrategier være i overensstemmelse med de lovgivningsmæssige rammer, der udspringer af DORA. I den forbindelse mener ECB, at der er behov for yderligere præcisering for at sikre, at de nationale cybersikkerhedsstrategier stemmer overens med sektorspecifik lovgivning.

Hvor ECB foreslår ændringer af direktivforslaget, vedlægges som bilag ændringsforslag med en begrundelse herfor i et separat teknisk arbejdsdokument. Det tekniske arbejdsdokument er tilgængeligt på engelsk på EUR-Lex.

Udfærdiget i Frankfurt am Main, den 11. april 2022.

Christine LAGARDE
Formand for ECB

([25]) Artikel 11, stk. 5, i Rådets generelle indstilling til direktivforslaget.
([26]) Betragtning 23a i Rådets generelle indstilling til direktivforslaget.
([27]) Betragtning 13 i Rådets generelle indstilling til direktivforslaget.
([28]) Artikel 49 i DORA.
([29]) Artikel 53 til 62 i 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, 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).
([30]) Artikel 2, stk. 5 og 4, i direktivforslaget.
([31]) Artikel 5 i direktivforslaget.
([32]) Betragtning 13 til direktivforslaget.