III

(Akty przygotowawcze)

EUROPEJSKI BANK CENTRALNY

OPINIA EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 25 lipca 2014 r.

w sprawie projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii

(CON/2014/58)

(2014/C 352/04)

Wprowadzenie i podstawa prawna

W dniu 7 lutego 2013 Komisja Europejska opublikowała projekt dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii ([1]) (zwany dalej „projektem dyrektywy").

Europejski Bank Centralny (EBC) zdecydował o wydaniu opinii z własnej inicjatywy wobec braku wniosku o wydanie takiej opinii ze strony projektodawców. Właściwość EBC do wydania opinii wynika z art 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, biorąc pod uwagę że projekt dyrektywy zawiera postanowienia dotyczące jednego z zadań Europejskiego Systemu Banków Centralnych (ESBC), to jest popierania należytego funkcjonowania systemów płatniczych, o którym mowa w art. 127 ust. 2 Traktatu. Dodatkowo art. 22 Statutu Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (zwanego dalej „Statutem ESBC") przewiduje, że EBC i krajowe banki centralne (KBC) mogą stwarzać udogodnienia, a EBC może uchwalać rozporządzenia, w celu zapewnienia skuteczności i rzetelności systemów rozliczeń i płatności w ramach Unii i z innymi krajami. Rada Prezesów wydała niniejszą opinię zgodnie ze zdaniem pierwszym art. 17 ust. 5 Regulaminu Europejskiego Banku Centralnego.

1. Cel projektu dyrektywy

1.1. Celem projektu dyrektywy jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji poprzez zwiększenie bezpieczeństwa internetu oraz sieci i systemów informatycznych stanowiących podstawę funkcjonowania naszego społeczeństwa i gospodarki. Projekt ten stanowi realizację głównego działania przewidzianego w europejskiej strategii bezpieczeństwa cybernetycznego ([2]).

1.2. Sieci i systemy informatyczne odgrywają istotną rolę w ułatwianiu transgranicznego przepływu towarów, usług i osób. Ze względu na ten nieunikniony wymiar ponadnarodowy zakłócenia w jednym państwie członkowskim mogą mieć również wpływ na inne państwa członkowskie oraz na Unię jako całość. Dodatkowo prawdopodobieństwo częstego występowania incydentów i niemożność zapewnienia skutecznej ochrony zmniejszają społeczne zaufanie do bezpieczeństwa sieci i informacji. Odporność i stabilność sieci i systemów informatycznych mają zatem zasadnicze znaczenie dla zapewnienia sprawnego funkcjonowania rynku wewnętrznego.

1.3. Projekt dyrektywy opiera się na dotychczasowych inicjatywach w tej dziedzinie ([3]). W odniesieniu do powyższego, w projekcie dyrektywy dostrzeżono potrzebę harmonizacji zasad dotyczących bezpieczeństwa sieci i informacji oraz stworzenia efektywnych mechanizmów współpracy między państwami członkowskimi.

([1]) COM(2013) 48 final.

([2]) Zob. wspólny komunikat skierowany do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", JOIN(2013) 1 final.

([3]) Odnoszą się do tego w szczególności następujące komunikaty: komunikat pt. „Network and Information Security: Proposal for a European Policy Approach" COM(2001) 298 final; „Strategia na rzecz bezpiecznego społeczeństwa informacyjnego – »Dialog, partnerstwo i przejmowanie inicjatywy«" COM(2006) 251 final; „Ochrona krytycznej infrastruktury informatycznej – »Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi: zwiększenie gotowości, bezpieczeństwa i odporności«" COM(2009) 149 final; „Europejska agenda cyfrowa" COM(2010) 245 final oraz „Ochrona krytycznej infrastruktury teleinformatycznej »Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni«" COM(2011) 163 final.

1.4. Projekt dyrektywy ustanawia wspólne unijne ramy prawne w zakresie bezpieczeństwa sieci i informacji w odniesieniu do zdolności państw członkowskich, mechanizmów współpracy na poziomie unijnym oraz wymogów dotyczących organów administracji publicznej i podmiotów prywatnych w określonych najważniejszych sektorach. Powinno to zapewnić odpowiednie przygotowanie na poziomie krajowym i przyczynić się do wytworzenia klimatu wzajemnego zaufania, co jest niezbędnym warunkiem skutecznej współpracy na poziomie Unii. Ustanowienie mechanizmów współpracy na poziomie Unii za pośrednictwem odpowiedniej sieci umożliwi zapobieganie transgranicznym incydentom i zagrożeniom w zakresie bezpieczeństwa sieci i informacji oraz reagowanie na nie w spójny i skoordynowany sposób.

1.5. Najważniejsze postanowienia projektu dyrektywy dotyczą:

a) zobowiązania wszystkich państw członkowskich do zagwarantowania minimalnego poziomu krajowych zdolności poprzez ustanowienie właściwych organów ds. bezpieczeństwa sieci i informacji, powołanie zespołów reagowania na incydenty komputerowe oraz przyjęcie krajowych strategii i planów współpracy w zakresie bezpieczeństwa sieci i informacji;

b) wymiany informacji wymaganej pomiędzy państwami członkowskimi należącymi do sieci, jak również stworzenie ogólnoeuropejskiego planu współpracy w ramach bezpieczeństwa sieci i informacji oraz koordynacji systemu wczesnego ostrzegania o incydentach związanych z bezpieczeństwem cybernetycznym;

c) opierając się na modelu, jakim jest dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady ([1]), zapewnienie rozwoju kultury wspierającej przeciwdziałanie zagrożeniom oraz wymiany informacji między sektorem prywatnym i publicznym. Przedsiębiorstwa w określonych najważniejszych sektorach oraz organy administracji publicznej będą zobowiązane do dokonania oceny zagrożeń, na jakie są narażone, oraz do przyjęcia odpowiednich i proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą również zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość krytycznych usług i dostaw towarów.

2. **Uwagi ogólne**

2.1. EBC popiera cel projektu dyrektywy, jakim jest zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii oraz zapewnienie spójności działań w tym zakresie pomiędzy sektorami gospodarki oraz państwami członkowskimi. Ważne jest zapewnienie, aby rynek wewnętrzny był bezpiecznym miejscem prowadzenia działalności gospodarczej, a państwa członkowskie miały określony minimalny poziom gotowości do reakcji na wypadek incydentów związanych z bezpieczeństwem cybernetycznym.

2.2. EBC uważa jednak, że projekt dyrektywy nie powinien naruszać istniejących rozwiązań w zakresie nadzoru sprawowanego przez Eurosystem nad systemami płatności i rozrachunku ([2]), który obejmuje stosowne rozwiązania m.in. w zakresie bezpieczeństwa sieci i informacji. Należy zaznaczyć, że EBC jest szczególnie zainteresowany poprawą funkcjonalności systemów płatności i rozrachunku ([3]) w celu poprawy należytego funkcjonowania systemów płatności oraz wspierania utrzymania zaufania do euro i funkcjonowania gospodarki w Unii.

2.3. Dodatkowo ocena rozwiązań w zakresie bezpieczeństwa oraz zgłaszanie incydentów dotyczących systemów płatności i rozrachunku oraz dostawców usług płatniczych jest jednym z podstawowych zadań nadzoru ostrożnościowego i banków centralnych. Odpowiedzialność za rozwijanie wymogów nadzorczych w powyższych obszarach powinna w związku z tym nadal spoczywać na tych podmiotach, a systemy płatności i rozrachunku oraz dostawcy usług płatniczych nie powinni być objęci potencjalnie sprzecznymi wymogami nałożonymi przez inne władze krajowe. Co więcej, zarządzanie ryzykiem, w tym wymogi bezpieczeństwa dotyczące systemów płatności i rozrachunku oraz innych infrastruktur rynku w strefie euro, prowadzone jest przez Eurosystem, składający się z EBC oraz KBC z państw członkowskich, które przyjęły euro. Poprzez tę funkcję nadzorczą Eurosystem dąży do zapewnienia należytego funkcjonowania systemów płatności i rozrachunku, stosując m.in. właściwe standardy nadzorcze i wymogi minimalne. Projekt dyrektywy powinien uwzględniać obowiązujące obecnie rozwiązania nadzorcze i zapewnić spójność regulacyjną na terenie Unii.

3. **Uwagi szczegółowe**

3.1. Zgodnie z motywem 5 oraz art. 1 projektu dyrektywy stosowne obowiązki, mechanizm współpracy oraz wymogi w zakresie bezpieczeństwa mają zastosowanie do wszystkich organów administracji publicznej i podmiotów gospodarczych. Obecne brzmienie motywu 5 oraz art. 1 nie uwzględnia przewidzianej w Traktacie właściwości Eurosystemu do sprawowania nadzoru nad systemami płatności i rozrachunku. Projekt dyrektywy powinien zatem zostać zmieniony, aby we właściwy sposób uwzględniał zadania Eurosystemu w tej dziedzinie.

([1]) Dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz.U. L 108 z 24.4.2002, s. 33).

([2]) Funkcje nadzorcze części członków ESBC sprawowane są na podstawie prawa krajowego, które uzupełnia, a w niektórych przypadkach powiela kompetencje Eurosystemu.

([3]) Termin „rozrachunek" użyty w tekście niniejszej opinii obejmuje również funkcję rozliczeniową.

3.2. Przewidziane w stosunku do banków centralnych oraz innych właściwych organów rozwiązania i procedury w zakresie nadzoru nad systemami płatności i rozrachunku papierów wartościowych zawarte są w szeregu dyrektyw i rozporządzeń unijnych, do których należą w szczególności:

a) dyrektywa 98/26/WE Parlamentu Europejskiego i Rady w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych (zwana dalej „dyrektywą o ostateczności rozrachunku") ([1]), która nadaje właściwym organom państw członkowskich uprawnienie do wdrażania rozwiązań nadzorczych w stosunku do podlegających ich właściwości systemów płatności i rozrachunku ([2]);

b) rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 ([3]) (zwane dalej „rozporządzeniem w sprawie infrastruktury rynku europejskiego": (EMIR)), które podkreśla rolę Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych (ESMA), Europejskiego Urzędu Nadzoru Bankowego (EBA) oraz ESBC w ustalaniu standardów regulacyjnych i nadzorze nad partnerami centralnymi; oraz

c) wniosek dotyczący rozporządzenia w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych (CDPW) oraz zmieniającego dyrektywę 98/26/WE ([4]) (zwanego dalej „rozporządzeniem w sprawie CDPW"), nakładający obowiązek powierzenia właściwym organom uprawnień nadzorczych i dochodzeniowych, a w szczególności art. 45 tego rozporządzenia, który wprowadza wymogi ostrożnościowe dotyczące centralnych depozytów papierów wartościowych, w tym ważne postanowienia dotyczące ograniczenia ryzyka operacyjnego.

3.3. Należy również zauważyć, że dnia 3 czerwca 2013 r. Rada Prezesów EBC przyjęła zasady dotyczące infrastruktury rynku finansowego wydane w kwietniu 2012 r. przez Komitet ds. Systemów Płatności i Rozrachunku (CPSS) Banku Rozrachunków Międzynarodowych i Komitet Techniczny Międzynarodowej Organizacji Komisji Papierów Wartościowych (IOSCO) ([5]) w zakresie sprawowania przez Eurosystem nadzoru nad różnymi rodzajami infrastruktury rynków finansowych. Następnym etapem były konsultacje społeczne dotyczące projektu rozporządzenia w sprawie wymogów nadzorczych w odniesieniu do systemów płatności o znaczeniu systemowym (zwanego dalej „rozporządzeniem SIPS") ([6]). Rozporządzenie SIPS wdraża zasady określone przez CPSS i IOSCO w sposób prawnie wiążący oraz obejmuje zarówno wysokokwotowe, jak i detaliczne systemy płatności o znaczeniu systemowym prowadzone przez KBC Eurosystemu lub podmioty prywatne.

3.4. Obecne rozwiązania nadzorcze ([7]) w odniesieniu do systemów płatności oraz dostawców usług płatniczych zawierają już procedury wczesnego ostrzegania ([8]) oraz skoordynowanych reakcji ([9]) wewnątrz Eurosystemu i poza nim na potrzeby przeciwdziałania możliwym zagrożeniom cybernetycznym, które to procedury odpowiadają przewidzianym w art. 10 i 11 projektu dyrektywy.

3.5. ESBC wprowadził standardy dotyczące sprawozdawczości oraz obowiązki w zakresie zarządzania ryzykiem w odniesieniu do systemów płatniczych. Dodatkowo EBC dokonuje regularnej oceny systemów rozrachunku papierów wartościowych w celu określenia możliwości wykorzystania ich na potrzeby operacji kredytowych Eurosystemu. W związku z tym EBC uważa za konieczne, aby zawarte w projekcie dyrektywy wymogi odnoszące się do najważniejszych infrastruktur rynku oraz podmiotów, które nimi zarządzają ([10]) nie były sprzeczne ze standardami przewidzianymi w rozporządzeniu SIPS, zasadami nadzorczymi Eurosystemu, ani innymi przepisami unijnymi, w szczególności rozporządzeniem EMIR oraz przyszłym rozporządzeniem CDPW. Co więcej, wymogi te nie powinny kolidować z zadaniami EBA, ESMA oraz innych nadzorców ostrożnościowych ([11]).

([1]) Dyrektywa 98/26/WE Parlamentu Europejskiego i Rady z dnia 19 maja 1998 r. w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych (Dz.U. L 166 z 11.6.1998, s. 45).

([2]) Zob. art. 10 ust. 1 pkt 3 dyrektywy o ostateczności rozrachunku.

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1).

([4]) COM(2012) 73 final.

([5]) Dokument dostępny na stronie internetowej Banku Rozrachunków Międzynarodowych pod adresem https://www.bis.org/publ/cpss94.pdf

([6]) Dokument dostępny na stronie internetowej EBC pod adresem http://www.ecb.europa.eu

([7]) Zob. komunikat prasowy EBC w sprawie protokołu ustaleń dotyczącego zasad ogólnych współpracy pomiędzy nadzorcami bankowymi a bankami centralnymi Unii Europejskiej w sytuacjach zarządzania kryzysowego (2003), dostępny na stronie internetowej EBC pod adresem www.ecb.europa.eu

([8]) Zob. zalecenie nr 3 dotyczące monitorowania i zgłaszania incydentów w dokumencie „Recommendations for the security of internet payments-final version after public consultation", Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych (forum SecurePay), styczeń 2013, dostępnym na stronie internetowej EBC pod adresem www.ecb.europa.eu

([9]) Mając na uwadze zasady międzynarodowego nadzoru opartego na współpracy, do których odnosi się raport nadzorczy CPSS z 2005 r., banki centralne Eurosystemu wielokrotnie z powodzeniem uczestniczyły we wspólnych przedsięwzięciach, czego przykładem są rozwiązania nadzorcze dla SWIFT (Stowarzyszenia Międzynarodowej Teletransmisji Danych Finansowych) oraz na rzecz systemu rozrachunku ciągłego (CLS).

([10]) Przykładowo wymóg, aby podmioty gospodarcze przestrzegały środków technicznych i organizacyjnych przewidzianych w art. 14 ust. 3 i 4 oraz uprawnienie do wydawania wiążących instrukcji wobec tych podmiotów przewidziane w art. 15 ust. 3 projektu dyrektywy.

([11]) Zob. pkt 2.12 opinii CON/2014/9 w sprawie projektu dyrektywy Parlamentu Europejskiego i Rady w sprawie usług płatniczych w ramach rynku wewnętrznego oraz zmieniającej dyrektywy 2002/65/WE, 2013/36/UE i 2009/110/WE i uchylającej dyrektywę 2007/64/WE (Dz.U. C 224 z 15.7.2014, s. 1). Opinie EBC są publikowane na stronie internetowej EBC pod adresem www.ecb.europa.eu

3.6. Z zastrzeżeniem powyższego EBC jest zdania, że istnieje wyraźna potrzeba ustalenia zasad wymiany informacji pomiędzy Eurosystemem a Komitetem ds. Bezpieczeństwa Sieci i Informacji, stosownie do art. 19 projektu dyrektywy. Na potrzeby efektywnej wymiany informacji, która może okazać się konieczna, EBC, EBA i ESMA powinny zostać zaproszone do oddelegowania przedstawiciela na spotkania Komitetu ds. Bezpieczeństwa Sieci i Informacji w sprawach, które mogłyby mieć znaczenie dla sprawowania powierzonych im zadań.

Sporządzono we Frankfurcie nad Menem dnia 25 lipca 2014 r.

Mario DRAGHI

Prezes Ebc

ZAŁĄCZNIK

Propozycje zmian

Tekst proponowany przez Komisję	Zmiany proponowane przez EBC [1]
Zmiana nr 1	
Motyw 5	
„(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych. Obowiązki nałożone na organy administracji publicznej i podmioty gospodarcze nie powinny mieć jednak zastosowania w odniesieniu do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) [2], które podlegają szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w art. 13a tej dyrektywy, ani nie powinny mieć zastosowania w odniesieniu do dostawców usług zaufania.”	„(5) W celu uwzględnienia wszystkich istotnych incydentów i zagrożeń niniejsza dyrektywa powinna mieć zastosowanie do wszystkich sieci i systemów informatycznych. Obowiązki nałożone na organy administracji publicznej i podmioty gospodarcze nie powinny mieć jednak zastosowania w odniesieniu do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) [2], które podlegają szczególnym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w art. 13a tej dyrektywy, ani nie powinny mieć zastosowania w odniesieniu do dostawców usług zaufania. **Dodatkowo, niezależnie od zastosowania niniejszej dyrektywy do organów administracji publicznej i podmiotów gospodarczych, niniejsza dyrektywa nie wpływa na zadania i obowiązki nałożone na Europejski System Banków Centralnych (ESBC) przez Traktat oraz Statut Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego, ani też na odpowiadające im zadania wykonywane przez członków ESBC na podstawie ich prawodawstwa krajowego, w szczególności w odniesieniu do zasad dotyczących nadzoru ostrożnościowego nad instytucjami kredytowymi oraz nadzoru nad systemami płatności i rozrachunku papierów wartościowych. Państwa członkowskie respektują funkcje w zakresie nadzoru ostrożnościowego i nadzoru wykonywane przez banki centralne oraz nadzorców takich podmiotów w granicach ich kompetencji.**”

Uzasadnienie

Motyw 5 powinien zostać zmieniony, aby uwzględniał zadania EBC oraz KBC w zakresie nadzoru nad systemami płatności i rozrachunku oraz w zakresie regulacji działalności tych systemów. Na podstawie art. 127 ust. 2 tiret 4 Traktatu jednym z zadań ESBC jest popierania należytego funkcjonowania systemów płatniczych. Również art. 22 Statutu ESBC nadaje EBC uprawnienia do przyjmowania rozporządzeń w celu zapewnienia skuteczności i rzetelności systemów rozliczeń i płatności. Na podstawie art. 127 ust. 5 Traktatu ESBC przyczynia się do należytego wykonywania polityk w odniesieniu do stabilności systemu finansowego. Dodatkowo, stosownie do dokumentu „Eurosystem's Oversight Policy Framework” z lipca 2011 r. [2], „nadzór nad systemami płatności i rozrachunku sprawowany jest przez bank centralny a cele dotyczące bezpieczeństwa i efektywności wspierane są przez monitorowanie istniejących i planowanych systemów, poprzez ich ocenę w stosunku do tych celów oraz wprowadzanie zmian tam, gdzie będzie to niezbędne”.

Innymi słowy, zapewnienie bezpieczeństwa i efektywności systemów jest ważnym warunkiem wstępnym przyczyniania się przez Eurosystem do utrzymania stabilności finansowej, prowadzenia polityki pieniężnej oraz utrzymania zaufania do euro.

Dodatkowo, zgodnie z uwagami EBC zgłoszonymi na potrzeby rewizji dyrektywy o usługach płatniczych, należy zauważyć, że nadzorcy krajowi oraz banki centralne są organami właściwymi na potrzeby wydawania wytycznych, zarządzania incydentami oraz zgłaszania incydentów do dostawców usług płatniczych, jak również do wydawania wytycznych dotyczących wymiany informacji w zakresie powiadomień o incydentach pomiędzy właściwymi władzami. Niniejszy motyw powinien również uwzględniać zadania powierzone EBC na podstawie rozporządzenia (UE) nr 1024/2013.

Tekst proponowany przez Komisję	Zmiany proponowane przez EBC [1]
Wreszcie, jeżeli na podstawie przepisów krajowych członkowie ESBC spoza strefy euro wykonują funkcje odpowiadające zadaniom zawartym w Traktacie oraz Statucie ESBC, funkcje te również nie powinny być naruszane przez postanowienia projektu dyrektywy.	

Zmiana nr 2

Artykuł 1 ust. 4 i 5 (dodany)

„4. Niniejszą dyrektywę stosuje się bez uszczerbku dla unijnych przepisów dotyczących cyberprzestępczości oraz dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony ([9]).	„4. Niniejszą dyrektywę stosuje się bez uszczerbku dla unijnych przepisów dotyczących cyberprzestępczości oraz dyrektywy Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony ([9]).
5. Niniejsza dyrektywa pozostaje również bez uszczerbku dla dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([10]), dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych ([11]).	**5. Niniejszą dyrektywę stosuje się bez uszczerbku dla nadzoru oraz zadań powierzonych EBC oraz ESBC w zakresie polityk odnoszących się do nadzoru ostrożnościowego nad instytucjami kredytowymi oraz systemami płatności i rozrachunku, dla których właściwe wymogi w zakresie zarządzania ryzykiem oraz bezpieczeństwa ustanowione zostały w ramach przepisów regulacyjnych ESBC oraz innych stosownych unijnych dyrektyw i rozporządzeń. W takim samym stopniu niniejsza dyrektywa pozostaje bez uszczerbku dla odpowiednich zadań wykonywanych przez członków ESBC na podstawie ich przepisów krajowych.**
6. Wymiana informacji w ramach sieci współpracy na mocy rozdziału III i zgłaszanie incydentów dotyczących bezpieczeństwa sieci i informacji na mocy art. 14 mogą wymagać przetwarzania danych osobowych. Państwo członkowskie zezwala na takie przetwarzanie, które jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym, zgodnie z ustawodawstwem krajowym implementującym art. 7 dyrektywy 95/46/WE i dyrektywę 2002/58/WE.”	~~6~~ **6.** Niniejsza dyrektywa pozostaje również bez uszczerbku dla dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych ([10]), dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych ([11]). ~~7~~ **7.** Wymiana informacji w ramach sieci współpracy na mocy rozdziału III i zgłaszanie incydentów dotyczących bezpieczeństwa sieci i informacji na mocy art. 14 mogą wymagać przetwarzania danych osobowych. Państwo członkowskie zezwala na takie przetwarzanie, które jest niezbędne do realizacji celów niniejszej dyrektywy będących w interesie publicznym, zgodnie z ustawodawstwem krajowym implementującym art. 7 dyrektywy 95/46/WE i dyrektywę 2002/58/WE.”

Uzasadnienie

Jak wskazano powyżej, w interesie ESBC pozostaje prawidłowe funkcjonowanie systemów płatności i rozrachunku. Wynika to z wagi systemów płatności, rozliczeń i rozrachunku dla należytego funkcjonowania operacji polityki pieniężnej oraz z roli, jaką odgrywają one w zapewnieniu ogólnej stabilności systemu finansowego. Dlatego też EBC zaleca, aby projekt dyrektywy uwzględnił rolę ESBC w odniesieniu do systemów płatności i rozrachunku oraz obowiązujące już rozwiązania nadzorcze. ESBC posiada wysoce efektywne narzędzia oceny poziomu bezpieczeństwa i efektywności tych systemów. Niniejszy motyw powinien również uwzględniać zadania powierzone EBC na podstawie rozporządzenia (UE) nr 1024/2013.

Projekt dyrektywy powinien również pozostać bez uszczerbku dla równoważnych zadań wykonywanych przez członków ESBC na podstawie ich przepisów krajowych.

Tekst proponowany przez Komisję	Zmiany proponowane przez EBC [1]
Zmiana nr 3	
Artykuł 6 ust. 1	
„1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych (»właściwy organ«)."	„1. Każde państwo członkowskie wyznacza właściwy organ krajowy ds. bezpieczeństwa sieci i systemów informatycznych (»właściwy organ«). **Należy zapewnić należytą współpracę pomiędzy właściwymi organami a organami regulacyjnymi na szczeblu europejskim i krajowym.**"
Uzasadnienie	
EBC zaleca zmianę art. 6 ust. 1 w celu zapewnienia właściwego poziomu współpracy na poziomie unijnym.	
Zmiana nr 4	
Artykuł 8 ust. 3	
„3. W ramach sieci współpracy właściwe organy:	„3. W ramach sieci współpracy właściwe organy:
a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;	a) przekazują wczesne ostrzeżenia dotyczące zagrożeń i incydentów zgodnie z art. 10;
b) zapewniają skoordynowaną reakcję zgodnie z art. 11;	b) zapewniają skoordynowaną reakcję zgodnie z art. 11;
c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;	c) regularnie publikują na wspólnej stronie internetowej niemające poufnego charakteru informacje na temat aktualnych wczesnych ostrzeżeń i skoordynowanych reakcji;
d) wspólnie omawiają i oceniają, na wniosek państwa członkowskiego lub Komisji, jedną krajową strategię w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, lub jeden krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, o których mowa w art. 5, w zakresie niniejszej dyrektywy;	d) wspólnie omawiają i oceniają, na wniosek państwa członkowskiego lub Komisji, jedną krajową strategię w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, lub jeden krajowy plan współpracy w zakresie bezpieczeństwa sieci i informacji, lub ich większą liczbę, o których mowa w art. 5, w zakresie niniejszej dyrektywy;
e) wspólnie omawiają i oceniają, na wniosek państwa członkowskiego lub Komisji, skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji przeprowadzane są na poziomie unijnym;	e) wspólnie omawiają i oceniają, na wniosek państwa członkowskiego lub Komisji, skuteczność CERT, zwłaszcza w przypadku gdy ćwiczenia w zakresie bezpieczeństwa sieci i informacji przeprowadzane są na poziomie unijnym;
f) współpracują i wymieniają się informacjami dotyczącymi wszystkich istotnych kwestii z działającym przy Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej;	f) współpracują i wymieniają się informacjami dotyczącymi wszystkich istotnych kwestii z działającym przy Europolu Europejskim Centrum ds. Walki z Cyberprzestępczością oraz z innymi właściwymi organami europejskimi, w szczególności w dziedzinach ochrony danych, energetyki, transportu, bankowości, obrotu papierami wartościowymi i opieki zdrowotnej;
g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;	g) wymieniają się informacjami i najlepszymi praktykami między sobą i z Komisją oraz udzielają sobie wzajemnie pomocy w budowaniu zdolności w zakresie bezpieczeństwa sieci i informacji;
h) regularnie organizują wzajemne oceny zdolności i gotowości;	h) regularnie organizują wzajemne oceny zdolności i gotowości;

Tekst proponowany przez Komisję	Zmiany proponowane przez EBC ([1])
i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji."	i) organizują ćwiczenia w zakresie bezpieczeństwa sieci i informacji na poziomie unijnym oraz uczestniczą, w stosownych przypadkach, w międzynarodowych ćwiczeniach w zakresie bezpieczeństwa sieci i informacji**.;** **j) zapewniają wymianę informacji z europejskimi oraz krajowymi organami regulacyjnymi (tj. w odniesieniu do sektora finansowego: Europejskim Systemem Banków Centralnych (ESBC), Europejskim Urzędem Nadzoru Bankowego (EBA) i Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych (ESMA), które ściśle współpracują w przypadku pojawienia się incydentów dotyczących bezpieczeństwa, który mogłyby negatywnie wpłynąć na należyte funkcjonowanie systemów płatności i rozrachunku).**"

Uzasadnienie

Istnieje wyraźna potrzeba wymiany informacji pomiędzy Europejską Agencją ds. Bezpieczeństwa Sieci i Informacji lub organami właściwymi na podstawie projektu dyrektywy a EBA lub ESMA jako organami właściwymi do koordynowania działań podejmowanych w odpowiedzi na incydenty związane z dostawcami usług płatniczych.

W związku z powyższym EBC proponuje niniejszą zmianę mając na uwadze wspieranie wymiany informacji oraz lepszą koordynację na poziomie Unii.

Zmiana nr 5

Artykuł 19 ust. 1

„1. Komisję wspomaga komitet (Komitet ds. Bezpieczeństwa Sieci i Informacji). Komitet jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011."	„1. Komisję wspomaga komitet (Komitet ds. Bezpieczeństwa Sieci i Informacji). Komitet jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011. **EBC, EBA i ESMA mają prawo delegowania przedstawicieli na spotkania Komitetu ds. Bezpieczeństwa Sieci i Informacji w sprawach, które mogą mieć wpływ na wykonywanie przez nich odpowiednich zadań EBC, EBA lub ESMA.**"

Uzasadnienie

EBC jest szczególnie zainteresowany wspieraniem bezpieczeństwa systemów płatności i rozrachunku oraz usług i instrumentów związanych z tymi systemami jako ważnego składnika utrzymywania zaufania do wspólnej waluty i sprawnego funkcjonowania gospodarki w Unii. EBC zaleca w tym zakresie umożliwienie jego przedstawicielom udziału w spotkaniach Komitetu ds. Bezpieczeństwa Sieci i Informacji. W każdym przypadku należy na podstawie Traktatu zasięgnąć formalnej opinii EBC w zakresie środków odnoszących się do systemów płatności lub jakichkolwiek innych kwestii będących w zakresie właściwości EBC.

W sprawach dotyczących dostawców usług płatniczych udział powinny brać również EBA i ESMA.

([1]) Pogrubienia użyte w tekście wskazują na fragmenty, gdzie EBC proponuje dodanie określonych sformułowań. Przekreślenie w tekście wskazuje na fragmenty, gdzie EBC proponuje usunięcie określonych sformułowań.
([2]) Dokument dostępny na stronie internetowej EBC pod adresem http://www.ecb.europa.eu