III

(Akty przygotowawcze)

EUROPEJSKI BANK CENTRALNY

OPINIA EUROPEJSKIEGO BANKU CENTRALNEGO

z dnia 4 czerwca 2021 r.

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego

(CON/2021/20)

(2021/C 343/01)

Wprowadzenie i podstawa prawna

W dniach 22, 23 i 29 grudnia 2020 r. Europejski Bank Centralny (EBC) otrzymał wnioski, odpowiednio, Parlamentu Europejskiego i Rady Unii Europejskiej o wydanie opinii w sprawie projektu rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014 ([1]) (zwanego dalej „projektem rozporządzenia") oraz w sprawie projektu dyrektywy zmieniającej dyrektywy 2006/43/WE, 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 i (UE) 2016/2341 ([2]) (zwanego dalej „projektem dyrektywy zmieniającej", a wraz z „projekprojektem rozporządzenia" zwanymi dalej „projektami aktów prawnych").

Właściwość EBC do wydania opinii wynika z art. 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, jako że projekty aktów prawnych zawierają przepisy leżące w zakresie kompetencji EBC, obejmującym w szczególności określanie i wdrażanie polityki pieniężnej, 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 pierwsze i czwarte, art. 127 ust. 5 i art. 127 ust. 6 Traktatu. Rada Prezesów wydała niniejszą opinię zgodnie ze zdaniem pierwszym art. 17 ust. 5 Regulaminu Europejskiego Banku Centralnego.

1. Uwagi ogólne

1.1. EBC z zadowoleniem przyjmuje projekt rozporządzenia, który ma na celu zwiększenie cyberbezpieczeństwa i odporności operacyjnej sektora finansowego. W szczególności EBC z zadowoleniem przyjmuje cel projektu rozporządzenia, jakim jest usunięcie przeszkód dla ustanowienia i funkcjonowania rynku wewnętrznego usług finansowych oraz usprawnienie tego procesu dzięki harmonizacji przepisów obowiązujących w obszarze zarządzania ryzykiem związanym z technologiami informacyjno-komunikacyjnymi (ICT), udostępniania informacji, testowania i w obszarze dotyczącym ryzyka ze strony zewnętrznych dostawców usług ICT. Ponadto EBC z zadowoleniem przyjmuje cel projektu rozporządzenia, jakim jest uproszczenie i harmonizacja pokrywających się wymogów regulacyjnych lub oczekiwań w zakresie nadzoru, jakim obecnie podlegają podmioty finansowe zgodnie z prawem Unii.

1.2. EBC rozumie, że w odniesieniu do podmiotów finansowych zidentyfikowanych jako operatorzy usług kluczowych ([3]) projekt rozporządzenia stanowi sektorowy akt prawny (*lex specialis*) w rozumieniu art. 1 ust. 7 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([4]) (zwanej dalej „dyrektywą dotyczącą cyberbezpieczeństwa"). Oznacza to, że wymogi wynikające z projektu rozporządzenia miałyby co do zasady pierwszeństwo przed dyrektywą dotyczącą cyberbezpieczeństwa. W praktyce oznaczałoby to m.in., że podmioty finansowe zidentyfikowane jako operatorzy usług kluczowych ([5]) zgłaszałyby incydenty na podstawie

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Zob. art. 1 ust. 2 projektu rozporządzenia.
([4]) Dyrektywa 2016/1148 Parlamentu Europejskiego i Rady z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194, 19.7.2016, s. 1).
([5]) Zob. art. 5 dyrektywy dotyczącej cyberbezpieczeństwa.

projektu rozporządzenia, a nie na podstawie dyrektywy dotyczącej cyberbezpieczeństwa. Podczas gdy EBC z zadowoleniem przyjmuje ograniczenie pokrywających się wymogów wobec podmiotów finansowych w zakresie zgłaszania incydentów, wzajemne relacje między projektem rozporządzenia a dyrektywą dotyczącą cyberbezpieczeństwa wymagają głębszego rozważenia. Na przykład zgodnie z projektem rozporządzenia zewnętrzny dostawca usług ICT ([6]) może być związany zaleceniami wydanymi przez wiodący organ nadzorczy ([7]). Jednocześnie ten sam zewnętrzny dostawca usług ICT może zostać zaklasyfikowany jako operator usług kluczowych w rozumieniu dyrektywy dotyczącej cyberbezpieczeństwa i być związany poleceniami wydanymi przez właściwy organ ([8]). W takim przypadku zewnętrzny dostawca usług ICT mógłby podlegać zaleceniom wydanym na podstawie projektu rozporządzenia oraz sprzecznym z nimi poleceniom wydanym na podstawie dyrektywy dotyczącej cyberbezpieczeństwa. EBC sugeruje, aby organy prawodawcze Unii głębiej rozważyły potencjalne niespójności pomiędzy projektem rozporządzenia a dyrektywą dotyczącą cyberbezpieczeństwa, które mogą stanąć na przeszkodzie harmonizacji i ograniczeniu pokrywających się i sprzecznych wymogów wobec podmiotów finansowych.

1.3. EBC rozumie także, że zgodnie z projektem dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 ([9]) (zwanym dalej „projektem dyrektywy NIS2"), „zdarzenia potencjalnie wypadkowe" ([10]) będą podlegały obowiązkom w zakresie zgłaszania incydentów ([11]). Chociaż motyw 39 projektu dyrektywy NIS2 odnosi się do znaczenia terminu „zdarzenia potencjalnie wypadkowe", nie jest jasne, czy intencją jest wprowadzenie wymogu zgłaszania zdarzeń potencjalnie wypadkowych przez podmioty wskazane w art. 2 projektu rozporządzenia. W tym względzie, a także biorąc pod uwagę, że zdarzenia potencjalnie wypadkowe mogą zostać zidentyfikowane jako takie dopiero po ich wystąpieniu, EBC z zadowoleniem przyjąłby fakt powiadamiania go o istotnych zdarzeniach potencjalnie wypadkowych w stosownym czasie od ich wystąpienia, tak jak obecnie ma to miejsce w przypadku cyberincydentów. EBC sugeruje zapewnienie większej koordynacji pomiędzy projektem rozporządzenia a projektem dyrektywy NIS2 w celu doprecyzowania dokładnego zakresu obowiązku zgłaszania, jakim może być objęty dany podmiot finansowy na podstawie tych dwóch różnych, lecz wzajemnie powiązanych aktów prawa Unii. Jednocześnie należałoby zdefiniować „zdarzenia potencjalnie wypadkowe" oraz opracować przepisy uściślające, kiedy należy uznawać je za istotne.

1.4. EBC z zadowoleniem przyjmuje zachęcanie podmiotów finansowych do dobrowolnego wymieniania się informacjami na temat danych wywiadowczych dotyczących cyberzagrożeń w celu wzmocnienia i wsparcia postaw cyberodporności. EBC również wspiera rynkową Inicjatywę wymiany informacji i danych wywiadowczych na temat incydentów cybernetycznych (CIISI-EU) i udostępnia rozwiązania ułatwiające tworzenie i rozwijanie takich inicjatyw ([12]).

1.5. EBC popiera współpracę pomiędzy właściwymi organami wyznaczonymi zgodnie z projektem rozporządzenia, Europejskimi Urzędami Nadzoru i zespołami reagowania na incydenty bezpieczeństwa komputerowego (zwanymi dalej „CSIRT") ([13]). Wymiana informacji ma zasadnicze znaczenie dla zapewnienia operacyjnej odporności Unii, gdyż przepływ informacji i współpraca pomiędzy organami może przyczynić się do zapobiegania cyberatakom i pomóc ograniczyć rozprzestrzenianie się zagrożeń związanych z ICT. Należy promować wspólne rozumienie ryzyk związanych z ICT i zapewnić spójną ocenę tych ryzyk na obszarze Unii. Niezwykle ważne jest, aby właściwe organy dzieliły się informacjami z pojedynczym punktem kontaktowym ([14]) i krajowymi CSIRT ([15]) dopiero wówczas, gdy zostaną jasno ustalone mechanizmy klasyfikacji i przekazywania informacji, przy odpowiednich zabezpieczeniach zapewniających poufność.

1.6. Wreszcie, EBC dostrzega potrzebę wprowadzenia do projektu rozporządzenia przepisów o ochronie danych osobowych i przechowywaniu danych. Czas przechowywania powinien uwzględniać dochodzenia i kontrole, wnioski o informacje, przekazywanie, publikację, ewaluację, weryfikację, ocenę oraz sporządzanie planów nadzoru lub kontroli, jakie właściwe organy mogą być zobowiązane prowadzić w ramach swoich obowiązków i zadań wynikających z projektu rozporządzenia. W tym względzie odpowiedni byłby okres 15 lat. Okres ten mógłby zostać skrócony lub wydłużony na potrzeby konkretnych przypadków. W tym względzie

([6]) Zob. art. 3 ust. 15 projektu rozporządzenia.
([7]) Zob. art. 31 ust. 1 lit. d) projektu rozporządzenia.
([8]) Zob. art. 15 ust. 3 dyrektywy dotyczącej cyberbezpieczeństwa.
([9]) COM(2020) 823 final.
([10]) Zdarzenia, które mogą spowodować szkodę, ale których pełnemu wystąpieniu udało się skutecznie zapobiec; zob. motyw 39 projektu dyrektywy NIS2.
([11]) Zob. art. 11 projektu dyrektywy NIS2.
([12]) Cyber threat Intelligence Information Sharing Initiative – Inicjatywa wymiany informacji i danych wywiadowczych na temat incydentów cybernetycznych (CIISI-EU), dostępna na stronie internetowej EBC pod adresem www.ecb.europa.eu.
([13]) Zob. art. 42 projektu rozporządzenia.
([14]) Zob. art. 8 ust. 3 dyrektywy dotyczącej cyberbezpieczeństwa.
([15]) Zob. także art. 11, 26 i 27 projektu dyrektywy NIS2.

EBC sugeruje, aby organy prawodawcze Unii, formułując właściwy przepis o danych osobowych i przechowywaniu danych, uwzględniły zasadę minimalizacji danych, a także dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych ([16]).

2. Uwagi szczegółowe dotyczące nadzoru oraz rozliczeń i rozrachunku papierów wartościowych

2.1. *Uprawnienia nadzorcze ESBC i Eurosystemu*

2.1.1. Traktat i Statut Europejskiego Systemu Banków Centralnych i Europejskiego Banku Centralnego (zwany dalej „Statutem ESBC") przewidują, że Eurosystem w ramach swojego mandatu sprawuje nadzór nad systemami rozliczeń i płatności, co jest ściśle powiązane z jego podstawowymi zadaniami w zakresie polityki pieniężnej. Zgodnie z art. 127 ust. 2 tiret czwarte Traktatu, odzwierciedlonym w art. 3 ust. 1 Statutu, jednym z podstawowych zadań realizowanych za pośrednictwem ESBC jest „popieranie sprawnego funkcjonowania systemów płatniczych". 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" ([17]). Zgodnie ze swoją rolą nadzorczą EBC przyjął rozporządzenie Europejskiego Banku Centralnego (UE) nr 795/2014 (EBC/2014/28) (zwane dalej „rozpoozporządzeniem SIPS") ([18]). Rozporządzenie SIPS wdraża, w normatywnej formie, zasady dotyczące infrastruktur rynku finansowego wydane w kwietniu 2012 r. przez Komitet ds. Systemów Płatności i Rozrachunku (CPSS) oraz Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO) ([19]), które są prawnie wiążące i obejmują zarówno systemy płatności wysokokwotowych, jak i systemy płatności detalicznych, o znaczeniu systemowym, prowadzone przez bank centralny Eurosystemu lub podmiot prywatny. Ramy polityki nadzorczej Eurosystemu ([20]) określają instrumenty płatnicze jako „integralną część systemów płatności" i tym samym włączają te instrumenty do zakresu nadzoru. Ramy nadzoru nad instrumentami płatniczymi są obecnie poddawane przeglądowi ([21]). W tych ramach instrument płatniczy (np. karta, polecenie przelewu, polecenie zapłaty, przekaz pieniądza elektronicznego i cyfrowy token płatniczy ([22])) definiuje się jako spersonalizowane urządzenie (lub zestaw urządzeń) lub zestaw procedur uzgodniony między użytkownikiem usług płatniczych a dostawcą usług płatniczych, wykorzystywane w celu zainicjowania transferu wartości ([23]).

2.1.2. W świetle powyższego EBC popiera wyłączenie z zakresu projektu rozporządzenia przepisów dotyczących operatorów systemów określonych w art. 2 lit. p) dyrektywy Parlamentu Europejskiego i Rady 98/26/WE ([24]), systemów płatności (w tym tych obsługiwanych przez banki centralne), schematów płatności i uzgodnień płatniczych ze względu na zastosowanie powyżej wskazanych ram nadzoru. Z tych przyczyn kompetencje ESBC wynikające z Traktatu i kompetencje Eurosystemu wynikające z rozporządzenia SIPS powinny zostać wyraźnie wymienione w motywach projektu rozporządzenia.

([16]) Zob. art. 4 ust. 1 lit. b) i art. 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295, 21.11.2018, s. 39).

([17]) Zob. art. 22 Statutu ESBC.

([18]) 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).

([19]) Dostępne na stronie internetowej BIS pod adresem www.bis.org.

([20]) „Eurosystem oversight policy framework", wersja uaktualniona z lipca 2016 r. dostępna na stronie internetowej EBC pod adresem www.ecb.europa.eu.

([21]) Zob. zmienione i skonsolidowane ramy nadzoru Eurosystemu dotyczące elektronicznych instrumentów płatniczych, schematów i uzgodnień (ramy PISA), dostępne na stronie internetowej EBC pod adresem www.ecb.europa.eu.

([22]) Cyfrowy token płatniczy to cyfrowe przedstawienie wartości zabezpieczonej roszczeniami lub aktywami zarejestrowanymi gdzie indziej i umożliwiające transfer wartości między użytkownikami końcowymi. W zależności od podstawowej struktury cyfrowe tokeny płatnicze mogą przewidywać transfer wartości bez konieczności angażowania centralnego podmiotu trzeciego lub korzystania z rachunków płatniczych.

([23]) „Transfer wartości" – działanie zainicjowane przez płatnika lub w imieniu płatnika lub przez odbiorcę płatności, polegające na transferze środków pieniężnych lub cyfrowych tokenów płatniczych lub lokowaniu lub gotówki na rachunku użytkownika wypłacaniu z tego rachunku, niezależnie od wszelkich leżących u jego podstaw zobowiązań między płatnikiem a odbiorcą płatności. Transfer może obejmować jednego dostawcę usług płatniczych lub wielu dostawców usług płatniczych". Definicja „transferu wartości" w ramach PISA odbiega od definicji transferu „środków pieniężnych" określonej w dyrektywie Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35). „Transfer wartości" w kontekście „instrumentu płatniczego" w rozumieniu tej dyrektywy może odnosić się wyłącznie do transferu „środków pieniężnych". Zgodnie z tą dyrektywą „środki pieniężne" nie obejmują cyfrowych tokenów płatniczych, chyba że tokeny te można sklasyfikować jako pieniądz elektroniczny (lub, bardziej hipotetycznie, jako zapisy księgowe).

([24]) Dyrektywa Parlamentu Europejskiego i Rady 98/26/WE 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).

2.1.3. Z tego samego powodu EBC popiera wyłączenie z zakresu stosowania ram nadzoru określonych w projekcie rozporządzenia zewnętrznych dostawców usług ICT, którzy podlegają ramom nadzoru ustanowionym na potrzeby wspierania realizacji zadań, o których mowa w art. 127 ust. 2 Traktatu ([25]). W tym względzie EBC pragnie podkreślić, że banki centralne ESBC działające w charakterze organów prowadzących politykę pieniężną ([26]) oraz Eurosystem, świadcząc usługi poprzez TARGET2, TARGET2-Securites (T2S) ([27]) oraz świadcząc rozrachunek płatności natychmiastowych (TARGET Instant Payment Settlement – TIPS) ([28]), nie są objęte zakresem projektu rozporządzenia, ani też nie mogą być uznane za zewnętrznych dostawców usług ICT i w ten sposób potencjalnie zaklasyfikowane jako kluczowi zewnętrzni dostawcy usług ICT w rozumieniu projektu rozporządzenia. Eurosystem nadzoruje T2S w związku ze swoim mandatem w zakresie zapewnienia sprawnych i solidnych systemów rozliczeń i systemów płatniczych. Ponadto ESMA wyjaśnił, że T2S nie jest dostawcą najważniejszych usług ([29]) w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 909/2014 ([30]) (zwanego dalej „rozporządzeniem w sprawie CDPW"). W związku z tym bezpieczeństwo organizacyjne i operacyjne, skuteczność i odporność T2S zapewniane są poprzez właściwe ramy prawne, regulacyjne i operacyjne oraz ustalone rozwiązania w zakresie zarządzania lub T2S, nie zaś poprzez rozporządzenie w sprawie CDPW.

2.1.4. Ponadto ramy polityki nadzorczej Eurosystemu ([31]) dotyczą dostawców najważniejszych usług, takich jak Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT). SWIFT jest spółką spółdzielczą z ograniczoną odpowiedzialnością z siedzibą w Belgii świadczącą usługi bezpiecznego międzynarodowego przekazywania informacji. Jako wiodący organ nadzorczy SWIFT działa Nationale Bank van België/Banque Nationale de Belgique, który na podstawie porozumienia o współpracy przy nadzorze prowadzi nadzór w odniesieniu do SWIFT, we współpracy z pozostałymi bankami centralnymi grupy G10, w tym EBC. Organy nadzorcze z grupy G10 rozumieją, że nadzór koncentruje się głównie na ryzyku operacyjnym SWIFT, gdyż jest ono uważane za główną kategorię ryzyka, poprzez które SWIFT może stwarzać ryzyko systemowe dla systemu finansowego Unii. W tym względzie Grupa Wspólnego Nadzoru (Cooperative Oversight Group) opracowała zbiór szczegółowych zasad i wysokich wymagań odnoszących się do SWIFT w takich obszarach jak identyfikacja ryzyka i zarządzanie ryzykiem, bezpieczeństwo informacji, niezawodność i odporność, planowanie technologii i komunikacja z użytkownikami. Organy nadzorcze z grupy G10 oczekują, że SWIFT będzie stosować się do wytycznych dotyczących cyberodporności Komitetu ds. Infrastruktury Płatności i Rynku (CPMI) i Międzynarodowej Organizacji Komisji Papierów Wartościowych (IOSCO) ([32]), a także do innych międzynarodowych standardów w zakresie bezpieczeństwa ICT, które łącznie przewyższają wymogi określone w projekcie rozporządzenia.

2.1.5. Nie można mieć pewności, że SWIFT, a być może także inni dostawcy usług podlegający ramom polityki nadzorczej Eurosystemu, mogą zostać objęci projektem rozporządzenia jako zewnętrzni dostawcy usług ICT, jeśli będą świadczyli usługi nieobjęte art. 172 ust. 2 Traktatu. EBC przyjmuje zatem z dużym zadowoleniem wyłączenie z zakresu ram nadzoru określonych w projekcie rozporządzenia usługodawców już objętych ramami polityki nadzorczej Eurosystemu, w tym także SWIFT.

([25]) Zob. art. 28 ust. 5 projektu rozporządzenia.

([26]) Zob. pkt 1.3 opinii Europejskiego Banku Centralnego z dnia 19 lutego 2021 r. w sprawie wniosku dotyczącego rozporządzenia w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937 (CON/2021/4). Wszystkie opinie EBC są publikowane w EUR-Lex.

([27]) Zob. załącznik IIa do wytycznych Europejskiego Banku Centralnego z dnia 5 grudnia 2012 r. w sprawie transeuropejskiego automatycznego błyskawicznego systemu rozrachunku brutto w czasie rzeczywistym (TARGET2) (EBC/2012/27) (Dz.U. L 30 z 30.1.2013, s. 1). Wytyczne EBC/2012/13 z dnia 18 lipca 2012 r. w sprawie TARGET2-Securities (Dz.U. L 215 z 11.8.2012, s. 19); Decyzja ECB/2011/20 Europejskiego Banku Centralnego z dnia 16 listopada 2011 r. ustanawiająca szczegółowe zasady i procedury stosowania kryteriów kwalifikowania centralnych depozytów papierów wartościowych do korzystania z usług TARGET2-Securities (Dz.U. L 319 z 2.12.2011, s. 117). Zob. także umowę ramową T2S (T2S Framework Agreement) i umowę zbiorową (Collective Agreement).

([28]) Zob. załącznik IIb do wytycznych ECB/2012/27.

([29]) Zob. art. 30 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U. L 257 z 28.8.2014, s. 1) i art. 68 rozporządzenia delegowanego Komisji (UE) 2017/392 z dnia 11 listopada 2016 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 w odniesieniu do regulacyjnych standardów technicznych dotyczących wymogów w zakresie udzielania zezwoleń oraz wymogów nadzorczych i operacyjnych dla centralnych depozytów papierów wartościowych (Dz.U. L 65 z 10.3.2017, s. 48).

([30]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U. L 257 z 28.8.2014, s. 1).

([31]) „Eurosystem oversight policy framework", wersja uaktualniona z lipca 2016 r., dostępna na stronie internetowej EBC www.ecb.europa.eu.

([32]) Dostępne na stronie internetowej BIS pod adresem www.bis.org.

2.2. *Kompetencje ESBC w zakresie rozrachunku papierów wartościowych*

2.2.1. Centralne depozyty papierów wartościowych (CDPW) są infrastrukturami rynku finansowego, które są ściśle regulowane i nadzorowane przez różne organy zgodnie z rozporządzeniem w sprawie CDPW, w którym określono wymogi dotyczące rozrachunku instrumentów finansowych oraz przepisy dotyczące organizacji i prowadzenia CDPW. Ponadto CDPW powinny zapoznać się z wytycznymi dotyczącymi cyberodporności Komitetu ds. Infrastruktury Płatności i Rynku (CPMI) i Międzynarodowej Organizacji Komisji Papierów Wartościowych (IOSCO), wprowadzonymi w ramach prognozy Eurosystemu w zakresie cyberodporności dla infrastruktur rynku finansowego (Eurosystem Cyber Resilience Oversight Expectations for FMIs) (grudzień 2018) ([33]). Oprócz posiadania kompetencji nadzorczych powierzonych właściwym organom krajowym na mocy rozporządzenia w sprawie CDPW członkowie ESBC pełnią rolę „odpowiednich organów" jako nadzorujący systemy rozrachunku papierów wartościowych prowadzone przez CDPW, jako banki centralne emitujące najbardziej istotne waluty, w których prowadzony jest rozrachunek, oraz jako banki centralne, w których prowadzony jest rozrachunek pieniężnej części transakcji ([34]). W tym względzie motyw 8 rozporządzenia w sprawie CDPW stanowi, że rozporządzenie powinno pozostawać bez uszczerbku dla obowiązków EBC oraz krajowych banków centralnych związanych z zapewnieniem wydajnych i rzetelnych systemów rozliczeń i płatności w ramach Unii i w innych państwach. Motyw 8 stanowi dalej, że rozporządzenie to nie powinno uniemożliwiać członkom ESBC dostępu do informacji istotnych z punktu widzenia wykonywania ich obowiązków ([35]), w tym nadzoru nad CDPW i innymi infrastrukturami rynku finansowego ([36]).

2.2.2. Ponadto członkowie ESBC często działają jako agenci rozrachunkowi w odniesieniu do pieniężnych części transakcji na papierach wartościowych, a Eurosystem oferuje usługi rozrachunkowe za pośrednictwem T2S centralnym depozytom papierów wartościowych. Nadzór Eurosystemu nad T2S jest związany z jego mandatem w zakresie zapewniania skuteczności i rzetelności systemów rozliczeń i płatności, natomiast właściwe organy i odpowiednie organy w poszczególnych jurysdykcjach dążą do zapewnienia sprawnego funkcjonowania CDPW, bezpieczeństwa i skuteczności rozrachunku oraz właściwego funkcjonowania rynków finansowych.

2.2.3. Zgodnie z projektem rozporządzenia ([37]) banki centralne ESBC nie biorą udziału w opracowywaniu regulacyjnych standardów technicznych w odniesieniu do określenia ryzyk związanych z ICT. Podobnie zgodnie z projektem rozporządzenia ([38]) odpowiednie organy nie są informowane o incydentach związanych z ICT. Banki centralne ESBC powinny być zaangażowane w takim samym stopniu, jak obecnie wynika to z rozporządzenia w sprawie CDPW, a odpowiednie organy powinny być informowane o incydentach związanych z ICT. Eurosystem jest odpowiednim organem dla wszystkich CDPW strefy euro, a także dla pewnej liczby innych CDPW na obszarze Unii. Banki centralne ESBC powinny być informowane o incydentach związanych z ICT, które mają znaczenie dla wykonywania ich zadań, w tym nadzoru nad CDPW i innymi infrastrukturami rynku finansowego. Ryzyka, na które narażone są CDPW, w tym ryzyka związane z ICT, mogą stanowić zagrożenie dla należytego funkcjonowania CDPW. Zatem ryzyka związane z ICT mają znaczenie dla odpowiednich organów, które powinny otrzymywać pełny i szczegółowy obraz tych ryzyk, aby dokonać ich oceny i wpłynąć na podejście CDPW do zarządzania ryzykiem. Projekt rozporządzenia nie powinien ustanawiać mniej surowych wymogów w odniesieniu do ryzyk dotyczących ICT w porównaniu do tych wynikających z rozporządzenia w sprawie CDPW i aktualnych właściwych regulacyjnych standardów technicznych.

2.2.4. Ponadto organy prawodawcze Unii powinny doprecyzować powiązania pomiędzy projektem rozporządzenia ([39]) a regulacyjnymi standardami technicznymi uzupełniającymi rozporządzenie w sprawie CDPW. W szczególności nie jest jasne, czy CDPW powinien być zwolniony z obowiązku posiadania drugiej lokalizacji, w przypadku gdy jego zewnętrzny dostawca usług ICT taką drugą lokalizację posiada ([40]). Jeżeli CDPW miałby być zwolniony z obowiązku posiadania drugiej lokalizacji, moc prawna takiego wymogu jest niejasna. Podobnie

([33]) Dostępne na stronie internetowej EBC www.ecb.europa.eu.

([34]) Zob. art. 12 rozporządzenia (UE) nr 909/2014.

([35]) Zob. także art. 13 oraz art. 17 ust. 4 i art. 22 ust. 6 rozporządzenia (UE) nr 909/2014.

([36]) Zob. pkt 7.3 opinii Europejskiego Banku Centralnego z dnia 6 kwietnia 2017 r. w sprawie rozpoznawania infrastruktury krytycznej dla celów bezpieczeństwa technologii informacyjnej (CON/2017/10); pkt 7.2 opinii Europejskiego Banku Centralnego z dnia 8 listopada 2018 r. w sprawie wyznaczenia usług kluczowych i operatorów usług kluczowych na potrzeby bezpieczeństwa sieci i systemów informatycznych (CON/2018/47); pkt 3.5.2 opinii Europejskiego Banku Centralnego z dnia 2 maja 2019 r w sprawie bezpieczeństwa sieci i systemów informatycznych (CON/2019/17) i pkt 3.5.2 opinii Europejskiego Banku Centralnego z dnia 11 listopada 2019 r. w sprawie bezpieczeństwa sieci i systemów informatycznych (CON/2019/38).

([37]) Zob. art. 54 ust. 5 projektu rozporządzenia i art. 45 ust. 7 rozporządzenia (UE) nr 909/2014.

([38]) Zob. art. 54 ust. 4 projektu rozporządzenia i art. 45 ust. 6 rozporządzenia (UE) nr 909/2014.

([39]) Zob. art. 11 ust. 5 projektu rozporządzenia.

([40]) Zob. art. 78 ust. 3 rozporządzenia delegowanego Komisji (UE) 2017/392 z dnia 11 listopada 2016 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 w odniesieniu do regulacyjnych standardów technicznych dotyczących wymogów w zakresie udzielania zezwoleń oraz wymogów nadzorczych i operacyjnych dla centralnych depozytów papierów wartościowych (Dz.U. L 65 z 10.3.2017, s. 48).

projekt rozporządzenia ([41]) odnosi się do zakładanego czasu wznowienia funkcji i akceptowalnego poziomu utraty danych dla każdej funkcji ([42]), podczas gdy regulacyjny standard techniczny wyróżnia najważniejsze funkcje ([43]) i najważniejsze operacje ([44]) w odniesieniu do czasu wznowienia funkcji określonego dla najważniejszych operacji CDPW. Dla uniknięcia ryzyka wzajemnie sprzecznych wymogów niezbędna jest pogłębiona refleksja i dalsze doprecyzowanie przez organy prawodawcze Unii powiązań pomiędzy projektem rozporządzenia a regulacyjnymi standardami technicznymi uzupełniającymi rozporządzenie w sprawie CDPW. Wreszcie, należy doprecyzować, że wyłączenia przyznane CDPW prowadzonym przez pewne podmioty publiczne rozporządzeniem w sprawie CDPW ([45]) zostają rozciągnięte także na proponowane rozporządzenie.

2.3. *Kompetencje ESBC w zakresie rozliczania papierów wartościowych*

2.3.1. Kompetencje w zakresie nadzoru nad kontrahentami centralnymi (CCP) zostały powierzone bankom centralnym ESBC. W tym względzie krajowe banki centralne Eurosystemu w wypełnianiu funkcji nadzoru i kontroli w odniesieniu do CCP często współpracują z właściwymi organami krajowymi i uczestniczą we właściwym kolegium CCP powołanym zgodnie z rozporządzenie (UE) nr 648/2012 Parlamentu Europejskiego i Rady ([46]) (zwanego dalej „rozrozporządzeniem EMIR"). Właściwi członkowie Eurosystemu ([47]) uczestniczą w kolegiach powołanych na podstawie rozporządzenia EMIR w ramach wykonywania swojej funkcji nadzorczej i reprezentują Eurosystem jako centralny bank emisji dla CCP, gdzie euro jest jedną z najważniejszych walut dla rozliczanych instrumentów finansowych (oraz dla eksterytorialnych CCP, które rozliczają znaczącą część instrumentów finansowych w euro). EBC jest bankiem centralnym emisji dla CCP spoza strefy euro.

2.3.2. Zgodnie z projektem rozporządzenia ([48]) banki centralne ESBC nie biorą udziału w opracowywaniu regulacyjnych standardów technicznych w odniesieniu do określenia ryzyk związanych z ICT. Ponadto w projekcie rozporządzenia ([49]) brak jest odniesienia do wymogów dotyczących zakładanego czasu wznowienia funkcji i akceptowalnego poziomu utraty danych dla każdej funkcji wynikających z rozporządzenia EMIR ([50]). Proponowane przepisy regulacyjne nie powinny ustanawiać mniej surowych wymogów w odniesieniu do ryzyk związanych z ICT niż istniejące obecnie. Stąd niezwykle istotne jest jasne określenie zakładanego czasu wznowienia funkcji i akceptowalnego poziomu utraty danych w celu uzyskania ram należytego zarządzania ciągłością działania. Utrzymanie zakładanego czasu wznowienia funkcji i akceptowalnego poziomu utraty danych jest również częścią zasad dotyczących infrastruktur rynku finansowego CPMI-IOSCO ([51]). Należy utrzymać obecny przepis rozporządzenia EMIR i dostosować odpowiednio projekt rozporządzenia. Banki centralne ESBC powinny brać udział w przygotowaniu aktów prawa pochodnego i w dalszym doprecyzowywaniu i rozważaniu przez organy prawodawcze Unii powiązań pomiędzy projektem rozporządzenia oraz uzupełnieniem regulacyjnych standardów technicznych w celu uniknięcia ryzyka wzajemnie sprzecznych lub pokrywających się wymogów.

3. **Uwagi szczegółowe dotyczące aspektów związanych z nadzorem ostrożnościowym**

3.1. Rozporządzenie Rady (UE) nr 1024/2013 ([52]) (zwane dalej „rozporządzeniem w sprawie Jednolitego Mechanizmu Nadzorczego") powierza EBC szczególne zadania w zakresie nadzoru ostrożnościowego nad instytucjami kredytowymi w strefie euro oraz nakłada na EBC odpowiedzialność za skuteczne i spójne funkcjonowanie Jednolitego Mechanizmu Nadzorczego, w ramach którego EBC i uczestniczące właściwe organy krajowe dzielą szczególne obowiązki w zakresie nadzoru ostrożnościowego. W szczególności EBC wykonuje zadanie udzielania i cofania zezwoleń wszystkim instytucjom kredytowym. EBC ma również między innymi za zadanie zapewnienie zgodności z odpowiednimi przepisami Unii nakładającymi na instytucje kredytowe wymogi ostrożnościowe, w tym wymóg posiadania solidnych zasad zarządzania, takich jak należyte procesy zarządzania ryzykiem i mechanizmy kontroli wewnętrznej ([53]). W tym celu EBC posiada wszelkie uprawnienia nadzorcze do ingerowania w działalność instytucji

([41]) Zob. art. 11 ust. 6 projektu rozporządzenia.
([42]) Zob. art. 3 ust. 17 projektu rozporządzenia.
([43]) Zob. art. 76 ust. 2 lit. d) i e) rozporządzenia delegowanego Komisji (UE) 2017/392.
([44]) Zob. art. 78 ust. 2 i 3 rozporządzenia delegowanego Komisji (UE) 2017/392.
([45]) Zob. art. 1 ust. 4 rozporządzenia (UE) nr 909/2014.
([46]) Rozporządzenie (UE) nr 648/2012 Parlamentu Europejskiego i Rady 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).
([47]) Zob. art. 18 ust. 2 lit. g) i h) rozporządzenia EMIR.
([48]) Zob. art. 53 ust. 2 lit. b) i ust. 3 projektu rozporządzenia i art. 34 ust. 3 rozporządzenia EMIR.
([49]) Zob. art. 53 ust. 2 lit. a) projektu rozporządzenia.
([50]) Zob. art. 34 rozporządzenia EMIR.
([51]) Zob. „Zasady dotyczące infrastruktur rynku finansowego CPMI-IOSCO" (Principles for Financial Market Infrastructures) dostępne na stronie internetowej BIS pod adresem www.bis.org.
([52]) Rozporządzenie Rady (UE) nr 1024/2013 z dnia 15 października 2013 r. powierzające Europejskiemu Bankowi Centralnemu szczególne zadania w odniesieniu do polityki związanej z nadzorem ostrożnościowym nad instytucjami kredytowymi (Dz.U. L 287 z 29.10.2013, s. 63).
([53]) Zob. art. 4 ust. 1 lit. e) i art. 6 ust. 4 rozporządzenia (UE) nr 1024/2013.

kredytowych, które są niezbędne do wykonywania jego funkcji. EBC i odpowiedni właściwy organ krajowy są właściwymi organami wykonującymi określone uprawnienia w zakresie nadzoru ostrożnościowego na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([54]) (zwanego dalej „rozporządzeniem w sprawie wymogów kapitałowych") oraz dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE ([55]) (zwanej dalej „dyrektywą w sprawie wymogów kapitałowych").

3.2. Projekt rozporządzenia stanowi, że należy rozbudować jednolity zbiór przepisów i system nadzoru, tak aby uwzględniały one również operacyjną odporności cyfrową i bezpieczeństwo ICT, poprzez rozszerzenie kompetencji organów nadzoru finansowego, którym powierzono zadanie monitorowania i ochrony stabilności finansowej i integralności rynku ([56]). Ma to na celu wspieranie kompleksowych ram dotyczących ICT lub ryzyka operacyjnego poprzez dalszą harmonizację najważniejszych wymogów w zakresie operacyjnej odporności cyfrowej dla wszystkich podmiotów finansowych ([57]). W szczególności projekt rozporządzenia ma na celu konsolidację i aktualizację wymogów dotyczących ryzyka związanego z ICT zawartych dotychczas w różnych aktach prawnych ([58]).

3.3. Wymogi dotyczące ryzyka związanego z ICT w sektorze finansowym obecnie rozsiane są w wielu aktach prawnych Unii, w tym w dyrektywie w sprawie wymogów kapitałowych i instrumentach „miękkiego prawa" (takich jak wytyczne EUNB), są rozbieżne i czasami niekompletne. W niektórych przypadkach odniesienia do ryzyka związanego z ICT są niebezpośrednie, w innych zupełnie brak jest takich odniesień. Sytuacja ta powinna zostać rozwiązana poprzez dostosowanie projektu rozporządzenia i tych aktów prawnych. W tym celu projekt dyrektywy zmieniającej wprowadza szereg zmian, które wydają się niezbędne dla zapewnienia jasności prawnej i spójności w odniesieniu do stosowania różnych wymogów w zakresie operacyjnej odporności cyfrowej. Jednakże zmiany w dyrektywie w sprawie wymogów kapitałowych proponowane w obecnym projekcie dyrektywy zmieniającej ([59]) odnoszą się tylko do przepisów w zakresie planów awaryjnych i planów utrzymania ciągłości działania ([60]), gdyż to one uznawane są za podstawę rozwiązywania zagadnień dotyczących zarządzania ryzykiem związanym z ICT.

3.4. Ponadto projekt rozporządzenia ([61]) stanowi, że podmioty finansowe, w tym instytucje kredytowe, mają obowiązek posiadać wewnętrzne ramy zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z ICT. Projekt rozporządzenia ([62]) przewiduje stosowanie wymogów w nim zawartych na poziomie indywidualnym i skonsolidowanym, lecz bez dostatecznej koordynacji z sektorowymi aktami prawnymi, o których mowa. Wreszcie, projekt rozporządzenia ([63]) stanowi, że – bez uszczerbku dla przepisów dotyczących zasad nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, o których mowa w projekcie rozporządzenia ([64]) – zgodność z obowiązkami określonymi w tym projekcie zapewnia – w odniesieniu do instytucji kredytowych – właściwy organ wyznaczony zgodnie z art. 4 dyrektywy w sprawie wymogów kapitałowych, bez uszczerbku dla szczególnych zadań powierzonych EBC na mocy rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego.

3.5. Mając na uwadze powyższe, EBC rozumie, że w odniesieniu do instytucji kredytowych, i z zastrzeżeniem przepisów projektu rozporządzenia dotyczących ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT ([65]), projekt rozporządzenia ma na celu ustanowienie ostrożnościowych wewnętrznych ram zarządzania w celu zarządzania ryzykiem związanym z ICT, które zostaną włączone w ogólne wewnętrzne ramy zarządzania wynikające z dyrektywy w sprawie wymogów kapitałowych. Ponadto, uwzględniając ostrożnościowy charakter proponowanych ram, właściwe organy odpowiedzialne za nadzór nad przestrzeganiem obowiązków wynikających z proponowanych ram, w tym ECB, będą organami odpowiedzialnymi za nadzór bankowy zgodnie z rozporządzeniem w sprawie Jednolitego Mechanizmu Nadzorczego.

([54]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 176 z 27.6.2013, s. 1).

([55]) Dyrektywa 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, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

([56]) Zob. motyw 8 projektu rozporządzenia.

([57]) Zob. motyw 11 projektu rozporządzenia.

([58]) Zob. motyw 12 projektu rozporządzenia.

([59]) Zob. motywy 4 i 5 projektu dyrektywy zmieniającej.

([60]) Zob. art. 85 dyrektywy w sprawie wymogów kapitałowych.

([61]) Zob. art. 4 ust. 1 projektu rozporządzenia.

([62]) Zob. art. 25 ust. 3 i 4 projektu rozporządzenia.

([63]) Zob. art. 41 projektu rozporządzenia.

([64]) Zob. sekcja II rozdziału V projektu rozporządzenia.

([65]) Zob. sekcja II rozdziału V projektu rozporządzenia.

3.6. Organy prawodawcze Unii mogą zatem uwzględnić poniższe sugestie w celu zwiększenia jasności i koordynacji pomiędzy projektem rozporządzenia a dyrektywą w sprawie wymogów kapitałowych. Po pierwsze, wymogi wynikające z projektu rozporządzenia mogą zostać wyraźnie określone jako ostrożnościowe, tak jak ma to miejsce między innymi w rozporządzeniu w sprawie CDPW ([66]). Po drugie, motywy proponowanej dyrektywy zmieniającej ([67]) mogą zostać poszerzone, jeśli wymogi projektu rozporządzenia wyjdą poza samą fazę planów awaryjnych i planów utrzymania ciągłości działania. Środki zarządzania ryzykiem związanym z ICT generalnie podlegają bardziej ogólnemu zakresowi solidnych zasad zarządzania zgodnie z art. 74 dyrektywy w sprawie wymogów kapitałowych ([68]). Po trzecie, projekt rozporządzenia ([69]) powinien zostać zmieniony tak, aby przywoływał w motywach kompetencje EBC w zakresie nadzoru ostrożnościowego nad instytucjami kredytowymi na postawie Traktatu i rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego. Po czwarte, odniesienie do stosowania wymogów w nim zawartych na poziomie indywidualnym i skonsolidowanym ([70]) powinno także zostać zrewidowane, gdyż poziomy subskonsolidowany i skonsolidowany nie zostały zdefiniowane w projekcie rozporządzenia, a pewne typy pośredników nie są objęte skonsolidowanym nadzorem na podstawie właściwych przepisów (np. instytucje płatnicze). Ponadto poziom stosowania wymogów wynikających z projektu rozporządzenia powinien mieć swoje źródło wyłącznie w aktach prawnych mających zastosowanie do każdego typu podmiotu finansowego. W przypadku instytucji kredytowych przewidziany został jasny związek pomiędzy dyrektywą w sprawie wymogów kapitałowych a projektem rozporządzenia, a zatem wymogi proponowanego rozporządzenia automatycznie znajdowałyby zastosowanie odpowiednio na poziomie indywidualnym, subskonsolidowanym i skonsolidowanym ([71]). Wreszcie, organy prawodawcze Unii mogą rozważyć ustanowienie systemu przejściowego, który obejmowałby czas przed wejściem w życie proponowanego rozporządzenia a wejściem w życie regulacyjnych standardów technicznych przewidzianych w projekcie rozporządzenia, przy uwzględnieniu, że część pośredników, w tym instytucje kredytowe, już podlega przepisom dotyczącym ryzyka związanego z ICT, które mają zastosowanie w poszczególnych sektorach i są bardziej szczegółowe niż ogólne przepisy projektu rozporządzenia.

3.7. Na mocy rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego EBC powierzono zadanie zapewnienia przestrzegania przez instytucje kredytowe przepisów prawa Unii nakładających na nie obowiązek posiadania solidnych procesów zarządzania ryzykiem i mechanizmów kontroli wewnętrznej ([72]). Oznacza to, że EBC musi zapewnić, aby instytucje kredytowe wdrażały polityki i procesy służące ocenie ekspozycji na ryzyko operacyjne, w tym ryzyko modelu, i ryzyko obejmujące zdarzenia rzadko występujące, lecz mające poważne skutki. Instytucje zobowiązane są także określać, co stanowi ryzyko operacyjne do celów wspomnianych polityk i procedur ([73]).

3.8. W lipcu 2017 r. Rada Prezesów Europejskiego Banku Centralnego (EBC) przyjęła ramy zgłaszania incydentów cybernetycznych Jednolitego Mechanizmu Nadzorczego (SSM Cyber Incident Reporting Framework, zwane dalej „Ramami"), na podstawie projektu Rady Prezesów zgodnie z art. 26 ust. 8 i art. 6 ust. 2 rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego i art. 21 ust. 1 rozporządzenia (UE) nr 468/2014 Europejskiego Banku Centralnego (EBC/2014/17) ([74]). Ramy przewidują wiążące wezwania (indywidualne decyzje adresowane do instytucji kredytowych) do udzielenia informacji lub zgłoszenia na podstawie art. 10 rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego ([75]). Niektóre państwa już posiadają procedury zgłaszania incydentów, zobowiązujące instytucje kredytowe do zgłaszania poważnych cyberincydentów właściwym organom krajowym. W tych państwach istotne instytucje kredytowe nadal zgłaszają incydenty do właściwych organów krajowych, które następnie bez zbędnej zwłoki przekazują je w imieniu nadzorowanych podmiotów do EBC. Zatem decyzje, o których mowa powyżej, są także skierowane do tych właściwych organów krajowych, aby przekazały one te informacje do EBC

([66]) Zob. tytuł rozdziału II, sekcja 4, „Wymogi ostrożnościowe" rozporządzenia w sprawie CDPW.

([67]) Zob. motyw 4 projektu dyrektywy zmieniającej.

([68]) Art. 85 dyrektywy 2013/36/UE stanowi wyłącznie specyfikację. W tym względzie zobacz także s. 4, 11 i 37 wytycznych Europejskiego Urzędu Nadzoru Bankowego w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem z dnia 29 listopada 2019 r. (zwanych dalej „wytycznymi EUNB"), dla których główna podstawa prawna jest wyraźnie wskazana jako art. 74 dyrektywy 2013/36/UE.

([69]) Zob. art. 41 ust. 1 projektu rozporządzenia.

([70]) Zob. art. 25 ust. 3 i 4 projektu rozporządzenia.

([71]) Zob. także art. 109 dyrektywy w sprawie wymogów kapitałowych.

([72]) Zob. art. 4 ust. 1 lit. e) rozporządzenia w sprawie Jednolitego Mechanizmu Nadzorczego.

([73]) Zob. art. 85 dyrektywy w sprawie wymogów kapitałowych.

([74]) Rozporządzenie (UE) nr 468/2014 Europejskiego Banku Centralnego z dnia 16 kwietnia 2014 r ustanawiające ramy współpracy pomiędzy Europejskim Bankiem Centralnym a właściwymi organami krajowymi oraz wyznaczonymi organami krajowymi w ramach Jednolitego Mechanizmu Nadzorczego (rozporządzenie ramowe w sprawie Jednolitego Mechanizmu Nadzorczego) (EBC/2014/17) (Dz.U. L 141 z 14.5.2014, s. 1).

([75]) Konkretnie cyberincydent (zidentyfikowane możliwe naruszenie bezpieczeństwa informacji, czy to w złym zamiarze, czy przypadkowe) musi zostać zgłoszony EBC, jeżeli spełniony jest przynajmniej jeden z następujących warunków: 1) potencjalne skutki finansowe mogą wynieść 5 milionów EUR lub 0,1% kapitału podstawowego Tier I; 2) incydent był ogłoszony publicznie lub powoduje negatywne skutki wizerunkowe; 3) incydent został przedstawiony urzędującemu przewodniczącemu poza drogą zwykłego zgłaszania; 4) bank poinformował o incydencie CERT/CSIRT, agencję bezpieczeństwa lub policję; 5) uruchomione zostały procedury przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej lub ciągłości działania, albo złożony został wniosek o wypłatę cyberubezpieczenia; 6) nastąpiło złamanie wymogów prawnych lub regulacyjnych; lub 7) bank na podstawie wewnętrznych kryteriów i oceny eksperckiej (w tym ewentualnego skutku systemowego) postanawia zawiadomić EBC.

w oparciu o Ramy. EBC wspiera starania organów prawodawczych Unii na rzecz harmonizacji i usprawnienia procedur, między innymi w odniesieniu do zasad i obowiązków mających zastosowanie do zgłaszania incydentów przez instytucje kredytowe. Mając to na uwadze, EBC wykazuje gotowość do zmiany (i ewentualnego uchylenia) Ram, jeśli okaże się to niezbędne w świetle możliwości przyjęcia projektu rozporządzenia.

4. Uwagi szczegółowe dotyczące zarządzania ryzykiem związanym z ICT, zgłaszania incydentów, testowania operacyjnej odporności cyfrowej i ryzyka ze strony zewnętrznych dostawców usług ICT

4.1. *Zarządzanie ryzykiem związanym z ICT*

4.1.1. EBC z zadowoleniem przyjmuje wprowadzenie w projekcie rozporządzenia solidnych i kompleksowych ram zarządzania ryzykiem związanym z ICT, obejmujących wytyczne dotyczące cyberodporności CPMI-IOSCO i ściśle dostosowanych do najlepszych praktyk, w tym do prognozy Eurosystemu w zakresie cyberodporności dla infrastruktur rynku finansowego (Eurosystem Cyber Resilience Oversight Expectations for FMIs).

4.1.2. EBC podziela przekonanie, że podmioty finansowe powinny przeprowadzać ocenę ryzyka przy każdej „większej zmianie" w infrastrukturze sieci i systemów informatycznych ([76]). Pomimo to jednak projekt rozporządzenia nie zawiera definicji „większej zmiany", co otwiera drogę dla rozbieżnych interpretacji podmiotów finansowych, a w konsekwencji może zagrozić realizacji celu rozporządzenia, jakim jest harmonizacja. Ze względu na pewność prawa organy prawodawcze Unii mogą rozważyć wprowadzenie do projektu rozporządzenia definicji „większej zmiany".

4.1.3. EBC co do zasady zgadza się, że podmioty finansowe inne niż mikroprzedsiębiorstwa powinny zgłaszać właściwym organom koszty i straty spowodowane zakłóceniami w funkcjonowaniu ICT oraz incydentami związanymi z ICT ([77]). Jednakże w celu zapewnienia ogólnej skuteczności systemu i dla uniknięcia możliwego przeciążenia właściwych organów i podmiotów finansowych z powodu nadmiernej liczby zgłoszeń korzystne mogłoby być rozważenie przez organy prawodawcze Unii wprowadzenia odpowiednich progów, np. o charakterze ilościowym.

4.1.4. EBC uznaje możliwość powierzenia przez podmioty finansowe zadań związanych ze sprawdzaniem zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT przedsiębiorstwom wewnątrz grupy lub przedsiębiorstwom zewnętrznym, za zgodą właściwych organów ([78]). Jednocześnie jednak bardzo ważne jest, aby organy prawodawcze Unii doprecyzowały, w jaki sposób ta zgoda właściwych organów powinna być udzielana w przypadkach, gdy dany podmiot finansowy podlega wielu właściwym organom. Taka sytuacja może mieć miejsce, gdy podmiot finansowy jest instytucją kredytową, dostawcą usług w zakresie kryptoaktywów lub dostawcą usług płatniczych. Wreszcie, w odniesieniu do identyfikacji i klasyfikacji dokonywanej przez podmioty finansowe zgodnie z projektem rozporządzenia ([79]), EBC uważa za pożądane, aby dla celów klasyfikacji zasobów projekt rozporządzenia wymagał od podmiotów finansowych uwzględnienia także krytyczności tych zasobów (tj. tego, czy wspierają one krytyczne funkcje).

4.2. *Zgłaszanie incydentów*

4.2.1. EBC z zadowoleniem przyjmuje przedstawione w projekcie rozporządzenia starania na rzecz harmonizacji zasad dotyczących zgłaszania incydentów związanych z ICT w kierunku centralizacji zgłaszania poważnych incydentów związanych z ICT ([80]). Wprowadzenie zharmonizowanych ram dla zgłaszania poważnych incydentów związanych z ICT ([81]) odpowiednim właściwym organom co do zasady złagodziłoby i zharmonizowało obciążenia dla podmiotów finansowych, w tym instytucji kredytowych, związane ze zgłaszaniem. Właściwe organy skorzystałyby na rozszerzeniu zakresu incydentów podlegających zgłaszaniu ponad zakres obejmujący incydenty związane z zagrożeniami cybernetycznymi określony istniejącymi ramami ([82]). Przyszłe przyjęcie projektu rozporządzenia wymagać będzie przeglądu i ewentualnie uchylenia istniejących ram, w tym ram zgłaszania incydentów cybernetycznych Jednolitego Mechanizmu Nadzorczego (SSM Cyber Incident Reporting Framework). Aby jednak osiągnąć rzeczywiste uproszczenie i pełne dostosowanie wszystkich ram, konieczne jest zapewnienie, aby zakres przepisów dotyczących zgłaszania incydentów wynikający z projektu rozporządzenia, w tym wszystkie odpowiednie definicje, progi i parametry zgłaszania, został w pełni dostosowane do odpowiednich ram. W szczególności niezwykle istotne jest zapewnienie zgodności pomiędzy projektem rozporządzenia z jednej strony a dyrektywą Parlamentu Europejskiego i Rady

([76]) Zob. art. 7 ust. 3 projektu rozporządzenia.
([77]) Zob. art. 10 ust. 9 projektu rozporządzenia.
([78]) Zob. art. 5 ust. 10 projektu rozporządzenia.
([79]) Zob. art. 7 projektu rozporządzenia.
([80]) Zob. art. 19 projektu rozporządzenia.
([81]) Zob. art. 3 ust. 7, art. 17 i 18 projektu rozporządzenia.
([82]) Zob. np. Ramy.

(UE) 2015/2366 ([83]) w sprawie usług płatniczych w ramach rynku wewnętrznego (zwaną dalej „drugą dyrektywą w sprawie usług płatniczych") oraz wytycznymi EUNB w sprawie zgłaszania poważnych incydentów (zwanymi dalej „wytycznymi EUNB") z drugiej strony. Projekt dyrektywy zmieniającej ([84]) zawiera poprawki do drugiej dyrektywy w sprawie usług płatniczych dotyczące rozgraniczenia zgłaszania incydentów na podstawie projektu rozporządzenia oraz drugiej dyrektywy w sprawie usług płatniczych, co miałoby znaczenie przede wszystkim dla dostawców usług płatniczych, którzy mogą być także uprawnieni do działania jako instytucje kredytowe, a także dla właściwych organów. Brak jest jasności co do procesu zgłaszania incydentów i istnieje możliwość pokrywania się wymogów w odniesieniu do pewnych incydentów, które podlegają zgłoszeniu jednocześnie na podstawie projektu rozporządzenia, jak i wytycznych EUNB.

4.2.2. Proces zgłaszania poważnych incydentów na podstawie – odpowiednio – projektu rozporządzenia ([85]), drugiej dyrektywy w sprawie usług płatniczych i odpowiednich wytycznych EUNB wymagałby od dostawców usług płatniczych złożenia odpowiednim właściwym organom sprawozdania z incydentu po dokonaniu klasyfikacji incydentu. Co istotne, wstępne powiadomienia nie ujmują istoty sprawy, przyczyn czy obszarów funkcjonalnych dotkniętych incydentem, a dostawcy usług płatniczych mogą dokonać takich ustaleń dopiero w późniejszej fazie, gdy dostępne są bardziej szczegółowe informacje na temat zdarzenia. W konsekwencji wstępne powiadomienia o incydentach mogłyby być przedkładane zarówno na podstawie projektu rozporządzenia, jak i wytycznych EUNB, lub też dostawcy usług płatniczych mogliby zdecydować się na jedne ramy, a następnie dokonać korekty swojego zgłoszenia w późniejszym terminie. Podobna niepewność (np. w odniesieniu do pierwotnej przyczyny każdego zdarzenia) znajduje swoje odzwierciedlenie także w odniesieniu do sprawozdań śródokresowych i sprawozdań końcowych. Tutaj także powstanie możliwość równoległego dokonywania zgłoszeń jednocześnie na podstawie projektu rozporządzenia i drugiej dyrektywy w sprawie usług płatniczych.

4.2.3. Pewne incydenty, które mogą być kategoryzowane jako związane z ICT, mogą także mieć wpływ na inne obszary i w związku z tym podlegać obowiązkowi zgłaszania na podstawie wytycznych EUNB. Taka sytuacja może mieć miejsce, kiedy incydent ma znaczenie z punktu widzenia ICT, lecz jednocześnie wpływa także bezpośrednio na świadczenie usług płatniczych lub na inne, niezwiązanych z ICT, obszary i kanały funkcjonalne. Dodatkowo może zdarzyć się, że rozróżnienie pomiędzy incydentami operacyjnymi a tymi związanymi z ICT nie będzie możliwe. Ponadto w przypadku, gdy ten sam podmiot finansowy jest istotną instytucją kredytową oraz dostawcą usług płatniczych, zgodnie z projektem rozporządzenia będzie on miał obowiązek zgłosić incydent związany z ICT dwukrotnie, jako że podlega on dwóm właściwym organom. Mając powyższe na względzie, projekt rozporządzenia powinien wyraźniej określać, w jaki sposób wzajemne oddziaływanie pomiędzy drugą dyrektywą w sprawie usług płatniczych a wytycznymi EUNB powinno wyglądać w praktyce. Co istotne, przez wzgląd na harmonizację i uproszczenie obowiązków dotyczących zgłaszania, ważne jest, aby organy prawodawcze Unii przeanalizowały pozostające do rozstrzygnięcia zagadnienia podwójnego zgłaszania i doprecyzowały, czy projekt rozporządzenia z jednej strony, i druga dyrektywa w sprawie usług płatniczych i wytyczne EUNB z drugiej strony, mają współistnieć, czy powinien istnieć jednolity zbiór wymogów dotyczących zgłaszania incydentów.

4.2.4. Projekt rozporządzenia wprowadza wymóg, aby właściwe organy ([86]), po otrzymaniu sprawozdania, potwierdzały otrzymanie powiadomienia i tak szybko, jak to możliwe, przekazały podmiotowi finansowemu wszelkie niezbędne informacje zwrotne lub wytyczne, w szczególności w celu omówienia środków zaradczych na poziomie danego podmiotu lub sposobów ograniczenia do minimum negatywnych skutków we wszystkich sektorach. Oznaczałoby to, że właściwe organy powinny brać aktywny udział w zarządzaniu incydentami i wdrażaniu środków naprawczych, jednocześnie oceniając reagowanie nadzorowanego podmiotu na krytyczne incydenty. EBC podkreśla, że odpowiedzialność za środki naprawcze i zarządzanie nimi oraz konsekwencje incydentu powinny w sposób wyłączny i jasny pozostać po stronie zainteresowanego podmiotu finansowego. EBC zaproponowałby zatem ograniczenie informacji zwrotnych i wytycznych wyłącznie do informacji zwrotnych i wytycznych wysokiej wagi o charakterze ostrożnościowym. Gdyby informacje zwrotne miały być szersze, wymagałoby to zaangażowania wyspecjalizowanych profesjonalistów dysponujących rozległą wiedzą techniczną, a tacy zazwyczaj nie są dostępni w zapleczu kadrowym, jakim dysponują organy ostrożnościowe.

4.3. *Testy operacyjnej odporności cyfrowej*

4.3.1. EBC z zadowoleniem przyjmuje ustanowienie w projekcie rozporządzenia wymogów ([87]) testowania operacyjnej odporności cyfrowej wszystkich podmiotów finansowych i obowiązek posiadania przez każdą instytucję własnego programu testowania. W projekcie rozporządzenia ([88]) wymienia się różne rodzaje testów w charakterze wskazówek

([83]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.U. L 337 z 23.12.2015, s. 35).

([84]) Zob. art. 7 ust. 9 projektu dyrektywy zmieniającej.

([85]) Zob. art. 17 ust. 3 projektu rozporządzenia.

([86]) Zob. art. 20 projektu rozporządzenia.

([87]) Zob. art. 21 i 22 projektu rozporządzenia.

([88]) Zob. art. 22 ust. 1 projektu rozporządzenia.

dla podmiotów finansowych. Rodzaje te nie są całkiem jasne i część testów, jak np. testy kompatybilności, kwestionariusze czy testy scenariuszowe, podlegają interpretacji przez Europejskie Urzędy Nadzoru, właściwe organy czy podmioty finansowe. Co więcej, nie ma wskazówek co do częstotliwości przeprowadzania poszczególnych testów. Możliwe byłoby zastosowanie podejścia, zgodnie z którym proponowane rozporządzenie określałoby ogólne wymogi testów, a dokładniejszy opis ich poszczególnych rodzajów byłby zawarty w regulacyjnych i wykonawczych standardach technicznych.

4.3.2. Testy penetracyjne pod kątem wyszukiwania zagrożeń (threat-led penetration testing – TLPT) stanowią ważne narzędzie testowania infrastruktury bezpieczeństwa i gotowości. EBC popiera zatem wykonywanie testów penetracyjnych pod kątem wyszukiwania zagrożeń przez podmioty finansowe. Narzędzie to pozwala na testowanie nie tylko środków technicznych, ale również personelu i procesów. Wyniki tych testów mogą znacząco podnieść świadomość bezpieczeństwa wśród kadry kierowniczej wyższego szczebla testowanych podmiotów. Europejskie ramy etycznych testów typu red teaming w oparciu o dane analityczne dotyczące zagrożeń (Threat Intelligence Based Ethical Red Teaming, TIBER-EU) ([89]) i inne testy penetracyjne pod kątem wyszukiwania zagrożeń już dostępne poza Unią stanowią podstawowe instrumenty samooceny, testowania, ćwiczenia i poprawy postaw odporności cyfrowej i obrony.

4.3.3. W większości państw członkowskich, w których testy TIBER-EU zostały wdrożone, organy nadzoru i organy nadzoru systemowego nie biorą aktywnego udziału we wdrażaniu lokalnego programu TIBER-XX, a personel TIBER Cyber Team (TCT) w prawie wszystkich przypadkach został zlokalizowany poza tymi funkcjami. Z tej przyczyny przeprowadzanie zaawansowanych testów w oparciu o projekt rozporządzenia ([90]) na podstawie testów penetracyjnych pod kątem wyszukiwania zagrożeń powinno być wdrażane raczej jako narzędzie wzmacniania ekosystemu finansowego i wspierania stabilności finansowej niż jako narzędzie czysto nadzorcze. Ponadto nie ma potrzeby rozwijania nowych zaawansowanych ram testowania cyberodporności, gdyż państwa członkowskie powszechnie przyjęły już TIBER-EU, jedyne takie ramy obecnie istniejące w Unii.

4.3.4. Wymogi dla testerów nie powinny być zawarte w podstawowym tekście projektu rozporządzenia, jako że sektor związany z testami penetracyjnymi pod kątem wyszukiwania zagrożeń jest jeszcze w fazie rozwoju i wprowadzenie obowiązkowych szczegółowych wymogów mogłoby ograniczyć innowacje w tym zakresie. EBC jest jednak zdania, że aby zapewnić wysoki stopień niezależności przy przeprowadzaniu testów, podmioty finansowe nie powinny zatrudniać na podstawie umowy o pracę czy na podstawie innych umów testerów, którzy są zatrudnieni na podstawie umowy o pracę czy na podstawie innych umów przez podmioty finansowe z tej samej grupy lub należące do testowanego podmiotu finansowego albo w inny sposób przez niego kontrolowane.

4.3.5. W celu ograniczenia ryzyka fragmentacji i zapewnienia harmonizacji projekt rozporządzenia powinien przewidywać jedne ramy dla testów penetracyjnych pod kątem wyszukiwania zagrożeń mające zastosowanie w sektorze finansowym całej Unii. Fragmentacja mogłaby prowadzić do wzrostu kosztów oraz wymagań technicznych, operacyjnych i dotyczących zasobów finansowych, zarówno po stronie właściwych organów, jak i instytucji finansowych. Taki wzrost kosztów i wymogów może z kolei mieć negatywny wpływ na wzajemne uznawanie testów. Brak harmonizacji i wynikające z niego problemy w zakresie wzajemnego uznawania są w szczególności istotne dla podmiotów finansowych, które mogą posiadać wiele licencji bądź działać w różnych jurysdykcjach na obszarze Unii. Regulacyjne i wykonawcze standardy techniczne dla testów penetracyjnych pod kątem wyszukiwania zagrożeń, jakie należy opracować na podstawie projektu rozporządzenia, powinny być zgodne z TIBER-EU. Ponadto EBC z zadowoleniem przyjmuje możliwość uczestniczenia w opracowaniu tych regulacyjnych i wykonawczych standardów technicznych we współpracy z Europejskimi Urzędami Nadzoru.

4.3.6. Czynny udział właściwych organów w testach mógłby skutkować potencjalnym konfliktem interesów w związku z drugą pełnioną przez nie funkcją, tj. oceną ram testowania podmiotu finansowego. W związku z powyższym EBC proponuje usunięcie z projektu rozporządzenia obowiązku zatwierdzania przez właściwe organy dokumentacji i wydawania potwierdzeń dla testów penetracyjnych pod kątem wyszukiwania zagrożeń.

4.4. Ryzyko ze strony zewnętrznych dostawców usług ICT

4.4.1. EBC z zadowoleniem przyjmuje wprowadzenie kompleksowego zbioru głównych zasad i solidnych ram nadzoru w celu identyfikacji ryzyka ze strony zewnętrznych dostawców usług ICT i zarządzania nim, niezależnie od tego, czy należą oni do tej samej grupy podmiotów finansowych. Tym niemniej dla osiągnięcia skutecznej identyfikacji i zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT konieczna jest prawidłowa identyfikacja i klasyfikacja m.in. kluczowych zewnętrznych dostawców usług ICT. W tym względzie, chociaż należy pozytywnie ocenić wprowadzenie aktów delegowanych ([91]), które uzupełnią kryteria stosowane do celów klasyfikacji ([92]), przed przyjęciem takich aktów delegowanych powinna być zasięgnięta opinia EBC.

([89]) Dostępne na stronie internetowej EBC pod adresem www.ecb.europa.eu.
([90]) Art. 23 i 24 projektu rozporządzenia.
([91]) Zob. art. 28 ust. 3 projektu rozporządzenia.
([92]) Zob. art. 28 ust. 2 projektu rozporządzenia.

4.4.2. W odniesieniu do struktury ram nadzoru ([93]) niezbędne jest dalsze wyjaśnienie roli, jaką pełnić ma Wspólny Komitet. Jednocześnie EBC z zadowoleniem przyjmuje włączenie go do forum nadzoru jako obserwatora, ponieważ zapewni to EBC taki sam dostęp do dokumentów i informacji, jaki posiadają członkowie z prawem głosu ([94]). EBC pragnie zwrócić uwagę organów prawodawczych Unii na fakt, że EBC w roli obserwatora może wnieść swój udział do prac forum nadzoru zarówno w ramach swoich kompetencji jako bank centralny emisji, odpowiedzialny za nadzór nad infrastrukturami rynkowymi, a także jako organ nadzoru ostrożnościowego nad instytucjami kredytowymi. Ponadto EBC wskazuje, że oprócz pełnienia roli obserwatora w forum nadzoru, może on także jako właściwy organ wchodzić w skład wspólnego zespołu ds. kontroli. W tym względzie pożądane byłoby dalsze rozważenie przez organy prawodawcze Unii składu wspólnych zespołów ds. kontroli ([95]), tak aby zapewnić odpowiedni stopień zaangażowania odpowiednich właściwych organów. Podobnie EBC jest zdania, że ze względu na krytyczność, stopień skomplikowania i zakres zewnętrznych usług ICT, należy zwiększyć maksymalną liczbę uczestników wspólnych zespołów ds. kontroli.

4.4.3. EBC zauważa, że zgodnie z projektem rozporządzenia wiodący organ nadzorczy posiada uprawnienie do zalecania kluczowym zewnętrznym dostawcom usług ICT odstąpienia od zawarcia umowy dalszego podwykonawstwa, jeżeli: (i) przewidzianym podwykonawcą jest zewnętrzny dostawca usług ICT lub podwykonawca usług ICT z siedzibą w państwie trzecim, i (ii) podwykonawstwo dotyczy kluczowej lub ważnej funkcji podmiotu finansowego. EBC pragnie podkreślić, że skorzystanie z tych uprawnień przez wiodący organ nadzorczy możliwe jest tylko w przypadku tych umów podwykonawstwa, w drodze których kluczowy zewnętrzny dostawca usług ICT zleca podwykonawstwo kluczowych lub ważnych funkcji odrębnej osobie prawnej mającej siedzibę w państwie trzecim. EBC rozumie, że wiodący organ nadzorczy nie ma porównywalnych uprawnień, aby zalecić kluczowym zewnętrznym dostawcom usług ICT odstąpienie od zawarcia umowy w odniesieniu do outsourcingu kluczowych lub ważnych funkcji podmiotu finansowego na rzecz zaplecza tego dostawcy usług, które zlokalizowane jest w państwie trzecim. Sytuacja taka może mieć miejsce np. wówczas, gdy z przyczyn operacyjnych kluczowe dane lub informacje są przechowywane lub przetwarzane przez zaplecze zlokalizowane poza Europejskim Obszarem Gospodarczym (EOG). W takim przypadku uprawnienia wiodącego organu nadzorczego mogą być niewystarczające do nadania właściwym organom odpowiednich praw dostępu do wszelkich informacji, lokali, infrastruktury i personelu istotnych z punktu widzenia wykonywania kluczowych lub ważnych funkcji podmiotu finansowego. W celu zapewnienia, że możliwość wykonywania zadań przez właściwe organy nie zostanie zakłócona, EBC sugeruje, aby wiodący organ nadzorczy otrzymał także uprawnienie do ograniczenia korzystania przez kluczowych zewnętrznych dostawców usług ICT z zaplecza zlokalizowanego poza EOG. Uprawnienie to mogłoby być wykonywane w tych szczególnych przypadkach, gdy nie zostały zawarte porozumienia administracyjne z właściwymi organami państw trzecich, o jakich mowa w projekcie rozporządzenia ([96]), lub gdy przedstawiciele kluczowego zewnętrznego dostawcy usług ICT nie przedstawią zgodnie z ramami właściwego państwa trzeciego dostatecznych gwarancji dotyczących dostępu do informacji, lokali, infrastruktury i personelu niezbędnych z punktu widzenia wykonywania zadań wynikających z funkcji nadzoru i kontroli.

4.4.4. Wreszcie, wymóg, aby właściwe organy monitorowały realizację zaleceń wiodącego organu nadzorczego ([97]) może okazać się nieskuteczny, gdyż właściwe organy mogą nie mieć pełnego oglądu ryzyk generowanych przez kluczowego zewnętrznego dostawcę usług ICT. Ponadto właściwe organy mogą być zobowiązane do podjęcia działań wobec nadzorowanych przez nie podmiotów finansowych, jeżeli ryzyko zidentyfikowane w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT nie zostało przez nie wyeliminowane. Zgodnie z projektem rozporządzenia ([98]) właściwe organy mogą zobowiązać nadzorowane przez siebie podmioty finansowe do tymczasowego zawieszenia korzystania z usługi świadczonej przez kluczowego zewnętrznego dostawcę usług ICT lub do wypowiedzenia pozostających w mocy umów zawartych z kluczowymi zewnętrznymi dostawcami usług ICT. Trudno jest przełożyć proces działań następczych na konkretne czynności. W szczególności nie jest jasne, czy nadzorowany podmiot finansowy będzie miał możliwość zawieszenia lub wypowiedzenia umów zawartych z zewnętrznym dostawcą usług ICT. Może tak być, jeżeli zewnętrzny dostawca usług ICT jest istotnym dostawcą dla tego podmiotu finansowego, czy też ze względu na koszty i odszkodowania, w postaci kar umownych lub inne, jakie podmiot finansowy musiałby ponieść w wyniku takiego zawieszenia lub wypowiedzenia. Ponadto podejście takie nie wspiera spójności w zakresie nadzoru, gdyż właściwe organy mogą interpretować te same zalecenia w różny sposób. Może to potencjalnie zagrozić planowanej harmonizacji i spójnemu podejściu w odniesieniu do monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT na poziomie Unii. W świetle powyższego organy prawodawcze Unii mogą rozważyć udzielenie organom nadzoru szczególnych uprawnień w zakresie egzekwowania przepisów wobec kluczowych zewnętrznych dostawców usług ICT, uwzględniając ograniczenia wynikające z zasady ustanowionej w wyroku w sprawie *Meroni*, złagodzonej częściowo przez Trybunał Sprawiedliwości w wyroku w sprawie ESMA ([99]).

([93]) Zob. art. 29 projektu rozporządzenia.
([94]) Zob. art. 29 ust. 3 projektu rozporządzenia.
([95]) Zob. art. 35 projektu rozporządzenia.
([96]) Zob. art. 39 ust. 1 projektu rozporządzenia.
([97]) Zob. art. 29 ust. 4 i art. 37 projektu rozporządzenia.
([98]) Zob. art. 37 ust. 3 projektu rozporządzenia.
([99]) Zob. wyrok Trybunału (wielka izba) z dnia 22 stycznia 2014 r. w sprawie C-270/12, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej – rozporządzenie (UE) nr 236/2012.

Szczegółowe propozycje zmiany brzmienia projektu rozporządzenia wraz z uzasadnieniem zostały zawarte w odrębnym roboczym dokumencie technicznym. Roboczy dokument techniczny jest dostępny w języku angielskim na stronie internetowej EUR-Lex.

Sporządzono we Frankfurcie nad Menem dnia 4 czerwca 2021 r.

Prezes EBC
Christine LAGARDE