OPINIA EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 11 kwietnia 2022 r.

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148

(CON/2022/14)

(2022/C 233/03)

Wprowadzenie i podstawa prawna

W dniu 16 grudnia 2020 r. Komisja Europejska przyjęła wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 ([1]) (zwany dalej „proponowaną dyrektywą"). W dniu 3 grudnia 2021 r. Rada Unii Europejskiej uzgodniła podejście ogólne w odniesieniu do proponowanej dyrektywy ([2]). Właściwość Europejskiego Banku Centralnego (EBC) do wydania opinii wynika z art. 127 ust. 4 Traktatu o funkcjonowaniu Unii Europejskiej, jako że proponowana dyrektywa zawiera przepisy leżące w zakresie kompetencji EBC, obejmującym w szczególności wspieranie sprawnego funkcjonowania systemów płatniczych, przyczynianie się do sprawnego prowadzenia polityki przez właściwe organy w odniesieniu do stabilności systemu finansowego, a także w zakresie zadań EBC dotyczących nadzoru ostrożnościowego nad instytucjami kredytowymi zgodnie z art. 127 ust. 2 tiret czwarte oraz art. 127 ust. 5 i 6 Traktatu. Rada Prezesów wydała niniejszą opinię zgodnie ze zdaniem pierwszym art. 17 ust. 5 Regulaminu Europejskiego Banku Centralnego.

Uwagi ogólne

EBC zdecydowanie popiera cele proponowanej dyrektywy dotyczące podniesienia poziomu cyberodporności we wszystkich odpowiednich sektorach, ograniczenia zróżnicowania na rynku wewnętrznym oraz podniesienia poziomu orientacji sytuacyjnej i zbiorowej zdolności do przygotowania się i reagowania poprzez zapewnienie skutecznej współpracy w Unii.

EBC uznaje znaczenie utrzymania silnego związku między proponowaną dyrektywą a sektorem finansowym, który powinien pozostać częścią ekosystemu sieci i systemów informatycznych, aby promować spójną ocenę ryzyka związanego z technologiami informacyjno-komunikacyjnymi (ICT) w całej Unii oraz wspierać skuteczną międzysektorową wymianę informacji i współpracę w reagowaniu na cyberzagrożenia. W tym celu na mocy proponowanego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego ([3]) (zwanego dalej „rozporządzeniem w sprawie operacyjnej odporności cyfrowej") właściwe organy powinny mieć możliwość uczestniczenia w strategicznych dyskusjach na temat polityki i pracach technicznych Grupy Współpracy ds. bezpieczeństwa sieci i systemów informatycznych, a także wymiany informacji i dalszej współpracy z pojedynczymi punktami kontaktowymi i krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego, o których mowa w proponowanej dyrektywie ([4]).

1. Zakres proponowanej dyrektywy

1.1 EBC rozumie, że w odniesieniu do podmiotów sektora finansowego rozporządzenie w sprawie operacyjnej odporności cyfrowej będzie uznawane za sektorowy akt prawny wprowadzający obowiązki dotyczące zarządzania ryzykiem w cyberprzestrzeni i zgłaszania incydentów, które są co najmniej równoważne pod względem skutku obowiązkom zawartym w proponowanej dyrektywie ([5]). W związku z tym przepisy proponowanej dyrektywy, które odnoszą się do zarządzania ryzykiem w cyberprzestrzeni, obowiązków w zakresie zgłaszania incydentów, wymiany informacji oraz nadzoru i egzekwowania przepisów, nie będą miały zastosowania do podmiotów finansowych objętych rozporządzeniem w sprawie operacyjnej odporności cyfrowej ([6]). Jak wyjaśniono w motywach proponowanej

([1]) COM(2020) 823 final.
([2]) Dostępne ma stronie internetowej Rady pod adresem www.consilium.europa.eu
([3]) COM(2020) 595 final.
([4]) Zob. pkt 1.5 opinii Europejskiego Banku Centralnego CON/2021/20 z dnia 4 czerwca 2021 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego (Dz.U. C 343 z 26.8.2021, s. 1). Opinie EBC są publikowane na stronie internetowej EUR-Lex. Art. 17 ust. 5 i art. 42 rozporządzenia w sprawie operacyjnej odporności cyfrowej; art. 11 proponowanej dyrektywy.
([5]) Art. 2 ust. 6 proponowanej dyrektywy.
([6]) Motyw 13 i art. 2 ust. 6 proponowanej dyrektywy.

dyrektywy, zamiast przepisów proponowanej dyrektywy zastosowanie powinny mieć przepisy rozporządzenia w sprawie operacyjnej odporności cyfrowej dotyczące środków zarządzania ryzykiem ICT, zarządzania incydentami związanymi z ICT i zgłaszania incydentów, testowania operacyjnej odporności cyfrowej, ustaleń dotyczących wymiany informacji i ryzyka związanego z zewnętrznymi dostawcami usług ICT ([7]).

1.2 EBC zauważa również, że w podejściu ogólnym do proponowanej dyrektywy Rada proponuje zmianę mającą na celu wyłączenie „podmiotów prowadzących działalność w obszarze sądownictwa, parlamentów lub banków centralnych" ([8]) z zakresu zastosowania proponowanej dyrektywy. EBC rozumie, że proponowana zmiana dotyczyłaby wszystkich podstawowych zadań i kompetencji Europejskiego Systemu Banków Centralnych (ESBC), określonych w art. 127 ust. 2 Traktatu oraz w art. 3 ust. 1 Statutu Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (zwanego dalej „Statutem ESBC"), takich jak wspieranie sprawnego funkcjonowania systemów płatniczych. W związku z tym uznaje się, że będące własnością Eurosystemu i obsługiwane przez Eurosystem infrastruktury rynku finansowego, takie jak systemy TARGET2 i TARGET2-Securities, wchodzą w zakres proponowanego przez Radę wyłączenia banków centralnych z zakresu zastosowania proponowanej dyrektywy.

2. **Uprawnienia nadzorcze ESBC i Eurosystemu**

2.1 Poza podstawowym celem ESBC, jakim jest utrzymanie stabilności cen, i zgodnie z art. 127 ust. 2 Traktatu, jednym z podstawowych zadań realizowanych za pośrednictwem ESBC jest popieranie sprawnego funkcjonowania systemów płatniczych ([9]). Wykonując to podstawowe zadanie, EBC i krajowe banki centralne 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 ([10]). Wykonując swoją rolę nadzorczą, EBC przyjął rozporządzenie Europejskiego Banku Centralnego (UE) nr 795/2014 (EBC/2014/28) ([11]) (zwane dalej „rozporządzeniem SIPS"), które przekłada zasady CPSS-IOSCO dotyczące infrastruktur rynku finansowego ([12]) na przepisy prawa mające bezpośrednie zastosowanie. W rozporządzeniu SIPS określono wymogi dotyczące zarówno systemów płatności wysokokwotowych, jak i systemów płatności detalicznych, o znaczeniu systemowym, zarówno publicznych, jak i prywatnych. Wymogi określone w rozporządzeniu SIPS obejmują już między innymi zarządzanie ryzykiem operacyjnym i ustanowienie ram dotyczących cyberodporności ([13]).

2.2 Oprócz systemów płatności o znaczeniu systemowym nadzór Eurosystemu obejmuje systemy płatności niemające znaczenia systemowego, instrumenty, systemy (schematy) i uzgodnienia w zakresie płatności elektronicznych oraz inne infrastruktury i dostawców usług krytycznych, zgodnie z ramami polityki nadzorczej Eurosystemu ([14]). Systemy płatności i inne uzgodnienia podlegające nadzorowi Eurosystemu nie są wyraźnie objęte zakresem zastosowania proponowanej dyrektywy ([15]). Jednocześnie, biorąc pod uwagę, że proponowana dyrektywa jest instrumentem minimalnej harmonizacji ([16]), przepisy ją wdrażające przyjęte przez państwa członkowskie mogłyby ostatecznie pokrywać się z kompetencjami Eurosystemu w zakresie nadzoru. Aby tego uniknąć, w motywach proponowanej dyrektywy powinno się wyraźnie wskazać kompetencje ESBC wynikające z Traktatu i Statutu ESBC oraz kompetencje Eurosystemu wynikające z rozporządzenia SIPS i ogólnie z ram polityki nadzorczej Eurosystemu.

([7]) Motyw 13 proponowanej dyrektywy.
([8]) Art. 2 ust. 3a akapit pierwszy lit. b) podejścia ogólnego Rady do proponowanej dyrektywy.
([9]) Art. 127 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej odzwierciedlony w art. 3 ust. 1 Statutu ESBC.
([10]) Art. 22 Statutu ESBC.
([11]) Rozporządzenie Europejskiego Banku Centralnego (UE) nr 795/2014 z dnia 3 lipca 2014 r. w sprawie wymogów nadzorczych w odniesieniu do systemów płatności o znaczeniu systemowym (EBC/2014/28) (Dz.U. L 217 z 23.7.2014, s. 16).
([12]) Zob. dokument Komitetu ds. Systemów Płatności i Rozliczeniowych (PSSC) i Komitetu Technicznego Międzynarodowej Organizacji Komisji Papierów Wartościowych (IOSCO) pt. „Principles for Financial Market Infrastructures" z kwietnia 2012 r. (Zasady dotyczące infrastruktur rynku finansowego) dostępny na stronie internetowej Banku Rozrachunków Międzynarodowych pod adresem www.bis.org. Odpowiedzialność D tego dokumentu stanowi, że „wszyscy członkowie PSSC i IOSCO powinni stosować zasady w odniesieniu do odpowiednich infrastruktur rynku finansowego w ich jurysdykcjach w jak najszerszym zakresie dozwolonym przez ramy prawne ich jurysdykcji".
([13]) Art. 15 rozporządzenia (UE) nr 795/2014 (EBC/2014/28).
([14]) „Eurosystem oversight policy framework", wersja uaktualniona z lipca 2016 r. dostępna na stronie internetowej EBC pod adresem www.ecb.europa.eu.
([15]) Art. 2 proponowanej dyrektywy oraz załączniki I i II do proponowanej dyrektywy.
([16]) Art. 3 proponowanej dyrektywy.

3. **Ryzyko ze strony zewnętrznych dostawców usług ICT, zarządzanie incydentami i kryzysami na dużą skalę, wymiana informacji i krajowa strategia cyberbezpieczeństwa**

3.1 *Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT*

3.1.1 Proponowana dyrektywa uprawnia właściwe organy, które wykonują swoje uprawnienia w zakresie egzekwowania przepisów wobec podmiotów niezbędnych, do wydawania wiążących poleceń lub nakazów zobowiązujących te podmioty do wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień lub naruszeń obowiązków wynikających z proponowanej dyrektywy ([17]). Jednocześnie „wiodący organ nadzorczy" wyznaczony na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej może kierować zalecenia do kluczowych zewnętrznych dostawców usług ICT w celu zarządzania potencjalnym ryzykiem systemowym spowodowanym praktykami dotyczącymi outsourcingu i koncentracją zewnętrznych dostawców usług ICT ([18]).

3.1.2 Biorąc pod uwagę, że podmiot niezbędny na mocy proponowanej dyrektywy może również zostać wyznaczony jako kluczowy zewnętrzny dostawca usług ICT zgodnie z rozporządzeniem w sprawie operacyjnej odporności cyfrowej, EBC ponawia swoje zalecenie ([19]) dotyczące unikania wydawania sprzecznych zaleceń i wiążących poleceń. W związku z tym EBC z zadowoleniem przyjmuje podejście ogólne Rady do proponowanej dyrektywy. Zgodnie z tym podejściem właściwe organy mają informować forum nadzoru ustanowione na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej o wykonywaniu swoich uprawnień w zakresie nadzoru i egzekwowania przepisów w odniesieniu do podmiotu niezbędnego wyznaczonego jako kluczowy zewnętrzny dostawca usług ICT na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej ([20]).

3.2 *Zarządzanie incydentami i kryzysami na dużą skalę*

3.2.1 Zgodnie z proponowaną dyrektywą ([21]) państwa członkowskie mają obowiązek wyznaczyć co najmniej jeden właściwy organ odpowiedzialny za zarządzanie incydentami i kryzysami na dużą skalę. Jak wyjaśniono w motywach proponowanej dyrektywy, incydent na dużą skalę powinien oznaczać incydent mający znaczący wpływ na co najmniej dwa państwa członkowskie lub taki, który powoduje na tyle duże zakłócenia, że dotknięte nimi państwo członkowskie nie jest samo w stanie na nie skutecznie zareagować. Incydenty na dużą skalę mogą przerodzić się w prawdziwe kryzysy zakłócające prawidłowe funkcjonowanie rynku wewnętrznego ([22]).

3.2.2 Podczas gdy właściwe organy wyznaczone na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej pozostają odpowiedzialne za zarządzanie cyberincydentami dotyczącymi podmiotów finansowych, współpraca ze strukturami i organami ustanowionymi na mocy proponowanej dyrektywy będzie miała kluczowe znaczenie dla zapewnienia skoordynowanej reakcji na terytorium Unii. W tym celu, w przypadku wpływu cyberincydentów i kryzysów cyberbezpieczeństwa na dużą skalę na sektor finansowy, EBC z zadowoleniem przyjąłby udział właściwych organów wyznaczonych na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej, w tym EBC, w europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ([23]).

3.3 *Wymiana informacji*

3.3.1 Jak wskazano powyżej, EBC zdecydowanie popiera współpracę między właściwymi organami wyznaczonymi na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej a strukturami i organami ustanowionymi na mocy proponowanej dyrektywy. W szczególności wymiana informacji między organami może umożliwić międzysektorowy proces uczenia się, przyczynić się do zapobiegania cyberatakom i skutecznego zarządzania nimi oraz promować spójną ocenę ryzyk związanych z ICT na obszarze Unii. EBC podkreśla jednak, że wymiana informacji powinna odbywać się przy jasno określonych mechanizmach klasyfikacji i przekazywania informacji, w połączeniu z odpowiednimi zabezpieczeniami zapewniającymi poufność ([24]). EBC z zadowoleniem przyjmuje podejście ogólne Rady do proponowanej dyrektywy, w którym proponuje się regularną wymianę istotnych informacji między orga-

([17]) Art. 29 ust. 4 lit. b) proponowanej dyrektywy.
([18]) Art. 31 rozporządzenia w sprawie operacyjnej odporności cyfrowej.
([19]) Zob. pkt 1.2 opinii CON/2021/20.
([20]) Art. 29 ust. 10 podejścia ogólnego Rady do proponowanej dyrektywy.
([21]) Art. 7 ust. 1 proponowanej dyrektywy.
([22]) Motyw 27 proponowanej dyrektywy.
([23]) Art. 14 proponowanej dyrektywy.
([24]) Zob. pkt 1.5 opinii CON/2021/20.

nami ([25]), ustanowienie mechanizmów współpracy określających mechanizm wymiany informacji ([26]) oraz automatyczne i bezpośrednie przekazywanie zgłoszeń incydentów ([27]). W związku z tym należy zapewnić, aby informacje będące informacjami poufnymi zgodnie z przepisami dotyczącymi tajemnicy zawodowej na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej ([28]) lub odpowiednich przepisów sektorowych ([29]) mogły być przedmiotem wymiany z właściwymi organami, o których mowa w proponowanej dyrektywie, tylko wtedy, gdy taka wymiana jest potrzebna do stosowania przez właściwe organy postanowień proponowanej dyrektywy ([30]).

3.4 *Krajowa strategia cyberbezpieczeństwa*

3.4.1 Zgodnie z proponowaną dyrektywą państwa członkowskie są zobowiązane do przyjęcia krajowych strategii cyberbezpieczeństwa określających cele strategiczne oraz odpowiednie środki polityczne i regulacyjne ukierunkowane na osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa ([31]). Jak wyjaśniono w motywach proponowanej dyrektywy, państwa członkowskie powinny w dalszym ciągu uwzględniać sektor finansowy w swoich strategiach w zakresie cyberbezpieczeństwa ([32]). W związku z tym w ramach krajowych strategii cyberbezpieczeństwa państwa członkowskie powinny przyjąć polityki dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów i usług ICT wykorzystywanych przez podmioty do świadczenia usług. Jeżeli chodzi o sektor finansowy, krajowe strategie cyberbezpieczeństwa powinny być spójne z ramami regulacyjnymi wyznaczonymi na mocy rozporządzenia w sprawie operacyjnej odporności cyfrowej. W tym względzie EBC uważa, że potrzebne jest dalsze doprecyzowanie, aby zapewnić spójność krajowych strategii cyberbezpieczeństwa z przepisami sektorowymi.

W przypadku gdy EBC zaleca zmianę projektowanej dyrektywy, szczegółowe propozycje zmian wraz z ich uzasadnieniem zostały zawarte w odrębnym roboczym dokumencie o charakterze technicznym. Roboczy dokument techniczny jest dostępny w języku angielskim na stronie internetowej EUR-Lex.

Sporządzono we Frankfurcie nad Menem dnia 11 kwietnia 2022 r.

Prezes EBC
Christine LAGARDE

([25]) Art. 11 ust. 5 podejścia ogólnego Rady do proponowanej dyrektywy.
([26]) Motyw 23a podejścia ogólnego Rady do proponowanej dyrektywy.
([27]) Motyw 13 podejścia ogólnego Rady do proponowanej dyrektywy.
([28]) Art. 49 rozporządzenia w sprawie operacyjnej odporności cyfrowej.
([29]) Art. 53–62 dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniającej dyrektywę 2002/87/WE i uchylającej dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).
([30]) Artykuł 2 ust. 5 i art. 11 ust. 4 proponowanej dyrektywy.
([31]) Art. 5 proponowanej dyrektywy.
([32]) Motyw 13 proponowanej dyrektywy.