EUROPEISKA CENTRALBANKENS YTTRANDE

av den 11 april 2022

om ett förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Inledning och rättslig grund

Den 16 december 2020 antog Europeiska kommissionen ett förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 ([1]) (nedan kallat *direktivförslaget*). Den 3 december 2021 enades Europeiska unionens råd om sina allmänna riktlinjer till direktivförslaget ([2]). Europeiska centralbankens behörighet att avge ett yttrande grundas på artikel 127.4 andra stycket i fördraget om Europeiska unionens funktionssätt eftersom direktivförslaget innehåller bestämmelser som berör ECB:s behörighetsområden, särskilt att främja väl fungerande betalningssystem, medverka till de behöriga myndigheternas smidiga genomförande av riktlinjerna för det finansiella systemets stabilitet samt ECB:s uppgifter i fråga om tillsyn över kreditinstitut i enlighet med artikel 127.2 fjärde strecksatsen och artikel 127.5 och 127.6 i fördraget. I enlighet med artikel 17.5 första meningen i arbetsordningen för Europeiska centralbanken har detta yttrande antagits av ECB-rådet.

Allmänna kommentarer

ECB är mycket positiv till direktivförslagets mål att öka cyberresiliensen inom alla relevanta sektorer, minska bristen på enhetlighet på den inre marknaden och förbättra den gemensamma situationsmedvetenheten och den kollektiva förmågan att förbereda sig och reagera genom att säkerställa ett effektivt samarbete inom unionen.

ECB är medveten om vikten av att upprätthålla starka kopplingar mellan direktivförslaget och finanssektorn, som bör förbli en del av nätverks- och informationssystemens ekosystem för att främja en konsekvent bedömning av risker i samband med informations- och kommunikationsteknik (IKT) i hela unionen och främja ett effektivt sektorsövergripande informationsutbyte och samarbete vid hanteringen av cyberhot. I detta syfte bör det vara möjligt för de behöriga myndigheterna enligt förslaget till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn ([3]) (nedan kallad *Dora*) att delta i de strategiska policydiskussionerna och det tekniska arbetet i samarbetsgruppen för nät- och informationssäkerhet, samt att utbyta information och samarbeta ytterligare med de gemensamma kontaktpunkterna och de nationella enheter för hantering av it-säkerhetsincidenter som avses i direktivförslaget ([4]).

1. Direktivförslagets tillämpningsområde

1.1 ECB förstår att Dora, i förhållande till enheter inom den finansiella sektorn, kommer att betraktas som sektorsspecifik lagstiftning som inför krav på hantering av cybersäkerhetsrisker och incidentrapportering som är minst likvärdiga med dem som fastställs i direktivförslaget ([5]). De bestämmelser i direktivförslaget som rör hantering av cybersäkerhetsrisker, rapporteringsskyldigheter, informationsutbyte samt tillsyn och verkställighet kommer därför inte att tillämpas på finansiella enheter som omfattas av Dora ([6]). Såsom klargörs i skälen till direktivförslaget bör de

([1]) COM(2020) 823 final.
([2]) Finns på rådets webbplats www.consilium.europa.eu.
([3]) COM(2020) 595 final.
([4]) Se punkt 1.5 i Europeiska centralbankens yttrande CON/2021/20 av den 4 juni 2021 om ett förslag till Europaparlamentets och rådets förordning om digital operativ motståndskraft för finanssektorn (EUT C 343, 26.8.2021, s. 1). Alla ECB:s yttranden publiceras i EUR-Lex. Artiklarna 17.5 och 42 i Dora; artikel 11 i direktivförslaget.
([5]) Artikel 2.6 i direktivförslaget.
([6]) Skäl 13 och artikel 2.6 i direktivförslaget.

bestämmelser i Dora som rör IKT-riskhanteringsåtgärder, hantering av IKT-relaterade incidenter och incidentrapportering, testning av digital operativ motståndskraft, arrangemang för informationsutbyte och IKT-tredjepartsrisk tillämpas i stället för bestämmelserna i direktivförslaget ([7]).

1.2 ECB noterar också att rådet i sina allmänna riktlinjer till direktivförslaget inkluderar en ändring för att undanta enheter som bedriver verksamhet inom rättsväsendet, parlamenten eller centralbankerna ([8]) från tillämpningen av direktivförslaget. Enligt ECB:s tolkning skulle den föreslagna ändringen omfatta Europeiska centralbankssystemets (ECBS) alla grundläggande uppgifter och befogenheter enligt artikel 127.2 i fördraget och artikel 3.1 i stadgan för Europeiska centralbankssystemet och Europeiska centralbanken (nedan kallad *ECBS-stadgan*), t.ex. att främja väl fungerande betalningssystem. I detta avseende anses finansmarknadsinfrastrukturer som ägs och drivs av Eurosystemet, såsom TARGET2 och TARGET2-Securities, omfattas av rådets förslag att undanta centralbanker från tillämpningen av direktivförslaget.

2. **ECBS och Eurosystemets tillsynsbefogenheter**

2.1 Parallellt med ECBS huvudmål att upprätthålla prisstabilitet, och i enlighet med artikel 127.2 i fördraget, är en de grundläggande uppgifterna för ECBS att främja väl fungerande betalningssystem ([9]). När denna grundläggande uppgift utförs får ECB och de nationella centralbankerna ställa anordningar till förfogande och ECB får utfärda förordningar för att säkerställa effektiva och sunda clearing- och betalningssystem inom unionen och i förbindelser med tredje land ([10]). Vid utövandet av sin tillsynsfunktion antog ECB Europeiska centralbankens förordning (EU) nr 795/2014 (ECB/2014/28) ([11]) (nedan kallad *SIPS-förordningen*), som omvandlar CPSS-IOSCO:s principer för finansmarknadens infrastruktur ([12]) till direkt tillämplig lagstiftning. I SIPS-förordningen fastställs krav för både omfattar systemviktiga betalningssystem för både större betalningar och massbetalningar, oavsett om de är offentliga eller privata aktörer. Kraven enligt SIPS-förordningen omfattar bl.a. hanteringen av operativa risker och inrättandet av en ram för cyberresiliens ([13]).

2.2 Utöver systemviktiga betalningssystem omfattar Eurosystemets tillsyn betalningssystem som inte är systemviktiga, elektroniska betalningsinstrument, -system och -arrangemang samt annan infrastruktur och kritiska tjänsteleverantörer, i enlighet med Eurosystemets tillsynsram ([14]). Betalningssystem och andra arrangemang som omfattas av Eurosystemets tillsyn omfattas inte uttryckligen av direktivförslagets tillämpningsområde ([15]). Samtidigt, med tanke på att direktivförslaget är ett instrument för minimiharmonisering ([16]), kan genomförandelagstiftning som medlemsstaterna antar i framtiden överlappa Eurosystemets tillsynsbefogenheter. För att undvika detta bör ECBS befogenheter enligt fördraget och ECBS-stadgan samt Eurosystemets befogenheter enligt SIPS-förordningen och rent allmänt enligt Eurosystemets tillsynsram uttryckligen erkännas i skälen i direktivförslaget.

([7]) Skäl 13 i direktivförslaget.
([8]) Artikel 2.3a, första stycket punkt b i rådets allmänna riktlinjer till direktivförslaget.
([9]) Artikel 127.2 FEUF, samt artikel 3.1 i ECBS-stadgan.
([10]) Artikel 22 i ECBS-stadgan.
([11]) Europeiska centralbankens förordning (EU) nr 795/2014 av den 3 juli 2014 om krav på övervakning av systemviktiga betalningssystem (ECB/2014/28) (EUT L 217, 23.7.2014, s. 16).
([12]) Se Kommittén för betalnings- och avvecklingssystem (PSSC) och Technical Committee of the International Organization of Securities Commissions (IOSCO), Principles for Financial Market Infrastructures, april 2012, finns på webbplatsen för Banken för internationell betalningsutjämning www.bis.org. Enligt ansvar D anges där att alla CPSS- och IOSCO-medlemmar förväntas tillämpa principerna på de relevanta finansmarknadsinfrastrukturerna inom sina jurisdiktioner i största möjliga utsträckning, i den mån detta är tillåtet enligt den rättsliga ramen inom deras jurisdiktion.
([13]) Artikel 15 i förordning (EU) nr 795/2014 (ECB/2014/28).
([14]) Eurosystemets tillsynsram, reviderad version (juli 2016), finns på ECB:s webbplats www.ecb.europa.eu.
([15]) Artikel 2 i direktivförslaget och bilagorna I och II i direktivförslaget.
([16]) Artikel 3 i direktivförslaget.

3. IKT-riskhantering av tredje parter, hantering av storskaliga incidenter och kriser, informationsutbyte och nationell strategi för cybersäkerhet

3.1 *IKT-riskhantering av tredje parter*

3.1.1 Direktivförslaget ger behöriga myndigheter befogenhet att, när de kontrollerar väsentliga entiteters efterlevnad, har befogenhet att utfärda bindande instruktioner eller ett föreläggande om att dessa entiteter ska avhjälpa konstaterade brister eller överträdelser av de skyldigheter som fastställs i direktivförslaget ([17]). Samtidigt får den ledande tillsynsmyndigheten som utsetts inom ramen för Dora rikta rekommendationer till kritiska tredjepartsleverantörer av IKT-tjänster för att hantera de potentiella systemrisker som kan uppstå till följd av utkontraktering och koncentrationsrisken för IKT-tredjeparter ([18]).

3.1.2 Med tanke på att en väsentlig entitet enligt direktivförslaget också kan utses till en kritisk tredjepartsleverantör av IKT-tjänster enligt Dora, upprepar ECB ([19]) att man bör undvika att utfärda motstridiga rekommendationer och bindande instruktioner. I detta avseende välkomnar ECB rådets allmänna riktlinjer om direktivförslaget. Enligt dessa riktlinjer ska de behöriga myndigheterna informera det tillsynsforum som inrättas enligt Dora när de utövar sina tillsyns- och verkställighetsbefogenheter avseende en väsentlig entitet som har utsetts till en kritisk tredjepartsleverantör av IKT-tjänster enligt Dora ([20]).

3.2 *Hantering av storskaliga incidenter och kriser*

3.2.1 I enlighet med direktivförslaget ([21]) ska medlemsstaterna utse en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga incidenter och kriser. Enligt skälen i direktivförslaget bör en storskalig incident anses vara en incident som påverkar två eller flera medlemsstater eller som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand. Storskaliga incidenter kan förvandlas till fullt utvecklade kriser, som hindrar den inre marknaden från att fungera korrekt ([22]).

3.2.2 Även om de behöriga myndigheter som utsetts enligt Dora förblir ansvariga för hanteringen av cybersäkerhetsincidenter som berör finansiella enheter, kommer samarbete med de strukturer och myndigheter som inrättats i enlighet med direktivförslaget att vara avgörande för att säkerställa samordnade insatser i hela unionen. I detta syfte skulle ECB välkomna att behöriga myndigheter som utsetts enligt Dora, däribland ECB, deltar i Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) ([23]), när storskaliga cyberincidenter och cyberkriser påverkar finanssektorn.

3.3 *Informationsutbyte*

3.3.1 Såsom anges ovan stöder ECB samarbetet mellan de behöriga myndigheter som utsetts enligt Dora och de strukturer och myndigheter som inrättas i enlighet med direktivförslaget. I synnerhet kan informationsutbyte mellan myndigheter möjliggöra sektorsövergripande lärande, bidra till förebyggande och effektiv hantering av cyberattacker och främja en konsekvent bedömning av IKT-relaterade risker i hela unionen. ECB betonar dock att informationsutbyte bör äga rum där det finns tydligt fastställda mekanismer för klassificering och informationsutbyte, tillsammans med lämpliga skyddsåtgärder för att säkerställa konfidentialitet ([24]). ECB välkomnar

([17]) Artikel 29.4 b i direktivförslaget.
([18]) Artikel 31 i Dora.
([19]) Se punkt 1.2 i yttrande CON/2021/20.
([20]) Artikel 29.10 i rådets allmänna riktlinjer avseende direktivförslaget.
([21]) Artikel 7.1 i direktivförslaget.
([22]) Skäl 27 i direktivförslaget.
([23]) Artikel 14 i direktivförslaget.
([24]) Se punkt 1.5 i yttrande CON/2021/20.

rådets allmänna riktlinjer avseende direktivförslaget där man föreslår ett regelbundet utbyte av relevant information mellan myndigheter ([25]), inrättande av samarbetsarrangemang som anger en mekanism för informationsutbytet ([26]) samt automatisk och direkt vidarebefordran av incidentrapporter ([27]). I detta avseende bör det säkerställas att information som är konfidentiell i enlighet med bestämmelserna om tystnadsplikt i DORA ([28]) eller relevant sektorsspecifik lagstiftning ([29]) endast kan utbytas med de behöriga myndigheter som avses i direktivförslaget om detta utbyte är nödvändigt för att de behöriga myndigheterna ska kunna tillämpa bestämmelserna direktivförslaget ([30]).

3.4 *Nationell strategi för cybersäkerhet*

3.4.1 Enligt direktivförslaget får medlemsstaterna en skyldighet att anta en nationell strategi för cybersäkerhet som anger strategiska mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå ([31]). Enligt skälen i direktivförslaget bör medlemsstaterna fortsätta att inkludera finanssektorn i sina respektive strategier för cybersäkerhet ([32]). Medlemsstaterna bör preliminärt, som en del av sina nationella strategier för cybersäkerhet, anta strategier för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter för tillhandahållandet av tjänster. När det gäller finanssektorn bör de nationella cybersäkerhetsstrategierna vara förenliga med det regelverk som härrör från Dora. I detta hänseende anser ECB att ytterligare förtydliganden behövs för att säkerställa att nationella strategier för cybersäkerhet är förenliga med sektorsspecifik lagstiftning.

I de fall där ECB rekommenderar att förslaget till direktiv ska ändras anges ett specifikt förslag i ett separat tekniskt arbetsdokument som åtföljs av en förklaring. Det tekniska arbetsdokumentet finns på engelska på i EUR-Lex.

Utfärdat i Frankfurt am Main den 11 april 2022.

Christine LAGARDE
ECB:s ordförande

([25]) Artikel 11.5 i rådets allmänna riktlinjer till direktivförslaget.
([26]) Artikel 23a i rådets allmänna riktlinjer till direktivförslaget.
([27]) Artikel 13 i rådets riktlinje till direktivförslaget.
([28]) Artikel 49 i Dora.
([29]) Artiklarna 53–62 i Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut, om ändring av direktiv 2002/87/EG och om upphävande av direktiven 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).
([30]) Artiklarna 2.5 och 11.4 i direktivförslaget.
([31]) Artikel 5 i direktivförslaget.
([32]) Skäl 13 i direktivförslaget.