ADVIES VAN DE EUROPESE CENTRALE BANK

van 11 april 2022

inzake een voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Inleiding en rechtsgrondslag

Op 16 december 2020 heeft de Europese Commissie een voorstel aangenomen voor een richtlijn van het Europees Parlement en de Raad betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie en tot intrekking van Richtlijn (EU) 2016/1148 ([1]) (hierna de "ontwerprichtlijn" genoemd). Op 3 december 2021 heeft de Raad van de Europese Unie overeenstemming bereikt over zijn algemene oriëntatie over de ontwerprichtlijn ([2]). De bevoegdheid van de Europese Centrale Bank (ECB) om advies uit te brengen is gebaseerd op de tweede subparagraaf van artikel 127, lid 4, van het Verdrag betreffende de werking van de Europese Unie, aangezien de ontwerprichtlijn bepalingen bevat die onder de bevoegdheid van de ECB vallen, met name de bevordering van de goede werking van het betalingsverkeer, de bijdrage aan het goede verloop van het beleid van de bevoegde autoriteiten met betrekking tot de stabiliteit van het financiële marktstelsel, en de taken van de ECB met betrekking tot het bedrijfseconomisch toezicht op kredietinstellingen overeenkomstig artikel 127, lid 2, vierde streepje, en artikel 127, lid 5 en lid 6, van het Verdrag. Overeenkomstig de eerste zin van artikel 17.5 van het reglement van orde van de Europese Centrale Bank heeft de Raad van bestuur dit advies goedgekeurd.

Algemene opmerkingen

De ECB staat volledig achter de doelstellingen van de ontwerprichtlijn om het niveau van cyberveerkracht in alle relevante sectoren te verhogen, inconsistenties op de interne markt te verminderen en het niveau van situatiekennis en het collectieve vermogen om zich voor te bereiden en te reageren te verbeteren door te zorgen voor efficiënte samenwerking in de Unie.

De ECB erkent het belang van het behoud van sterke banden tussen de ontwerprichtlijn en de financiële sector, die deel moeten blijven uitmaken van het ecosysteem voor de netwerk- en informatiesystemen (NIS) om de consistente beoordeling van risico's in verband met informatie- en communicatietechnologie (ICT) in de hele Unie te bevorderen en doeltreffende sectoroverschrijdende informatie-uitwisseling en samenwerking bij het aanpakken van cyberbedreigingen te stimuleren. Daartoe moet het voor de bevoegde autoriteiten in het kader van de ontwerpverordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector ([3]) (hierna "DORA" genoemd) mogelijk zijn deel te nemen aan de strategische beleidsdiscussies en de technische werkzaamheden van de NIS-samenwerkingsgroep, alsook informatie uit te wisselen en nader samen te werken met de centrale contactpunten en de nationale Computer Security Incident Response Teams ([4]) waarnaar in de ontwerprichtlijn wordt verwezen.

1. Toepassingsgebied van de ontwerprichtlijn

1.1 De ECB begrijpt dat DORA met betrekking tot entiteiten uit de financiële sector zal worden beschouwd als sectorspecifieke wetgeving die vereisten inzake risicobeheer op het gebied van cyberbeveiliging en melding van incidenten invoert die qua werking ten minste gelijkwaardig zijn aan die van de ontwerprichtlijn ([5]). Daarom zullen de bepalingen van de ontwerprichtlijn die betrekking hebben op risicobeheer op het gebied van cyberbeveiliging, rapportageverplichtingen, informatie-uitwisseling en toezicht en handhaving niet van toepassing zijn op financiële entiteiten die onder DORA vallen ([6]). Zoals verduidelijkt in de overwegingen van de ontwerprichtlijn, moeten de

([1]) COM (2020) 823 final.
([2]) Beschikbaar op de website van de Raad onder www.consilium.europa.eu
([3]) COM (2020) 595 final.
([4]) Zie paragraaf 1.5 van Advies CON/2021/20 van de Europese Centrale Bank van 4 juni 2021 inzake een voorstel voor een Verordening van het Europees Parlement en de Raad betreffende digitale operationele veerkracht voor de financiële sector (PB C 343 van 26.8.2021, blz. 1). Alle ECB-adviezen worden gepubliceerd op EUR-Lex. Artikel 17, lid 5, en artikel 42 van DORA; artikel 11 van de ontwerprichtlijn.
([5]) Artikel 2, lid 6, van de ontwerprichtlijn.
([6]) Overweging 13 en artikel 2, lid 6, van de ontwerprichtlijn.

DORA-bepalingen die betrekking hebben op ICT-risicobeheersmaatregelen, het beheer van ICT-gerelateerde incidenten en incidentrapportage, het testen van digitale operationele veerkracht, regelingen voor informatie-uitwisseling en ICT-risico's van derde aanbieders van toepassing zijn in plaats van die van de ontwerprichtlijn ([7]).

1.2 De ECB merkt ook op dat de Raad in zijn algemene oriëntatie over de ontwerprichtlijn als wijziging voorstelt om "entiteiten die activiteiten uitoefenen op het gebied van de rechterlijke macht, parlementen of centrale banken" ([8]) uit te sluiten van de toepassing van de ontwerprichtlijn. De ECB begrijpt dat de voorgestelde wijziging zich uitstrekt tot alle fundamentele taken en bevoegdheden van het Europees Stelsel van centrale banken (ESCB), zoals bepaald in artikel 127, lid 2, van het Verdrag en in artikel 3.1 van de statuten van het Europees Stelsel van centrale banken en van de Europese Centrale Bank (hierna de "ESCB-statuten"), zoals de bevordering van de goede werking van het betalingsverkeer. In dit verband worden financiële marktinfrastructuren die eigendom zijn van het Eurosysteem en daardoor beheerd worden, zoals TARGET2 en TARGET2-Securities, geacht te vallen onder de door de Raad voorgestelde uitsluiting van centrale banken van de toepassing van de ontwerprichtlijn.

2. **Bevoegdheden op het gebied van oversight door het ESCB en het Eurosysteem**

2.1 Naast het hoofddoel van het ESCB, namelijk het handhaven van prijsstabiliteit, is het bevorderen van de goede werking van het betalingsverkeer een van de fundamentele taken die via het ESCB moeten worden uitgevoerd overeenkomstig artikel 127, lid 2, van het Verdrag ([9]). Bij de uitvoering van deze fundamentele taak mogen de ECB en de nationale centrale banken faciliteiten ter beschikking stellen, en kan de ECB verordeningen vaststellen ter verzekering van doelmatige en deugdelijke clearing- en betalingssystemen binnen de Unie en met andere landen ([10]). Bij de uitoefening van haar toezichthoudende rol heeft de ECB Verordening van de Europese Centrale Bank (EU) nr. 795/2014 (ECB/2014/28) ([11]) (hierna de "SIPS-verordening" genoemd) vastgesteld, die de CPSS-IOSCO Principles for Financial Market Infrastructures ([12]) omzet in rechtstreeks toepasselijk recht. De SIPS-verordening stelt vereisten vast voor zowel systemen voor het betalen van grote bedragen als systeemrelevante retailbetalingssystemen, ongeacht of deze systemen openbaar of particulier eigendom zijn. De vereisten in het kader van de SIPS-verordening omvatten reeds onder meer operationeel risicobeheer en de totstandbrenging van een kader voor cyberveerkracht ([13]).

2.2 Naast systeemrelevante betalingssystemen omvat het toezicht van het Eurosysteem ook niet-systeemrelevante betalingssystemen, elektronische betaalinstrumenten, -systemen en -regelingen, en andere infrastructuren en cruciale dienstverleners, zoals uiteengezet in het toezichtbeleidskader van het Eurosysteem ([14]). Betalingssystemen en andere regelingen die onder toezicht van het Eurosysteem vallen, vallen niet uitdrukkelijk onder het toepassingsgebied van de ontwerprichtlijn ([15]). Tegelijkertijd zou, aangezien de ontwerprichtlijn een minimumharmonisatie-instrument ([16]) is, de door de lidstaten aangenomen uitvoeringswetgeving uiteindelijk kunnen overlappen met de toezichtbevoegdheid van het Eurosysteem. Om dit te voorkomen, moeten de bevoegdheden van het ESCB uit hoofde van het Verdrag en de ESCB-statuten en de bevoegdheden van het Eurosysteem uit hoofde van de SIPS-verordening en in het algemeen uit hoofde van het toezichtbeleidskader van het Eurosysteem uitdrukkelijk worden erkend in de overwegingen van de ontwerprichtlijn.

([7]) Overweging 13 van de ontwerprichtlijn.
([8]) Artikel 2, lid 3 bis, eerste subparagraaf, punt b), van de algemene oriëntatie van de Raad over het richtlijnvoorstel.
([9]) Artikel 127, lid 2, VWEU, zoals weergegeven in artikel 3.1 van de ESCB-statuten.
([10]) Artikel 22 van de ESCB-statuten.
([11]) Verordening van de Europese Centrale Bank (EU) nr. 795/2014 van 3 juli 2014 met betrekking tot oversightvereisten voor systeemrelevante betalingssystemen (ECB/2014/28) (PB L 217 van 23.7.2014, blz. 16).
([12]) Zie Committee on Payment and Settlement Systems (CPSS)/ Technical Committee of the International Organization of Securities Commissions (IOSCO), Principles for Financial Market Infrastructures, april 2012, beschikbaar op de website van de Bank for International Settlements onder www.bis.org. Verantwoordelijkheid D daarvan bepaalt dat van alle leden van de CPSS en de IOSCO wordt verwacht dat zij de beginselen zo volledig mogelijk toepassen op de relevante FMI's in hun rechtsgebied, in de hoogste mate waarin het rechtskader in hun rechtsgebied dit toelaat.
([13]) Artikel 15 van Verordening (EU) nr. 795/2014 (ECB/2014/28).
([14]) Eurosystem oversight policy framework, herziene versie (juli 2016), beschikbaar in het Engels op de website van de ECB onder www.ecb.europa.eu.
([15]) Artikel 2 van de ontwerprichtlijn en bijlagen I en II bij de ontwerprichtlijn.
([16]) Artikel 3 van de ontwerprichtlijn .

3. **ICT-risico van derde aanbieders, beheer van grootschalige incidenten en crises, informatie-uitwisseling en nationale cyberbeveiligingsstrategie**

3.1 *Risicobeheer van ICT-derden*

3.1.1 De ontwerprichtlijn geeft de bevoegde autoriteiten de bevoegdheid om bij de uitoefening van hun handhavingsbevoegdheden ten aanzien van essentiële entiteiten bindende instructies te geven of een bevel uit te vaardigen aan die essentiële entiteiten om de vastgestelde tekortkomingen of inbreuken op de verplichtingen van de ontwerprichtlijn te verhelpen ([17]). Tegelijkertijd kan de in het kader van DORA aangewezen "leidende toezichthouder" aanbevelingen doen aan cruciale derde aanbieders van ICT-diensten om de potentiële systeemrisico's van aanbestedingspraktijken en concentratie van ICT-derde aanbieders te beheren ([18]).

3.1.2 Aangezien een essentiële entiteit in het kader van de ontwerprichtlijn ook kan worden aangewezen als cruciale derde aanbieder van ICT-diensten overeenkomstig DORA, herhaalt de ECB ([19]) dat het geven van tegenstrijdige aanbevelingen en bindende instructies moet worden vermeden. In dit verband is de ECB ingenomen met de algemene oriëntatie van de Raad over de ontwerprichtlijn. Volgens die oriëntatie moeten de bevoegde autoriteiten het in het kader van DORA opgerichte "Oversight Forum" informeren bij de uitoefening van hun toezichts- en handhavingsbevoegdheden met betrekking tot een essentiële entiteit die in het kader van DORA is aangewezen als cruciale derde aanbieder van ICT-diensten ([20]).

3.2 *Beheer van grootschalige incidenten en crises*

3.2.1 Overeenkomstig de ontwerprichtlijn ([21]) moeten de lidstaten een of meer bevoegde autoriteiten aanwijzen die verantwoordelijk zijn voor het beheer van grootschalige incidenten en crises. Zoals in de overwegingen van de ontwerprichtlijn wordt verduidelijkt, moet onder een grootschalig incident worden verstaan een incident met significante gevolgen voor ten minste twee lidstaten of waarvan de verstoring het vermogen van een lidstaat om daarop te reageren te boven gaat. Grootschalige incidenten kunnen uitmonden in volwaardige crises, waardoor de goede werking van de interne markt wordt verstoord ([22]).

3.2.2 Hoewel de in het kader van DORA aangewezen bevoegde autoriteiten verantwoordelijk blijven voor het beheer van cyberbeveiligingsincidenten met betrekking tot financiële entiteiten, zal samenwerking met de overeenkomstig de ontwerprichtlijn opgerichte structuren en autoriteiten van cruciaal belang zijn om een gecoördineerde respons in de hele Unie te waarborgen. Daartoe zou de ECB graag zien dat de in het kader van DORA aangewezen bevoegde autoriteiten, waaronder de ECB, deelnemen aan het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) ([23]), wanneer grootschalige cyberincidenten en crises gevolgen hebben voor de financiële sector.

3.3 *Uitwisseling van informatie*

3.3.1 Zoals hierboven aangegeven, is de ECB sterk voorstander van samenwerking tussen de in het kader van DORA aangewezen bevoegde autoriteiten met de structuren en autoriteiten die krachtens de ontwerprichtlijn zijn opgericht. Met name informatie-uitwisseling tussen autoriteiten kan sectoroverschrijdend leren mogelijk maken, bijdragen tot de preventie en doeltreffende beheersing van cyberaanvallen, en de consistente beoordeling van ICT-gerelateerde risico's in de hele Unie bevorderen. Niettemin benadrukt de ECB dat informatie-uitwisseling moet plaatsvinden wanneer er duidelijk vastgestelde classificatie- en informatieuitwisselingsmechanismen bestaan, in combinatie met passende waarborgen om de vertrouwelijkheid te waarborgen ([24]). De ECB is ingenomen met de

([17]) Artikel 29, lid 4, punt b, van de ontwerprichtlijn.
([18]) Artikel 31 van DORA.
([19]) Zie punt 1.2 van Advies CON/2021/20.
([20]) Artikel 29, lid 10, van de algemene oriëntatie van de Raad over de ontwerprichtlijn.
([21]) Artikel 7, lid 1, van de ontwerprichtlijn.
([22]) Overweging 27 van de ontwerprichtlijn.
([23]) Artikel 14 van de ontwerprichtlijn.
([24]) Zie punt 1.5 van Advies CON/2021/20.

algemene oriëntatie van de Raad met betrekking tot de ontwerprichtlijn, die voorziet in de regelmatige uitwisseling van relevante informatie tussen autoriteiten ([25]), de instelling van samenwerkingsregelingen die een mechanisme voor de uitwisseling van informatie specificeren ([26]), en de automatische en rechtstreekse doorzending van meldingen van incidenten ([27]). In dit verband moet ervoor worden gezorgd dat informatie die vertrouwelijk is op grond van de bepalingen inzake het beroepsgeheim in het kader van DORA ([28]) of de relevante sectorspecifieke wetgeving ([29]), alleen met de in de ontwerprichtlijn bedoelde bevoegde autoriteiten kan worden uitgewisseld wanneer die uitwisseling noodzakelijk is voor de bevoegde autoriteiten om de bepalingen van de ontwerprichtlijn toe te passen ([30]).

3.4 *Nationale cyberbeveiligingsstrategie*

3.4.1 Op grond van de ontwerprichtlijn moeten de lidstaten nationale cyberbeveiligingsstrategieën vaststellen om de strategische doelstellingen en passende beleids- en regelgevingsmaatregelen vast te stellen met het oog op het bereiken en handhaven van een hoog niveau van cyberbeveiliging ([31]). Zoals verduidelijkt in de overwegingen van de ontwerprichtlijn, moeten de lidstaten de financiële sector blijven betrekken in hun respectieve cyberbeveiligingsstrategieën ([32]). In het kader van hun nationale cyberbeveiligingsstrategieën moeten de lidstaten bij wijze van indicatie beleid vaststellen dat gericht is op cyberbeveiliging in de toeleveringsketen voor ICT-producten en -diensten die door entiteiten worden gebruikt voor de verlening van hun diensten. Wat de financiële sector betreft, moeten de nationale cyberbeveiligingsstrategieën in overeenstemming zijn met het regelgevingskader dat voortvloeit uit DORA. In dit verband is de ECB van mening dat verdere verduidelijkingen nodig zijn om ervoor te zorgen dat de nationale cyberbeveiligingsstrategieën consistent zijn met sectorspecifieke wetgeving.

Indien de ECB wijzigingen van de ontwerprichtlijn aanbeveelt, worden daartoe in een apart technisch werkdocument specifiek onderbouwde formuleringsvoorstellen opgenomen. Het technische werkdocument is in de Engelse taal beschikbaar op Eur-Lex.

Gedaan te Frankfurt am Main, 11 april 2022.

De president van de ECB
Christine LAGARDE

([25]) Artikel 11, lid 5, van de algemene oriëntatie van de Raad over de ontwerprichtlijn.
([26]) Overweging 23a van de algemene oriëntatie van de Raad over de ontwerprichtlijn.
([27]) Overweging 13 van de algemene oriëntatie van de Raad over de ontwerprichtlijn.
([28]) Artikel 49 van DORA.
([29]) Artikelen 53 tot en met 62 van Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).
([30]) Artikel 2, lid 5, en artikel 11, lid 4, van de ontwerprichtlijn.
([31]) Artikel 5 van de ontwerprichtlijn.
([32]) Overweging 13 van de ontwerprichtlijn.