

III

(Vorbereidende handelingen)

EUROPESE CENTRALE BANK

ADVIES VAN DE EUROPESE CENTRALE BANK

van 25 juli 2014

inzake een voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen**(CON/2014/58)**

(2014/C 352/04)

Inleiding en rechtsgrondslag

Op 7 februari 2013 publiceerde de Europese Commissie een voorstel voor een richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen⁽¹⁾ (hierna het „voorstel”).

Aangezien de Europese Centrale Bank (ECB) formeel niet door de wetgevers geraadpleegd werd, heeft zij besloten een eigen-initiatiefadvies in te dienen. 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, aangezien het voorstel bepalingen bevat betreffende de taak van het Europees Stelsel van centrale banken (ESCB) een goede werking van het betalingsverkeer te bevorderen, zoals bedoeld in artikel 127, lid 2 van het Verdrag. Voorts bepaalt artikel 22 van de statuten van het Europees Stelsel van centrale banken en van de Europese Centrale Bank (hierna de „ESCB-statuten”) dat de ECB en de nationale centrale banken (NCB's) faciliteiten ter beschikking kunnen stellen, en de ECB verordeningen kan vaststellen, ter verzekering van doelmatige en deugdelijke verrekenings- en betalingssystemen binnen de Unie en met andere landen. Overeenkomstig de eerste volzin 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 een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging (NIB) in de Unie te waarborgen door de beveiliging van het internet en netwerk- en informatiesystemen die aan onze maatschappij en economie ten grondslag liggen, te verbeteren. Dit voorstel is het belangrijkste optreden uit hoofde van de Europese strategie voor cyberbeveiliging⁽²⁾.
- 1.2 Netwerk- en informatiesystemen zijn essentieel voor het faciliteren van grensoverschrijdende verplaatsingen van goederen, diensten en mensen. Gezien de intrinsieke transnationale dimensie kan een verstoring in een lidstaat ook andere lidstaten en de Unie als geheel betreffen. Bovendien, de waarschijnlijkheid dat incidenten vaker plaatsvinden en het onvermogen efficiënte bescherming te waarborgen, ondermijnen het publieke vertrouwen en geloof in NIS. De weerbaarheid en de stabiliteit van NIS is derhalve kritiek voor de goede werking van de interne markt.
- 1.3 Het voorstel borduurt voort op eerdere initiatieven op dit vlak⁽³⁾. Tegen die achtergrond erkent het voorstel de noodzaak regels aangaande NID te harmoniseren en tussen de lidstaten effectieve samenwerkingsmechanismen in het leven te roepen.

⁽¹⁾ COM(2013) 48 final.

⁽²⁾ Zie Gemeenschappelijke Verklaring aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's, „Cyberbeveiligingsstrategie van de Europese Unie: Een Open, Veilige en Beveiligde Cyberruimte”, JOIN(2013) 1 final.

⁽³⁾ Deze omvatten de volgende verklaringen: „Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak” COM(2001) 298 final; „Een strategie voor een veilige Informatiemaatschappij: „Dialog, partnerschap en empowerment” COM(2006) 251 final; „Bescherming van kritieke informatie-infrastructuur — „Europa beschermen tegen grootschalige cyberaanvallen en verstoringen: verbeteren van de paraatheid, beveiliging en veerkracht” COM(2009) 149 final; „Een digitale agenda voor Europa” COM(2010) 245 final; „De bescherming van kritieke informatie-infrastructuur — „Bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid” COM(2011) 163 final.

1.4 Het voorstel richt een gemeenschappelijk Unierechtskader voor NIS op betreffende de mogelijkheden voor lidstaten, mechanismes voor samenwerking op unieniveau en vereisten voor overheidsinstanties en particuliere entiteiten in specifieke kritieke sectoren. Dit moeten een adequate paraatheid op nationaal niveau waarborgen en ertoe bijdragen dat een klimaat van wederzijds vertrouwen ontstaat, hetgeen een voorwaarde is voor effectieve samenwerking op unieniveau. Het inrichten van samenwerkingsmechanismen op unieniveau via het netwerk zal resulteren in een coherent en gecoördineerd instrument voor het vermijden van en reageren op grensoverschrijdende NIB-incidenten en -risico's.

1.5 De belangrijkste bepalingen betreffen het volgende:

- a) een vereiste dat alle lidstaten over een minimum nationale capaciteit beschikken door voor NIB bevoegde autoriteiten aan te wijzen, computercrisisteams op te zetten (Computer Emergency Response Teams — CERT's) en nationale NIB-strategieën en -samenwerkingsplannen vast te stellen;
- b) vereiste informatiedeling tussen lidstaten binnen een netwerk, alsook het opzetten van een pan-Europees NIB-samenwerkingsplan en gecoördineerde vroegtijdige waarschuwingen voor cyberbeveiligingsincidenten;
- c) Uitgaande van het model van Richtlijn 2002/21/EG van het Europees Parlement en de Raad ⁽¹⁾, waardoor een cultuur van risicobeheer ontstaat en dat informatie gedeeld wordt tussen particuliere en overheidssectoren. Bedrijven in de specifieke kritieke sectoren en overheidsinstanties moeten risico's beoordelen waarmee zij geconfronteerd worden en passende en evenredige maatregelen nemen om NIB te waarborgen. Zij zullen de nationale bevoegde autoriteiten van incidenten in kennis moeten stellen die hun netwerken en informatiesystemen ernstig in gevaar brengen en die de continuïteit van kritieke diensten en goederenleveringen significant beïnvloeden.

2. Algemene opmerkingen

- 2.1 De ECB steunt het doel van het voorstel om in de hele Unie een hoog gemeenschappelijk niveau van NIB te waarborgen en op dit gebied een consistente aanpak te realiseren in alle zakensectoren en lidstaten. Het is van belang te waarborgen dat de interne markt een veilige plaats voor zakendoen is en dat alle lidstaten een minimaal paraatheidsniveau hebben ingeval van een cyberveiligheidsincident.
- 2.2 De ECB is evenwel van mening dat het voorstel de regeling voor oversight op betalings- en afwikkelingssystemen van het Eurosysteem ⁽²⁾ onverlet moet laten, hetgeen passende regelingen omvat onder meer op het gebied van NIB. Opgemerkt zij dat de ECB een bijzonder belang heeft bij een aangescherpte beveiliging van betalings- en afwikkelingssystemen ⁽³⁾ om de goede werking van die betaalsystemen te bevorderen en bij te dragen aan het handhaven van het vertrouwen in de euro en de werking van de economie in de Unie.
- 2.3 Bovendien, de beoordeling van beveiligingsregelingen en incidentennotificaties voor betalings- en afwikkelingssystemen en betalingsdienstverleners (PSP's) is een van de kernbevoegdheden van prudentiële toezichhouders en centrale banken. Verantwoordelijkheid voor het ontwikkelen van oversightvoorschriften voor de bovengenoemde gebied moet derhalve de verantwoordelijkheid van deze autoriteiten blijven, en betalings- en afwikkelingssystemen en PSP's moeten niet blootgesteld worden aan door andere nationale autoriteiten opgelegde mogelijkerwijze conflicterende voorschriften. Bovendien, risicobeheer, waaronder beveiligingsvoorschriften aangaande betalings- en afwikkelingssystemen en andere marktinfrastructuren binnen het eurogebied, wordt door het Eurosysteem vastgesteld, met inbegrip van de ECB en NCB's van de lidstaten die de euro als munt hebben. Middels deze oversightfunctie beoogt het Eurosysteem de goede werking van betalings- en afwikkelingssystemen te waarborgen door onder meer passende oversightnormen en minimumvoorschriften te hanteren. Het voorstel moet rekening houden met het reeds vigerende oversightkader en regelgevende consistentie in de hele Unie waarborgen.

3. Specifieke opmerkingen

- 3.1 Overweging 5 en artikel 1 van het voorstel bepalen dat de betrokken verplichtingen, samenwerkingsmechanismen en beveiligingsregelingen van toepassing zijn op alle overheden en marktdeelnemers. De huidige tekst van overweging 5 en artikel 1 houdt geen rekening met het Eurosysteemmandaat, vastgelegd in het Verdrag, tot het voeren van oversight op betalings- en afwikkelingssystemen. Het voorstel moet derhalve gewijzigd worden om de verantwoordelijkheden van het Eurosysteem op dit vlak correct weer te geven.

⁽¹⁾ Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische-communicatienetwerken en -diensten (PB L 108 van 24.4.2002, blz. 33).

⁽²⁾ De oversighttaken van een aantal ESCB-leden worden op basis van nationale wetgeving uitgevoerd die de Eurosysteem-bevoegdheid aanvullen en in sommige geval dupliceren.

⁽³⁾ De term „afwikkeling” in dit advies omvat tevens de verrekeningsfunctie.

3.2 De regelingen en procedures voor centrale banken en andere bevoegde autoriteiten tot het voeren van oversight op betalings- en afwikkelingssystemen zijn vastgelegd in een aantal Unierichtlijnen en –verordeningen, met name:

- a) Richtlijn 98/26/EG van het Europees Parlement en de Raad (hierna de „Finaliteitsrichtlijn” ⁽¹⁾), op grond waarvan de bevoegde autoriteiten van lidstaten toezichtregelingen kunnen opleggen aan betalings- en afwikkelingssyste­men die onder hun jurisdictie vallen ⁽²⁾;
- b) Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad ⁽³⁾ (hierna de „EMIR-verordening”) die de rol van de Europese Autoriteit voor effecten en markten (EAEM), de Europese Bankautoriteit (EBA) en het ESCB erkent inzake het uitwerken van regelgevende normen en het uitoefenen van toezicht op centrale wederpartijen, en
- c) het voorstel voor een verordening tot verbetering van de effectenafwikkeling in de Europese Unie en betreffende centraleeffectenbewaarinstellingen (CSD’s) en tot wijziging van Richtlijn 98/26/EG ⁽⁴⁾ (hierna de „CSD-verordening”) die vereist dat de bevoegde autoriteiten met toezichthoudende en onderzoeksbevoegdheden bekleed worden, en met name artikel 45 van die verordening die prudentiële voorschriften voor CSD’s invoert, waaronder belangrijke bepalingen betreffende het limiteren van operationele risico’s.

3.3 Bovendien zij opemerkt dat op 3 juni 2013 de Raad van bestuur van de ECB de „Beginselen voor financiëlemarktinfra­structuren” („Principles for financial market infrastructures”) heeft goedgekeurd, welke beginselen in april 2012 werden ingevoerd door het „Committee on Payment and Settlement Systems (CPSS)” van de Bank voor Internationale Betalingen en het „Technical Committee of the International Organization of Securities Commissions (IOSCO)” ⁽⁵⁾, betreffende het uitoefenen van Eurosysteemoversight met betrekking tot alle soorten financiëlemarktinfra­structuren. Daarop volgde een publieke raadpleging aangaande een voorstel voor een verordening betreffende oversightvoorschriften voor systeemrelevante betalingssystemen (hierna de „SIPS-verordening”) ⁽⁶⁾. De SIPS-verorde­ning implementeert de CPSS-IOSCO-beginselen juridisch bindend en bestrijkt zowel systemen voor het betalen van grote bedragen als systeemrelevante detailhandelbetalingssystemen, al dan niet geëxploiteerd door Eurosysteem-NCB’s of particuliere entiteiten.

3.4 De huidige oversightregelingen ⁽⁷⁾ voor betalingssystemen en PSP’s omvatten reeds procedures voor vroegtijdige waarschuwingen ⁽⁸⁾ en gecoördineerde antwoorden ⁽⁹⁾ binnen het Eurosysteem en daarbuiten voor de aanpak van cyberbeveiligingsbedreigingen die gelijkaardig zijn aan de in artikel 10 en 11 van het voorstel bedoelde richtlijn.

3.5 Het ESCB heeft standaard vastgelegd voor rapportage en risicobeheerverplichtingen voor betalingssystemen. De ECB beoordeelt effectenafwikkelingssyste­men regelmatig om vast te stellen of zij voor gebruik in Eurosysteemkrediettransacties in aanmerking komt. Derhalve acht de ECB het noodzakelijk dat de vereisten in het voorstel die kritieke marktinfra­structuren en hun exploitanten ⁽¹⁰⁾ betreffen geen afbreuk aan de standaarden in de SIPS-verordening, het Eurosysteemoversightbeleidskader of andere unieregelingen en met name EMIR en het toekomstige CSDR. Bovendien moeten zij de taken van de EBA of EAEM en andere prudentiële toezichthouders ⁽¹¹⁾ onverlet laten.

⁽¹⁾ Richtlijn 98/26/EG van het Europees Parlement en de Raad van 19 mei 1998 betreffende het definitieve karakter van de afwikkeling van betalingen en effectentransacties in betalings- en afwikkelingssyste­men (PB L 166 van 11.6.1998, blz. 45).

⁽²⁾ Zie de derde alinea van artikel 10, lid 1 van de Finaliteitsrichtlijn.

⁽³⁾ Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad van 4 juli 2012 betreffende otc-derivaten, centrale tegenpartijen en transactieregisters (PB L 201 van 27.7.2012, blz. 1).

⁽⁴⁾ COM(2012) 73 final.

⁽⁵⁾ Beschikbaar op de website van de Bank voor Internationale Betalingen: <https://www.bis.org/publ/cpss94.pdf>

⁽⁶⁾ Beschikbaar op de ECB-website: www.ecb.europa.eu

⁽⁷⁾ Zie het ECB-perscommuniqué betreffende het Memorandum of Understanding (MoU) inzake hoogniveaubeginselen van samenwerking tussen de banktoezichthouders en centrale banken van de Europese Unie in crisisbeheersituaties (2003), beschikbaar op de ECB-website: www.ecb.europa.eu

⁽⁸⁾ Zie aanbeveling 3: incidentmonitoring en -rapportage in „Recommendations for the security of internet payments-final version after public consultation”, The European Forum on the Security of Retail Payments (SecuRe Pay), januari 2013, beschikbaar op de ECB-website: www.ecb.europa.eu

⁽⁹⁾ Gebaseerd op de beginselen voor samenwerking in internationaal oversight, zoals aangehaald door het CPSS-rapport van 2005, hebben centrale banken van het Eurosysteem in een aantal gevallen met succes deelgenomen aan samenwerkingsregelingen, zoals bijvoorbeeld blijkt uit de oversightregelingen voor SWIFT (the Society for Worldwide Interbank Financial Telecommunications) en de Continuous Linked Settlement (CLS).

⁽¹⁰⁾ Bijvoorbeeld, de voorschriften voor marktdeelnemers om te voldoen aan technische en organisatorische maatregelen in artikel 14, lid 3 en 4 en de bevoegdheid bindende instructies aan marktdeelnemers uit te vaardigen in artikel 15, lid 3 van het voorstel.

⁽¹¹⁾ Zie paragraaf 2.12 van ECB-advies CON/2014/9 inzake een voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende betalingsdiensten in de interne markt en houdende wijziging van de Richtlijnen 2002/65/EG, 2013/36/EU en 2009/110/EG en houdende intrekking van Richtlijn 2007/64/EG (PB C 224 van 15.7.2014, blz. 1). Alle ECB-adviezen worden gepubliceerd op de ECB-website: www.ecb.europa.eu

3.6 Niettegenstaande het voorgaande is de ECB van mening dat veel pleit voor het delen van relevante gegevens tussen het Eurosysteem en het NIB-Comité, zoals bedoeld krachtens artikel 19 van het voorstel. Voor mogelijkerwijze noodzakelijke effectieve informatiedeling, moeten de ECB, EBA en EAEM uitgenodigd worden vertegenwoordigers af te vaardigen naar vergaderingen van het NIB-comité voor agendapunten die van belang kunnen zijn voor de uitvoering van hun respectieve mandaten.

Gedaan te Frankfurt am Main, 25 juli 2014.

De president van de ECB

Mario DRAGHI

BIJLAGE

Formuleringsvoorstellen

Door de Commissie voorgestelde tekst	Door de ECB voorgestelde wijzigingen (1)
<p>Wijziging 1</p> <p>Overweging 5</p>	
<p>„(5) Om in alle relevante incidenten en risico's te voorzien, moet deze richtlijn van toepassing zijn op alle netwerk- en informatiesystemen. De verplichtingen ten aanzien van overheden en marktdeelnemers mogen echter niet van toepassing zijn op ondernemingen die openbare communicatienetwerken of openbare elektronischecommunicatie- diensten in de zin van Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische- communicatienetwerken en -diensten (kaderrichtlijn)(?) aanbieden, welke zijn onderworpen aan de in artikel 13 bis van die richtlijn vastgestelde specifieke veiligheids- en integriteitseisen, noch op aanbieders van vertrouwensdiensten.”</p>	<p>„(5) Om in alle relevante incidenten en risico's te voorzien, moet deze richtlijn van toepassing zijn op alle netwerk- en informatiesystemen. De verplichtingen ten aanzien van overheden en marktdeelnemers mogen echter niet van toepassing zijn op ondernemingen die openbare communicatienetwerken of openbare elektronischecommunicatie- diensten in de zin van Richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronische- communicatienetwerken en -diensten (kaderrichtlijn) (?) aanbieden, welke zijn onderworpen aan de in artikel 13 bis van die richtlijn vastgestelde specifieke veiligheids- en integriteitseisen, noch op aanbieders van vertrouwensdiensten. Voorts, niettegenstaande de toepassing van deze richtlijn op overheidsinstanties en marktdeelnemers, laat deze richtlijn de aan het Europees Stelsel van centrale banken (ESCB) uit hoofde van het Verdrag en de Statuten van het Europees Stelsel van centrale banken en van de Europese Centrale Bank toebedeelde taken en de werkzaamheden onverlet, alsook de equivalente taken die ESCB-leden uit hoofde van hun nationale wetgeving uitvoeren, met name het beleid aangaande het prudentieel toezicht op kredietinstellingen en het oversight op betalings- en afwikkelingssystemen. Lidstaten vertrouwen op het prudentieel toezicht en de oversighttaken uitgeoefend door de centrale banken en toezichhouders van die exploitanten, zulks binnen het gebied van hun bevoegdheid.”</p>

Toelichting

Overweging 5 moet gewijzigd worden om de verantwoordelijkheden van de ECB en de NCB's inzake oversight over en het reguleren van betalings- en afwikkelingssystemen. Krachtens het vierde streepje van artikel 127, lid 2 van het Verdrag is een van de ESCB-basistaken de goede werking van het betalingsverkeer te bevorderen. Uit hoofde van artikel 22 van de ESCB-statuten kan de ECB verordeningen opstellen om efficiënte en gezonde verrekenings- en betalingssystemen te waarborgen. Overwogen moet worden dat uit hoofde van artikel 127, lid 5 van het Verdrag het ESCB bijdraagt tot een goede beleidsvoering ten aanzien van de stabiliteit van het financiële stelsel. Bovendien luidens het oversightbeleidskader van het Eurosysteem van juli 2011 (2), „is het uitoefenen van oversight op betalings- en afwikkelingssystemen een centralebankfunctie krachtens welke de doelstellingen van veiligheid en efficiency bevorderd worden door monitoring van huidige en geplande systemen, welke systemen tegen deze doelstellingen beoordeeld worden en, indien nodig, tot veranderingen aanzetten”.

Anders geformuleerd, waarborgen dat systemen veilig en efficiënt zijn is een belangrijke voorwaarde voor de bijdrage van het Eurosysteem aan financiële stabiliteit, om monetair beleid uit te voeren en het publieke vertrouwen in de euro te handhaven.

Voorts, overeenkomst de ECB-opmerkingen betreffende de voorgenomen herziening van de richtlijn betreffende betalingsdiensten (PSD2), zij opgemerkt dat nationale toezichthouders en centrale banken de bevoegde autoriteiten zijn die richtsnoeren inzake incidentbeheer en incident-notificaties voor PSP's uitvaardigen, alsook richtsnoeren uitvaardigen betreffende het delen van incidentnotificaties tussen de betreffende autoriteiten. De overweging moet ook genoegzaam rekening houden met de bij Verordening (EU) nr. 1024/2013 aan de ECB toegekende taken.

Door de Commissie voorgestelde tekst

Door de ECB voorgestelde wijzigingen (1)

Tenslotte, indien niet-eurogebied ESCB-leden uit hoofde van nationale wetgeving taken uitvoeren die equivalent zijn aan verdragstaken en taken uit de ESCB-statuten, dan moeten die functies eveneens ongemoeid blijven.

Wijziging 2

Artikel 1, lid 4, en artikel 1, lid 5 (nieuw)

<p>„4. Deze richtlijn laat de EU-wetgeving inzake cybercriminaliteit en Richtlijn 2008/114/EG van de Raad 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, onverlet (9).</p> <p>5. Deze richtlijn laat Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (10) en Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie alsmede de verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (11), eveneens onverlet.</p> <p>6. Voor de uitwisseling van informatie in het samenwerkingsnetwerk krachtens hoofdstuk III en de melding van NIB-incidenten krachtens artikel 14 kan de verwerking van persoonsgegevens vereist zijn. Deze verwerking, die noodzakelijk is ter verwezenlijking van de met deze richtlijn nagestreefde doelstellingen van algemeen belang, wordt door de lidstaten toegestaan uit hoofde van artikel 7 van Richtlijn 95/46/EG en Richtlijn 2002/58/EG, zoals in de nationale wetgeving ten uitvoer gelegd.”</p>	<p>„4. Deze richtlijn laat de EUUnie-wetgeving inzake cybercriminaliteit en Richtlijn 2008/114/EG van de Raad 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, onverlet (9).</p> <p>5. Deze richtlijn laat het oversight en de taken, die aan de ECB en het ECB zijn toegekend, op het gebied van beleidsvoering met betrekking tot het prudentieel toezicht op kredientinstellingen en betalings- en afwikkelingssystemen waarvoor binnen het ESCB-regelgevende kader en andere verband houde richtlijnen en verordeningen van de Unie specifieke risicobeheer- en beveiligingsvoorschriften vastgesteld zijn. Evenzeer laat deze richtlijn gelijkaardige door ESCB-leden uit hoofde van hun nationale wetgeving uitgeoefende functies onverlet.</p> <p>56. Deze richtlijn laat Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (10) en Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie alsmede de verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (11), eveneens onverlet.</p> <p>67. Voor de uitwisseling van informatie in het samenwerkingsnetwerk krachtens hoofdstuk III en de melding van NIB-incidenten krachtens artikel 14 kan de verwerking van persoonsgegevens vereist zijn. Deze verwerking, die noodzakelijk is ter verwezenlijking van de met deze richtlijn nagestreefde doelstellingen van algemeen belang, wordt door de lidstaten toegestaan uit hoofde van artikel 7 van Richtlijn 95/46/EG en Richtlijn 2002/58/EG, zoals in de nationale wetgeving ten uitvoer gelegd.”</p>
---	---

Toelichting

Zoals boven opgemerkt heeft het ESCB er een groot belang bij te waarborgen dat betalings- en afwikkelingssystemen naar behoren functioneren. Dit heeft te maken met het belang van betalings-, verrekenings- en afwikkelingssystemen voor het goede verloop van monetairebeleidstransacties en met de rol die zij spelen bij het waarborgen van de stabiliteit van het financiële stelsel in het algemeen. Daarom beveelt de ECB aan dat het voorstel rekening houdt met de rol van het ESCB aangaande de huidige betalings- en afwikkelingssystemen en het oversightkader. Het ESCB beschikt over zeer effectieve instrumenten om de veiligheids- en efficiëncyniveaus van deze systemen te beoordelen. De overweging moet ook genoegzaam rekening houden met de bij Verordening (EU) nr. 1024/2013 aan de ECB toegekende taken.

Het voorstel moet ook de equivalent functies onverlet laten die niet-eurogebied ESCB-leden uit hoofde van hun nationale wetgeving uitoefenen.

Door de Commissie voorgestelde tekst	Door de ECB voorgestelde wijzigingen (1)
<p>Wijziging 3</p> <p>Artikel 6, lid 1</p>	
<p>„1. Elke lidstaat wijst een voor de beveiliging van netwerk- en informatiesystemen bevoegde nationale autoriteit (de „bevoegde autoriteit”) aan.”</p>	<p>„1. Elke lidstaat wijst een voor de beveiliging van netwerk- en informatiesystemen bevoegde nationale autoriteit (de „bevoegde autoriteit”) aan.</p> <p>Effectieve samenwerking wordt ingesteld tussen de bevoegde autoriteit en de Europese en nationale regelgevende autoriteiten.”</p>

Toelichting

De ECB beveelt aan dat artikel 6, lid 1 gewijzigd wordt om een goed samenwerkingsniveau op unieniveau te waarborgen.

<p>Wijziging 4</p> <p>Artikel 8, lid 3</p>	
<p>„3. Binnen het samenwerkingsnetwerk doen de bevoegde autoriteiten het volgende:</p> <p>a) zij verspreiden vroegtijdige waarschuwingen over risico's en incidenten overeenkomstig artikel 10;</p> <p>b) zij zorgen voor een gecoördineerde reactie overeenkomstig artikel 11;</p> <p>c) zij maken regelmatig niet-vertrouwelijke informatie over vroegtijdige waarschuwingen en gecoördineerde reacties die op dat moment worden verspreid of aan de gang zijn, bekend op een gemeenschappelijke website;</p> <p>d) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, een of meer in artikel 5 bedoelde nationale NIB-strategieën en nationale NIB-samenwerkingsplannen, binnen het toepassingsgebied van deze richtlijn;</p> <p>e) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, de doeltreffendheid van de CERT's, met name wanneer er NIB-oefeningen worden verricht op het niveau van de Unie;</p> <p>f) zij werken samen met en wisselen informatie over alle relevante kwesties uit met het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol, en met andere relevante Europese instanties, met name op het gebied van gegevensbescherming, energie, vervoer, bankieren, effectenbeurzen en gezondheid;</p> <p>g) zij wisselen onderling en met de Commissie beste praktijken uit en verlenen elkaar bijstand bij het opbouwen van capaciteit op het gebied van NIB;</p> <p>h) zij organiseren regelmatig collegiale toetsingen met betrekking tot capaciteit en paraatheid;</p>	<p>„3. Binnen het samenwerkingsnetwerk doen de bevoegde autoriteiten het volgende:</p> <p>a) zij verspreiden vroegtijdige waarschuwingen over risico's en incidenten overeenkomstig artikel 10;</p> <p>b) zij zorgen voor een gecoördineerde reactie overeenkomstig artikel 11;</p> <p>c) zij maken regelmatig niet-vertrouwelijke informatie over vroegtijdige waarschuwingen en gecoördineerde reacties die op dat moment worden verspreid of aan de gang zijn, bekend op een gemeenschappelijke website;</p> <p>d) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, een of meer in artikel 5 bedoelde nationale NIB-strategieën en nationale NIB-samenwerkingsplannen, binnen het toepassingsgebied van deze richtlijn;</p> <p>e) zij bespreken en beoordelen gezamenlijk, op verzoek van een lidstaat of van de Commissie, de doeltreffendheid van de CERT's, met name wanneer er NIB-oefeningen worden verricht op het niveau van de Unie;</p> <p>f) zij werken samen met en wisselen informatie over alle relevante kwesties uit met het Europees Centrum voor de bestrijding van cybercriminaliteit van Europol, en met andere relevante Europese instanties, met name op het gebied van gegevensbescherming, energie, vervoer, bankieren, effectenbeurzen en gezondheid;</p> <p>g) zij wisselen onderling en met de Commissie beste praktijken uit en verlenen elkaar bijstand bij het opbouwen van capaciteit op het gebied van NIB;</p> <p>h) zij organiseren regelmatig collegiale toetsingen met betrekking tot capaciteit en paraatheid;</p>

Door de Commissie voorgestelde tekst	Door de ECB voorgestelde wijzigingen ⁽¹⁾
i) zij organiseren NIB-oefeningen op het niveau van de Unie en nemen indien passend deel aan internationale NIB-oefeningen.”	i) zij organiseren NIB-oefeningen op het niveau van de Unie en nemen indien passend deel aan internationale NIB-oefeningen; j) waarborgen de informatie-uitwisseling met Europese en nationale regelgevende autoriteiten (bv. voor de financiële sector: het Europees Stelsel van centrale banken, de Europese Bankautoriteit (EBA), Europese Autoriteit voor effecten en markten (EAEM) die nauw samenwerken indien beveiligingsincidenten vastgesteld worden die mogelijkerwijze de goede werking van betalings- en afwikkelingssystemen zouden kunnen belemmeren). ”

Toelichting

Er pleit veel voor informatie te delen met het Europese Netwerk en Informatieveiligheid Agentschap of uit hoofde van het voorstel bevoegde autoriteiten, en met de EBA of EAEM als de bevoegde autoriteit voor de coördinatie van met PSP's verbandhoudende incidenten.

Derhalve stelt de ECB deze wijziging voor om informatiedeling en betere coördinatie op unieniveau te bevorderen.

Wijziging 5

Artikel 19, lid 1

„1. De Commissie wordt bijgestaan door een comité (het comité Netwerk- en informatiebeveiliging). Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.”	„1. De Commissie wordt bijgestaan door een comité (het comité Netwerk- en informatiebeveiliging). Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011. De ECB, de EBA en de EAEM worden uitgenodigd een vertegenwoordiger af te vaardigen naar de vergadering van het Comité Netwerk en Informatieveiligheid aangaande agenda-punten die implicaties zouden kunnen hebben voor de uitvoering vna de respectieve mandaten van de ECB, EBA of EAEM. ”
--	--

Toelichting

De ECB heeft er een gevestigd belang bij de beveiliging van betalings- en afwikkelingssystemen, diensten en instrumenten te versterken, zijnde belangrijke onderdelen voor het handhaven van het vertrouwen in de gemeenschappelijke munt en de goede werking van de economie in de Unie. Daarom beveelt de ECB aan dat zij uitgenodigd wordt voor de vergaderingen van het NIB-comité. In elk geval moet de ECB uit hoofde van het Verdrag formeel geraadpleegd worden ten aanzien van dergelijke maatregelen die verband houden met betalingssystemen, en enige andere gelegenheid die binnen de ECB-bevoegdheidsgebieden vallen.

De EBA of EAEM moet ook betrokken worden bij met PSP's verbandhoudende aangelegenheden.

⁽¹⁾ De vet gedrukte tekst geeft aan waar de ECB voorstelt om een nieuwe tekst toe te voegen Doorhaling betreft tekst die de ECB voorstelt te schrappen.

⁽²⁾ Beschikbaar op de ECB-website: www.ecb.europa.eu