EUROPESE CENTRALE BANK

EUROSYSTEEM

NL **ECB-PUBLIC**

ADVIES VAN DE EUROPESE CENTRALE BANK

van 18 mei 2018

inzake de vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang

(CON/2018/27)

Inleiding en rechtsgrondslag

Op 18 april 2018 ontving de Europese Centrale Bank (ECB) een verzoek van de Belgische Minister van Financiën om een advies inzake een wetsontwerp betreffende de vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang (hierna genoemd het „voorstel").

De ECB-adviesbevoegdheid is gebaseerd op artikel 127, lid 4 en artikel 282, lid 5 van het Verdrag betreffende de werking van de Europese Unie, in samenhang met artikel 127, lid 6 van het Verdrag en artikel 2, lid 1, het derde, vijfde en zesde streepje van Beschikking 98/415/EG van de Raad[1], aangezien het voorstel betrekking heeft op de Nationale Bank van België (NBB), betalings- en afwikkelingssystemen, regels die van toepassing zijn op financiële instellingen voor zover deze van wezenlijke invloed zijn op de financiële stabiliteit van financiële instellingen en markten en de ECB-taken betreffende het prudentiële toezicht op kredietinstellingen. 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.

1. Doel van het voorstel

1.1 Het voorstel beoogt de implementatie van Richtlijn (EU) 2016/1148 van 6 juli 2016 van het Europees Parlement en de Raad houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie[2] (hierna genoemd de „NIS-Richtlijn"), rekening houdend met artikel 1, lid 7 van die richtlijn, krachtens welke bepaling sectorspecifieke rechtshandelingen van de Unie van toepassing zijn die equivalente verplichtingen opleggen aan essentiëledienstenexploitanten ter waarborging van de beveiliging van hun netwerk- en informatiesystemen of voor de melding van incidenten[3].

1.2 Met name de Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren[4] (hierna genoemd de „Wet op kritieke infrastructuren"), die Richtlijn 2008/114/EU

1 Beschikking van de Raad 98/415/EG van 29 juni 1998 betreffende de raadpleging van de Europese Centrale Bank door de nationale autoriteiten over ontwerpen van wettelijke bepalingen (PB L 189 van 3.7.1998, blz. 42).

2 PB L 194 van 19.7.2016, blz. 1.

3 Toelichting bij het voorstel, blz. 6.

4 *Wet van 1 juli betreffende de beveiliging en de bescherming van de kritieke infrastructuren*.

van 8 december 2008 inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren[5] implementeerde, voerde in België een alomvattend kader in voor kritieke infrastructuren, welke is gedefinieerd als een activum, systeem, of een deel daarvan, dat essentieel is voor de instandhouding van vitale maatschappelijke functies, gezondheid, beveiliging, economisch of sociaal welbevinden van burgers, waarvan de verstoring of vernietiging een significante impact zou hebben indien die functies niet in stand kunnen worden gehouden. Deze kritieke infrastructuren worden door de sectorale overheid vastgesteld, aangewezen en nauwgezet gemonitord om te verzekeren dat de exploitanten ervan een beveiligingsplan vaststellen en implementeren om de mogelijke verstoring of vernietiging van hun werking te voorkomen, te verlichten en te neutraliseren. De NBB is aangewezen als de sectorale overheid voor de financiële sector.

1.3 Om consistentie te bewerkstelligen met de Wet op kritieke infrastructuren zijn door de NBB aangewezen kritieke infrastructuren automatisch essentiëledienstenexploitanten binnen het kader van het voorstel. Voorts gelden alle bepalingen van het voorstel, krachtens welke de sectorale overheid op essentiëledienstenexploitanten beveiligingsvereisten, interne en externe audit, controle, verificaties en inspecties mogen toepassen, voor alle sectoren, behalve voor de financiële sector. Op de essentiëledienstenexploitanten die ressorteren onder de financiële sector zijn alleen de bepalingen betreffende incidentmeldingen en administratieve sancties van toepassing. Enerzijds zal de NBB te dien einde optreden als de sectorale overheid voor kredietinstellingen en centrale tegenpartijen, anderzijds zal de Autoriteit voor Financiële Diensten en Markten in die hoedanigheid optreden voor de exploitanten van handelsplatforms.

1.4 Het voorstel voert voorts op nationaal en internationaal niveau samenwerkings- en/of informatie-uitwisselingsregelingen in. Op nationaal niveau vindt die samenwerking en informatie-uitwisseling, onder meer voor incidentmeldingen, plaats tussen het Centrum voor Cybersecurity België (CCB), de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken (ADCC), de sectorale overheden, alsook, indien nodig, met het Openbaar Ministerie, de politie en de Gegevensbeschermingsautoriteit. Op internationaal niveau vindt de samenwerking en informatie-uitwisseling plaats met de overheden van de Europese Unie en buitenlandse of nationale autoriteiten, indien de implementatie van het voorstel dat vereist.

1.5 Het voorstel wijzigt de Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de NBB[6] (hierna genoemd de „Organieke Wet NBB") om formeel vast te leggen dat NBB bevoegd is te verifiëren of financiëlesectorexploitanten de bepalingen van de Organieke Wet NBB naleven, om de Sanctiecommissie te machtigen de vastgelegde administratieve sancties toe te passen, en informatie-uitwisseling toe te staan met de nationale autoriteiten die bevoegd zijn inzake de beveiliging van netwerk- en informatiesystemen van algemeen belang.

---

5 PB L 345 van 23.12.2008, blz. 75

6 *Wet van 22 februari 1998 tot vaststelling van het organiek statuut van de Nationale Bank van België*.

2. Algemene opmerkingen

2.1 Het voorstel implementeert de NIS-Richtlijn die luidens artikel 3 van die richtlijn een minimumharmonisatierichtlijn is, wat inhoudt dat lidstaten bepalingen kunnen vaststellen of in stand kunnen houden om een hoger niveau van netwerk- en informatiesysteembeveiliging te verwezenlijken dan in de richtlijn is voorzien.

2.2 De ECB[7] heeft er eerder op gewezen dat de ECB het doel van de NIS-Richtlijn ondersteunt om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIS) in de hele Unie te waarborgen en om ter zake een consistente benadering te verwezenlijken in bedrijfstakken en lidstaten. Het is van belang te waarborgen dat op de interne markt veilig zaken kunnen worden gedaan en dat alle lidstaten een minimumvoorbereidingsniveau hebben aangaande cybersecurityincidenten.

2.3 In een eerder advies[8] heeft de ECB verwelkomt dat de NBB werd aangewezen als de betrokken autoriteit binnen het kader van de Wet op kritieke infrastructuren waardoor NBB financiële stabiliteit beter kan waarborgen en systeemrisico's beter kan voorkomen of mitigeren.

2.4 De ECB neemt nota van de specifieke wetgevingsmethode van het voorstel.

Enerzijds breidt het voorstel de werkingssfeer van de NIS-Richtlijn uit die van toepassing is op kredietinstellingen, centraletegenpartijen (CTP's) en handelsplatformexploitanten die een vestiging in België hebben en die in België daadwerkelijk werkzaamheden uitoefenen die verband houden met de verlening van minstens één essentiële dienst. Kritieke infrastructuren die de NBB krachtens het voorstel aanmeldt, zijn automatisch essentiëledienstenexploitanten.

Anderzijds zijn luidens het voorstel op essentiëledienstenexploitanten in de financiële sector slechts incidentmeldingsplichten en administratieve sancties van toepassing. Ten aanzien van de financiële sector zijn alle overige voor alle andere sectoren toepasselijke bepalingen inzake beveiligingsvereisten, interne en externe audit, controle, verificaties en inspecties niet van toepassing op de financiële sector. Aldus, en overeenkomstig artikel 1, lid 7 van de NIS-Richtlijn steunt het voorstel op de bestaande toezicht- en oversightbevoegdheden van de betrokken bevoegde autoriteiten die reeds equivalente verplichtingen opleggen aan essentiëledienstenexploitanten om de beveiliging van hun netwerk- en informatiesystemen te waarborgen. Deze betrokken autoriteiten omvatten op Europees niveau de ECB binnen het kader van het Gemeenschappelijk Toezichtsmechanisme en het Eurosysteem binnen het kader van het oversight op marktinfrastructuren. Op nationaal niveau zijn de bestaande toezicht- en oversightbevoegdheden van de NBB vastgelegd in de Organieke Wet NBB die de NBB ter uitvoering van haar taken tevens bekleedt met regelgevende bevoegdheden, onderzoeks- en sanctiebevoegdheden ten aanzien van alle financiële instellingen. Specifieke vereisten en aanbevelingen inzake het beheer van operationeel risico zijn vastgelegd in sectorale wetgeving en

7 Zie paragraaf 2.1 van Advies CON/2014/58, paragraaf 2.1 van Advies CON/2017/10 en paragraaf 2.2 van Advies CON/2018/22. Alle ECB-adviezen worden bekendgemaakt op de ECB-website onder www.ecb.europa.eu.

8 Zie paragraaf 1.2 en 3.1 van Advies CON/2014/17.

kaders die van toepassing zijn op kredietinstellingen[9], systeemrelevante betalingssystemen[10], zeer relevante retailbetalingssystemen en overige retailbetalingssystemen[11], overige financiëlemarktinfrastructuren (waaronder CTP's en centrale effectenbewaarinstellingen)[12], betaalkaarten, overmakingen, automatische afschrijvingen en elektronisch geld[13], betalingsdienstverleners[14], kritiekedienstenverleners zoals bedoeld binnen het kader van het Eurosystem's Oversight Policy Framework[15], alsook verwerkers van betalingstransacties binnen het kader van de Belgische Wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties[16].

2.5 Door deze wetgevingsmethode doet het voorstel geen afbreuk aan de bestaande ECB-, en NBB-bevoegdheden inzake het toezicht op krediet- en financiële instellingen en het oversight op marktinfrastructuren. Dienaangaande blijft de NBB krachtens haar bestaande toezicht- en oversightbevoegdheden, waaronder de Wet op kritieke infrastructuren, bij uitsluiting bevoegd om beveiligingsvereisten, interne en externe audit, controle, verificaties en inspecties toe te passen op essentiëledienstexploitanten, alsook om sancties op te leggen. De nieuwe krachtens het voorstel in België ingevoerde nieuwe administratieve autoriteiten (namelijk, de CCB en de ADCC) moeten deze NBB-bevoegdheden onverlet laten en derhalve is de institutionele en operationele onafhankelijkheid van NBB gewaarborgd.

2.6 Door deze gehanteerde methode laat het voorstel de ECB- en de Eurosysteem-bevoegdheden onverlet en druist niet in tegen rechtshandelingen van de Unie, aangezien de incidentmeldingsverplichtingen van essentiëledienstenexploitanten in de financiële sector een

---

9 Krachtens artikel 85 van Richtlijn (EU) 2013/36 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), passen kredietinstellingen beleidslijnen en procedures toe om de blootstellingen aan operationeel risico te beoordelen en te beheren waarmee rekening moet worden gehouden bij de berekening van kapitaalvereisten uit hoofde van Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).

10 Zie artikel 15 van Verordening (EU) nr. 795/2014 van de Europese Centrale Bank van 3 juli 2014 met betrekking tot oversightvereisten voor systeemrelevante betalingssystemen (ECB/2014/28) (PB L 217 van 23.7.2014, blz. 16), gewijzigd bij Verordening (EU) 2017/2094 van de Europese Centrale Bank van 3 november 2017 tot wijziging van Verordening (EU) nr. 795/2014 met betrekking tot oversightvereisten voor systeemrelevante betalingssystemen (ECB/2017/32) (PB L 299 van 16.11.2017, blz. 11). De wijziging scherpte de operationele risico's vereisten en NIS-vereisten aan, rekening houdend met onder meer met de Committee on Payments and Market Infrastructures-International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures, juni 2016 (beschikbaar op de BIS-website onder www.bis.org).

11 Zie met name Principle 17 van 'Revised Oversight Framework for retail payment systems' van het Eurosysteem, februari 2016, beschikbaar op de ECB-website.

12 Artikel 45 van Verordening (EU) nr. 909/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de verbetering van de effectenafwikkeling in de Europese Unie, betreffende centrale effectenbewaarinstellingen en tot wijziging van Richtlijnen 98/26/EG en 2014/65/EU en Verordening (EU) nr. 236/2012 (PB L 257 van 28.4.2014, blz. 172), legt strikte vereisten op met betrekking tot operationele risico's.

13 Zie het 'Oversight Policy Framework' van het Eurosysteem, juli 2016, beschikbaar op de ECB-website.

14 Zie artikelen van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PB L 337 van 23.12.2015, blz. 35) betreffende melding van incidenten (artikel 96), beveiligingsmaatregelen voor operationeel risico en beveiligingsrisico (artikel 95) en technische reguleringsnormen inzake sterke cliëntauthenticatie en beveiligde communicatie (artikel 98).

15 Zie voetnoot 13.

16 Zie artikel 11 van de *wet van 24 maart 2017 houdende het toezicht op verwerkers van betalingstransacties*.

aanvulling zijn op het vigerende toezicht- en oversightkader dat van toepassing blijft zonder ongepaste invloed van het voorstel.

3. Taken van de NBB

3.1 Het voorstel voert in de Organieke Wet NBB een nieuw hoofdstuk in waarin de NBB bevoegd wordt verklaard om te controleren of exploitanten uit de financiële sector voldoen aan het voorstel. Dit nieuwe hoofdstuk dat is opgenomen in het hoofdstuk betreffende het micro- en macrotoezicht op financiële instellingen en het oversight op marktinfrastructuren, vult de vigerende toezicht- en oversightbevoegdheden van de NBB ten aanzien van de financiële sector aan, met name vanuit de invalshoek van de beveiliging, integriteit en veerkracht van netwerk- en informatiesystemen. Bovendien, zoals eerder opgemerkt, is de NBB de bevoegde autoriteit inzake de beveiliging van kritieke financiële infrastructuren[17] op basis van de Wet op kritieke infrastructuren, aangezien het voorstel derhalve geen waarlijk nieuwe taken toekent aan de NBB, waardoor de toekenning van nieuwe taken aan een nationale centrale bank vanuit de invalshoek van het verbod op monetaire financiering niet beoordeeld moet worden[18].

4. Informatie-uitwisseling met de ECB

4.1 Krachtens artikel 9, lid 1 van het voorstel mogen gegevens betreffende essentiëledienstenexploitanten worden gedeeld met EU-autoriteiten ‘indien deze uitwisseling noodzakelijk is voor de toepassing van deze wet’.

4.2 Deze formulering is te restrictief, aangezien informatie inzake bij de NBB door essentiëledienstenexploitanten ingediende incidentmeldingen in een andere context relevant kan zijn. Die informatie kan bv. van belang zijn voor de uitvoering van oversightwerkzaamheden waarbij de ECB is betrokken. Die informatie kan ook van belang zijn in verband met de ECB-taken inzake prudentieel toezicht op kredietinstellingen in België[19]. Dit prudentiële toezicht bestrijkt met NIS verband houdende aangelegenheden als onderdeel van het prudentieel toezicht op operationeel risico (i.e., het risico van verliezen die voortvloeien uit inadequate of falende interne processen, mensen en systemen of uit externe gebeurtenissen)[20].

4.3 Dat overziende beveelt de ECB aan de formulering van artikel 9 van het voorstel aan te scherpen om te verzekeren dat de NBB deze informatie tijdig en efficiënt met de ECB deelt, zulks binnen het kader van de ECB-verantwoordelijkheden voor het oversight op betalingssystemen en het prudentieel toezicht op kredietinstellingen[21].

---

17 Met betrekking tot de rol van NBB’s rol als bevoegde autoriteit voor de beveiliging en bescherming van kritieke infrastructuren, Advies CON/2014/17, paragraaf 3.1 and 3.5.

18 Zie paragraaf 2.3 van Advies CON/2018/15.

19 Zie Verordening (EU) nr. 1024/2013 van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen (PB L 287 van 29.10.2013, blz. 63).

20 Zie paragraaf 4.3 van Advies CON/2018/22.

21 Zie paragraaf 6.2 van Advies CON/2018/22.

Dit advies wordt bekendgemaakt op de ECB-website.

Gedaan te Frankfurt am Main, 18 mei 2018.

[getekend]

De President van de ECB

Mario DRAGHI