Rada
Unii Europejskiej

Bruksela, 24 września 2020 r.
(OR. en)

11051/20

Międzyinstytucjonalny numer referencyjny:
2020/0266 (COD)

EF 228
ECOFIN 846
TELECOM 159
CYBER 168
IA 61
CODEC 871

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej, (podpisał dyrektor Jordi AYET PUIGARNAU)
Data otrzymania:	24 września 2020 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2020) 595 final
Dotyczy:	Wniosek dotyczący ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

Delegacje otrzymują w załączeniu dokument COM(2020) 595 final.

Zał.: COM(2020) 595 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 24.9.2020 r.
COM(2020) 595 final

2020/0266 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

(Tekst mający znaczenie dla EOG)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

- Przyczyny i cele wniosku

Niniejszy wniosek stanowi część pakietu dotyczącego finansów cyfrowych, czyli pakietu środków umożliwiających i wspierających wykorzystanie potencjału finansów cyfrowych w zakresie innowacyjności i konkurencji przy jednoczesnym ograniczeniu związanego z nimi ryzyka. Jest on zgodny z priorytetami Komisji dotyczącymi zbudowania Europy na miarę ery cyfrowej i utworzenia gospodarki gotowej na przyszłość, która będzie przynosić korzyści obywatelom. Pakiet dotyczący finansów cyfrowych obejmuje nową strategię w zakresie finansów cyfrowych dla unijnego sektora finansowego[1], której celem jest zapewnienie, aby UE była przygotowana na rewolucję cyfrową i przewodziła jej wraz z innowacyjnymi przedsiębiorstwami europejskimi, zapewniając konsumentom i przedsiębiorstwom dostęp do korzyści wynikających z finansów cyfrowych. Oprócz niniejszego wniosku pakiet zawiera także wniosek dotyczący rozporządzenia w sprawie rynków kryptoaktywów[2], wniosek dotyczący rozporządzenia w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru (DLT)[3] oraz wniosek dotyczący dyrektywy w sprawie wyjaśnienia lub zmiany niektórych powiązanych unijnych przepisów w zakresie usług finansowych[4]. Cyfryzacja i odporność operacyjna w sektorze finansowym stanowią dwie strony tego samego medalu. Z technologiami cyfrowymi, lub technologiami informacyjno-komunikacyjnymi (ICT), wiążą się zarówno szanse, jak i zagrożenia. Należy je dobrze zrozumieć i odpowiednio nim zarządzać, zwłaszcza w trudnych okresach.

W związku z tym decydenci i organy nadzoru zwracają coraz większą uwagę na zagrożenia wynikające z uzależnienia od ICT. Podejmują oni w szczególności próby zwiększenia odporności przedsiębiorstw dzięki ustanowieniu norm i koordynacji prac regulacyjnych lub nadzorczych. Prace te prowadzone są zarówno na szczeblu międzynarodowym, jak i europejskim, a także zarówno przekrojowo w odniesieniu do wszystkich gałęzi gospodarki, jak i w odniesieniu do szeregu konkretnych sektorów, w tym branży usług finansowych.

Ryzyko związane z ICT nadal stanowi jednak wyzwanie dla odporności operacyjnej, wydajności i stabilności unijnego systemu finansowego. Reforma, którą przeprowadzono po kryzysie finansowym z 2008 r., doprowadziła przede wszystkim do wzmocnienia odporności finansowej[5] unijnego sektora finansowego, zapobiegając jedynie pośrednio ryzyku związanemu z ICT w niektórych obszarach w ramach środków mających na celu łagodzenie ryzyka operacyjnego w szerszym ujęciu.

---

1 Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Banku Centralnego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 23 września 2020 r. w sprawie strategii dla UE w zakresie finansów cyfrowych, COM(2020) 591.

2 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów i zmieniającego dyrektywę (UE) 2019/1937, COM(2020) 593.

3 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie systemu pilotażowego na potrzeby infrastruktur rynkowych opartych na technologii rozproszonego rejestru, COM(2020) 594.

4 Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady 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, COM(2020) 596.

5 Podstawowym celem poszczególnych przyjętych środków było zwiększenie zasobów kapitałowych i płynności podmiotów finansowych, a także ograniczenie ryzyka rynkowego i kredytowego.

Chociaż w wyniku zmian unijnych przepisów dotyczących usług finansowych dokonanych po kryzysie przyjęto jednolity zbiór przepisów regulujących znaczne części ryzyka finansowego związanego z usługami finansowymi, nie zapewniono w pełni operacyjnej odporności cyfrowej. Środki wprowadzone w związku z tą odpornością posiadały szereg cech, które ograniczały ich skuteczność. Na przykład często były projektowane jako dyrektywy w sprawie minimalnej harmonizacji lub rozporządzenia oparte na zasadach, co zostawiało znaczne możliwości przyjmowania rozbieżnych podejść w ramach jednolitego rynku. Ponadto zwracano jedynie częściową lub niepełną uwagę na ryzyko związane z ICT w kontekście zakresu ochrony przed ryzykiem operacyjnym. Ponadto w przepisach sektorowych dotyczących usług finansowych przewidziano różne tego typu środki. W związku z tym interwencja na szczeblu Unii nie odpowiadała w pełni potrzebom europejskich podmiotów finansowych w zakresie zarządzania ryzykiem operacyjnym w sposób pozwalający przetrwać skutki incydentów związanych z ICT, zareagować na te skutki i je zwalczyć. Nie zapewniła ona również organom nadzoru finansowego najodpowiedniejszych narzędzi pozwalających wykonywać ich obowiązki polegające na zapobieganiu niestabilności finansowej spowodowanej wystąpieniem tego ryzyka związanego z ICT.

Brak szczegółowych i kompleksowych przepisów w zakresie operacyjnej odporności cyfrowej na poziomie UE doprowadził do powstania licznych krajowych inicjatyw regulacyjnych (np. w sprawie badania operacyjnej odporności cyfrowej) i podejść nadzorczych (np. dotyczących zależności od zewnętrznych dostawców usług ICT). Działania na poziomie państwa członkowskiego mają jednak jedynie ograniczony wpływ ze względu na transgraniczny charakter ryzyka związanego z ICT. Ponadto nieskoordynowane inicjatywy krajowe doprowadziły do pokrywania się działań, niespójności, powielających się wymogów, wysokich kosztów administracyjnych i kosztów przestrzegania przepisów – zwłaszcza dla transgranicznych podmiotów finansowych – lub utrzymującego się niewykrywania – a co za tym idzie nieuwzględniania – ryzyka związanego z ICT. Sytuacja ta prowadzi do fragmentacji jednolitego rynku, osłabia stabilność i integralność unijnego sektora finansowego oraz zagraża ochronie konsumentów i inwestorów.

W związku z tym konieczne jest wprowadzenie szczegółowych i kompleksowych ram operacyjnej odporności cyfrowej dla unijnych podmiotów finansowych. Ramy te wzmocnią wymiar jednolitego zbioru przepisów dotyczący zarządzania ryzykiem cyfrowym. W szczególności przyczynią się one do wzmocnienia i usprawnienia procesu zarządzania ryzykiem związanym z ICT, wprowadzenia dokładnych testów systemów ICT, zwiększenia świadomości organów nadzoru na temat ryzyka w cyberprzestrzeni oraz incydentów związanych z ICT, w obliczu których stają podmioty finansowe, a także wprowadzenia uprawnień dla organów nadzoru finansowego w zakresie nadzorowania ryzyka wynikającego z zależności podmiotów finansowych od zewnętrznych dostawców usług ICT. We wniosku przewiduje się stworzenie spójnego mechanizmu zgłaszania incydentów, który przyczyni się do zmniejszenia obciążeń administracyjnych ciążących na podmiotach finansowych oraz wzmocni skuteczność nadzoru.

- Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Niniejszy wniosek stanowi część szerszych prac prowadzonych na szczeblu europejskim i międzynarodowym, które mają na celu wzmocnienie cyberbezpieczeństwa usług finansowych oraz przeciwdziałanie bardziej ogólnie rozumianemu ryzyku operacyjnemu[6].

[6] Bazylejski Komitet Nadzoru Bankowego, *Cyber-resilience: Range of practices*, grudzień 2018 r. oraz *Principles for sound management of operational risk (PSMOR)*, październik 2014 r.

Stanowi on również odpowiedź na wspólną poradę techniczną z 2019 r.[7] Europejskich Urzędów Nadzoru, w której wezwano do przyjęcia spójniejszego podejścia do przeciwdziałania ryzyku związanemu z ICT w sektorze finansów oraz zalecono Komisji wzmocnienie, w sposób proporcjonalny, operacyjnej odporności cyfrowej sektora usług finansowych za pośrednictwem unijnej inicjatywy sektorowej. Porada Europejskich Urzędów Nadzoru stanowiła odpowiedź na Plan działania Komisji w zakresie technologii finansowej z 2018 r.[8]

- Spójność z innymi politykami Unii

Jak stwierdziła przewodnicząca Ursula von der Leyen w swoich wytycznych politycznych[9], a także jak określono w komunikacie zatytułowanym „Kształtowanie cyfrowej przyszłości Europy”[10], Europa musi wykorzystać wszystkie możliwości, jakie daje era cyfrowa, a także wzmocnić swoje zdolności przemysłowe i innowacyjne, w granicach bezpieczeństwa i norm etycznych. W europejskiej strategii w zakresie danych[11] wskazano cztery filary – ochronę danych, prawa podstawowe, bezpieczeństwo i cyberbezpieczeństwo – jako podstawowe warunki wstępne istnienia społeczeństwa posiadającego mocną pozycję dzięki korzystaniu z danych. W ostatnim czasie Parlament Europejski pracuje nad sprawozdaniem w sprawie finansów cyfrowych, w którym wzywa między innymi do przyjęcia wspólnego podejścia do cyberodporności sektora finansowego[12]. Ramy legislacyjne wzmacniające operacyjną odporność cyfrową unijnych podmiotów finansowych są spójne z tymi celami polityki. Wniosek zapewni również wsparcie strategii politycznych mających na celu zwalczenie skutków koronawirusa, ponieważ zapewni, by większa zależność od finansów cyfrowych szła w parze z odpornością operacyjną.

W ramach tej inicjatywy utrzymano by korzyści związane z horyzontalnymi ramami w zakresie cyberbezpieczeństwa (np. dyrektywą w sprawie bezpieczeństwa sieci i informacji – dyrektywą dotyczącą cyberbezpieczeństwa) dzięki utrzymaniu objęcia sektora finansowego jej zakresem. Sektor finansowy nadal byłby ściśle związany z organem ds. współpracy w zakresie bezpieczeństwa sieci i informacji, a organy nadzoru finansowego byłyby w stanie wymieniać istotne informacje w ramach istniejącego ekosystemu bezpieczeństwa sieci i informacji. Inicjatywa ta byłaby spójna z dyrektywą w sprawie europejskiej infrastruktury krytycznej, która jest obecnie poddawana przeglądowi w celu zwiększenia poziomu ochrony i odporności infrastruktur krytycznych na zagrożenia niezwiązane z cyberatakami. Ponadto niniejszy wniosek jest całkowicie zgodny ze strategią w zakresie unii bezpieczeństwa[13],

---

7 Wspólna porada Europejskich Urzędów Nadzoru skierowana do Komisji Europejskiej dotycząca konieczności wprowadzenia usprawnień legislacyjnych związanych z wymogami w zakresie zarządzania ryzykiem związanym z ICT w unijnym sektorze finansowym, JC 2019 26 (2019).

8 Komisja Europejska, *Plan działania w zakresie technologii finansowej*, COM(2018) 109 final.

9 Przewodnicząca Ursula von der Leyen, Wytyczne polityczne na następną kadencję Komisji Europejskiej, lata 2019–2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pl.pdf

10 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Kształtowanie cyfrowej przyszłości Europy*, COM(2020) 67 final.

11 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Europejska strategia w zakresie danych*, COM(2020) 66 final.

12 „Sprawozdanie zawierające zalecenia dla Komisji w sprawie finansów cyfrowych: pojawiające się ryzyko związane z kryptoaktywami – wyzwania w zakresie regulacji i nadzoru w obszarze usług, instytucji i rynków finansowych” (2020/2034(INL) https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en

13 Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie strategii UE w zakresie unii bezpieczeństwa, COM(2020) 605 final.

w której wezwano do podjęcia inicjatywy dotyczącej operacyjnej odporności cyfrowej w sektorze finansowym ze względu na jego dużą zależność od usług ICT i jego znaczną podatność na cyberataki.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- Podstawa prawna

Podstawą niniejszego wniosku dotyczącego rozporządzenia jest art. 114 TFUE.

Wniosek usuwa przeszkody dla ustanowienia i funkcjonowania rynku wewnętrznego usług finansowych oraz usprawnia ten proces dzięki harmonizacji przepisów obowiązujących w obszarze zarządzania ryzykiem związanym z ICT, udostępniania informacji, testowania i ryzyka ze strony zewnętrznych dostawców usług ICT. Obecne rozbieżności w tym obszarze, zarówno na szczeblu legislacyjnym, jak i nadzorczym, a także na szczeblu krajowym i unijnym, stanowią przeszkody dla jednolitego rynku usług finansowych, ponieważ podmioty finansowe, które prowadzą działalność transgraniczną, mierzą się z różnymi – jeżeli nie dochodzi do ich pokrywania się – wymogami regulacyjnymi lub oczekiwaniami w zakresie nadzoru, co może ograniczyć korzystanie z przysługującej im swobody przedsiębiorczości i swobody świadczenia usług. Różniące się przepisy zakłócają również konkurencję między tego samego rodzaju podmiotami finansowymi w różnych państwach członkowskich. Ponadto w obszarach, w których harmonizacja nie istnieje, jest częściowa lub ograniczona, rozwój rozbieżnych przepisów lub podejść krajowych, czy to już obowiązujących, czy to będących w trakcie przyjmowania i wdrażania na szczeblu krajowym, może stanowić przeszkodę dla korzystania ze swobód jednolitego rynku w przypadku usług finansowych. Ma to zwłaszcza miejsce w przypadku ram operacyjnego testowania cyfrowego oraz nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT.

Biorąc pod uwagę, że wniosek ma wpływ na kilka dyrektyw Parlamentu Europejskiego i Rady przyjętych na podstawie art. 53 ust. 1 TFUE, jednocześnie przyjmuje się również wniosek w sprawie dyrektywy, aby odzwierciedlić niezbędne zmiany w tych dyrektywach.

- Pomocniczość

Wysoki stopień wzajemnych powiązań między usługami finansowymi, znacząca działalność transgraniczna podmiotów finansowych oraz silne uzależnienie całego sektora finansowego od zewnętrznych dostawców usług ICT wymaga zapewnienia silnej operacyjnej odporności cyfrowej będącej przedmiotem wspólnego zainteresowania w celu zachowania solidności unijnych rynków finansowych. Rozbieżności wynikające z nierównych lub częściowych systemów regulacji, pokrywania się wymogów lub wielu wymogów mających zastosowanie do tych samych podmiotów finansowych prowadzących działalność transgraniczną lub posiadających kilka zezwoleń[14] na całym jednolitym rynku można zniwelować skutecznie tylko na szczeblu Unii.

Niniejszy wniosek harmonizuje cyfrowy element operacyjny silnie zintegrowanego i wzajemnie powiązanego sektora, który korzysta już z jednego zestawu przepisów i nadzoru w większości innych najważniejszych obszarów. W przypadku kwestii takich jak zgłaszanie incydentów związanych z ICT jedynie unijne zharmonizowane przepisy mogłyby ograniczyć

[14] Ten sam podmiot finansowy może posiadać zezwolenia na prowadzenie działalności bankowej, jako firma inwestycyjna i jako instytucja płatnicza, wydane przez różne organy nadzoru w jednym lub w kilku państwach członkowskich.

poziom obciążeń administracyjnych i kosztów finansowych związanych ze zgłaszaniem tego samego incydentu związanego z ICT różnym organom unijnym i krajowym. Działania unijne są również konieczne, aby ułatwić wzajemne uznawanie wyników zaawansowanych testów operacyjnej odporności cyfrowej dotyczących podmiotów prowadzących działalność transgraniczną, które w przypadku braku unijnych przepisów podlegają lub mogą podlegać różnym ramom w różnych państwach członkowskich. Jedynie działania na szczeblu unijnym mogą zlikwidować różnice w podejściach do testowania, które wprowadziły państwa członkowskie. Ogólnounijne działania są również konieczne, aby zwalczyć brak odpowiednich uprawnień nadzorczych umożliwiających monitorowanie ryzyka związanego z zewnętrznymi dostawcami usług ICT, w tym ryzyka koncentracji i wystąpienia efektu domina w odniesieniu do unijnego sektora finansowego.

- Proporcjonalność

Proponowane przepisy nie wykraczają poza to, co jest konieczne do osiągnięcia celów wniosku. Obejmują one jedynie te aspekty, których państwa członkowskie nie mogą osiągnąć samodzielnie i w których obciążenia i koszty administracyjne są współmierne do celów szczególnych i ogólnych, które mają zostać osiągnięte.

Pod względem zakresu i intensywności proporcjonalność opracowano za pomocą kryteriów oceny jakościowej i ilościowej. Mają one na celu zapewnienie, by nowe przepisy obejmujące wszystkie podmioty finansowe były jednocześnie dostosowane do ryzyka i potrzeb wynikających z ich szczególnych właściwości pod względem ich rozmiaru i profilu działalności. Proporcjonalność jest również zakorzeniona w przepisach dotyczących zarządzania ryzykiem związanym z ICT, testowania odporności cyfrowej, zgłaszania poważnych incydentów związanych z ICT oraz nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT.

- Wybór instrumentu

Środki niezbędne do uregulowania zarządzania ryzykiem związanym z ICT, zgłaszania incydentów związanych z ICT, testowania oraz nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT należy zawrzeć w rozporządzeniu, tak aby zapewnić, by szczegółowe wymogi były skutecznie i bezpośrednio stosowane w jednolity sposób, bez uszczerbku dla proporcjonalności i nie naruszając przepisów szczegółowych przewidzianych w tym rozporządzeniu. Spójność pod względem przeciwdziałania cyfrowemu ryzyku operacyjnemu przyczynia się do wzmocnienia zaufania do systemu finansowego i chroni jego stabilność. Biorąc pod uwagę, że zastosowanie formy rozporządzenia przyczynia się do ograniczenia złożoności przepisów regulacyjnych, wspiera spójność w zakresie nadzoru i zwiększa pewność prawa, niniejsze rozporządzenie przyczynia się również do zmniejszenia kosztów przestrzegania przepisów przez podmioty finansowe, zwłaszcza w przypadku podmiotów finansowych prowadzących działalność transgraniczną, co z kolei może pomóc usunąć zakłócenia konkurencji.

W ramach niniejszego rozporządzenia likwiduje się również rozbieżności legislacyjne i różne krajowe podejścia regulacyjne lub nadzorcze do ryzyka związanego z ICT, a zatem usuwa się przeszkody dla jednolitego rynku usług finansowych, w szczególności dla sprawnego korzystania ze swobody przedsiębiorczości i swobody świadczenia usług w przypadku podmiotów finansowych obecnych na rynku transgranicznym.

Ponadto jednolity zbiór przepisów opracowano głównie w formie rozporządzeń, więc aktualizację rozszerzającą go o element dotyczący operacyjnej odporności cyfrowej należy przeprowadzić za pośrednictwem tego samego instrumentu prawnego.

3. WYNIKI OCEN *EX POST*, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa

Jak dotąd żadne unijne przepisy w zakresie usług finansowych nie dotyczyły głównie odporności operacyjnej i nie uwzględniały kompleksowo zagrożeń wynikających z cyfryzacji – nawet przepisy odnoszące się w bardziej ogólnym ujęciu do wymiaru ryzyka operacyjnego, którego elementem jest ryzyko związane z ICT. Dotychczasowa interwencja Unii przyczyniła się do zajęcia się potrzebami i problemami, które stanowiły następstwo kryzysu finansowego z 2008 r.: instytucje kredytowe nie posiadały wystarczającego kapitału, rynki finansowe nie były wystarczająco zintegrowane, a do tego momentu harmonizacja miała minimalny wymiar. Ryzyka związanego z ICT nie uznawano wówczas za priorytet i w rezultacie ramy prawne dla poszczególnych podsektorów finansowych uległy zmianie w nieskoordynowany sposób. Osiągnięto jednak cele działań Unii dotyczące zapewnienia stabilności finansowej i ustanowienia jednego zestawu zharmonizowanych wymogów ostrożnościowych i zasad dotyczących zachowań na rynku mających zastosowanie do podmiotów finansowych w całej UE. Biorąc pod uwagę, że czynniki wywołujące w przeszłości unijną interwencję legislacyjną nie zapewniły szczegółowych lub kompleksowych przepisów uwzględniających powszechne stosowanie technologii cyfrowych i wynikających z tego zagrożeń w sektorze finansowym, przeprowadzenie bezpośredniej oceny wydaje się problematyczne. Dorozumianą ocenę i wynikające z niej zmiany legislacyjne odzwierciedlono w każdym z filarów niniejszego rozporządzenia.

- Konsultacje z zainteresowanymi stronami

W trakcie procesu przygotowywania niniejszego wniosku Komisja prowadziła konsultacje z zainteresowanymi stronami, w szczególności:

(i) Komisja przeprowadziła specjalne otwarte konsultacje publiczne (od 19 grudnia 2019 r. do 19 marca 2020 r.)[15];

(ii) Komisja przeprowadziła konsultacje publiczne za pośrednictwem wstępnej oceny skutków (od 19 grudnia 2019 r. do 16 stycznia 2020 r.)[16];

(iii) Służby Komisji przeprowadziły dwukrotnie konsultacje z ekspertami państw członkowskich w ramach Grupy Ekspertów ds. Bankowości, Płatności i Ubezpieczeń (w dniach 18 maja 2020 r. i 16 lipca 2020 r.)[17];

(iv) Służby Komisji zorganizowały specjalne webinarium na temat operacyjnej odporności cyfrowej podczas serii wydarzeń w ramach kampanii informacyjnej na temat finansów cyfrowych w 2020 r. (w dniu 19 maja 2020 r.).

---

15 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation

16 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

17 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en

Celem konsultacji publicznych było zebranie przez Komisję informacji na temat możliwości opracowania potencjalnych ram UE w zakresie międzysektorowej operacyjnej odporności cyfrowej w obszarze usług finansowych. W odpowiedziach wyrażono szerokie poparcie dla wprowadzenia specjalnych ram obejmujących działania skupiające się na czterech obszarach objętych konsultacjami oraz podkreślono konieczność zapewnienia proporcjonalności i starannego uwzględnienia i wyjaśnienia interakcji z horyzontalnymi przepisami dyrektywy dotyczącej cyberbezpieczeństwa. Komisja otrzymała dwie odpowiedzi dotyczące wstępnej oceny skutków, w których respondenci wypowiedzieli się na temat szczególnych aspektów związanych ze swoim obszarem działalności.

Podczas posiedzenia Grupy Ekspertów ds. Bankowości, Płatności i Ubezpieczeń zorganizowanego w dniu 18 maja 2020 r. państwa członkowskie wyraziły szerokie poparcie dla wzmocnienia operacyjnej odporności cyfrowej sektora finansowego za pośrednictwem działań przewidzianych w ramach czterech elementów nakreślonych przez Komisję. Państwa członkowskie podkreśliły również konieczność wyraźnego powiązania nowych przepisów z przepisami dotyczącymi ryzyka operacyjnego (zawartymi w unijnych przepisach w sprawie usług finansowych) oraz horyzontalnymi przepisami w sprawie cyberbezpieczeństwa (dyrektywa dotycząca cyberbezpieczeństwa). W trakcie drugiego posiedzenia niektóre państwa członkowskie podkreśliły konieczność zapewnienia proporcjonalności i uwzględnienia szczególnej sytuacji małych przedsiębiorstw lub spółek zależnych większych grup, a także konieczność wprowadzenia dużego zakresu uprawnień właściwych organów krajowych sprawujących nadzór.

We wniosku wykorzystano i uwzględniono również informacje zwrotne uzyskane podczas spotkań z zainteresowanymi stronami oraz organami i instytucjami unijnymi. Zainteresowane strony, w tym zewnętrzni dostawcy usług ICT, wyrażali na ogół wsparcie. Z analizy otrzymanych informacji zwrotnych wynika konieczność ochrony proporcjonalności oraz przestrzegania zasad i stosowania opartego na analizie ryzyka podejścia podczas tworzenia przepisów. Na płaszczyźnie instytucjonalnej główny wkład wniosły Europejska Rada ds. Ryzyka Systemowego (ERRS), Europejskie Urzędy Nadzoru, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz Europejski Bank Centralny (EBC), a także właściwe organy państw członkowskich.

- Gromadzenie i wykorzystanie wiedzy eksperckiej

Przygotowując niniejszy wniosek, Komisja opierała się na dowodach jakościowych i ilościowych zgromadzonych z uznanych źródeł, w tym na dwóch wspólnych poradach technicznych Europejskich Urzędów Nadzoru. Ich uzupełnieniem były dane poufne oraz publicznie dostępne sprawozdania organów nadzoru, międzynarodowych organów normalizacyjnych i czołowych instytutów badawczych, jak również wkład ilościowy i jakościowy określonych zainteresowanych stron z całego światowego sektora finansowego.

- Ocena skutków

Niniejszemu wnioskowi towarzyszy ocena skutków[18] przedstawiona Radzie ds. Kontroli Regulacyjnej w dniu 29 kwietnia 2020 r. i zatwierdzona w dniu 29 maja 2020 r. Rada ds. Kontroli Regulacyjnej zaleciła wprowadzenie usprawnień w niektórych obszarach w celu: (i)

[18] Dokument roboczy służb Komisji – Sprawozdanie z oceny skutków towarzyszące wnioskowi dotyczącemu 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, SWD(2020) 198 z 24 września 2020 r.

udzielenia większej ilości informacji na temat sposobu zapewnienia proporcjonalności; (ii) dokładniejszego określenia zakresu, w jakim preferowany wariant różni się od wspólnej porady technicznej Europejskich Urzędów Nadzoru oraz wyjaśnienia, dlaczego wariant ten jest rozwiązaniem optymalnym; oraz (iii) dalszego podkreślenia interakcji wniosku z istniejącymi przepisami UE, w tym z przepisami objętymi obecnie przeglądem. Ocenę skutków dostosowano tak, aby uwzględnić w niej te punkty, a także bardziej szczegółowe uwagi Rady ds. Kontroli Regulacyjnej.

Komisja rozważyła szereg wariantów strategicznych dotyczących opracowania ram operacyjnej odporności cyfrowej:

- „brak działań": przepisy dotyczące odporności operacyjnej będą nadal wynikać z obecnego, różniącego się zestawu unijnych przepisów dotyczących usług finansowych, częściowo z dyrektywy dotyczącej cyberbezpieczeństwa oraz z istniejących lub przyszłych systemów krajowych;
- Wariant 1: wzmocnienie buforów kapitałowych: wprowadzone zostaną dodatkowe bufory kapitałowe mające na celu zwiększenie zdolności podmiotów finansowych do pokrywania strat, które mogą pojawić się ze względu na brak operacyjnej odporności cyfrowej;
- Wariant 2: wprowadzenie aktu prawnego dotyczącego operacyjnej odporności cyfrowej usług finansowych: zapewnienie kompleksowych ram na szczeblu UE zawierających spójne przepisy zaspokajające potrzeby w zakresie operacyjnej odporności cyfrowej wszystkich podmiotów finansowych objętych regulacjami oraz ustanowienie ram nadzoru w odniesieniu do kluczowych zewnętrznych dostawców usług ICT;
- Wariant 3: akt prawny dotyczący operacyjnej odporności cyfrowej usług finansowych połączony ze scentralizowanym nadzorem nad kluczowymi zewnętrznymi dostawcami usług ICT: poza aktem prawnym dotyczącym operacyjnej odporności cyfrowej (wariant 2) ustanowiono by nowy organ mający nadzorować świadczenie usług przez zewnętrznych dostawców usług ICT.

Przyjęto wariant drugi, ponieważ pozwala osiągnąć największą liczbę z zakładanych celów w sposób skuteczny, efektywny i spójny z innymi unijnymi strategiami politycznymi. Większość zainteresowanych stron również opowiedziała się za tym wariantem.

Przyjęty wariant może wiązać się z powstaniem zarówno jednorazowych, jak i okresowych kosztów[19]. Koszty jednorazowe wynikają głównie z inwestycji w systemy IT i w związku z tym ich określenie ilościowe jest trudne, biorąc pod uwagę aktualny stan złożonych środowisk informatycznych poszczególnych przedsiębiorstw oraz w szczególności ich dotychczasowych systemów IT. Mimo to w przypadku dużych przedsiębiorstw koszty te będą prawdopodobnie ograniczone, ponieważ dokonały już one znacznych inwestycji związanych z ICT. Oczekuje się, że koszty te będą również ograniczone w przypadku mniejszych przedsiębiorstw, ponieważ ze względu na niższe ryzyko zastosowanie będą miały proporcjonalne środki.

Przyjęty wariant będzie miał pozytywne skutki dla MŚP działających w sektorze usług finansowych pod względem wpływu na gospodarkę, społeczeństwo i środowisko. Wniosek

[19] *Ibidem, s. 89–94.*

zapewni MŚP jasność co do przepisów, które obowiązują, co ograniczy koszty przestrzegania przepisów.

Główne skutki społeczne przyjętego wariantu strategicznego będą dotyczyć konsumentów i inwestorów. Wyższe poziomy operacyjnej odporności cyfrowej unijnego systemu finansowego doprowadzą do zmniejszenia liczby i średnich kosztów incydentów. Całe społeczeństwo skorzysta dzięki większemu zaufaniu do sektora usług finansowych.

Ponadto pod względem wpływu na środowisko wybrany wariant strategiczny zachęci do powszechniejszego stosowania najnowszej generacji infrastruktur i usług ICT, w przypadku których oczekuje się, że staną się bardziej zrównoważone pod względem wpływu na środowisko.

- Sprawność regulacyjna i uproszczenie

Usunięcie pokrywających się wymogów w zakresie zgłaszania incydentów związanych z ICT doprowadziłoby do ograniczenia obciążeń administracyjnych i zmniejszenia powiązanych z tym kosztów. Ponadto zharmonizowane testy operacyjnej odporności cyfrowej obejmujące wzajemne uznawanie na całym jednolitym rynku ograniczy koszty, zwłaszcza dla przedsiębiorstw transgranicznych, które w przeciwnym razie podlegają licznym testom w różnych państwach członkowskich[20].

- Prawa podstawowe

UE dąży do zapewnienia najwyższych standardów ochrony praw podstawowych. Wszystkie uzgodnienia dotyczące dobrowolnej wymiany informacji między podmiotami finansowymi, do których zachęca się w niniejszym rozporządzeniu, będą przeprowadzane w zaufanych otoczeniach, w pełnej zgodności z unijnymi przepisami o ochronie danych, zwłaszcza rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[21], w szczególności gdy przetwarzanie danych osobowych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.

4. WPŁYW NA BUDŻET

Jeśli chodzi o wpływ na budżet, biorąc pod uwagę, że w proponowanym rozporządzeniu przewidziano silniejszą rolę Europejskich Urzędów Nadzoru dzięki uprawnieniom przyznanym im w celu sprawowania odpowiedniego nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, wniosek może skutkować koniecznością zwiększenia zasobów, aby w szczególności wypełnić misje nadzorcze (takie jak kontrole na miejscu i kontrole internetowe oraz audyty), oraz korzystania z usług personelu posiadającego szczególną wiedzę specjalistyczną w zakresie bezpieczeństwa ICT.

Skala i podział tych kosztów będą zależeć od zakresu nowych uprawnień nadzorczych oraz (dokładnych) zadań, jakie będą miały wykonywać Europejskie Urzędy Nadzoru. Jeżeli chodzi o zapewnienie nowych zasobów ludzkich, konieczne będzie zatrudnienie w EUNB, ESMA i EIOPA łącznie 18 pracowników zatrudnionych w pełnym wymiarze czasu pracy (EPC) – 6 EPC w każdym organie – w momencie rozpoczęcia stosowania poszczególnych przepisów

[20] *Ibidem*.

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

wniosku (szacowane koszty: 15,71 mln EUR w okresie 2022–2027). Europejskie Urzędy Nadzoru będą również ponosić dodatkowe koszty związane z IT, koszty podróży służbowych w celu przeprowadzenia kontroli na miejscu i koszty tłumaczeń (szacowane na 12 mln EUR w okresie 2022–2027), a także inne wydatki administracyjne (szacowane na 2,48 mln EUR w okresie 2022–2027). W związku z tym szacowany łączny wpływ na koszty będzie wynosić około 30,19 mln EUR w okresie 2022–2027.

Należy również zauważyć, że chociaż liczba pracowników (np. nowi członkowskie personelu i inne wydatki związane z nowymi zadaniami) potrzebnych do sprawowania bezpośredniego nadzoru będzie z czasem zależeć od zmian pod względem liczby i wielkości kluczowych zewnętrznych dostawców usług ICT, którzy mają podlegać nadzorowi, stosowne wydatki będą w pełni finansowane z opłat pobieranych od tych uczestników rynku. W związku z tym nie przewiduje się żadnego wpływu na środki budżetowe UE (z wyjątkiem dodatkowego personelu), ponieważ koszty te będą w pełni finansowane z opłat.

Wpływ niniejszego wniosku na finanse i budżet wyjaśniono szczegółowo w ocenie skutków finansowych regulacji dołączonej do niniejszego wniosku.

5. ELEMENTY FAKULTATYWNE

- Plany wdrażania oraz uzgodnienia dotyczące monitorowania, oceny i udostępniania informacji

Wniosek obejmuje ogólny plan monitorowania i oceny wpływu na konkretne cele, co wymaga od Komisji przeprowadzenia przeglądu co najmniej trzy lata po wejściu w życie oraz przedłożenia sprawozdania dla Parlamentu Europejskiego i Rady w sprawie głównych ustaleń tego przeglądu.

Przegląd przeprowadza się zgodnie z wytycznymi Komisji dotyczącymi lepszego stanowienia prawa.

- Szczegółowe objaśnienia poszczególnych przepisów wniosku

Wniosek opracowano wokół kilku głównych obszarów polityki, które są najważniejszymi, wzajemnie powiązanymi filarami zgodnie uwzględnionymi w europejskich i międzynarodowych wytycznych oraz najlepszych praktykach mających na celu wzmocnienie cyberodporności i odporności operacyjnej sektora finansowego.

Zakres rozporządzenia i zgodne z proporcjonalnością zastosowanie wymaganych środków (art. 2)

Aby zapewnić spójność wymogów w zakresie zarządzania ryzykiem związanym z ICT mających zastosowanie do sektora finansowego, rozporządzenie obejmuje szereg podmiotów finansowych regulowanych na szczeblu unijnym, a mianowicie instytucje kredytowe, instytucje płatnicze, instytucje pieniądza elektronicznego, firmy inwestycyjne, dostawców usług w zakresie kryptoaktywów, centralne depozyty papierów wartościowych, kontrahentów centralnych, systemy obrotu, repozytoria transakcji, zarządzających alternatywnymi funduszami inwestycyjnymi i spółki zarządzające, dostawców usług w zakresie udostępniania informacji, zakłady ubezpieczeń i zakłady reasekuracji, pośredników ubezpieczeniowych, instytucje pracowniczych programów emerytalnych, agencje ratingowe, biegłych rewidentów i firmy audytorskie, administratorów kluczowych wskaźników referencyjnych i dostawców usług finansowania społecznościowego.

Taki zakres ułatwia jednolite i spójne stosowanie wszystkich elementów zarządzania ryzykiem w obszarach związanych z ICT przy jednoczesnym zabezpieczeniu równych warunków działania wśród podmiotów finansowych w odniesieniu do ich obowiązków regulacyjnych w zakresie ryzyka związanego z ICT. Jednocześnie w rozporządzeniu przyznano, że istnieją znaczące różnice między podmiotami finansowymi pod względem rozmiaru, profilu działalności lub związane z ich narażeniem na ryzyko cyfrowe. Biorąc pod uwagę, że większe podmioty finansowe mają więcej zasobów, jedynie podmioty finansowe niekwalifikujące się jako mikroprzedsiębiorstwa mają obowiązek na przykład ustanowić złożone zasady zarządzania, specjalne stanowiska kierownicze, przeprowadzać szczegółowe oceny w następstwie istotnych zmian w infrastrukturach sieci i systemów informatycznych, regularnie przeprowadzać analizy ryzyka w odniesieniu do starszych wersji systemów ICT, rozszerzyć zakres testowania ciągłości działania oraz planów reagowania i przywrócenia gotowości do pracy w celu uwzględnienia scenariuszy pracy awaryjnej w trakcie przełączania się z podstawowej infrastruktury ICT na urządzenia redundantne. Co więcej, jedynie podmioty finansowe, które uznano za znaczące do celów zaawansowanego testowania odporności cyfrowej, będą miały obowiązek przeprowadzenia testów penetracyjnych pod kątem wyszukiwania zagrożeń.

Chociaż zasięg ten jest szeroki, nie jest on wyczerpujący. W szczególności niniejsze rozporządzenie nie obejmuje operatorów systemów zdefiniowanych w art. 2 lit. p) dyrektywy 98/26/WE[22] w sprawie zamknięcia rozliczeń w systemach płatności i rozrachunku papierów wartościowych (dyrektywy o ostateczności rozrachunku) ani żadnych uczestników systemu, chyba że taki uczestnik sam jest podmiotem finansowym regulowanym na szczeblu unijnym i jako taki będzie objęty zakresem niniejszego rozporządzenia we własnym imieniu (tj. instytucja kredytowa, firma inwestycyjna, kontrahent centralny). Ponadto unijny rejestr uprawnień do emisji, który funkcjonuje – zgodnie z dyrektywą 2003/87/WE[23] – pod egidą Komisji Europejskiej, również nie wchodzi w jego zakres.

Takie wyłączenia z dyrektywy o ostateczności rozrachunku uwzględniają potrzebę dalszego przeglądu kwestii prawnych i politycznych związanych z operatorami i uczestnikami systemów, o których mowa w dyrektywie o ostateczności rozrachunku, przy należytym uwzględnieniu wpływu obecnie obowiązujących ram na systemy płatności[24] obsługiwane przez banki centralne. Biorąc pod uwagę, że kwestie te mogą obejmować aspekty, które pozostają odrębne od zagadnień objętych zakresem niniejszego rozporządzenia, Komisja będzie nadal oceniać konieczność i wpływ dalszego rozszerzenia zakresu niniejszego rozporządzenia na podmioty i infrastruktury ICT wykraczające obecnie poza jego zakres.

Wymogi związane z zarządzaniem (art. 4)

Niniejsze rozporządzenie opracowano, aby lepiej dostosować strategie biznesowe podmiotów finansowych i proces zarządzania ryzykiem związanym z ICT. W tym celu organ zarządzający będzie miał obowiązek utrzymać zasadniczą, aktywną rolę w ramach sterowania

---

22 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).

23 Dyrektywa 2003/87/WE Parlamentu Europejskiego i Rady z dnia 13 października 2003 r. ustanawiająca system handlu przydziałami emisji gazów cieplarnianych we Wspólnocie oraz zmieniająca dyrektywę Rady 96/61/WE (Dz.U. L 275 z 25.10.2003, s. 32).

24 W szczególności 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.

ramami zarządzania ryzykiem związanym z ICT i powinien dążyć do przestrzegania odpowiedniej higieny cyberbezpieczeństwa. Pełna odpowiedzialność organu zarządzającego za zarządzanie ryzykiem związanym z ICT podmiotu finansowego będzie stanowić nadrzędną zasadę, która przełoży się następnie na zestaw szczególnych wymogów, takich jak przypisanie wyraźnych ról i obowiązków w odniesieniu do wszystkich funkcji związanych z ICT, ciągłe zaangażowanie w kontrolę monitorowania zarządzania ryzykiem związanym z ICT, a także w cały proces zatwierdzania i kontroli oraz odpowiedni przydział inwestycji i szkoleń związanych z ICT.

Wymogi w zakresie zarządzania ryzykiem związanym z ICT (art. 5–14)

Operacyjna odporność cyfrowa opiera się na zestawie najważniejszych zasad i wymogów w zakresie ram zarządzania ryzykiem związanym z ICT zgodnie ze wspólną poradą techniczną Europejskich Urzędów Nadzoru. Wymogi te, oparte na właściwych międzynarodowych, krajowych i branżowych normach, wytycznych i zaleceniach, dotyczą szczególnych funkcji w ramach zarządzania ryzykiem związanym z ICT (identyfikacja, ochrona i zapobieganie, wykrywanie, reagowanie i przywrócenie gotowości do pracy, uczenie się i rozwój oraz komunikacja). Aby nadążyć za szybko zmieniającym się spektrum cyberzagrożeń, podmioty finansowe mają obowiązek utworzenia i utrzymywania odpornych systemów i narzędzi ICT w celu zminimalizowania skutków ryzyka związanego z ICT, ciągłego identyfikowania wszystkich źródeł ryzyka związanego z ICT, utworzenia środków ochrony i zapobiegania, szybkiego wykrywania nietypowych działań, wprowadzenia specjalnych i kompleksowych strategii dotyczących ciągłości działania oraz planów przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej będących integralną częścią polityki w zakresie operacyjnej ciągłości działania. Te ostatnie elementy są niezbędne do szybkiego przywrócenia gotowości do pracy po incydentach związanych z ICT, w szczególności po cyberatakach, dzięki ograniczeniu szkód i priorytetowemu traktowaniu bezpiecznego wznowienia działalności. W samym rozporządzeniu nie przewidziano konkretnej standaryzacji, ale raczej oparto się na europejskich i międzynarodowych uznanych standardach technicznych lub najlepszych praktykach branżowych, w zakresie w jakim są one w pełni zgodne z instrukcjami w zakresie nadzoru dotyczącymi stosowania i włączania takich norm międzynarodowych. Niniejsze rozporządzenie obejmuje również kwestie integralności, bezpieczeństwa i odporności infrastruktur fizycznych i urządzeń, które wspierają wykorzystywanie technologii oraz odpowiednich procesów i osób związanych z ICT w ramach śladu cyfrowego działań podmiotu finansowego.

Zgłaszanie incydentów związanych z ICT (art. 15–20)

Harmonizację i usprawnienie procesu zgłaszania incydentów związanych z ICT osiągnięto, po pierwsze, dzięki ogólnemu wymogowi dla podmiotów finansowych dotyczącemu ustanowienia i wdrożenia procesu zarządzania w celu monitorowania i rejestrowania incydentów związanych z ICT, a także obowiązkowi klasyfikowania ich na podstawie kryteriów określonych szczegółowo w rozporządzeniu i dalej rozwijanych przez Europejskie Urzędy Nadzoru w celu określenia progów istotności. Po drugie, właściwym organom należy zgłaszać wyłącznie incydenty związane z ICT, które uznano za poważne. Zgłoszenie należy przetwarzać, stosując wspólny szablon i zgodnie ze zharmonizowaną procedurą opracowaną przez Europejskie Urzędy Nadzoru. Podmioty finansowe powinny przedkładać sprawozdania wstępne, śródokresowe i końcowe oraz informować swoich użytkowników i klientów w przypadku, gdy incydent ma lub może mieć wpływ na ich interesy finansowe. Właściwe organy powinny przekazywać istotne informacje szczegółowe na temat incydentów innym instytucjom lub organom: Europejskim Urzędom Nadzoru, EBC oraz pojedynczym punktom kontaktowym wyznaczonym zgodnie z dyrektywą (UE) 2016/1148.

Aby rozpocząć dialog między podmiotami finansowymi a właściwymi organami, który przyczyniłby się do zminimalizowania wpływu i wskazania właściwych środków zaradczych, zgłaszanie poważnych incydentów związanych z ICT należy uzupełnić informacjami zwrotnymi z nadzoru oraz wytycznymi.

Ponadto należy dokonać dalszej analizy możliwości centralizacji na szczeblu unijnym zgłaszania incydentów związanych z ICT we wspólnym sprawozdaniu Europejskich Urzędów Nadzoru, EBC i ENISA, w którym oceniona zostanie wykonalność ustanowienia jednego unijnego węzła informacyjnego na potrzeby zgłaszania poważnych incydentów związanych z ICT przez podmioty finansowe.

Testowanie operacyjnej odporności cyfrowej (art. 21–24)

Zdolności i funkcje uwzględnione w ramach zarządzania ryzykiem związanym z ICT należy poddawać okresowym testom pod kątem gotowości i wykrywania słabych punktów, niedociągnięć lub braków, a także szybkiego wdrażania działań naprawczych. W niniejszym rozporządzeniu przewidziano proporcjonalne stosowanie wymogów w zakresie testowania operacyjnej odporności cyfrowej w zależności od rozmiaru, profilu działalności i profilu ryzyka podmiotów finansowych: chociaż wszystkie podmioty powinny przeprowadzać testy narzędzi i systemów ICT, jedynie podmioty, które właściwe organy (na podstawie kryteriów określonych w niniejszym rozporządzeniu i dalej rozwiniętych przez Europejskie Urzędy Nadzoru) wskazały jako istotne i dojrzałe pod względem cyfrowym, powinny mieć obowiązek przeprowadzania zaawansowanych testów na podstawie testów penetracyjnych wykorzystujących scenariusz zagrożenia. W niniejszym rozporządzeniu określono również wymogi dla testerów oraz dotyczące uznawania wyników testów penetracyjnych wykorzystujących scenariusz zagrożenia w całej Unii w przypadku podmiotów finansowych działających w większej liczbie państwach członkowskich.

Ryzyko ze strony zewnętrznych dostawców usług ICT (art. 25–39)

Rozporządzenie opracowano w celu zapewnienia należytego monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT. Cel ten zostanie osiągnięty, po pierwsze, dzięki przestrzeganiu opartych na zasadach przepisów mających zastosowanie do monitorowania przez podmioty finansowe ryzyka związanego z zewnętrznymi dostawcami usług ICT. Po drugie, w niniejszym rozporządzeniu zharmonizowano najważniejsze elementy usług i relacji z zewnętrznymi dostawcami usług ICT. Elementy te obejmują minimalne aspekty uznane za kluczowe, aby umożliwić pełne monitorowanie przez podmiot finansowy ryzyka ze strony zewnętrznych dostawców usług ICT na etapach zawierania, wykonywania i zakończenia relacji oraz w okresie po zakończeniu relacji.

Przede wszystkim umowy, które regulują tę relację, będą musiały zawierać pełny opis usług, wskazanie lokalizacji, w których mają być przetwarzane dane, pełne opisy poziomu usług wraz z ilościowymi i jakościowymi celami w zakresie wydajności, stosowne postanowienia w sprawie dostępu, dostępności, integralności, bezpieczeństwa i ochrony danych osobowych oraz gwarancje dostępu, odzyskiwania i zwrotu w przypadku awarii zewnętrznych dostawców usług ICT, okresy wypowiedzenia i obowiązki sprawozdawcze zewnętrznych dostawców usług ICT, prawa dostępu, kontroli i audytu podmiotu finansowego lub wyznaczonego podmiotu zewnętrznego, jasne prawa do odstąpienia od umowy i specjalne strategie wyjścia. Ponadto, biorąc pod uwagę, że w przypadku niektórych z tych elementów umownych można również dokonać standaryzacji, rozporządzenie promuje dobrowolne stosowanie standardowych klauzul umownych, które mają zostać opracowane na potrzeby stosowania usług w chmurze przez Komisję.

Ponadto rozporządzenie ma na celu promowanie konwergencji podejść nadzorczych do ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym poprzez objęcie kluczowych zewnętrznych dostawców usług ICT unijnymi ramami nadzoru. Za pośrednictwem nowych zharmonizowanych ram legislacyjnych Europejski Urząd Nadzoru wyznaczony jako wiodący organ nadzorczy dla każdego takiego kluczowego zewnętrznego dostawcy usług ICT otrzymuje uprawnienia pozwalające zapewnić, by dostawcy usług technologicznych odgrywający kluczową rolę w funkcjonowaniu sektora finansowego byli objęci odpowiednim monitorowaniem na skalę paneuropejską. Ramy nadzoru przewidziane w niniejszym rozporządzeniu opierają się na istniejącej strukturze instytucjonalnej w obszarze usług finansowych, w przypadku której Wspólny Komitet Europejskich Urzędów Nadzoru zapewnia międzysektorową koordynację w odniesieniu do wszystkich kwestii dotyczących ryzyka związanego z ICT, zgodnie z jego zadaniami w zakresie cyberbezpieczeństwa, przy wsparciu właściwego podkomitetu (forum nadzoru) przeprowadzającego prace przygotowawcze na potrzeby indywidualnych decyzji i wspólnych zaleceń skierowanych do kluczowych zewnętrznych dostawców usług ICT.

Wymiana informacji (art. 40)

Aby zwiększyć świadomość na temat ryzyka związanego z ICT, zminimalizować jego rozprzestrzenianie się, wspierać zdolności obronne podmiotów finansowych oraz techniki wykrywania zagrożeń, w rozporządzeniu zapewniono podmiotom finansowym możliwość tworzenia ustaleń w celu wymiany między sobą informacji i danych wywiadowczych na temat cyberzagrożeń.

2020/0266 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr 909/2014

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Banku Centralnego[25],

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[26],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W epoce cyfrowej technologie informacyjno-komunikacyjne (ICT) wspierają złożone systemy wykorzystywane w codziennych działaniach społecznych. Napędzają one naszą gospodarkę w najważniejszych sektorach, w tym w sektorze finansów, oraz wzmacniają funkcjonowanie jednolitego rynku. Większy zakres cyfryzacji i wzajemnych powiązań zwiększa również ryzyko związane z ICT, przez co całe społeczeństwo – i w szczególności system finansowy – staje się bardziej narażone na cyberzagrożenia lub zakłócenia w funkcjonowaniu ICT. Chociaż powszechne wykorzystanie systemów ICT i wysoki stopień cyfryzacji oraz łączności stanowią obecnie podstawowe cechy wszystkich działań podmiotów finansowych w Unii, stopień uwzględnienia odporności cyfrowej w ich ramach operacyjnych nie jest jeszcze wystarczający.

(2) W ostatnich dziesięcioleciach stosowanie ICT zaczęło odgrywać kluczową rolę w sektorze finansów i obecnie ICT mają zasadnicze znaczenie dla wykonywania typowych codziennych funkcji wszystkich podmiotów finansowych. Cyfryzacja obejmuje na przykład płatności, które w coraz większym stopniu przechodzą z metod gotówkowych i papierowych na rzecz stosowania rozwiązań cyfrowych, a także rozliczanie i rozrachunek papierów wartościowych, handel elektroniczny i algorytmiczny, operacje udzielania pożyczek i finansowania, finansowanie „peer to peer", rating kredytowy, ubezpieczenia, obsługę roszczeń i operacje działów zaplecza. Finanse nie tylko stały się w dużej mierze cyfrowe w całym sektorze, ale cyfryzacja

[25] [*dodać odniesienie*] Dz.U. C […] z […], s. […].
[26] [*dodać odniesienie*] Dz.U. C […] z […], s. […].

wzmocniła również wzajemne połączenia i zależności w ramach sektora finansowego oraz z infrastrukturą zewnętrzną i zewnętrznymi dostawcami usług.

(3) W sprawozdaniu z 2020 r. dotyczącym systemowego ryzyka w cyberprzestrzeni[27] Europejska Rada ds. Ryzyka Systemowego (ERRS) potwierdziła, że istniejący wysoki poziom wzajemnych powiązań między podmiotami finansowymi, rynkami finansowymi i infrastrukturami rynku finansowego, a w szczególności wzajemne zależności między ich systemami ICT mogą potencjalnie stanowić słabą stronę o charakterze systemowym, ponieważ lokalne cyberincydenty mogłyby szybko rozprzestrzenić się z każdego z około 22 000 unijnych podmiotów finansowych[28] na cały system finansowy nieograniczony granicami geograficznymi. Poważne naruszenia związane z ICT występujące w sektorze finansów nie dotyczą wyłącznie podmiotów finansowych postrzeganych osobno. Naruszenia te zwiększają również ryzyko rozpowszechnienia lokalnych słabych stron we wszystkich kanałach transmisji finansowej oraz potencjalnie wywołują niekorzystne konsekwencje dla stabilności unijnego systemu finansowego, powodując utratę płynności i ogólną utratę pewności i zaufania w odniesieniu do rynków finansowych.

(4) W ostatnich latach ryzyko związane z ICT przyciągnęło uwagę krajowych, europejskich i międzynarodowych decydentów, organów regulacyjnych i podmiotów normalizacyjnych, które starają się zwiększyć odporność, określić standardy i koordynować prace regulacyjne lub nadzorcze w tym zakresie. Na szczeblu międzynarodowym Bazylejski Komitet Nadzoru Bankowego, Komitet ds. Systemów Płatności i Rozrachunku, Rada Stabilności Finansowej, Instytut Stabilności Finansowej, a także grupy krajów G-7 i G-20 dążą do zapewnienia właściwym organom i podmiotom gospodarczym z różnych jurysdykcji narzędzi mających na celu wzmocnienie odporności ich systemów finansowych.

(5) Pomimo krajowych i europejskich ukierunkowanych polityk i inicjatyw ustawodawczych ryzyko związane z ICT nadal stanowi wyzwanie dla odporności operacyjnej, wydajności i stabilności unijnego systemu finansowego. Reforma, którą przeprowadzono po kryzysie finansowym z 2008 r., doprowadziła przede wszystkim do wzmocnienia odporności finansowej unijnego sektora finansowego, a także miała na celu zabezpieczenie konkurencyjności i stabilności Unii z punktu widzenia gospodarki, standardów ostrożnościowych i zachowań rynkowych. Chociaż bezpieczeństwo ICT i odporność cyfrowa są częścią ryzyka operacyjnego, elementy te zajmowały mniej centralne miejsce w agendzie regulacyjnej po kryzysie i zostały opracowane tylko w niektórych obszarach unijnej polityki dotyczącej usług finansowych oraz otoczenia regulacyjnego lub jedynie w niektórych państwach członkowskich.

---

27 Sprawozdanie ERRS pt. „Systemowe ryzyko w cyberprzestrzeni" z lutego 2020 r. https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

28 Zgodnie z oceną skutków towarzyszącą przeglądowi Europejskich Urzędów Nadzoru – SWD(2017) 308 – istnieje około 5 665 instytucji kredytowych, 5 934 firmy inwestycyjne, 2 666 zakładów ubezpieczeń, 1 573 instytucje pracowniczych programów emerytalnych, 2 500 przedsiębiorstw zarządzających inwestycjami, 350 infrastruktur rynkowych (takich jak kontrahenci centralni, giełdy, podmioty systematycznie internalizujące transakcje, repozytoria transakcji i wielostronne platformy obrotu (MTF)), 45 agencji ratingowych oraz 2 500 autoryzowanych instytucji płatniczych i instytucji pieniądza elektronicznego. Łącznie daje to około 21 233 podmioty, bez uwzględnienia podmiotów finansowania społecznościowego, biegłych rewidentów i firm audytorskich, dostawców usług w zakresie kryptoaktywów oraz administratorów wskaźników referencyjnych.

(6) W Planie działania Komisji w zakresie technologii finansowej z 2018 r.[29] podkreślono kluczowe znaczenie zwiększenia cyberodporności unijnego sektora finansowego również z operacyjnego punktu widzenia, dla zapewnienia jego bezpieczeństwa technologicznego oraz sprawnego funkcjonowania, szybkiego przywracania gotowości do pracy po naruszeniach i incydentach związanych z ICT, umożliwiając ostatecznie skuteczne i sprawne świadczenie usług finansowych w całej Unii, w tym w sytuacjach skrajnych, przy jednoczesnej ochronie konsumenta oraz zaufania i pewności w odniesieniu do rynku.

(7) W kwietniu 2019 r. Europejski Urząd Nadzoru Bankowego (EUNB), Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) oraz Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA) (nazywane wspólnie „Europejskimi Urzędami Nadzoru") opublikowały wspólnie dwa zalecenia techniczne, w których wezwały do przyjęcia spójnego podejścia do ryzyka związanego z ICT w sektorze finansów oraz zaleciły wzmocnienie, w sposób proporcjonalny, operacyjnej odporności cyfrowej sektora usług finansowych za pośrednictwem unijnej inicjatywy sektorowej.

(8) Unijny sektor finansowy jest regulowany za pomocą zharmonizowanego jednolitego zbioru przepisów i podlega Europejskiemu Systemowi Nadzoru Finansowego. Przepisy dotyczące operacyjnej odporności cyfrowej i bezpieczeństwa ICT nie zostały jednak jeszcze w pełni lub spójnie zharmonizowane, mimo że operacyjna odporność cyfrowa ma zasadnicze znaczenie dla zapewnienia stabilności finansowej i integralności rynku w epoce cyfrowej i nie jest mniej ważna niż na przykład wspólne standardy ostrożnościowe lub zachowań rynkowych. Należy zatem rozbudować jednolity zbiór przepisów i system nadzoru, tak aby uwzględniały również ten element, poprzez rozszerzenie kompetencji organów nadzoru finansowego, którym powierzono zadanie monitorowania i ochrony stabilności finansowej i integralności rynku.

(9) Rozbieżności legislacyjne i niejednolite krajowe podejścia regulacyjne lub nadzorcze do ryzyka związanego z ICT powodują powstanie przeszkód dla jednolitego rynku usług finansowych, utrudniając sprawne korzystanie ze swobody przedsiębiorczości i swobody świadczenia usług podmiotom finansowym działających w skali transgranicznej. Może zostać również zakłócona konkurencja między tego samego rodzaju podmiotami finansowymi działającymi w różnych państwach członkowskich. Zwłaszcza w przypadku obszarów, w których unijna harmonizacja jest bardzo ograniczona – takich jak testowanie operacyjnej odporności cyfrowej – lub nie istnieje – takich jak monitorowanie ryzyka ze strony zewnętrznych dostawców usług ICT – rozbieżności wynikające ze zmian planowanych na szczeblu krajowym mogłyby spowodować dalsze przeszkody dla funkcjonowania jednolitego rynku ze szkodą dla uczestników rynku i stabilności finansowej.

(10) Dotychczasowe częściowe tylko uwzględnienie przepisów dotyczących ryzyka związanego z ICT na szczeblu Unii świadczy o brakach lub pokrywaniu się działań w ważnych obszarach takich jak zgłaszanie incydentów związanych z ICT i testowanie operacyjnej odporności cyfrowej oraz prowadzi do niespójności wynikających

[29] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Banku Centralnego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Plan działania w zakresie technologii finansowej: w kierunku bardziej konkurencyjnego i innowacyjnego europejskiego sektora finansowego*, COM(2018) 109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en

z wprowadzanych rozbieżnych przepisów krajowych lub kosztownego stosowania nakładających się przepisów. Ma to szczególnie szkodliwy wpływ na użytkowników intensywnie wykorzystujących ICT, takich jak sektor finansów, ponieważ ryzyko związane z technologią nie zna granic państwowych, a sektor finansowy wprowadza swoje usługi na szeroką, transgraniczną skalę w Unii i poza nią.

Indywidualne podmioty finansowe prowadzące działalność transgraniczną lub posiadające kilka zezwoleń (np. jeden podmiot finansowy może posiadać zezwolenia na prowadzenie działalności bankowej, jako firma inwestycyjna i jako instytucja płatnicza, przy czym wszystkie z nich mogą być wydane przez różne właściwe organy w jednym lub w kliku państwach członkowskich) stają przed wyzwaniami operacyjnymi przy samodzielnym zwalczaniu ryzyka związanego z ICT oraz łagodzeniu szkodliwych skutków incydentów związanych z ICT w spójny, opłacalny sposób.

(11) Biorąc pod uwagę, że do jednolitego zbioru przepisów nie dołączono kompleksowych ram dotyczących ICT lub ryzyka operacyjnego, konieczna jest dalsza harmonizacja najważniejszych wymogów w zakresie operacyjnej odporności cyfrowej dla wszystkich podmiotów finansowych. Zdolności i ogólna odporność, jakie – na podstawie takich najważniejszych wymogów – rozwiną podmioty finansowe w celu przetrwania przestojów operacyjnych, przyczyniłyby się do ochrony stabilności i integralności unijnych rynków finansowych, a tym samym do zapewnienia wysokiego poziomu ochrony inwestorów i konsumentów w Unii. Biorąc pod uwagę, że niniejsze rozporządzenie ma na celu przyczynienie się do sprawnego funkcjonowania jednolitego rynku, powinno ono opierać się na przepisach art. 114 TFUE zgodnie z jego wykładnią przyjętą w świetle utrwalonego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej.

(12) Niniejsze rozporządzenie ma przede wszystkim na celu konsolidację i aktualizację wymogów dotyczących ryzyka związanego z ICT zawartych dotychczas osobno w poszczególnych rozporządzeniach i dyrektywach. Chociaż te unijne akty prawne obejmowały główne kategorie ryzyka finansowego (np. ryzyko kredytowe, ryzyko rynkowe, ryzyko kredytowe kontrahenta i ryzyko płynności, ryzyko związane z zachowaniem rynkowym), nie było możliwości kompleksowego uwzględnienia w nich, w momencie ich przyjęcia, wszystkich elementów odporności operacyjnej. Wymogi dotyczące ryzyka operacyjnego, jeżeli zostały szerzej opracowane w tych unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do uwzględniania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie określeniu ukierunkowanych wymogów jakościowych, aby zwiększyć zdolności za pośrednictwem wymogów mających na celu stworzenie zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania gotowości do pracy i odbudowy w odniesieniu do incydentów związanych z ICT lub za pośrednictwem określenia zdolności w zakresie udostępniania informacji i testowania cyfrowego. Wspomniane dyrektywy i rozporządzenia miały przede wszystkim obejmować podstawowe przepisy dotyczące nadzoru ostrożnościowego, integralności rynku lub zachowań rynkowych.

W ramach niniejszego działania, które ma na celu konsolidację i aktualizację przepisów w sprawie ryzyka związanego z ICT, wszystkie przepisy dotyczące ryzyka cyfrowego w sektorze finansów zostaną po raz pierwszy zebrane w spójny sposób w jednym akcie ustawodawczym. Niniejsza inicjatywa powinna zatem wypełnić braki lub usunąć niespójności w niektórych z tych aktów prawnych, w tym związane ze stosowaną w nich terminologią, oraz powinna wyraźnie odnosić się do ryzyka

związanego z ICT za pośrednictwem ukierunkowanych przepisów w sprawie zdolności w zakresie zarządzania ryzykiem związanym z ICT, udostępniania informacji i testowania oraz monitorowania ryzyka ze strony podmiotów zewnętrznych.

(13) Podmioty finansowe powinny przyjąć to samo podejście i stosować się do tych samych, opartych na zasadach przepisach podczas radzenia sobie z ryzykiem związanym z ICT. Spójność przyczynia się do wzmocnienia zaufania do systemu finansowego oraz ochrony jego stabilności, zwłaszcza w czasach nadużywania systemów, platform i infrastruktur ICT, co powoduje większe ryzyko cyfrowe.

Przestrzeganie zasad podstawowej higieny cyberbezpieczeństwa powinno również pozwolić uniknąć obciążania gospodarki znacznymi kosztami dzięki zminimalizowaniu wpływu i kosztów zakłóceń funkcjonowania ICT.

(14) Zastosowanie rozporządzenia sprzyja ograniczeniu złożoności regulacyjnej, wspiera spójność w zakresie nadzoru, zwiększa pewność prawa, przyczyniając się jednocześnie do ograniczenia kosztów przestrzegania przepisów, zwłaszcza dla podmiotów finansowych prowadzących działalność transgraniczną, i zmniejszenia zakłóceń konkurencji. Wybór rozporządzenia na potrzeby ustanowienia wspólnych ram operacyjnej odporności cyfrowej podmiotów finansowych wydaje się zatem najbardziej odpowiednim sposobem zagwarantowania jednolitego i spójnego stosowania wszystkich elementów zarządzania ryzykiem związanym z ICT przez unijny sektor finansowy.

(15) Obecnie poza przepisami w sprawie usług finansowych ogólne ramy cyberbezpieczeństwa na poziomie Unii określa dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148[30]. Siedem sektorów krytycznych, do których dyrektywa ta ma zastosowanie, obejmuje również trzy rodzaje podmiotów finansowych, a mianowicie instytucje kredytowe, systemy obrotu i kontrahentów centralnych. Jednak biorąc pod uwagę, że w dyrektywie (UE) 2016/1148 określono mechanizm identyfikacji na szczeblu krajowym operatorów usług kluczowych, jedynie niektóre instytucje kredytowe i systemy obrotu oraz niektórzy kontrahenci centralni (zidentyfikowane lub zidentyfikowani przez państwa członkowskie) są w praktyce objęci jej zakresem i w związku z tym mają obowiązek spełniać określone w niej wymogi w zakresie bezpieczeństwa ICT i zgłaszania incydentów.

(16) Biorąc pod uwagę, że niniejsze rozporządzenie zwiększa poziom harmonizacji w zakresie elementów odporności cyfrowej dzięki wprowadzeniu wymogów w zakresie zarządzania ryzykiem związanym z ICT i zgłaszania incydentów związanych z ICT, które są bardziej rygorystyczne w porównaniu z wymogami określonymi w obecnych unijnych przepisach w sprawie usług finansowych, zapewnia to zwiększoną harmonizację również w porównaniu z wymogami określonymi w dyrektywie (UE) 2016/1148. W związku z tym niniejsze rozporządzenie stanowi *lex specialis* wobec dyrektywy (UE) 2016/1148.

Utrzymanie silnego związku między sektorem finansowym a unijnymi horyzontalnymi ramami cyberbezpieczeństwa ma zasadnicze znaczenie, ponieważ pozwoliłoby zapewnić spójność z już przyjętymi przez państwa członkowskie

[30] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 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 z 19.7.2016, s. 1).

strategiami w zakresie cyberbezpieczeństwa oraz umożliwiłoby organom nadzoru finansowego uzyskanie informacji na temat cyberincydentów wpływających na inne sektory objęte dyrektywą (UE) 2016/1148.

(17) Aby umożliwić międzysektorowy proces uczenia się i skutecznie czerpać z doświadczeń innych sektorów podczas reagowania na cyberzagrożenia, podmioty finansowe, o których mowa w dyrektywie (UE) 2016/1148, powinny pozostać częścią „ekosystemu" tej dyrektywy (np. grupa współpracy NIS i CSIRT).

Europejskie Urzędy Nadzoru i właściwe organy krajowe powinny być w stanie uczestniczyć odpowiednio w dyskusjach na temat strategicznej polityki i technicznych pracach grupy współpracy NIS, wymianach informacji oraz w dalszym ciągu współpracować z pojedynczymi punktami kontaktowymi wyznaczonymi zgodnie z dyrektywą (UE) 2016/1148. Właściwe organy zgodnie z niniejszym rozporządzeniem powinny również prowadzić konsultacje i współpracować z krajowymi CSIRT wyznaczonymi zgodnie z art. 9 dyrektywy (UE) 2016/1148.

(18) Ważne jest również zapewnienie spójności z dyrektywą w sprawie europejskiej infrastruktury krytycznej, która jest obecnie poddawana przeglądowi w celu zwiększenia poziomu ochrony i odporności infrastruktur krytycznych na zagrożenia niezwiązane z cyberatakami, z uwzględnieniem możliwych skutków dla sektora finansowego[31].

(19) Dostawcy usług w chmurze stanowią jedną z kategorii dostawców usług cyfrowych objętych zakresem stosowania dyrektywy (UE) 2016/1148. W związku z tym podlegają oni nadzorowi *ex post* sprawowanemu przez organy krajowe wyznaczone zgodnie z tą dyrektywą, który jest ograniczony do wymogów w zakresie bezpieczeństwa ICT i zgłaszania incydentów określonych w tym akcie. Biorąc pod uwagę, że ramy nadzoru ustanowione niniejszym rozporządzeniem mają zastosowanie do wszystkich kluczowych zewnętrznych dostawców usług ICT, w tym dostawców usług w chmurze, jeżeli świadczą oni usługi ICT na rzecz podmiotów finansowych, należy uznać, że stanowią one uzupełnienie nadzoru sprawowanego zgodnie z dyrektywą (UE) 2016/1148. Ponadto, wobec braku unijnych horyzontalnych ogólnosektorowych ram ustanawiających organ nadzoru cyfrowego, ramy nadzoru ustanowione w niniejszym rozporządzeniu powinny obejmować dostawców usług w chmurze.

(20) Aby zachować pełną kontrolę nad ryzykiem związanym z ICT, podmioty finansowe muszą posiadać kompleksowe umiejętności umożliwiające solidne i skuteczne zarządzanie ryzykiem związanym z ICT, wraz z konkretnymi mechanizmami oraz strategiami dotyczącymi zgłaszania incydentów związanych z ICT, testowania systemów ICT, kontroli i procesów, a także zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT. Należy zaostrzyć wymogi dotyczące operacyjnej odporności cyfrowej systemu finansowego, umożliwiając jednocześnie proporcjonalne stosowanie wymogów w odniesieniu do podmiotów finansowych będących mikroprzedsiębiorstwami zgodnie z definicją zawartą w zaleceniu Komisji 2003/361/WE[32].

---

[31] Dyrektywa 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 (Dz.U. L 345 z 23.12.2008, s. 75).

[32] Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

(21) Progi i systematyki dotyczące zgłaszania incydentów związanych z ICT różnią się znacznie na szczeblu krajowym. Chociaż płaszczyznę porozumienia można osiągnąć dzięki właściwym pracom podejmowanym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[33] i grupę współpracy NIS na rzecz podmiotów finansowych zgodnie z dyrektywą (UE) 2016/1148, rozbieżne podejścia do progów i systematyki nadal istnieją lub mogą pojawić się w przypadku pozostałych podmiotów finansowych. Wiąże się to z licznymi wymogami, które muszą spełnić podmioty finansowe, zwłaszcza podczas prowadzenia działalności w kilku unijnych jurysdykcjach i w przypadku, gdy są częścią grupy finansowej. Ponadto rozbieżności te mogą utrudniać tworzenie dalszych unijnych jednolitych lub scentralizowanych mechanizmów przyspieszających proces zgłaszania oraz wspierających szybką i sprawną wymianę informacji między właściwymi organami, co ma zasadnicze znacznie dla zwalczenia ryzyka związanego z ICT w przypadku ataków na wielką skalę, które mogą mieć konsekwencje systemowe.

(22) Aby umożliwić właściwym organom wykonywanie ich zadań nadzorczych poprzez uzyskanie pełnego przeglądu charakteru, częstotliwości, znaczenia i skutków incydentów związanych z ICT oraz aby wzmocnić wymianę informacji między właściwymi organami publicznymi, w tym organami ścigania i organami ds. restrukturyzacji i uporządkowanej likwidacji, konieczne jest ustanowienie przepisów w celu uzupełnienia systemu zgłaszania incydentów związanych z ICT o wymogi, których nie ma obecnie w przepisach dotyczących podsektora finansowego oraz zniesienie wszelkich istniejących pokrywających się i dublujących się przepisów w celu obniżenia kosztów. W związku z tym harmonizacja systemu zgłaszania incydentów związanych z ICT poprzez zobowiązanie wszystkich podmiotów finansowych do zgłaszania ich wyłącznie właściwym dla nich właściwym organom ma zatem zasadnicze znaczenie. Ponadto należy przyznać Europejskim Urzędom Nadzoru uprawnienia do doprecyzowania elementów zgłaszania incydentów związanych z ICT takich jak systematyka, ramy czasowe, zbiory danych, wzory i obowiązujące progi.

(23) Wymogi w zakresie testowania operacyjnej odporności cyfrowej opracowano w niektórych podsektorach finansowych w ramach kilku nieskoordynowanych ram krajowych, w których poruszono te same kwestie w różny sposób. Prowadzi to do dublowania kosztów transgranicznych podmiotów finansowych i utrudnia wzajemne uznawanie wyników. Nieskoordynowane testowanie może zatem dzielić jednolity rynek.

(24) Ponadto w przypadku braku wymogu testowania luki pozostają niewykryte, co naraża podmiot finansowy, a w ostatecznym rozrachunku również stabilność i integralność całego sektora finansowego, na większe ryzyko. Bez interwencji Unii testowanie operacyjnej odporności cyfrowej pozostałoby niepełne i nie istniałoby wzajemne uznawanie wyników testowania między różnymi jurysdykcjami. Ponadto, biorąc pod uwagę, że prawdopodobieństwo, że inne podsektory finansowe przyjęłyby takie systemy na szeroką skalę, jest niewielkie, ominęłyby je potencjalne korzyści, takie jak ujawnianie luk i zagrożeń, testowanie zdolności obronnych i ciągłości działania oraz większe zaufanie konsumentów, dostawców i partnerów biznesowych. Aby

[33] ENISA Reference Incident Classification Taxonomy, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

zlikwidować takie pokrywające się przepisy oraz rozbieżności i luki w przepisach, należy wprowadzić przepisy mające na celu skoordynowane testowanie przez podmioty finansowe oraz właściwe organy, ułatwiając tym samym wzajemne uznawanie zaawansowanego testowania w odniesieniu do znaczących podmiotów finansowych.

(25) Zależność podmiotów finansowych od usług ICT wynika częściowo z ich potrzeby dostosowania się do powstającej konkurencyjnej globalnej gospodarki cyfrowej, zwiększenia skuteczności ich działalności oraz zaspokojenia potrzeb konsumentów. Charakter i zakres takiej zależności stale zmieniał się w ostatnich latach, co przyczyniło się do obniżenia kosztów pośrednictwa finansowego, umożliwienia rozszerzania działalności i skalowalności w ramach prowadzenia działalności finansowej, przy jednoczesnym zapewnieniu szerokiego zakresu narzędzi ICT służących zarządzaniu złożonymi procesami wewnętrznymi.

(26) O intensywnym korzystaniu z usług ICT świadczą złożone ustalenia umowne, przy czym podmioty finansowe często napotykają trudności podczas negocjacji warunków umownych, które byłyby dostosowane do standardów ostrożnościowych lub innych wymogów regulacyjnych, którym podlegają, lub podczas innego rodzaju egzekwowania konkretnych praw, takich jak prawa dostępu lub prawa do audytu, jeżeli prawa te są zapisane w umowach. Ponadto w wielu takich umowach nie przewidziano wystarczających gwarancji umożliwiających pełnoprawne monitorowanie procesów podwykonawstwa, pozbawiając tym samym podmiot finansowy możliwości oceny powiązanych zagrożeń. Ponadto biorąc pod uwagę, że zewnętrzni dostawcy usług ICT często świadczą znormalizowane usługi na rzecz różnego rodzaju klientów, takie umowy mogą nie zawsze odpowiednio uwzględniać indywidualne lub szczególne potrzeby podmiotów sektora finansowego.

(27) Pomimo kilku ogólnych przepisów dotyczących outsourcingu zawartych w niektórych unijnych aktach prawnych dotyczących usług finansowych monitorowanie wymiaru umownego nie jest w pełni zakorzenione w unijnym prawodawstwie. Z uwagi na brak wyraźnych i dostosowanych do potrzeb standardów unijnych, które miałyby zastosowanie do ustaleń umownych zawieranych z zewnętrznymi dostawcami usług ICT, nie można kompleksowo uwzględnić zewnętrznego źródła ryzyka związanego z ICT. W związku z tym konieczne jest określenie pewnych najważniejszych zasad mających wyznaczać kierunek zarządzania przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT, którym towarzyszyć będzie zestaw podstawowych praw umownych związanych z kilkoma elementami związanymi z wykonywaniem i rozwiązywaniem umów w celu zapisania pewnych minimalnych gwarancji stanowiących podstawę zdolności podmiotów finansowych do skutecznego monitorowania wszystkich zagrożeń powstających na poziomie zewnętrznego dostawcy usług ICT.

(28) Brakuje jednorodności i spójności w zakresie ryzyka związanego z zewnętrznymi dostawcami usług ICT oraz zależnością od zewnętrznych dostawców usług ICT. Pomimo pewnych starań na rzecz uwzględnienia obszaru outsourcingu, między innymi w postaci zaleceń z 2017 r. w sprawie outsourcingu zlecanego dostawcom usług w chmurze.[34], kwestii ryzyka systemowego, które może powstać w wyniku kontaktu sektora finansowego z ograniczoną liczbą kluczowych zewnętrznych

[34] „Zalecenia dotyczące zlecania zadań dostawcom usług w chmurze" (EBA/REC/2017/03), obecnie uchylone przez wytyczne EUNB w sprawie outsourcingu (EBA/GL/2019/02).

dostawców usług ICT, poświęcono w unijnych przepisach niewielką uwagę. Ten brak odniesienia do tej kwestii na szczeblu unijnym jest spotęgowany brakiem konkretnych kompetencji i narzędzi umożliwiających krajowym organom nadzoru osiągnięcie właściwego zrozumienia zależności od zewnętrznych dostawców usług ICT i odpowiednie monitorowanie zagrożeń wynikających z koncentracji takich zależności od zewnętrznych dostawców usług ICT.

(29) Biorąc pod uwagę potencjalne ryzyko systemowe spowodowane rozpowszechnieniem się praktyk dotyczących outsourcingu oraz koncentracją zewnętrznych dostawców usług ICT, a także mając na uwadze niewystarczający charakter krajowych mechanizmów umożliwiających organom nadzoru finansowego określanie ilościowo i jakościowo konsekwencji ryzyka związanego z ICT występującego u kluczowych zewnętrznych dostawców usług ICT, a także łagodzenie tych konsekwencji, konieczne jest ustanowienie odpowiednich unijnych ram nadzoru umożliwiających stałe monitorowanie działań zewnętrznych dostawców usług ICT będących kluczowymi dostawcami dla podmiotów finansowych.

(30) Biorąc pod uwagę, że zagrożenia związane z ICT stają się bardziej złożone i zaawansowane, odpowiednie środki wykrywania i zapobiegania zależą w dużej mierze od regularnej wymiany danych wywiadowczych na temat zagrożeń i luk między podmiotami finansowymi. Wymiana informacji przyczynia się do większej świadomości na temat cyberzagrożeń, co z kolei wzmacnia zdolność podmiotów finansowych do zapobiegania urzeczywistnieniu się zagrożeń oraz umożliwia podmiotom finansowym skuteczniejsze ograniczanie skutków incydentów związanych z ICT oraz sprawniejsze przywracanie gotowości. Wydaje się, że wobec braku wytycznych na szczeblu unijnym szereg czynników ogranicza taką wymianę danych wywiadowczych, zwłaszcza niepewność co do zgodności z ochroną danych osobowych, przepisami antymonopolowymi i zasadami dotyczącymi odpowiedzialności.

(31) Ponadto obawy dotyczące rodzaju informacji, które można udostępnić innym uczestnikom rynku lub organom innym niż organy nadzoru (takim jak ENISA – w przypadku wkładu analitycznego, lub Europol – w odniesieniu do celów egzekwowania prawa), skutkują wstrzymaniem przekazywania przydatnych informacji. Zakres i jakość wymiany informacji pozostają ograniczone i podzielone, a istotne wymiany przeprowadzane są w większości lokalnie (za pośrednictwem inicjatyw krajowych) oraz bez żadnych spójnych ogólnounijnych ustaleń w zakresie wymiany informacji dostosowanych do potrzeb zintegrowanego sektora finansowego.

(32) Należy zatem zachęcać podmioty finansowe do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed cyberzagrożeniami i reagowania na cyberzagrożenia. W związku z tym konieczne jest umożliwienie powstania na szczeblu Unii mechanizmów ustaleń dotyczących dobrowolnej wymiany informacji, które – pod warunkiem wdrożenia w zaufanych środowiskach – pomogłyby społeczności finansowej zapobiegać zagrożeniom i wspólnie na nie reagować dzięki szybkiemu ograniczeniu rozpowszechnienia ryzyka związanego z ICT i utrudnieniu wystąpienia potencjalnego efektu domina we wszystkich kanałach finansowych. Mechanizmy te powinno się stosować w pełnej

zgodności z mającymi zastosowanie unijnymi przepisami prawa konkurencji[35], a także w sposób gwarantujący pełną zgodność z unijnymi przepisami o ochronie danych, głównie rozporządzeniem (UE) 2016/679 Parlamentu Europejskiego i Rady[36], w szczególności w kontekście przetwarzania danych osobowych, które jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, o czym jest mowa w art. 6 ust. 1 lit. f) tego rozporządzenia.

(33) Niezależnie od szerokiego zakresu stosowania przewidzianego w niniejszym rozporządzeniu, stosując zasady dotyczące operacyjnej odporności cyfrowej, należy uwzględniać istotne różnice między podmiotami finansowymi pod względem wielkości, profilu działalności lub narażenia na ryzyko cyfrowe. Co do zasady, ukierunkowując zasoby i zdolności na wdrażanie ram zarządzania ryzykiem w zakresie ryzyka związanego z ICT, podmioty finansowe powinny odpowiednio dostosować swoje potrzeby w obszarze ICT do swojej wielkości i profilu działalności, natomiast właściwe organy powinny nadal oceniać i weryfikować podejście do takiego podziału.

(34) Ponieważ większe podmioty finansowe mogą korzystać z większych zasobów i są w stanie szybko przeznaczyć fundusze na opracowanie struktur zarządzania i stworzenie szeregu strategii korporacyjnych, wyłącznie od podmiotów finansowych, które nie są mikroprzedsiębiorstwami w rozumieniu niniejszego rozporządzenia, powinno wymagać się tworzenia bardziej złożonych rozwiązań w zakresie zarządzania. Podmioty takie są lepiej przygotowane w szczególności do ustanowienia specjalnych stanowisk w strukturach zarządzania w celu nadzorowania ustaleń umownych z zewnętrznymi dostawcami usług ICT lub w celu zarządzania kryzysowego, organizowania zarządzania w zakresie ryzyka związanego z ICT zgodnie z modelem trzech linii obrony lub do przyjęcia dokumentu dotyczącego zasobów ludzkich, który kompleksowo objaśniałby politykę w zakresie praw dostępu.

Z tego samego powodu tylko od takich podmiotów finansowych powinno wymagać się przeprowadzania dogłębnych ocen po istotnych zmianach w infrastrukturze sieci i systemów informatycznych oraz powiązanych procedurach, do regularnego przeprowadzania analiz ryzyka w odniesieniu do starszych wersji systemów ICT lub do rozszerzenia zakresu testowania ciągłości działania oraz planów reagowania i przywrócenia gotowości do pracy w celu uwzględnienia scenariuszy pracy awaryjnej obejmujących przełączanie się z podstawowej infrastruktury ICT na urządzenia redundantne.

(35) Co więcej, ponieważ jedynie od tych podmiotów finansowych, które uznano za znaczące do celów zaawansowanego testowania odporności cyfrowej, powinno wymagać się przeprowadzenia testów penetracyjnych pod kątem wyszukiwania zagrożeń, procesy administracyjne i koszty finansowe związane z przeprowadzeniem takich testów powinny zostać przeniesione na niewielki odsetek podmiotów finansowych. Ponadto w celu zmniejszenia obciążeń regulacyjnych tylko podmioty finansowe niebędące mikroprzedsiębiorstwami powinny być proszone o regularne

---

35 Komunikat Komisji – Wytyczne w sprawie stosowania art. 101 Traktatu o funkcjonowaniu Unii Europejskiej do horyzontalnych porozumień kooperacyjnych (Dz.U. 2011/C 11/01).

36 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

zgłaszanie właściwym organom wszystkich kosztów i strat spowodowanych zakłóceniami w funkcjonowaniu ICT oraz wyników przeglądów powypadkowych dokonanych w następstwie poważnych zakłóceń w funkcjonowaniu ICT.

(36) Aby zapewnić pełną zgodność i ogólną spójność między strategiami biznesowymi poszczególnych podmiotów finansowych a zarządzaniem ryzykiem związanym z ICT, należy zobowiązać organ zarządzający do utrzymania kluczowej i aktywnej roli w kierowaniu i dostosowywaniu ram zarządzania ryzykiem związanym z ICT oraz ogólnej strategii w zakresie odporności cyfrowej. W podejściu, które przyjmie organ zarządzający, należy nie tylko skoncentrować się na środkach zapewniających odporność systemów ICT, ale także uwzględnić ludzi i procesy poprzez zestaw polityk, w których na każdym szczeblu struktury korporacyjnej i w odniesieniu do wszystkich pracowników buduje się świadomość czynników ryzyka w cyberprzestrzeni i zaangażowanie na rzecz ścisłego przestrzegania zasad w zakresie higieny cyberbezpieczeństwa na wszystkich szczeblach.

Ostateczna odpowiedzialność organu zarządzającego za zarządzanie w zakresie ryzyka związanego z ICT podmiotu finansowego powinna stanowić nadrzędną zasadę w tym kompleksowym podejściu, przekładającą się dodatkowo na ciągłe zaangażowanie organu zarządzającego w kontrolę monitorowania zarządzania w zakresie ryzyka związanego z ICT.

(37) Ponadto pełna rozliczalność organu zarządzającego idzie w parze z zabezpieczeniem poziomu inwestycji w ICT oraz ogólnego budżetu ICT podmiotu finansowego, tak aby mógł on osiągnąć swój podstawowy poziom operacyjnej odporności cyfrowej.

(38) W niniejszym rozporządzeniu, inspirowanym odpowiednimi międzynarodowymi, krajowymi i branżowymi normami, wytycznymi, zaleceniami lub podejściami w zakresie zarządzania ryzykiem w cyberprzestrzeni[37], promuje się zestaw funkcji ułatwiających ustanowienie ogólnej struktury zarządzania ryzykiem związanym z ICT. Dopóki główne funkcjonalności, jakie wdrażają podmioty finansowe, spełniają potrzeby w zakresie celów przewidzianych w funkcjach (identyfikacja, ochrona i zapobieganie, wykrywanie, reagowanie i przywrócenie gotowości do pracy, uczenie się i rozwój oraz komunikacja) określonych w niniejszym rozporządzeniu, podmioty finansowe zachowują swobodę korzystania z modeli zarządzania ryzykiem związanym z ICT, dla których opracowano inne ramy lub kategorie.

(39) Aby nadążyć za zmieniającym się krajobrazem cyberzagrożeń, podmioty finansowe powinny na bieżąco aktualizować systemy ICT, które muszą być niezawodne i posiadać wystarczającą zdolność nie tylko do zagwarantowania przetwarzania danych, które jest niezbędne do świadczenia ich usług, ale również do zapewnienia odporności technologicznej pozwalającej podmiotom finansowym na odpowiednie zaspokajanie dodatkowych potrzeb w zakresie przetwarzania danych, jakie mogą wynikać z trudnych warunków rynkowych lub innych niekorzystnych sytuacji.

---

37 CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures (Wytyczne w sprawie cyberodporności infrastruktur rynku finansowego)*, https://www.bis.org/cpmi/publ/d146.pdf G7, *Fundamental Elements of Cybersecurity for the Financial Sector (Podstawowe elementy cyberbezpieczeństwa dla sektora finansowego)*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Ramy cyberbezpieczeństwa NIST, https://www.nist.gov/cyberframework; Rada Stabilności Finansowej, *CIRR toolkit (zestaw narzędzi w zakresie reagowania na cyberincydenty i odzyskiwania danych)*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document

Niniejsze rozporządzenie nie pociąga za sobą żadnej normalizacji określonych systemów, narzędzi lub technologii ICT, lecz opiera się na odpowiednim stosowaniu przez podmioty finansowe europejskich i uznanych na szczeblu międzynarodowym norm technicznych (np. ISO) lub najlepszych praktyk branżowych, o ile takie stosowanie jest w pełni zgodne ze szczególnymi instrukcjami w zakresie nadzoru dotyczącymi stosowania i włączania norm międzynarodowych.

(40) Aby umożliwić podmiotom finansowym szybkie i sprawne rozwiązywanie incydentów związanych z ICT, w szczególności cyberataków, poprzez ograniczenie szkód i priorytetowe traktowanie wznowienia działalności i działań naprawczych, konieczne jest opracowanie skutecznych planów ciągłości działania i planów przywrócenia gotowości do pracy. Chociaż systemy kopii zapasowych powinny rozpocząć przetwarzanie bez zbędnej zwłoki, ich uruchomienie nie powinno jednak w żaden sposób zagrażać integralności i bezpieczeństwu sieci i systemów informatycznych lub poufności danych.

(41) Podczas gdy niniejsze rozporządzenie pozwala podmiotom finansowym na określenie w sposób elastyczny zakładanego czasu wznowienia funkcji, a tym samym na wyznaczanie go poprzez pełne uwzględnienie charakteru i krytyczności danej funkcji oraz wszelkich szczególnych potrzeb biznesowych, przy określaniu zakładanego czasu wznowienia funkcji należy również wymagać oceny potencjalnego ogólnego wpływu na efektywność rynku.

(42) Poważne konsekwencje cyberataków nasilają się, gdy dochodzi do nich w sektorze finansowym, który jest obszarem o wiele bardziej narażonym na to, że stanie się celem złośliwych propagatorów dążących do osiągnięcia zysków finansowych bezpośrednio u źródła. Aby ograniczyć takie ryzyko i zapobiec niedostępności lub utracie integralności systemów ICT oraz naruszeniu poufnych danych lub uszkodzeniu fizycznej infrastruktury ICT, należy znacznie usprawnić procedurę zgłaszania przez podmioty finansowe poważnych incydentów związanych z ICT.

Udostępnianie informacji w zakresie incydentów związanych z ICT powinno być ujednolicone w odniesieniu do wszystkich podmiotów finansowych poprzez nałożenie na nie obowiązku zgłaszania ich wyłącznie właściwym dla nich właściwym organom. Chociaż takie udostępnianie informacji obejmowałoby wszystkie podmioty finansowe, nie powinno ono obejmować wszystkich w ten sam sposób, ponieważ odpowiednie progi w zakresie istotności i ramy czasowe powinny być skalibrowane w taki sposób, aby uwzględniać jedynie poważne incydenty związane z ICT. Bezpośrednie udostępnianie informacji umożliwiłoby organom sprawującym nadzór finansowy dostęp do informacji na temat incydentów związanych z ICT. Niemniej jednak organy sprawujące nadzór finansowy powinny przekazywać te informacje niefinansowym organom publicznym (właściwym organom ds. bezpieczeństwa sieci i informacji, krajowym organom ochrony danych i organom ścigania w przypadku zdarzeń o charakterze przestępczym). Informacje na temat incydentów związanych z ICT powinny być wzajemnie przekazywane: organy sprawujące nadzór finansowy powinny przekazywać podmiotowi finansowemu wszelkie niezbędne informacje zwrotne lub wytyczne, natomiast Europejskie Urzędy Nadzoru powinny udostępniać zanonimizowane dane na temat zagrożeń i luk związanych z danym zdarzeniem, aby wspomóc szerzej pojętą zbiorową obronę.

(43) Należy rozważyć ewentualną centralizację zgłoszeń dotyczących incydentów związanych z ICT za pomocą jednego centralnego unijnego węzła informacyjnego, który odpowiednie zgłoszenia otrzymywałby bezpośrednio i automatycznie

powiadamiał właściwe organy krajowe albo służyłby jedynie jako centralne miejsce do przekazywania zgłoszeń przez właściwe organy krajowe i pełniłby funkcję koordynującą. Europejskie Urzędy Nadzoru powinny być zobowiązane do przygotowania, w porozumieniu z EBC i ENISA, w określonym terminie, wspólnego sprawozdania badającego możliwość ustanowienia takiego centralnego unijnego węzła informacyjnego.

(44) W celu osiągnięcia solidnej operacyjnej odporności cyfrowej oraz zgodnie z normami międzynarodowymi (np. określonymi przez G-7 podstawowymi elementami dotyczącymi testów penetracyjnych pod kątem wyszukiwania zagrożeń) podmioty finansowe powinny regularnie testować swoje systemy ICT i personel pracujący z ICT pod kątem skuteczności ich zdolności w zakresie zapobiegania, wykrywania, reagowania i przywrócenia gotowości do pracy, aby wykrywać i eliminować potencjalne luki w obszarze ICT. Aby uwzględnić różnice między podsektorami finansowymi i w ramach tych podsektorów w zakresie gotowości podmiotów finansowych do reagowania w obszarze cyberbezpieczeństwa, testy powinny obejmować szeroki zakres narzędzi i działań, począwszy od oceny podstawowych wymogów (np. oceny narażenia i skanowanie pod tym kątem, analizy otwartego oprogramowania, oceny bezpieczeństwa sieci, analizy braków, fizyczne kontrole bezpieczeństwa, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, w miarę możliwości przeglądy kodu źródłowego, testy scenariuszowe, testy kompatybilności, testy wydajności lub testy typu „end-to-end”), aż po bardziej zaawansowane testy (np. testy penetracyjne pod kątem wyszukiwania zagrożeń w przypadku podmiotów finansowych wystarczająco zaawansowanych z punktu widzenia ICT, aby były w stanie przeprowadzić takie testy). Test operacyjnej odporności cyfrowej powinien być zatem bardziej wymagający dla znaczących podmiotów finansowych (takich jak duże instytucje kredytowe, giełdy papierów wartościowych, centralne depozyty papierów wartościowych, kontrahenci centralni itp.). Jednocześnie test operacyjnej odporności cyfrowej powinien także mieć większe znaczenie w przypadku niektórych podsektorów odgrywających kluczową rolę systemową (np. płatności, bankowość, systemy rozliczeń i rozrachunku), a mniejsze w przypadku innych (np. podmiotów zarządzających aktywami, agencji ratingowych itp.). Transgraniczne podmioty finansowe korzystające ze swobody przedsiębiorczości lub świadczenia usług w Unii powinny spełniać jeden zestaw wymogów w zakresie zaawansowanych testów (np. testów penetracyjnych pod kątem wyszukiwania zagrożeń) w swoim macierzystym państwie członkowskim, a test ten powinien obejmować infrastrukturę ICT we wszystkich jurysdykcjach, w których grupa transgraniczna prowadzi działalność w Unii, co pozwoli grupom transgranicznym ponosić koszty przeprowadzenia testów tylko w jednej jurysdykcji.

(45) Aby zapewnić należyte monitorowanie ryzyka ze strony zewnętrznych dostawców usług ICT, konieczne jest ustanowienie zbioru opartych na zasadach przepisów regulujących monitorowanie przez podmioty finansowe ryzyka występującego w kontekście funkcji zlecanych zewnętrznym dostawcom usług ICT oraz, w bardziej ogólnym zakresie, w kontekście zależności pod względem ICT od osób trzecich.

(46) Podmiot finansowy powinien przez cały czas ponosić pełną odpowiedzialność za wypełnianie obowiązków wynikających z niniejszego rozporządzenia. Proporcjonalne monitorowanie zagrożeń występujących na poziomie zewnętrznego dostawcy usług ICT należy zorganizować tak, aby odpowiednio uwzględnić skalę, złożoność i znaczenie zależności w zakresie ICT, krytyczność lub znaczenie usług, procesów lub funkcji objętych ustaleniami umownymi, a ostatecznie na podstawie starannej oceny

jakiegokolwiek potencjalnego wpływu na ciągłość i jakość usług finansowych na szczeblu indywidualnym i grupowym, w zależności od przypadku.

(47) Takie monitorowanie należy prowadzić zgodnie ze strategicznym podejściem do ryzyka ze strony zewnętrznych dostawców usług ICT sformalizowanym poprzez przyjęcie przez organ zarządzający podmiotu finansowego specjalnej strategii, opartej na ciągłym badaniu wszystkich takich zależności w zakresie ICT od osób trzecich. Aby zwiększyć świadomość organów sprawujących nadzór co do zależności w zakresie ICT od osób trzecich, a także w celu dalszego wspierania ram dotyczących nadzoru ustanowionych w niniejszym rozporządzeniu, organy sprawujące nadzór powinny regularnie otrzymywać istotne informacje z rejestrów i powinny mieć możliwość żądania wyciągów z tych rejestrów na zasadzie *ad hoc*.

(48) Gruntowna analiza poprzedzająca zawarcie umowy powinna mieć miejsce przed formalnym dokonaniem ustaleń umownych oraz stanowić ich podstawę, natomiast wypowiedzenie umowy powinno być spowodowane co najmniej szeregiem okoliczności wskazujących na braki po stronie zewnętrznego dostawcy usług ICT.

(49) Aby zaradzić skutkom systemowym koncentracji ryzyka ze strony osób trzecich w obszarze ICT, należy promować zrównoważone rozwiązania poprzez elastyczne i stopniowe podejście, ponieważ sztywne limity lub ścisłe ograniczenia mogą utrudniać prowadzenie działalności gospodarczej i swobodę zawierania umów. Podmioty finansowe powinny dokładnie oceniać ustalenia umowne w celu określenia prawdopodobieństwa wystąpienia takiego ryzyka, w tym poprzez dogłębną analizę ustaleń dotyczących podoutsourcingu, zwłaszcza w przypadku zawierania ich z zewnętrznymi dostawcami usług ICT mającymi siedzibę w państwie trzecim. Na tym etapie oraz w celu osiągnięcia odpowiedniej równowagi między koniecznością zachowania swobody zawierania umów a koniecznością zagwarantowania stabilności finansowej, nie uważa się za właściwe wprowadzenia sztywnych limitów i ograniczeń dotyczących ekspozycji wobec osób trzecich w obszarze ICT. Europejskie Urzędy Nadzoru wyznaczone do sprawowania nadzoru nad każdym z kluczowych zewnętrznych dostawców usług ICT („wiodący organ nadzorczy") podczas wykonywania zadań w zakresie nadzoru powinny zwrócić szczególną uwagę na pełne zrozumienie skali wzajemnych zależności i wykrycie konkretnych przypadków, w których wysoki poziom koncentracji kluczowych zewnętrznych dostawców usług ICT w Unii może stanowić zagrożenie dla stabilności i integralności systemu finansowego Unii, a także powinny zapewnić dialog z kluczowymi zewnętrznymi dostawcami usług ICT w przypadku stwierdzenia takiego zagrożenia[38].

(50) Aby móc regularnie oceniać i monitorować zdolność zewnętrznego dostawcy usług ICT do bezpiecznego świadczenia usług na rzecz podmiotu finansowego bez negatywnego wpływu na odporność tego podmiotu, należy ujednolicić kluczowe elementy umowne w trakcie realizacji umów z zewnętrznymi dostawcami usług ICT. Elementy te obejmują jedynie minimum aspektów umownych uznawanych za kluczowe dla umożliwienia pełnego monitorowania przez podmiot finansowy z punktu widzenia zapewnienia jego odporności cyfrowej uzależnionej od stabilności i bezpieczeństwa usług ICT.

---

[38] Ponadto w przypadku wystąpienia ryzyka nadużyć ze strony zewnętrznego dostawcy usług ICT, którego uznano za dominującego, podmioty finansowe powinny mieć również możliwość wniesienia formalnej lub nieformalnej skargi do Komisji Europejskiej lub do krajowych organów ds. prawa konkurencji.

(51) W ustaleniach umownych należy w szczególności zawrzeć specyfikację kompletnych opisów funkcji i usług, miejsc, w których takie funkcje i usługi są świadczone i w których przetwarzane są dane, jak również wskazanie pełnych opisów poziomu usług wraz z ilościowymi i jakościowymi celami w zakresie wydajności w ramach uzgodnionych poziomów usług, aby umożliwić podmiotowi finansowemu skuteczne monitorowanie. Podobnie przepisy dotyczące dostępu, dostępności, integralności, bezpieczeństwa i ochrony danych osobowych, jak również gwarancji dostępu, odzyskiwania i zwrotu w przypadku niewypłacalności, rozwiązania lub zaprzestania działalności gospodarczej przez zewnętrznego dostawcę usług ICT, powinno się również uznawać za istotne elementy zapewniające zdolność podmiotu finansowego do zapewnienia monitorowania ryzyka ze strony osób trzecich.

(52) W celu zapewnienia, aby podmioty finansowe zachowały pełną kontrolę nad wszelkimi wydarzeniami, które mogą mieć negatywny wpływ na ich bezpieczeństwo w obszarze ICT, należy określić okresy wypowiedzenia i obowiązki sprawozdawcze zewnętrznego dostawcy usług ICT w przypadku wydarzeń, które mogą mieć istotny wpływ na zdolność skutecznego wykonywania przez tego dostawcę kluczowych lub ważnych funkcji, w tym udzielania przez niego pomocy w przypadku wystąpienia incydentu związanego z ICT, bez dodatkowych kosztów lub po kosztach określonych *ex ante*.

(53) Prawa dostępu oraz prawo do kontroli i audytu przez podmiot finansowy lub wyznaczoną osobę trzecią stanowią kluczowe instrumenty bieżącego monitorowania przez podmioty finansowe wyników zewnętrznego dostawcy usług ICT w połączeniu z pełną współpracą tego ostatniego podczas kontroli. Analogicznie właściwemu organowi podmiotu finansowego powinny przysługiwać, na podstawie otrzymanych zawiadomień, podobne prawa do kontroli i audytu zewnętrznego dostawcy usług ICT, z zastrzeżeniem zachowania poufności.

(54) W ustaleniach umownych należy zawrzeć wyraźne prawo do rozwiązania umowy i związane z nim minimalne okresy wypowiedzenia, a także specjalne strategie wyjścia umożliwiające w szczególności obowiązkowe okresy przejściowe, w których zewnętrzni dostawcy usług ICT powinni nadal pełnić odpowiednie funkcje, aby zmniejszyć ryzyko zakłóceń na poziomie podmiotu finansowego lub umożliwić temu ostatniemu skuteczne przejście do innego zewnętrznego dostawcy usług ICT lub alternatywnie skorzystanie z rozwiązań dostępnych na miejscu, zgodnie ze złożonością świadczonej usługi.

(55) Ponadto dobrowolne stosowanie standardowych klauzul umownych opracowanych przez Komisję na potrzeby usług w chmurze może zapewnić dodatkowy komfort podmiotom finansowym i ich zewnętrznym dostawcom usług ICT poprzez zwiększenie poziomu pewności prawa w zakresie korzystania z usług w chmurze przez sektor finansowy, z zachowaniem pełnej zgodności z wymogami i oczekiwaniami określonymi w regulacjach dotyczących usług finansowych. Prace te opierają się na środkach przewidzianych już w Planie działania w zakresie technologii finansowej z 2018 r., w którym zapowiedziano, że Komisja zamierza wspierać i ułatwiać opracowywanie standardowych klauzul umownych dotyczących korzystania z usług w chmurze na zasadzie outsourcingu przez podmioty finansowe, czerpiąc z międzysektorowych wysiłków zainteresowanych stron świadczących usługi w chmurze, które Komisja ułatwiła dzięki zaangażowaniu sektora finansowego.

(56) Aby wesprzeć ujednolicenie i poprawę efektywności podejść w zakresie nadzoru nad ryzykiem ze strony zewnętrznych dostawców usług ICT w sektorze finansowym,

wzmocnić operacyjną odporność cyfrową podmiotów finansowych, które przy wykonywaniu funkcji operacyjnych polegają na kluczowych zewnętrznych dostawcach usług ICT, a tym samym przyczynić się do utrzymania stabilności systemu finansowego Unii oraz integralności jednolitego rynku usług finansowych, kluczowi zewnętrzni dostawcy usług ICT powinni podlegać unijnym ramom nadzoru.

(57) Ponieważ szczególne traktowanie jest uzasadnione wyłącznie w przypadku kluczowych zewnętrznych dostawców usług, należy wprowadzić mechanizm wyznaczania do celów stosowania unijnych ram nadzoru, aby uwzględnić wymiar i charakter zależności sektora finansowego od takich zewnętrznych dostawców usług ICT, co przekłada się na zestaw kryteriów ilościowych i jakościowych, które określałyby parametry w zakresie krytyczności jako podstawę do objęcia ramami nadzoru. Kluczowi zewnętrzni dostawcy usług ICT, którzy nie zostali automatycznie wyznaczeni na podstawie wspomnianych wyżej kryteriów, powinni mieć możliwość dobrowolnego przystąpienia do ram nadzoru, natomiast ci zewnętrzni dostawcy usług ICT, których objęto już mechanizmami ram nadzoru ustanowionymi na poziomie Eurosystemu w celu wspierania realizacji zadań, o których mowa w art. 127 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej, nie powinni w związku z tym podlegać tym kryteriom.

(58) Wymóg bycia zarejestrowanym w Unii odnoszący się do zewnętrznych dostawców usług ICT, których uznano za kluczowych, nie przekłada się na lokalizację danych, ponieważ niniejsze rozporządzenie nie pociąga za sobą żadnych dalszych wymogów w zakresie podejmowania w Unii działań związanych z przechowywaniem lub przetwarzaniem danych.

(59) Ramy te powinny pozostawać bez uszczerbku dla kompetencji państw członkowskich w zakresie prowadzenia własnych misji w zakresie sprawowania nadzoru w odniesieniu do zewnętrznych dostawców usług ICT, których nie uznano za kluczowych w świetle niniejszego rozporządzenia, ale którzy mogą być uznani za ważnych na szczeblu krajowym.

(60) Aby wykorzystać obecną wielowarstwową strukturę instytucjonalną w obszarze usług finansowych, Wspólny Komitet Europejskich Urzędów Nadzoru powinien nadal zapewniać ogólną międzysektorową koordynację w odniesieniu do wszystkich kwestii dotyczących ryzyka związanego z ICT, zgodnie ze swoimi zadaniami w zakresie cyberbezpieczeństwa, i powinien być przy tym wspierany przez nowy podkomitet (forum nadzoru), który będzie prowadził prace przygotowawcze zarówno w zakresie indywidualnych decyzji skierowanych do kluczowych zewnętrznych dostawców usług ICT, jak i zbiorowych zaleceń, w szczególności w zakresie analizy porównawczej programów dotyczących sprawowania nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, a także określania najlepszych praktyk w zakresie rozwiązywania problemów związanych z ryzykiem koncentracji w obszarze ICT.

(61) Aby zapewnić odpowiedni nadzór w całej Unii nad zewnętrznymi dostawcami usług ICT odgrywającymi kluczową rolę w funkcjonowaniu sektora finansowego, jeden z Europejskich Urzędów Nadzoru powinien zostać wyznaczony jako wiodący organ nadzorczy w odniesieniu do każdego kluczowego zewnętrznego dostawcy usług ICT.

(62) Wiodące organy nadzorcze powinny posiadać niezbędne uprawnienia do prowadzenia dochodzeń, kontroli na miejscu i kontroli zdalnych u kluczowych zewnętrznych dostawców usług ICT, dostępu do wszystkich istotnych lokali i lokalizacji oraz pełnych i aktualnych informacji, co umożliwi im uzyskanie rzeczywistego wglądu

w rodzaj, wymiar i wpływ ryzyka ze strony zewnętrznych dostawców usług ICT dla podmiotów finansowych i ostatecznie dla systemu finansowego Unii.

Powierzenie Europejskim Urzędom Nadzoru roli wiodących organów nadzorczych jest warunkiem wstępnym do zrozumienia i wyeliminowania systemowego wymiaru ryzyka związanego z ICT w sektorze finansowym. Wpływ wywierany w Unii przez kluczowych zewnętrznych dostawców usług ICT oraz związane z nim potencjalne problemy dotyczące ryzyka koncentracji w obszarze ICT wymagają przyjęcia wspólnego podejścia na poziomie Unii. Przeprowadzanie licznych audytów i korzystanie z praw dostępu przez szereg właściwych organów osobno przy niewielkiej lub braku jakiejkolwiek koordynacji nie zapewniłoby pełnego przeglądu ryzyka ze strony zewnętrznych dostawców usług ICT, powodując jednocześnie niepotrzebną redundancję, obciążenie i złożoność na poziomie kluczowych zewnętrznych dostawców usług ICT mierzących się z tak dużą liczbą wniosków.

(63) Ponadto wiodące organy nadzorcze powinny mieć możliwość przedstawiania zaleceń w zakresie ryzyka związanego z ICT oraz odpowiednich środków zaradczych, w tym sprzeciwiania się określonym ustaleniom umownym, które ostatecznie wpływają na stabilność podmiotu finansowego lub systemu finansowego. Właściwe organy krajowe powinny należycie uwzględniać przestrzeganie takich zaleceń merytorycznych wydanych przez wiodące organy nadzorcze w ramach swoich funkcji związanych z nadzorem ostrożnościowym nad podmiotami finansowymi.

(64) Ramy nadzoru w żaden sposób ani w żadnej części nie zastępują zarządzania przez podmioty finansowe ryzykiem wynikającym z korzystania z zewnętrznych dostawców usług ICT, w tym obowiązku bieżącego monitorowania ustaleń umownych uzgodnionych z kluczowymi zewnętrznymi dostawcami usług ICT, oraz nie wpływają na pełną odpowiedzialność podmiotów finansowych za przestrzeganie i wywiązywanie się ze wszystkich wymogów niniejszego rozporządzenia i odpowiednich przepisów dotyczących usług finansowych. Aby uniknąć powielania i nakładania się działań, właściwe organy powinny powstrzymać się od samodzielnego podejmowania jakichkolwiek działań mających na celu monitorowanie ryzyka ze strony kluczowych zewnętrznych dostawców usług ICT. Wszelkie takie działania należy uprzednio skoordynować i uzgodnić w kontekście ram nadzoru.

(65) Aby wspierać ujednolicenie na szczeblu międzynarodowym najlepszych praktyk, które mają być stosowane przy dokonywaniu przeglądu cyfrowego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT, należy zachęcać Europejskie Urzędy Nadzoru do zawierania porozumień o współpracy z odpowiednimi właściwymi organami nadzoru i organami regulacyjnymi państw trzecich w celu ułatwienia opracowania najlepszych praktyk w zakresie zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT.

(66) Aby wykorzystać wiedzę techniczną ekspertów właściwych organów w zakresie zarządzania operacyjnego i zarządzania ryzykiem związanym z ICT, wiodące organy nadzorcze powinny korzystać z doświadczeń poszczególnych krajów w zakresie nadzoru i ustanowić specjalne zespoły ds. kontroli dla każdego z poszczególnych kluczowych zewnętrznych dostawców usług ICT, łącząc multidyscyplinarne zespoły w celu wspierania zarówno przygotowania, jak i rzeczywistej realizacji działań nadzorczych, w tym kontroli na miejscu u kluczowych zewnętrznych dostawców usług ICT, a także niezbędnych działań następczych.

(67) Właściwe organy powinny posiadać wszelkie niezbędne uprawnienia w zakresie sprawowania nadzoru, prowadzenia dochodzeń i nakładania sankcji, aby zapewnić

stosowanie niniejszego rozporządzenia. Informacje o karach administracyjnych powinny być co do zasady publikowane. Ponieważ podmioty finansowe i zewnętrzni dostawcy usług ICT mogą mieć siedziby w różnych państwach członkowskich oraz podlegać nadzorowi różnych właściwych organów sektorowych, należy zapewnić ścisłą współpracę pomiędzy odpowiednimi właściwymi organami, w tym EBC w zakresie zadań szczególnych powierzonych mu na mocy rozporządzenia Rady (UE) nr 1024/2013[39], oraz konsultacje z Europejskimi Urzędami Nadzoru, a współpraca ta powinna opierać się na wzajemnej wymianie informacji i zapewnieniu pomocy w kontekście działalności nadzorczej.

(68) W celu dalszego ilościowego i jakościowego określenia kryteriów wyznaczania kluczowych zewnętrznych dostawców usług ICT oraz ujednolicenia opłat z tytułu nadzoru, należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do: bardziej szczegółowego określenia skutków systemowych, jakie niedopełnienie obowiązków przez zewnętrznego dostawcę usług ICT mogłoby mieć dla obsługiwanych przez niego podmiotów finansowych, liczby globalnych instytucji o znaczeniu systemowym lub innych instytucji o znaczeniu systemowym, które polegają na danym zewnętrznym dostawcy usług ICT, liczby zewnętrznych dostawców usług ICT działających na określonym rynku, kosztów przejścia na usługi innego zewnętrznego dostawcy usług ICT, liczby państw członkowskich, w których dany zewnętrzny dostawca usług ICT świadczy usługi i w których działają podmioty finansowe korzystające z usług takiego dostawcy, a także wysokości opłat z tytułu nadzoru oraz sposobu ich uiszczania.

Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[40]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup ekspertów Komisji zajmujących się przygotowaniem aktów delegowanych.

(69) Ponieważ niniejsze rozporządzenie, wraz z dyrektywą Parlamentu Europejskiego i Rady (UE) nr 20xx/xx[41], pociąga za sobą konsolidację przepisów dotyczących zarządzania ryzykiem związanym z ICT, obejmujących wiele rozporządzeń i dyrektyw z dorobku prawnego UE w zakresie usług finansowych, w tym rozporządzenia (WE) nr 1060/2009, rozporządzenia (UE) nr 648/2012, rozporządzenia (UE) nr 600/2014 oraz rozporządzenia (UE) nr 909/2014, w celu zapewnienia pełnej spójności należy zmienić te rozporządzenia, aby wyjaśnić, że odpowiednie przepisy dotyczące ryzyka związanego z ICT ustanowiono w niniejszym rozporządzeniu.

Standardy techniczne powinny zapewniać spójną harmonizację wymogów określonych w niniejszym rozporządzeniu. Opracowanie projektów regulacyjnych standardów technicznych, które nie wymagają podejmowania decyzji politycznych, w celu przedłożenia Komisji, należy powierzyć Europejskim Urzędom Nadzoru jako

---

39 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).

40 Dz.U. L 123 z 12.5.2016, s. 1.

41 [*Proszę wstawić pełne odniesienie*]

organom dysponującym wysokim poziomem wiedzy specjalistycznej. Należy opracować regulacyjne standardy techniczne w dziedzinie zarządzania ryzykiem związanym z ICT, udostępniania informacji, testowania i kluczowych wymogów dotyczących należytego monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT.

(70) Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym z udziałem ekspertów. Komisja i Europejskie Urzędy Nadzoru powinny zapewnić, aby wspomniane standardy i wymogi mogły być stosowane przez wszystkie podmioty finansowe w sposób proporcjonalny do charakteru, skali i stopnia złożoności tych podmiotów oraz ich działalności.

(71) W celu ułatwienia porównywalności sprawozdań dotyczących poważnych incydentów związanych z ICT oraz zapewnienia przejrzystości w zakresie ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT, Europejskie Urzędy Nadzoru należy upoważnić do opracowania projektów wykonawczych standardów technicznych ustanawiających standardowe szablony, formularze i procedury dla podmiotów finansowych na potrzeby zgłaszania poważnych incydentów związanych z ICT, jak również standardowych szablonów na potrzeby rejestrowania informacji. Przy opracowywaniu tych standardów Europejskie Urzędy Nadzoru powinny uwzględnić wielkość i złożoność podmiotów finansowych oraz charakter i poziom ryzyka prowadzonej przez nie działalności. Komisja powinna być uprawniona do przyjmowania tych wykonawczych standardów technicznych w drodze aktów wykonawczych zgodnie z art. 291 TFUE oraz zgodnie z art. 15, odpowiednio, rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 oraz rozporządzenia (UE) nr 1095/2010. Ponieważ dalsze wymogi określono już w aktach delegowanych i wykonawczych opartych na regulacyjnych i wykonawczych standardach technicznych odpowiednio w rozporządzeniach (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) nr 909/2014, należy upoważnić Europejskie Urzędy Nadzoru, indywidualnie albo wspólnie za pośrednictwem Wspólnego Komitetu, do przedłożenia Komisji regulacyjnych i wykonawczych standardów technicznych w celu przyjęcia aktów delegowanych i wykonawczych przenoszących i aktualizujących istniejące przepisy dotyczące zarządzania ryzykiem związanym z ICT.

(72) Działanie to będzie się wiązało z późniejszymi zmianami istniejących aktów delegowanych i wykonawczych przyjętych w poszczególnych obszarach prawodawstwa dotyczącego usług finansowych. Należy zmienić zakres artykułów dotyczących ryzyka operacyjnego, na podstawie których uprawnienia zawarte w tych aktach upoważniały do przyjmowania aktów delegowanych i wykonawczych, w celu przeniesienia do niniejszego rozporządzenia wszystkich przepisów dotyczących operacyjnej odporności cyfrowej, które stanowią obecnie część tych rozporządzeń.

(73) Ponieważ cele niniejszego rozporządzenia, a mianowicie osiągnięcie wysokiego poziomu operacyjnej odporności cyfrowej w odniesieniu do wszystkich podmiotów finansowych, nie mogą zostać w wystarczającym stopniu osiągnięte przez państwa członkowskie, gdyż wymaga to harmonizacji wielu różnych przepisów istniejących obecnie w niektórych aktach Unii albo w systemach prawnych poszczególnych państw członkowskich, natomiast ze względu na skalę i skutki tych celów osiągnięcie ich może być bardziej skuteczne na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsze rozporządzenie nie wykracza poza zakres niezbędny do osiągnięcia tego celu,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

1. Niniejszym rozporządzeniem ustanawia się następujące jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych wspierających procesy biznesowe podmiotów finansowych, niezbędne do osiągnięcia wysokiego wspólnego poziomu operacyjnej odporności cyfrowej:

   a) wymogi mające zastosowanie do podmiotów finansowych w odniesieniu do:

   – zarządzania ryzykiem związanym z wykorzystaniem technologii informacyjno-komunikacyjnych (ICT);

   – zgłaszania poważnych incydentów związanych z ICT właściwym organom;

   – testowania operacyjnej odporności cyfrowej;

   – wymiany informacji i danych wywiadowczych w związku z cyberzagrożeniami i lukami w tym obszarze;

   – środków na rzecz należytego zarządzania przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT;

   b) wymogi w odniesieniu do ustaleń umownych zawartych między zewnętrznymi dostawcami usług ICT a podmiotami finansowymi;

   c) ramy nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT świadczącymi usługi na rzecz podmiotów finansowych;

   d) zasady współpracy między właściwymi organami oraz zasady nadzoru i egzekwowania przepisów przez właściwe organy w odniesieniu do wszystkich kwestii objętych niniejszym rozporządzeniem.

2. W odniesieniu do podmiotów finansowych zidentyfikowanych jako operatorzy usług kluczowych na mocy przepisów krajowych transponujących art. 5 dyrektywy (UE) 2016/1148 niniejsze rozporządzenie uznaje się za sektorowy akt prawny Unii do celów art. 1 ust. 7 tej dyrektywy.

Artykuł 2

Zakres podmiotowy

1. Niniejsze rozporządzenie ma zastosowanie do następujących podmiotów:

   a) instytucji kredytowych;

   b) instytucji płatniczych;

   c) instytucji pieniądza elektronicznego;

   d) firm inwestycyjnych;

e) dostawców usług w zakresie kryptoaktywów, emitentów kryptoaktywów, emitentów tokenów powiązanych z aktywami oraz emitentów znaczących tokenów powiązanych z aktywami;

f) centralnych depozytów papierów wartościowych;

g) kontrahentów centralnych;

h) systemów obrotu;

i) repozytoriów transakcji;

j) zarządzających alternatywnymi funduszami inwestycyjnymi;

k) spółek zarządzających;

l) dostawców usług w zakresie udostępniania informacji;

m) zakładów ubezpieczeń i zakładów reasekuracji;

n) pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające;

o) instytucji pracowniczych programów emerytalnych;

p) agencji ratingowych;

q) biegłych rewidentów i firm audytorskich;

r) administratorów kluczowych wskaźników referencyjnych;

s) dostawców usług finansowania społecznościowego;

t) repozytoriów sekurytyzacji;

u) zewnętrznych dostawców usług ICT.

2. Do celów niniejszego rozporządzenia podmioty, o których mowa w lit. a)–t), są wspólnie określane jako „podmioty finansowe”.

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „operacyjna odporność cyfrowa” oznacza zdolność podmiotu finansowego do budowania, gwarantowania i weryfikowania swojej integralności operacyjnej z technologicznego punktu widzenia przez zapewnianie, bezpośrednio albo pośrednio (korzystając z usług zewnętrznych dostawców usług ICT), pełnego zakresu możliwości w obszarze ICT niezbędnych do zapewnienia bezpieczeństwa sieci i systemów informatycznych, z których korzysta podmiot finansowy i które wspierają ciągłe świadczenie usług finansowych oraz ich jakość;

2) „sieci i systemy informatyczne” oznaczają sieci i systemy informatyczne w rozumieniu art. 4 pkt 1 dyrektywy (UE) 2016/1148;

3) „bezpieczeństwo sieci i systemów informatycznych” oznacza bezpieczeństwo sieci i systemów informatycznych w rozumieniu art. 4 pkt 2 dyrektywy (UE) 2016/1148;

4) „ryzyko związane z ICT” oznacza każdą dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, w tym nieprawidłowe funkcjonowanie, przekroczenie przepustowości, awarię, zakłócenie, zaburzenie, niewłaściwe użytkowanie, utratę lub inny rodzaj złośliwego lub niezłośliwego

zdarzenia, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, działania i procesu lub świadczenia usług, tym samym naruszając integralność lub dostępność danych, oprogramowania lub jakiegokolwiek innego składnika usług i infrastruktury ICT lub powodując naruszenie poufności, uszkodzenie fizycznej infrastruktury ICT lub inne niekorzystne skutki;

5) „zasoby informacyjne” oznaczają zbiór informacji, w formie materialnej albo niematerialnej, który jest wart ochrony;

6) „incydent związany z ICT” oznacza nieprzewidziane, stwierdzone zdarzenie w sieciach i systemach informatycznych, wynikające z działalności złośliwej lub nie, które zagraża bezpieczeństwu sieci i systemów informatycznych, informacji przetwarzanych, przechowywanych lub przesyłanych przez te systemy lub ma negatywny wpływ na dostępność, poufność, ciągłość lub autentyczność usług finansowych świadczonych przez podmiot finansowy;

7) „poważny incydent związany z ICT” oznacza incydent związany z ICT o potencjalnie dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne funkcje podmiotu finansowego;

8) „cyberzagrożenie” oznacza cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881[42];

9) „cyberatak” oznacza złośliwy incydent związany z ICT polegający na próbie zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieuprawnionego dostępu do składnika aktywów lub jego nieuprawnionego wykorzystania przez jakiegokolwiek agresora;

10) „analiza zagrożeń” oznacza informacje, które zostały zagregowane, przekształcone, przeanalizowane, zinterpretowane lub wzbogacone w celu zapewnienia niezbędnego kontekstu na potrzeby podejmowania decyzji i które umożliwiają odpowiednie i wystarczające zrozumienie w celu złagodzenia skutków incydentu związanego z ICT lub cyberzagrożenia, w tym informacje dotyczące technicznych szczegółów cyberataku, osób odpowiedzialnych za atak oraz ich sposobu działania i motywacji;

11) „ochrona w głąb” oznacza strategię związaną z ICT, integrującą ludzi, procesy i technologie w celu ustanowienia szeregu barier na wielu poziomach i w zakresie wielu wymiarów podmiotu;

12) „luka” oznacza słabość, podatność lub wadę zasobu, systemu, procesu lub kontroli, które mogą być wykorzystane do stworzenia zagrożenia;

13) „testy penetracyjne pod kątem wyszukiwania zagrożeń” oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów stanowiących cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (zespół atakujący) testy działających na bieżąco krytycznych systemów produkcji podmiotu;

14) „ryzyko ze strony zewnętrznych dostawców usług ICT” oznacza ryzyko związane z ICT, które może wystąpić w przypadku podmiotu finansowego w związku

[42] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

z korzystaniem przez niego z usług ICT świadczonych przez zewnętrznych dostawców usług ICT lub przez ich podwykonawców;

15) „zewnętrzny dostawca usług ICT” oznacza przedsiębiorstwo świadczące usługi cyfrowe i usługi w zakresie danych, w tym dostawców usług w chmurze, oprogramowania, usług analizy danych, ośrodków przetwarzania danych, ale z wyłączeniem dostawców komponentów sprzętowych i przedsiębiorstw, które uzyskały zezwolenie na mocy prawa Unii i świadczą usługi łączności elektronicznej, o których mowa w art. 2 pkt 4 of dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972[43];

16) „usługi ICT” oznaczają usługi cyfrowe i usługi w zakresie danych świadczone za pośrednictwem systemów ICT na rzecz użytkownika wewnętrznego lub zewnętrznego lub większej liczby takich użytkowników, w tym dostarczanie danych, wprowadzanie danych, przechowywanie danych, przetwarzanie danych i usługi w zakresie udostępniania informacji, monitorowanie danych, a także oparte na danych usługi w zakresie wspierania działalności gospodarczej i podejmowania decyzji;

17) „kluczowa lub ważna funkcja” oznacza funkcję, której zaprzestanie lub wadliwe lub zakończone niepowodzeniem działanie mogłoby stanowić istotne zagrożenie dla dalszego wypełniania przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych, dla wyników finansowych podmiotu finansowego lub dla bezpieczeństwa lub ciągłości usług i działalności tego podmiotu;

18) „kluczowy zewnętrzny dostawca usług ICT” oznacza zewnętrznego dostawcę usług ICT wyznaczonego na mocy art. 29 i podlegającego ramom nadzoru, o których mowa w art. 30–37;

19) „zewnętrzny dostawca usług ICT z siedzibą w państwie trzecim” oznacza zewnętrznego dostawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim, nie założył działalności gospodarczej ani nie jest obecny w Unii i zawarł z podmiotem finansowym umowę o świadczenie usług ICT;

20) „podwykonawca usług ICT z siedzibą w państwie trzecim” oznacza podwykonawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim, nie założył działalności gospodarczej ani nie jest obecny w Unii i zawarł umowę z zewnętrznym dostawcą usług ICT lub z zewnętrznym dostawcą usług ICT mającym siedzibę w państwie trzecim;

21) „ryzyko koncentracji w obszarze ICT” oznacza ekspozycję na poszczególnych lub wielu powiązanych ze sobą kluczowych zewnętrznych dostawców usług ICT, która prowadzi do takiego stopnia uzależnienia od takich dostawców, że niedostępność, awaria lub innego rodzaju niedociągnięcie tych ostatnich może potencjalnie zagrozić zdolności podmiotu finansowego, a ostatecznie także całego systemu finansowego Unii, do wypełniania kluczowych funkcji lub przyczynić się do poniesienia innego rodzaju negatywnych skutków, w tym dużych strat;

[43] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (Dz.U. L 321 z 17.12.2018, s. 36).

22) „organ zarządzający” oznacza organ zarządzający w rozumieniu art. 4 ust. 1 pkt 36 dyrektywy 2014/65/UE, art. 3 ust. 1 pkt 7 dyrektywy 2013/36/UE, art. 2 ust. 1 lit. s) dyrektywy 2009/65/WE, art. 2 ust. 1 pkt 45 rozporządzenia (UE) nr 909/2014, art. 3 ust. 1 pkt 20 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1011[44], art. 3 ust. 1 lit. u) rozporządzenia Parlamentu Europejskiego i Rady (UE) 20xx/xx[45] [MiCA] lub równorzędne osoby, które faktycznie zarządzają podmiotem lub pełnią kluczowe funkcje zgodnie z odpowiednimi przepisami unijnymi lub krajowymi;

23) „instytucja kredytowa” oznacza instytucję kredytową w rozumieniu art. 4 ust. 1 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013[46];

24) „firma inwestycyjna” oznacza firmę inwestycyjną w rozumieniu art. 4 ust. 1 pkt 1 dyrektywy 2014/65/UE;

25) „instytucja płatnicza” oznacza instytucję płatniczą w rozumieniu art. 1 ust. 1 lit. d) dyrektywy (UE) 2015/2366;

26) „instytucja pieniądza elektronicznego” oznacza instytucję pieniądza elektronicznego w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE[47];

27) „kontrahent centralny” oznacza kontrahenta centralnego w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 648/2012;

28) „repozytorium transakcji” oznacza repozytorium transakcji w rozumieniu art. 2 pkt 2 rozporządzenia (UE) nr 648/2012;

29) „centralny depozyt papierów wartościowych” oznacza centralny depozyt papierów wartościowych w rozumieniu art. 2 ust. 1 pkt 1 rozporządzenia (UE) nr 909/2014;

30) „system obrotu” oznacza system obrotu w rozumieniu art. 4 ust. 1 pkt 24 dyrektywy 2014/65/UE;

31) „zarządzający alternatywnymi funduszami inwestycyjnymi” oznacza zarządzającego alternatywnymi funduszami inwestycyjnymi w rozumieniu art. 4 ust. 1 lit. b) dyrektywy 2011/61/UE;

32) „spółka zarządzająca” oznacza spółkę zarządzającą w rozumieniu art. 2 ust. 1 lit. b) dyrektywy 2009/65/WE;

33) „dostawca usług w zakresie udostępniania informacji” oznacza dostawcę usług w zakresie udostępniania informacji w rozumieniu art. 4 ust. 1 pkt 63 dyrektywy 2014/65/UE;

---

44 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1011 z dnia 8 czerwca 2016 r. w sprawie indeksów stosowanych jako wskaźniki referencyjne w instrumentach finansowych i umowach finansowych lub do pomiaru wyników funduszy inwestycyjnych i zmieniające dyrektywy 2008/48/WE i 2014/17/UE oraz rozporządzenie (UE) nr 596/2014 (Dz.U. L 171 z 29.6.2016, s. 1).

45 [*Proszę wstawić pełny tytuł i szczegółowe informacje dotyczące publikacji w Dz.U.*]

46 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).

47 Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz.U. L 267 z 10.10.2009, s. 7).

34) „zakład ubezpieczeń” oznacza zakład ubezpieczeń w rozumieniu art. 13 pkt 1 dyrektywy 2009/138/WE;

35) „zakład reasekuracji” oznacza zakład reasekuracji w rozumieniu art. 13 pkt 4 dyrektywy 2009/138/WE;

36) „pośrednik ubezpieczeniowy” oznacza pośrednika ubezpieczeniowego w rozumieniu art. 2 ust. 1 pkt 3 dyrektywy (UE) 2016/97;

37) „pośrednik oferujący ubezpieczenia uzupełniające” oznacza pośrednika oferującego ubezpieczenia uzupełniające w rozumieniu art. 2 ust. 1 pkt 4 dyrektywy (UE) 2016/97;

38) „pośrednik reasekuracyjny” oznacza pośrednika reasekuracyjnego w rozumieniu art. 2 ust. 1 pkt 5 dyrektywy (UE) 2016/97;

39) „instytucja pracowniczych programów emerytalnych” oznacza instytucję pracowniczych programów emerytalnych w rozumieniu art. 1 pkt 6 dyrektywy (UE) 2016/2341;

40) „agencja ratingowa” oznacza agencję ratingową w rozumieniu art. 3 pkt 1 lit. a) rozporządzenia (WE) nr 1060/2009;

41) „biegły rewident” oznacza biegłego rewidenta w rozumieniu art. 2 pkt 2 dyrektywy 2006/43/WE;

42) „firma audytorska” oznacza firmę audytorską w rozumieniu art. 2 pkt 3 dyrektywy 2006/43/WE;

43) „dostawca usług w zakresie kryptoaktywów” oznacza dostawcę usług w zakresie kryptoaktywów w rozumieniu art. 3 ust. 1 lit. n) rozporządzenia (UE) 202x/xx r. [*do Urzędu Publikacji: wstawić odniesienie do MiCA*];

44) „emitent kryptoaktywów” oznacza emitenta kryptoaktywów w rozumieniu art. 3 ust. 1 lit. h) [*do Urzędu Publikacji: wstawić odniesienie do MiCA*];

45) „emitent tokenów powiązanych z aktywami” oznacza emitenta tokenów powiązanych z aktywami w rozumieniu art. 3 ust. 1 lit. i) [*do Urzędu Publikacji: wstawić odniesienie do MiCA*];

46) „emitent znaczących tokenów powiązanych z aktywami” oznacza emitenta znaczących tokenów powiązanych z aktywami w rozumieniu art. 3 ust. 1 lit. j) [*do Urzędu Publikacji: wstawić odniesienie do MiCA*];

47) „administrator kluczowych wskaźników referencyjnych” oznacza administratora kluczowych wskaźników referencyjnych w rozumieniu art. x pkt x rozporządzenia xx/202x r. [*do Urzędu Publikacji: wstawić odniesienie do rozporządzenia o wskaźnikach referencyjnych*];

48) „dostawca usług finansowania społecznościowego” oznacza dostawcę usług finansowania społecznościowego w rozumieniu art. x pkt x rozporządzenia (UE) 202x/xx r. [*do Urzędu Publikacji: wstawić odniesienie do rozporządzenia w sprawie finansowania społecznościowego*];

49) „repozytorium sekurytyzacji” oznacza repozytorium sekurytyzacji w rozumieniu art. 2 pkt 23 rozporządzenia (UE) 2017/2402;

50) „mikroprzedsiębiorstwo” oznacza mikroprzedsiębiorstwo w rozumieniu art. 2 ust. 3 załącznika do zalecenia 2003/361/WE.

ROZDZIAŁ II

ZARZĄDZANIE RYZYKIEM ZWIĄZANYM Z ICT

SEKCJA I

Artykuł 4

Zarządzanie i organizacja

1. Podmioty finansowe posiadają wewnętrzne ramy zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z ICT.

2. Organ zarządzający podmiotu finansowego określa, zatwierdza i nadzoruje wdrażanie wszystkich ustaleń dotyczących ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, oraz ponosi odpowiedzialność za ich wdrażanie.

   Do celów akapitu pierwszego organ zarządzający:

   a) ponosi ostateczną odpowiedzialność za zarządzanie ryzykiem związanym z ICT podmiotu finansowego;

   b) ustala wyraźne role i obowiązki w odniesieniu do wszystkich funkcji związanych z ICT;

   c) określa odpowiedni poziom tolerancji ryzyka związanego z ICT podmiotu finansowego, o którym mowa w art. 5 ust. 9 lit. b);

   d) zatwierdza i nadzoruje wdrażanie polityki ciągłości działania podmiotu finansowego w zakresie ICT oraz planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT, o których mowa odpowiednio w art. 10 ust. 1 i 3, i okresowo dokonuje przeglądu ich wdrażania;

   e) zatwierdza plany audytów ICT, audyty ICT i ich istotne zmiany i okresowo dokonuje ich przeglądu;

   f) przydziela odpowiedni budżet w celu zaspokojenia potrzeb podmiotu finansowego w zakresie operacyjnej odporności cyfrowej w odniesieniu do wszystkich rodzajów zasobów, w tym szkoleń poświęconych ryzyku związanemu z ICT i umiejętności wszystkich odpowiednich pracowników, i okresowo dokonuje jego przeglądu;

   g) zatwierdza politykę podmiotu finansowego w zakresie ustaleń dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT i okresowo dokonuje jej przeglądu;

   h) jest należycie informowany o ustaleniach zawartych z zewnętrznymi dostawcami usług ICT w sprawie korzystania z usług ICT, o wszelkich odnośnych planowanych istotnych zmianach dotyczących zewnętrznych dostawców usług ICT oraz o potencjalnym wpływie takich zmian na kluczowe lub ważne funkcje objęte tymi ustaleniami, w tym otrzymuje streszczenie analizy ryzyka w celu oceny wpływu tych zmian;

i) jest należycie informowany o incydentach związanych z ICT i ich skutkach oraz o środkach reagowania, środkach przywrócenia gotowości do pracy i środkach naprawczych.

3. Podmioty finansowe inne niż mikroprzedsiębiorstwa ustanawiają funkcję polegającą na monitorowaniu ustaleń zawartych z zewnętrznymi dostawcami usług ICT w sprawie korzystania z usług ICT lub wyznaczają członka kadry kierowniczej wyższego szczebla jako odpowiedzialnego za nadzorowanie związanej z tym ekspozycji na ryzyko i odpowiedniej dokumentacji.

4. Członkowie organu zarządzającego regularnie odbywają specjalne szkolenia w celu zdobycia i aktualizacji wiedzy i umiejętności wystarczających do zrozumienia i oceny ryzyka związanego z ICT i jego wpływu na działalność podmiotu finansowego.

SEKCJA II

Artykuł 5

Ramy zarządzania ryzykiem związanym z ICT

1. Podmioty finansowe dysponują solidnymi, kompleksowymi i dobrze udokumentowanymi ramami zarządzania ryzykiem związanym z ICT, które umożliwiają im szybkie, skuteczne i kompleksowe reagowanie na ryzyko związane z ICT oraz zapewnienie wysokiego poziomu operacyjnej odporności cyfrowej odpowiadającego ich potrzebom biznesowym oraz wielkości i złożoności tych podmiotów.

2. Ramy zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1, obejmują strategie, polityki, procedury, protokoły i narzędzia ICT niezbędne do właściwej i skutecznej ochrony wszystkich odpowiednich elementów fizycznych i infrastruktury, w tym sprzętu komputerowego, serwerów, a także wszystkich odpowiednich obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych, w celu zapewnienia odpowiedniej ochrony wszystkich tych elementów fizycznych przed ryzykiem, w tym przed uszkodzeniem i nieuprawnionym dostępem lub użytkowaniem.

3. Podmioty finansowe minimalizują wpływ ryzyka związanego z ICT, wdrażając odpowiednie strategie, polityki, procedury, protokoły i narzędzia określone w ramach zarządzania ryzykiem związanym z ICT. Dostarczają one pełnych i aktualnych informacji na temat ryzyka związanego z ICT zgodnie z wymogami właściwych organów.

4. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1, podmioty finansowe inne niż mikroprzedsiębiorstwa wdrażają system zarządzania bezpieczeństwem informacji oparty na uznanych normach międzynarodowych i zgodny z wytycznymi nadzorczymi oraz regularnie dokonują jego przeglądu.

5. Podmioty finansowe inne niż mikroprzedsiębiorstwa zapewniają odpowiednie rozdzielenie funkcji zarządzania ICT, funkcji kontroli oraz funkcji audytu wewnętrznego, zgodnie z modelem trzech linii obrony lub wewnętrznym modelem zarządzania ryzykiem i kontroli ryzyka.

6. Ramy zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1, są dokumentowane i poddawane przeglądowi co najmniej raz w roku, a także

w przypadku wystąpienia poważnych incydentów związanych z ICT oraz zgodnie z instrukcjami nadzorczymi lub wnioskami wynikającymi z odpowiednich testów lub procesów audytu operacyjnej odporności cyfrowej. Są one stale ulepszane na podstawie wniosków płynących z wdrażania i monitorowania.

7. Ramy zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1, są regularnie kontrolowane przez audytorów w zakresie ICT posiadających wystarczającą wiedzę, umiejętności i wiedzę fachową w zakresie ryzyka związanego z ICT. Częstotliwość i przedmiot audytów ICT są współmierne do ryzyka związanego z ICT podmiotu finansowego.

8. Ustanawia się formalny proces działań następczych, w tym zasady terminowej weryfikacji oraz wdrażania środków naprawczych w następstwie krytycznych ustaleń audytu ICT, biorąc pod uwagę wnioski z przeglądu audytu, przy jednoczesnym należytym uwzględnieniu charakteru, skali i złożoności usług i działalności podmiotów finansowych.

9. Ramy zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1, obejmują strategię odporności cyfrowej, w której określono sposób wdrażania tych ram. W tym celu zawierają one metody przeciwdziałania ryzyku związanemu z ICT i osiągania szczególnych celów w dziedzinie ICT,

   a) wyjaśniając, w jaki sposób ramy zarządzania ryzykiem związanym z ICT wspierają strategię biznesową i cele biznesowe podmiotu finansowego;

   b) ustalając poziom tolerancji ryzyka w odniesieniu do ryzyka związanego z ICT, zgodnie z apetytem na ryzyko podmiotu finansowego, oraz analizując tolerancję wpływu zakłóceń w funkcjonowaniu ICT;

   c) określając jasne cele w zakresie bezpieczeństwa informacji;

   d) objaśniając referencyjną architekturę ICT oraz wszelkie zmiany niezbędne do osiągnięcia konkretnych celów biznesowych;

   e) przedstawiając poszczególne mechanizmy wprowadzone w celu wykrywania skutków incydentów związanych z ICT, ochrony przed nimi i zapobiegania im;

   f) dokumentując liczbę zgłoszonych poważnych incydentów związanych z ICT oraz skuteczność środków zapobiegawczych;

   g) określając całościową strategię obejmującą wielu dostawców ICT na poziomie podmiotu, w której pokazano kluczowe zależności od zewnętrznych dostawców usług ICT i uzasadniono łączenie zamówień u różnych zewnętrznych dostawców usług ICT;

   h) wdrażając testowanie operacyjnej odporności cyfrowej;

   i) przedstawiając strategię komunikacji w przypadku incydentów związanych z ICT.

10. Za zgodą właściwych organów podmioty finansowe mogą powierzyć zadania związane ze sprawdzaniem zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT przedsiębiorstwom wewnątrz grupy lub przedsiębiorstwom zewnętrznym.

Artykuł 6

Systemy, protokoły i narzędzia ICT

1. Podmioty finansowe stosują i utrzymują zaktualizowane systemy, protokoły i narzędzia ICT, które spełniają następujące warunki:

   a) systemy i narzędzia są odpowiednie do charakteru, różnorodności, złożoności i skali operacji wspierających prowadzenie ich działalności;

   b) są niezawodne;

   c) mają wystarczającą zdolność do dokładnego przetwarzania danych niezbędnych do prowadzenia działalności i świadczenia usług w odpowiednim czasie oraz do obsługi wolumenów zleceń, komunikatów lub transakcji występujących w okresach szczytowego obciążenia, w zależności od potrzeb, w tym w przypadku wprowadzenia nowej technologii;

   d) są odporne pod względem technologicznym, aby odpowiednio poradzić sobie z dodatkowymi potrzebami w zakresie przetwarzania informacji, które mogą być wymagane w skrajnych warunkach rynkowych lub w innych niekorzystnych sytuacjach.

2. W przypadku gdy podmioty finansowe stosują uznane na szczeblu międzynarodowym normy techniczne i wiodące praktyki branżowe w zakresie bezpieczeństwa informacji i wewnętrznych kontroli ICT, stosują one te normy i praktyki zgodnie z wszelkimi odpowiednimi zaleceniami nadzorczymi dotyczącymi ich włączenia.

Artykuł 7

Identyfikowanie

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe identyfikują, klasyfikują i odpowiednio dokumentują wszystkie funkcje biznesowe związane z ICT, zasoby informacyjne wspierające te funkcje oraz konfiguracje i wzajemne połączenia systemu ICT z wewnętrznymi i zewnętrznymi systemami ICT. Podmioty finansowe dokonują w miarę potrzeb, a co najmniej raz w roku, przeglądu adekwatności klasyfikacji zasobów informacyjnych i wszelkiej stosownej dokumentacji.

2. Podmioty finansowe na bieżąco identyfikują wszystkie źródła ryzyka związanego z ICT, w szczególności ekspozycję na ryzyko w odniesieniu do innych podmiotów finansowych i pochodzące od tych podmiotów, oraz oceniają cyberzagrożenia i luki w obszarze ICT istotne dla ich funkcji biznesowych i zasobów informacyjnych związanych z ICT. Podmioty finansowe dokonują regularnie, a co najmniej raz w roku, przeglądu scenariuszy ryzyka, które mają na nie wpływ.

3. Podmioty finansowe inne niż mikroprzedsiębiorstwa przeprowadzają ocenę ryzyka przy każdej większej zmianie w infrastrukturze sieci i systemów informatycznych, w procesach lub procedurach mających wpływ na ich funkcje, procesach wspierających lub zasobach informacyjnych.

4. Podmioty finansowe wskazują wszystkie konta systemów ICT, w tym konta zdalne, zasoby sieciowe i cały sprzęt komputerowy, oraz ewidencjonują urządzenia materialne uznane za krytyczne. Podmioty finansowe ewidencjonują konfigurację

zasobów ICT oraz powiązania i współzależności między poszczególnymi zasobami ICT.

5. Podmioty finansowe określają i dokumentują wszystkie procesy, które zależą od zewnętrznych dostawców usług ICT, oraz określają wzajemne powiązania z zewnętrznymi dostawcami usług ICT.

6. Do celów ust. 1, 4 i 5 podmioty finansowe prowadzą i regularnie aktualizują odpowiednie zapasy.

7. Podmioty finansowe inne niż mikroprzedsiębiorstwa regularnie, a co najmniej raz w roku, przeprowadzają szczegółową ocenę ryzyka związanego z ICT w odniesieniu do wszystkich starszych wersji systemów ICT, w szczególności przed połączeniem i po połączeniu starych i nowych technologii, aplikacji lub systemów.

Artykuł 8

Ochrona i zapobieganie

1. Na potrzeby odpowiedniej ochrony systemów ICT oraz w celu organizacji środków reagowania podmioty finansowe na bieżąco monitorują i kontrolują funkcjonowanie systemów i narzędzi ICT oraz minimalizują wpływ powiązanego ryzyka, wdrażając odpowiednie narzędzia, polityki i procedury w zakresie bezpieczeństwa ICT.

2. Podmioty finansowe opracowują, nabywają i wdrażają strategie, polityki, procedury, protokoły i narzędzia w zakresie bezpieczeństwa ICT, których celem jest w szczególności zapewnienie odporności, ciągłości działania i dostępności systemów ICT oraz utrzymanie wysokich standardów bezpieczeństwa, poufności i integralności danych, zarówno gdy są przechowywane, jak i wykorzystywane lub przesyłane.

3. Aby osiągnąć cele, o których mowa w ust. 2, podmioty finansowe stosują najnowocześniejsze technologie i procesy ICT, które:

   a) gwarantują bezpieczeństwo środków przekazu informacji;

   b) minimalizują ryzyko uszkodzenia lub utraty danych, nieuprawnionego dostępu i usterek technicznych, które mogą utrudniać prowadzenie działalności gospodarczej;

   c) zapobiegają wyciekowi informacji;

   d) zapewniają ochronę danych przed ryzykiem związanym z niewłaściwym administrowaniem lub przetwarzaniem, w tym nieodpowiednim prowadzeniem dokumentacji.

4. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe:

   a) opracowują i dokumentują politykę bezpieczeństwa informacji określającą zasady ochrony poufności, integralności i dostępności zasobów, danych i zasobów informacyjnych ICT tych podmiotów oraz ich klientów;

   b) zgodnie z podejściem opartym na analizie ryzyka ustalają należyte zarządzanie siecią i infrastrukturą z wykorzystaniem odpowiednich technik, metod i protokołów, w tym wdrażając automatyczne mechanizmy izolowania zasobów informacyjnych, które były przedmiotem cyberataku;

   c) wdrażają polityki ograniczające fizyczny i wirtualny dostęp do zasobów i danych systemu ICT do tego, co jest wymagane jedynie do uzasadnionych

i zatwierdzonych funkcji i działań, oraz ustanawiają w tym celu zestaw polityk, procedur i kontroli dotyczących uprawnień do dostępu i należytego zarządzania nimi;

d) wdrażają polityki i protokoły dotyczące silnych mechanizmów uwierzytelniania, oparte na odpowiednich normach i specjalnych systemach kontroli, aby uniemożliwić dostęp do kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka;

e) wdrażają polityki, procedury i kontrole w zakresie zarządzania zmianą w systemach ICT, w tym zmianami w oprogramowaniu, sprzęcie komputerowym, komponentach oprogramowania układowego, systemie lub zmianami dotyczącymi bezpieczeństwa, które opierają się na podejściu opartym na ocenie ryzyka i stanowią integralną część ogólnego procesu zarządzania zmianami w podmiocie finansowym, w celu zapewnienia rejestrowania, testowania, oceniania, zatwierdzania, wdrażania i weryfikowania w sposób kontrolowany wszystkich zmian w systemach ICT;

f) mają odpowiednią i kompleksową politykę dotyczącą poprawek i aktualizacji.

Do celów lit. b) podmioty finansowe projektują infrastrukturę przyłączeniową do sieci w sposób umożliwiający jej natychmiastowe wydzielenie i zapewniają jej podział i segmentację w celu zminimalizowania efektu domina i zapobiegania mu, zwłaszcza w przypadku wzajemnie powiązanych procesów finansowych.

Do celów lit. e) proces zarządzania zmianami ICT zatwierdzają właściwe struktury kierownicze i obejmuje on specjalne protokoły umożliwiające wprowadzanie zmian w sytuacjach nadzwyczajnych.

Artykuł 9

Wykrywanie

1. Podmioty finansowe dysponują mechanizmami pozwalającymi na szybkie wykrywanie nietypowych działań, zgodnie z art. 15, w tym problemów związanych z wydajnością sieci ICT i incydentów związanych z ICT, oraz na identyfikację wszystkich potencjalnych pojedynczych istotnych punktów awarii.

   Wszystkie mechanizmy wykrywania, o których mowa w akapicie pierwszym, są regularnie testowane zgodnie z art. 22.

2. Mechanizmy wykrywania, o których mowa w ust. 1, umożliwiają wielopoziomową kontrolę, określają progi alarmowe i kryteria uruchamiania procesów wykrywania incydentów związanych z ICT oraz reagowania na incydenty związane z ICT, a także wprowadzają automatyczne mechanizmy ostrzegawcze dla odpowiednich pracowników odpowiedzialnych za reagowanie na incydenty związane z ICT.

3. Podmioty finansowe przeznaczają wystarczające zasoby i zdolności, z należytym uwzględnieniem swojej wielkości, profilu działalności i profilu ryzyka, na monitorowanie działalności użytkowników, występowania nieprawidłowości w zakresie ICT oraz incydentów związanych z ICT, w szczególności cyberataków.

4. Podmioty finansowe, o których mowa w art. 2 ust. 1 lit. l), dodatkowo posiadają systemy umożliwiające skuteczną kontrolę sprawozdań z transakcji pod kątem

kompletności, wykrywanie przeoczeń i oczywistych błędów oraz żądanie ponownego przesłania wszelkich takich błędnych sprawozdań.

Artykuł 10

Reagowanie i przywracanie gotowości do pracy

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, oraz w oparciu o wymogi dotyczące identyfikacji określone w art. 7, podmioty finansowe wprowadzają specjalną i kompleksową politykę ciągłości działania w zakresie ICT stanowiącą integralną część polityki w zakresie operacyjnej ciągłości działania podmiotu finansowego.

2. Podmioty finansowe realizują politykę ciągłości działania w zakresie ICT, o której mowa w ust. 1, poprzez specjalne, odpowiednie i udokumentowane ustalenia, plany, procedury i mechanizmy, których celem jest:

   a) rejestrowanie wszystkich incydentów związanych z ICT;

   b) zapewnienie ciągłości pełnienia przez podmiot finansowy jego kluczowych funkcji;

   c) szybkie, właściwe i skuteczne reagowanie na wszystkie incydenty związane z ICT, w szczególności między innymi cyberataki, i ich rozwiązywanie w sposób ograniczający szkody i nadający priorytet wznowieniu działań i działaniom mającym na celu przywrócenie gotowości do pracy;

   d) bezzwłoczne uruchamianie specjalnych planów umożliwiających zastosowanie środków, procesów i technologii ograniczających rozprzestrzenianie się, dostosowanych do każdego rodzaju incydentu związanego z ICT i zapobiegających dalszym szkodom, jak również dostosowanych do potrzeb procedur reagowania i przywracania gotowości do pracy ustanowionych zgodnie z art. 11;

   e) szacowanie wstępnych skutków, szkód i strat;

   f) określanie działań w zakresie komunikacji i zarządzania kryzysowego, które zapewniają przekazywanie aktualnych informacji wszystkim odpowiednim pracownikom wewnętrznym i zewnętrznym zainteresowanym stronom zgodnie z art. 13 i zgłaszanie ich właściwym organom zgodnie z art. 17.

3. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe wdrażają powiązany z ich działalnością plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT, który w przypadku podmiotów finansowych innych niż mikroprzedsiębiorstwa podlega niezależnym przeglądom audytowym.

4. Podmioty finansowe wprowadzają, utrzymują i okresowo testują odpowiednie plany ciągłości działania w zakresie ICT, w szczególności w odniesieniu do kluczowych lub ważnych funkcji zlecanych zewnętrznym dostawcom usług ICT lub będących przedmiotem ustaleń z tymi dostawcami.

5. W ramach kompleksowego zarządzania ryzykiem związanym z ICT podmioty finansowe:

   a) co najmniej raz w roku oraz po wprowadzeniu istotnych zmian w systemach ICT testują politykę ciągłości działania w zakresie ICT oraz plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT;

b) testują plany działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej ustanowione zgodnie z art. 13.

Do celów lit. a) podmioty finansowe inne niż mikroprzedsiębiorstwa uwzględniają w planach testów scenariusze cyberataków i pracy awaryjnej w trakcie przełączania się z podstawowej infrastruktury ICT na nadmiarowe zdolności w zakresie ICT, kopie zapasowe i urządzenia redundantne, które są konieczne do wypełniania obowiązków określonych w art. 11.

Podmioty finansowe dokonują regularnych przeglądów swojej polityki ciągłości działania w zakresie ICT oraz planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT, uwzględniając wyniki testów przeprowadzonych zgodnie z akapitem pierwszym oraz zalecenia wynikające z kontroli audytowych lub przeglądów nadzorczych.

6. Podmioty finansowe inne niż mikroprzedsiębiorstwa posiadają funkcję zarządzania w sytuacji kryzysowej, w której – w przypadku uruchomienia ich polityki ciągłości działania w zakresie ICT lub planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT – określono jasne procedury zarządzania wewnętrznymi i zewnętrznymi działaniami informacyjnymi na wypadek wystąpienia sytuacji kryzysowej zgodnie z art. 13.

7. W przypadku uruchomienia polityki ciągłości działania w zakresie ICT lub planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT podmioty finansowe prowadzą ewidencję działań prowadzonych przed wystąpieniem zakłóceń i w trakcie ich wystąpienia. Taka ewidencja jest łatwo dostępna.

8. Podmioty finansowe, o których mowa w art. 2 ust. 1 lit. f), dostarczają właściwym organom kopie wyników testów ciągłości działania w zakresie ICT lub podobnych testów przeprowadzonych w okresie objętym przeglądem.

9. Podmioty finansowe inne niż mikroprzedsiębiorstwa zgłaszają właściwym organom wszystkie koszty i straty spowodowane zakłóceniami w funkcjonowaniu ICT oraz incydentami związanymi z ICT.

Artykuł 11

Zasady tworzenia kopii zapasowych i metody odzyskiwania danych

1. W celu zapewnienia przywrócenia systemów ICT przy minimalnym przestoju i ograniczonych zakłóceniach, w kontekście ram zarządzania ryzykiem związanym z ICT podmioty finansowe opracowują:

   a) zasady tworzenia kopii zapasowych, w których określono zakres danych, które obejmuje kopia zapasowa, oraz minimalną częstotliwość tworzenia kopii zapasowej, w oparciu o krytyczność informacji lub wrażliwość danych;

   b) metody odzyskiwania danych.

2. Systemy kopii zapasowych rozpoczynają przetwarzanie bez zbędnej zwłoki, chyba że ich uruchomienie zagrażałoby bezpieczeństwu sieci i systemów informatycznych lub integralności bądź poufności danych.

3. Przy przywracaniu danych z kopii zapasowych przy użyciu własnych systemów podmioty finansowe korzystają z systemów ICT, które mają inne środowisko operacyjne niż środowisko główne, które nie jest bezpośrednio połączone ze

środowiskiem głównym i które jest zabezpieczone przed wszelkim nieupoważnionym dostępem lub zakłóceniem integralności ICT.

W przypadku podmiotów finansowych, o których mowa w art. 2 ust. 1 lit. g), plany naprawcze umożliwiają odzyskanie wszystkich transakcji realizowanych w chwili wystąpienia zakłócenia, tak aby umożliwić kontrahentowi centralnemu dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie.

4. Podmioty finansowe utrzymują nadmiarowe zdolności w zakresie ICT posiadające zasoby i funkcje, które są wystarczające i odpowiednie do zaspokojenia potrzeb biznesowych.

5. Podmioty finansowe, o których mowa w art. 2 ust. 1 lit. f), utrzymują lub zapewniają utrzymanie przez swoich zewnętrznych dostawców usług ICT co najmniej drugiej lokalizacji przetwarzania danych, wyposażonej w zasoby, zdolności, funkcje i personel wystarczające i odpowiednie do zaspokojenia potrzeb biznesowych.

Druga lokalizacja przetwarzania danych:

a) znajduje się w takiej odległości geograficznej od głównego miejsca przetwarzania danych, która zapewnia posiadanie odmiennego profilu ryzyka i zapobiega oddziaływaniu na nią zdarzenia, które wpłynęło na główne miejsce przetwarzania danych;

b) może zapewnić ciągłość kluczowych usług identycznie jak w przypadku głównego miejsca przetwarzania danych lub świadczyć usługi na poziomie niezbędnym do zapewnienia realizacji przez podmiot finansowy kluczowych działań w ramach celów związanych ze wznowieniem funkcji;

c) jest niezwłocznie dostępna dla personelu podmiotu finansowego, aby zapewnić ciągłość świadczenia kluczowych usług, w przypadku gdy główne miejsce przetwarzania danych stanie się niedostępne.

6. Określając zakładany czas wznowienia oraz akceptowalny poziom utraty danych w odniesieniu do każdej funkcji, podmioty finansowe biorą pod uwagę potencjalny ogólny wpływ na efektywność rynku. Takie zakładane czasy wznowienia funkcji zapewniają osiągnięcie uzgodnionych poziomów usług w scenariuszach warunków skrajnych.

7. Podczas odzyskiwania danych po incydencie związanym z ICT podmioty finansowe przeprowadzają wielokrotne kontrole, w tym uzgodnienia, w celu zapewnienia najwyższego poziomu integralności danych. Kontrole te przeprowadza się również podczas odtwarzania danych pochodzących od zewnętrznych zainteresowanych stron, aby zapewnić spójność wszystkich danych między systemami.

Artykuł 12

Uczenie się i rozwój

1. Podmioty finansowe dysponują zdolnościami i personelem, dostosowanymi do ich wielkości, profilu działalności i profilu ryzyka, umożliwiającymi im gromadzenie informacji na temat luk oraz cyberzagrożeń, incydentów związanych z ICT, w szczególności cyberataków, oraz analizę ich prawdopodobnego wpływu na operacyjną odporność cyfrową podmiotów finansowych.

2. Podmioty finansowe przeprowadzają przeglądy incydentów związanych z ICT po wystąpieniu istotnych zakłóceń w ich głównej działalności związanych z funkcjonowaniem ICT, analizując przyczyny zakłócenia i identyfikując wymagane ulepszenia operacji ICT lub polityki ciągłości działania w zakresie ICT, o której mowa w art. 10.

   W przypadku wprowadzenia zmian podmioty finansowe inne niż mikroprzedsiębiorstwa informują o tych zmianach właściwe organy.

   W ramach przeglądów incydentów związanych z ICT, o których mowa w akapicie pierwszym, przeprowadzanych po ich wystąpieniu bada się, czy przestrzegano ustalonych procedur i czy podjęte działania były skuteczne, w tym pod względem:

   a) szybkości reagowania na ostrzeżenia dotyczące bezpieczeństwa i określania skutków incydentów związanych z ICT oraz ich wagi;

   b) jakości i szybkości przeprowadzania analizy śledczej;

   c) skuteczności eskalacji incydentów w podmiocie finansowym;

   d) skuteczności komunikacji wewnętrznej i zewnętrznej.

3. W procesie oceny ryzyka związanego z ICT należycie uwzględnia się na bieżąco wnioski z testów operacyjnej odporności cyfrowej przeprowadzonych zgodnie z art. 23 i 24 oraz z rzeczywistych incydentów związanych z ICT, w szczególności cyberataków, wraz z wyzwaniami związanymi z uruchomieniem planów ciągłości działania lub planów przywrócenia gotowości do pracy, a także z odpowiednimi informacjami wymienianymi z kontrahentami i ocenianymi podczas przeglądów nadzorczych. Ustalenia te przekładają się na stosowne przeglądy odpowiednich elementów ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1.

4. Podmioty finansowe monitorują skuteczność wdrażania swojej strategii odporności cyfrowej określonej w art. 5 ust. 9. Ewidencjonują one zmiany ryzyka związanego z ICT w czasie, analizują częstotliwość, rodzaje, skalę i zmiany incydentów związanych z ICT, w szczególności cyberataków i ich wzorców, w celu zrozumienia poziomu narażenia na ryzyko związane z ICT oraz zwiększenia dojrzałości i gotowości podmiotu finansowego do działania w cyberprzestrzeni.

5. Kadra kierownicza ds. ICT składa organowi zarządzającemu co najmniej raz w roku sprawozdanie z ustaleń, o których mowa w ust. 3, i przedstawia zalecenia.

6. Podmioty finansowe w ramach swoich programów szkoleniowych dla personelu przygotowują obowiązkowe moduły obejmujące programy zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkolenia w zakresie operacyjnej odporności cyfrowej. Skierowane są one do wszystkich pracowników oraz do kadry kierowniczej wyższego szczebla.

   Podmioty finansowe na bieżąco monitorują zmiany technologiczne, również aby zrozumieć możliwy wpływ wdrażania takich nowych technologii na wymogi bezpieczeństwa ICT i operacyjną odporność cyfrową. Śledzą one rozwój najnowszych procesów zarządzania ryzykiem związanym z ICT, skutecznie przeciwdziałając dotychczasowym lub nowym formom cyberataków.

Artykuł 13

Komunikacja

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe posiadają plany działań informacyjnych umożliwiające odpowiedzialne ujawnianie incydentów związanych z IT lub poważnych luk klientom i kontrahentom, a także, w stosownych przypadkach, opinii publicznej.

2. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe realizują politykę komunikacyjną dla pracowników i zewnętrznych zainteresowanych stron. W polityce komunikacyjnej skierowanej do pracowników uwzględnia się potrzebę rozróżnienia między pracownikami zaangażowanymi w zarządzanie ryzykiem związanym z ICT, w szczególności w zakresie reagowania i przywracania gotowości do pracy, a pracownikami, których należy informować.

3. Co najmniej jednej osobie w podmiocie powierza się zadanie wdrożenia strategii komunikacyjnej w zakresie incydentów związanych z ICT oraz rolę rzecznika ds. kontaktów z opinią publiczną i mediami.

Artykuł 14

Dalsza harmonizacja narzędzi, metod, procesów i polityk zarządzania ryzykiem związanym z ICT

Europejski Urząd Nadzoru Bankowego (EUNB), Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (ESMA) oraz Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych (EIOPA) opracowują, w porozumieniu z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), projekty regulacyjnych standardów technicznych do następujących celów:

a) doprecyzowanie elementów, które należy uwzględnić w politykach, procedurach, protokołach i narzędziach w zakresie bezpieczeństwa ICT, o których mowa w art. 8 ust. 2, w celu zapewnienia bezpieczeństwa sieci, odpowiednich zabezpieczeń przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem, zachowania autentyczności i integralności danych, w tym technik kryptograficznych, oraz zagwarantowania dokładnego i szybkiego przesyłania danych bez poważnych zakłóceń;

b) określenie, w jaki sposób polityki, procedury i narzędzia w zakresie bezpieczeństwa ICT, o których mowa w art. 8 ust. 2, zapewniają włączenie kontroli bezpieczeństwa do systemów od ich powstania (bezpieczeństwo już na etapie projektowania), umożliwiają dostosowanie do zmieniającego się krajobrazu zagrożeń oraz wykorzystanie technologii ochrony w głąb;

c) doprecyzowanie właściwych technik, metod i protokołów, o których mowa w art. 8 ust. 4 lit. b);

d) doprecyzowanie elementów kontroli praw zarządzania dostępem, o których mowa w art. 8 ust. 4 lit. c), oraz związanej z nimi polityki zasobów ludzkich określającej prawa dostępu, procedury przyznawania i cofania praw, monitorowanie nietypowych zachowań w odniesieniu do ryzyka związanego z ICT za pomocą odpowiednich wskaźników, w tym dotyczących wzorców wykorzystania sieci, godzin, działalności informatycznej i nieznanych urządzeń;

e) doprecyzowanie elementów określonych w art. 9 ust. 1 umożliwiających szybkie wykrywanie nietypowych działań oraz kryteriów, o których mowa w art. 9 ust. 2, uruchamiania procesów wykrywania incydentów związanych z ICT i reagowania na nie;

f) doprecyzowanie elementów polityki ciągłości działania w zakresie ICT, o której mowa w art. 10 ust. 1;

g) doprecyzowanie testowania planów ciągłości działania w zakresie ICT, o których mowa w art. 10 ust. 5, aby zapewnić należyte uwzględnienie scenariuszy, w których jakość pełnienia kluczowej lub ważnej funkcji pogarsza się do niedopuszczalnego poziomu lub funkcja ta przestaje być pełniona, a także należyte uwzględnienie potencjalnego wpływu niewypłacalności lub innych rodzajów awarii któregokolwiek z odnośnych zewnętrznych dostawców usług ICT oraz, w stosownych przypadkach, ryzyka politycznego w jurysdykcjach odnośnych dostawców;

h) doprecyzowanie elementów planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT, o którym mowa w art. 10 ust. 3.

EUNB, ESMA i EIOPA przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia [*Dz.U.: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie pierwszym, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

ROZDZIAŁ III

INCYDENTY ZWIĄZANE Z ICT

ZARZĄDZANIE, KLASYFIKACJA i ZGŁASZANIE

Artykuł 15

Proces zarządzania incydentami związanymi z ICT

1. Podmioty finansowe ustanawiają i wdrażają proces zarządzania incydentami związanymi z ICT w celu wykrywania incydentów związanych z ICT, zarządzania nimi i ich zgłaszania oraz wprowadzają jako ostrzeżenia wskaźniki wczesnego ostrzegania.

2. Podmioty finansowe ustanawiają odpowiednie procesy mające zapewnić spójne i zintegrowane monitorowanie incydentów związanych z ICT i postępowanie z takimi incydentami oraz działania następcze w związku z takimi incydentami, aby zagwarantować zidentyfikowanie i wyeliminowanie podstawowych przyczyn, co ma zapobiec występowaniu takich incydentów.

3. Proces zarządzania incydentami związanymi z ICT, o którym mowa w ust. 1, obejmuje:

a) ustanowienie procedur identyfikowania, śledzenia, rejestrowania, kategoryzowania i klasyfikowania incydentów związanych z ICT według ich

priorytetu oraz wagi i krytyczności usług, na które incydenty te mają wpływ, zgodnie z kryteriami, o których mowa w art. 16 ust. 1;

b) przydzielenie ról i obowiązków, które należy wprowadzić w odniesieniu do różnych rodzajów i scenariuszy incydentów związanych z ICT;

c) określenie planów działań informacyjnych skierowanych do pracowników, zewnętrznych zainteresowanych stron i mediów zgodnie z art. 13 oraz powiadamiania klientów, wewnętrznych procedur eskalacji, w tym skarg klientów związanych z ICT, jak również, w stosownych przypadkach, dostarczania informacji podmiotom finansowym działającym jako kontrahenci;

d) zapewnienie zgłaszania poważnych incydentów związanych z ICT właściwej kadrze kierowniczej wyższego szczebla oraz informowanie organu zarządzającego o poważnych incydentach związanych z ICT wraz z wyjaśnieniem wpływu, reakcji i dodatkowych kontroli, które należy ustanowić w wyniku incydentów związanych z ICT;

e) ustanowienie procedur reagowania na incydenty związane z ICT w celu złagodzenia skutków i zapewnienia przywrócenia operacyjności i bezpieczeństwa usług w rozsądnym terminie.

Artykuł 16

Klasyfikacja incydentów związanych z ICT

1. Podmioty finansowe dokonują klasyfikacji incydentów związanych z ICT i określają ich wpływ na podstawie następujących kryteriów:

a) liczby użytkowników lub kontrahentów finansowych, których dotknęło zakłócenie spowodowane incydentem związanym z ICT, oraz to, czy incydent związany z ICT spowodował skutki wizerunkowe;

b) czasu trwania incydentu związanego z ICT, w tym przerwa w świadczeniu usług;

c) zasięgu geograficznego, który ma incydent związany z ICT, w szczególności jeżeli dotyczy on więcej niż dwóch państw członkowskich;

d) utraty danych, którą powoduje incydent związany z ICT, np. utraty integralności, utraty poufności lub utraty dostępności;

e) wagi wpływu incydentu związanego z ICT na systemy ICT podmiotu finansowego;

f) krytyczności usług, których dotyczy incydent związany z ICT, w tym transakcji i operacji podmiotu finansowego;

g) wpływu gospodarczego incydentu związanego z ICT, zarówno w kategoriach bezwzględnych, jak i względnych.

2. Europejskie Urzędy Nadzoru – za pośrednictwem Wspólnego Komitetu Europejskich Urzędów Nadzoru („Wspólny Komitet”) i po konsultacji z Europejskim Bankiem Centralnym (EBC) i ENISA – opracowują wspólne projekty regulacyjnych standardów technicznych, doprecyzowując:

a) kryteria określone w ust. 1, w tym progi istotności do celów ustalania poważnych incydentów związanych z ICT, które podlegają obowiązkowi zgłaszania określonemu w art. 17 ust. 1;

b) kryteria, które mają być stosowane przez właściwe organy do celów oceny znaczenia poważnych incydentów związanych z ICT dla jurysdykcji innych państw członkowskich, oraz szczegółowe informacje dotyczące zgłaszania incydentów związanych z ICT, które mają być udostępniane innym właściwym organom zgodnie z art. 17 ust. 5 i 6.

3. Opracowując wspólne projekty regulacyjnych standardów technicznych, o których mowa w ust. 2, Europejskie Urzędy Nadzoru biorą pod uwagę normy międzynarodowe, jak również specyfikacje opracowane i opublikowane przez ENISA, w tym, w stosownych przypadkach, specyfikacje dotyczące innych sektorów gospodarki.

Europejskie Urzędy Nadzoru przedstawiają Komisji te wspólne projekty regulacyjnych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w ust. 2, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

Artykuł 17

Zgłaszanie poważnych incydentów związanych z ICT

1. Podmioty finansowe zgłaszają poważne incydenty związane z ICT odpowiedniemu właściwemu organowi, o którym mowa w art. 41, w terminach określonych w ust. 3.

Do celów akapitu pierwszego podmioty finansowe – po zebraniu i przeanalizowaniu wszystkich istotnych informacji – sporządzają sprawozdanie z incydentu, wykorzystując wzór, o którym mowa w art. 18, i przedkładają je właściwemu organowi.

Sprawozdanie to zawiera wszystkie informacje niezbędne właściwemu organowi do określenia znaczenia poważnego incydentu związanego z ICT oraz do oceny ewentualnych skutków transgranicznych.

2. W przypadku gdy poważny incydent związany z ICT ma lub może mieć wpływ na interesy finansowe użytkowników usług i klientów, podmioty finansowe bez zbędnej zwłoki informują swoich użytkowników usług i klientów o poważnym incydencie związanym z ICT oraz jak najszybciej informują ich o wszystkich środkach, które podjęto w celu ograniczenia niekorzystnych skutków takiego incydentu.

3. Podmioty finansowe przedkładają właściwemu organowi, o którym mowa w art. 41:

a) wstępne powiadomienie, niezwłocznie, ale nie później niż do końca dnia roboczego, lub, w przypadku poważnego incydentu związanego z ICT, który miał miejsce później niż 2 godziny przed końcem dnia roboczego, nie później niż 4 godziny od początku następnego dnia roboczego, lub, jeżeli kanały dokonywania zgłoszeń są niedostępne, niezwłocznie po ich udostępnieniu;

b) sprawozdanie śródokresowe, nie później niż tydzień po wstępnym powiadomieniu, o którym mowa w lit. a), po którym, w stosownych przypadkach, składa się uaktualnione powiadomienia za każdym razem, gdy dostępna jest odpowiednia aktualizacja statusu, jak również na specjalny wniosek właściwego organu;

c) sprawozdanie końcowe, po zakończeniu analizy podstawowych przyczyn, niezależnie od tego, czy wdrożono już środki ograniczające niekorzystne skutki incydentu, oraz po udostępnieniu danych dotyczących rzeczywistego oddziaływania zastępujących dane szacunkowe, jednak nie później niż w terminie jednego miesiąca od chwili przesłania wstępnego powiadomienia.

4. Podmioty finansowe mogą powierzyć obowiązki zgłaszania na podstawie niniejszego artykułu zewnętrznemu dostawcy usług wyłącznie po zatwierdzeniu przekazania przez odpowiedni właściwy organ, o którym mowa w art. 41.

5. Po otrzymaniu sprawozdania, o którym mowa w ust. 1, właściwy organ bez zbędnej zwłoki przekazuje szczegółowe informacje dotyczące incydentu:

a) EUNB, ESMA lub EIOPA, stosownie do przypadku;

b) EBC, w stosownych przypadkach, w przypadku podmiotów finansowych, o których mowa w art. 2 ust. 1 lit. a), b) i c); oraz

c) pojedynczemu punktowi kontaktowemu wyznaczonemu zgodnie z art. 8 dyrektywy (UE) 2016/1148.

6. EUNB, ESMA lub EIOPA i EBC oceniają istotność poważnego incydentu związanego z ICT dla innych odpowiednich organów publicznych i jak najszybciej odpowiednio je powiadamiają. EBC powiadamia członków Europejskiego Systemu Banków Centralnych o kwestiach mających znaczenie dla systemu płatności. Na podstawie tego powiadomienia właściwe organy podejmują w stosownych przypadkach wszelkie niezbędne środki w celu ochrony bieżącej stabilności systemu finansowego.

Artykuł 18

Harmonizacja treści i wzorów zgłoszeń

1. Europejskie Urzędy Nadzoru, za pośrednictwem Wspólnego Komitetu i po konsultacji z ENISA oraz EBC, opracowują:

a) wspólne projekty regulacyjnych standardów technicznych w celu:

1) ustalenia treści zgłoszeń dotyczących poważnych incydentów związanych z ICT;

2) doprecyzowania warunków, na jakich podmioty finansowe mogą powierzyć zewnętrznemu dostawcy usług, po uprzednim zatwierdzeniu przez właściwy organ, obowiązki sprawozdawcze określone w niniejszym rozdziale;

b) wspólne projekty wykonawczych standardów technicznych w celu ustanowienia standardowych formularzy, wzorów i procedur stosowanych przez podmioty finansowe do celów zgłaszania poważnych incydentów związanych z ICT.

Europejskie Urzędy Nadzoru przedkładają Komisji wspólne projekty regulacyjnych standardów technicznych, o których mowa w ust. 1 lit. a), oraz wspólne projekty wykonawczych standardów technicznych, o których mowa w ust. 1 lit. b), do dnia xx 202x r. [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*].

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania wspólnych regulacyjnych standardów technicznych, o których mowa w ust. 1 lit. a), zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

Komisja jest uprawniona do przyjmowania wspólnych wykonawczych standardów technicznych, o których mowa w ust. 1 lit. b), zgodnie z art. 15 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

Artykuł 19

Centralizacja zgłaszania poważnych incydentów związanych z ICT

1. Europejskie Urzędy Nadzoru, za pośrednictwem Wspólnego Komitetu oraz w porozumieniu z EBC i ENISA, przygotowują wspólne sprawozdanie, w którym oceniona zostanie wykonalność dalszej centralizacji zgłaszania incydentów poprzez ustanowienie jednego unijnego węzła informacyjnego na potrzeby zgłaszania poważnych incydentów związanych z ICT przez podmioty finansowe. W sprawozdaniu zbadane zostają sposoby ułatwienia przepływu zgłoszeń incydentów związanych z ICT, ograniczenia związanych z nimi kosztów i wsparcia analiz tematycznych w celu zwiększenia konwergencji w zakresie nadzoru.

2. Sprawozdanie, o którym mowa w ust. 1, obejmuje co najmniej:

   a) warunki wstępne do utworzenia takiego unijnego węzła informacyjnego;

   b) korzyści, ograniczenia i możliwe ryzyko;

   c) elementy zarządzania operacyjnego;

   d) warunki członkostwa;

   e) zasady dostępu podmiotów finansowych i właściwych organów krajowych do unijnego węzła informacyjnego;

   f) wstępną ocenę kosztów finansowych związanych z utworzeniem platformy operacyjnej wspierającej unijny węzeł informacyjny, w tym wymaganą wiedzę fachową.

3. Europejskie Urzędy Nadzoru przedkładają Komisji, Parlamentowi Europejskiemu i Radzie sprawozdanie, o którym mowa w ust. 1, do dnia xx 202x r. [*Urząd Publikacji: należy wstawić datę przypadającą 3 lata od dnia wejścia w życie niniejszego rozporządzenia*].

Artykuł 20

Informacje zwrotne od organów nadzoru

1. Po otrzymaniu sprawozdania, o którym mowa w art. 17 ust. 1, właściwy organ potwierdza otrzymanie powiadomienia i jak najszybciej przekazuje 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.

2. Europejskie Urzędy Nadzoru – za pośrednictwem Wspólnego Komitetu – składają corocznie, na podstawie zanonimizowanych i zbiorczych danych, sprawozdanie dotyczące powiadomień o incydentach związanych z ICT otrzymanych od

właściwych organów, określając co najmniej liczbę poważnych incydentów związanych z ICT, ich charakter, wpływ na działalność podmiotów finansowych lub klientów, koszty i podjęte działania naprawcze.

Europejskie Urzędy Nadzoru wydają ostrzeżenia i opracowują dane statystyczne wysokiego poziomu w celu wsparcia oceny zagrożeń i luk w obszarze ICT.

ROZDZIAŁ IV

TESTOWANIE OPERACYJNEJ ODPORNOŚCI CYFROWEJ

Artykuł 21

Ogólne wymogi dotyczące przeprowadzania testów operacyjnej odporności cyfrowej

1. Do celów oceny gotowości na wypadek incydentów związanych z ICT, określania braków, niedociągnięć lub słabych punktów w zakresie operacyjnej odporności cyfrowej oraz niezwłocznego wdrażania środków naprawczych podmioty finansowe ustanawiają i utrzymują, z należytym uwzględnieniem swojej wielkości, profilu działalności i profilu ryzyka, solidny i kompleksowy program testowania operacyjnej odporności cyfrowej stanowiący integralną część ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5, oraz dokonują przeglądu tego programu.
2. Program testowania operacyjnej odporności cyfrowej obejmuje szereg ocen, testów, metodyk, praktyk i narzędzi, które należy stosować zgodnie z przepisami art. 22 i 23.
3. Podczas realizacji programu testowania operacyjnej odporności cyfrowej, o którym mowa w ust. 1, podmioty finansowe stosują podejście oparte na analizie ryzyka, uwzględniając zmieniające się środowisko ryzyka związanego z ICT, wszelkie szczególne rodzaje ryzyka, na które podmiot finansowy jest lub może być narażony, krytyczność zasobów informacyjnych i świadczonych usług, jak również wszelkie inne czynniki, które podmiot finansowy uzna za stosowne.
4. Podmioty finansowe zapewniają, aby testy były przeprowadzane przez niezależne strony wewnętrzne lub zewnętrzne.
5. Podmioty finansowe ustanawiają procedury i zasady ustalania hierarchii, klasyfikowania i rozwiązywania wszystkich problemów stwierdzonych w trakcie przeprowadzania testów oraz ustanawiają wewnętrzne metody zatwierdzania w celu dopilnowania, aby w pełni usunięto wszystkie stwierdzone braki, niedociągnięcia lub słabe punkty.
6. Podmioty finansowe co najmniej raz w roku testują wszystkie kluczowe systemy i aplikacje ICT.

Artykuł 22

Testowanie narzędzi i systemów ICT

1. Program testowania operacyjnej odporności cyfrowej, o którym mowa w art. 21, przewiduje przeprowadzenie pełnego zakresu odpowiednich testów, w tym ocen narażenia i skanowania pod tym kątem, analiz otwartego oprogramowania, ocen bezpieczeństwa sieci, analiz braków, fizycznych kontroli bezpieczeństwa, kwestionariuszy i rozwiązań w zakresie oprogramowania skanującego, w miarę możliwości przeglądów kodu źródłowego, testów scenariuszowych, testów

kompatybilności, testów wydajności, testów typu „end-to-end” lub testów penetracyjnych.

2. Podmioty finansowe, o których mowa w art. 2 ust. 1 lit. f) i g), przeprowadzają oceny narażenia przed każdym wdrożeniem lub przeniesieniem nowych lub istniejących usług wspierających kluczowe funkcje, aplikacje i elementy infrastruktury podmiotu finansowego.

Artykuł 23

Zaawansowane testowanie narzędzi, systemów i procesów ICT z wykorzystaniem testów penetracyjnych pod kątem wyszukiwania zagrożeń

1. Podmioty finansowe określone zgodnie z ust. 4 przeprowadzają co najmniej raz na trzy lata zaawansowane testy za pomocą testów penetracyjnych pod kątem wyszukiwania zagrożeń.

2. Testy penetracyjne pod kątem wyszukiwania zagrożeń obejmują co najmniej kluczowe funkcje i usługi podmiotu finansowego i są przeprowadzane na działających systemach produkcyjnych wspierających takie funkcje. Dokładny zakres testów penetracyjnych pod kątem wyszukiwania zagrożeń, na podstawie oceny kluczowych funkcji i usług, określają podmioty finansowe i zatwierdzają właściwe organy.

   Do celów akapitu pierwszego podmioty finansowe określają wszystkie istotne bazowe procesy, systemy i technologie ICT wspierające kluczowe funkcje i usługi, w tym funkcje i usługi zlecone zewnętrznym dostawcom usług ICT lub będące przedmiotem umowy z takimi dostawcami.

   W przypadku zakres zadań związanych z testami penetracyjnymi pod kątem wyszukiwania zagrożeń obejmuje zewnętrznych dostawców usług ICT, podmiot finansowy stosuje niezbędne środki w celu zapewnienia udziału tych dostawców.

   Podmioty finansowe stosują skuteczne środki kontroli zarządzania ryzykiem w celu ograniczenia ryzyka potencjalnego wpływu na dane, zniszczenia zasobów i zakłócenia kluczowych usług lub operacji samego podmiotu finansowego, jego kontrahentów lub sektora finansowego.

   Na koniec testu, po uzgodnieniu sprawozdań i planów naprawczych, podmiot finansowy i testerzy zewnętrzni przedstawiają właściwemu organowi dokumentację potwierdzającą, że test penetracyjny pod kątem wyszukiwania zagrożeń przeprowadzono zgodnie z wymogami. Właściwe organy zatwierdzają dokumentację i wydają potwierdzenie.

3. Zgodnie z art. 24 podmioty finansowe zawierają z testerami umowy, których przedmiotem jest przeprowadzenie testów penetracyjnych pod kątem wyszukiwania zagrożeń.

   Właściwe organy określają podmioty finansowe, które mają przeprowadzić testy penetracyjne pod kątem wyszukiwania zagrożeń, w sposób proporcjonalny do wielkości, skali, działalności i ogólnego profilu ryzyka podmiotu finansowego, w oparciu o ocenę:

   a) czynników związanych z wpływem, w szczególności krytyczności świadczonych usług oraz działań podejmowanych przez podmiot finansowy;

b) ewentualnych obaw dotyczących stabilności finansowej, w tym systemowego charakteru podmiotu finansowego na poziomie krajowym lub unijnym, w stosownych przypadkach;

c) specyficznego profilu ryzyka związanego z ICT, poziomu zaawansowania podmiotu finansowego pod względem ICT lub rozwiązań technologicznych, które są z nim związane.

4. EUNB, ESMA i EIOPA, po konsultacji z EBC i z uwzględnieniem odpowiednich ram obowiązujących w Unii, które mają zastosowanie do testów penetracyjnych opartych na analizie zagrożeń, opracowują projekty regulacyjnych standardów technicznych, aby doprecyzować:

a) kryteria wykorzystywane do celów stosowania ust. 6 niniejszego artykułu;

b) wymogi dotyczące:

a) zakresu testów penetracyjnych pod kątem wyszukiwania zagrożeń, o których mowa w ust. 2 niniejszego artykułu;

b) metodyki testowania i podejścia, które należy stosować na każdym konkretnym etapie procesu testowania;

c) etapów testów odnoszących się do wyników, zamykania i środków naprawczych;

c) rodzaj współpracy w zakresie nadzoru potrzebny do przeprowadzenia testów penetracyjnych pod kątem wyszukiwania zagrożeń w kontekście podmiotów finansowych, które działają w więcej niż jednym państwie członkowskim, aby umożliwić odpowiedni poziom zaangażowania organów nadzoru i elastyczne wdrażanie uwzględniające specyfikę podsektorów finansowych lub lokalnych rynków finansowych.

Europejskie Urzędy Nadzoru przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 2 miesiące przed dniem wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie drugim, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

Artykuł 24

Wymogi dotyczące testerów

1. Przy przeprowadzaniu testów penetracyjnych pod kątem wyszukiwania zagrożeń podmioty finansowe korzystają wyłącznie z usług testerów, którzy:

a) są najbardziej odpowiedni do tego zadania i cieszą się największą renomą;

b) posiadają zdolności techniczne i organizacyjne oraz wykazują się szczególną wiedzą fachową w zakresie analizy zagrożeń, testów penetracyjnych lub testów z udziałem zespołów atakujących;

c) posiadają certyfikat wydany przez jednostkę akredytującą w państwie członkowskim lub stosują się do formalnych kodeksów postępowania lub ram etycznych;

d) w przypadku testerów zewnętrznych – przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z wykonywaniem testów penetracyjnych pod kątem wyszukiwania zagrożeń, w tym należytej ochrony poufnych informacji jednostki finansowej i dochodzenia roszczeń z tytułu ryzyka biznesowego jednostki finansowej;

e) w przypadku testerów zewnętrznych – są należycie i w pełni objęci odpowiednimi ubezpieczeniami od odpowiedzialności cywilnej z tytułu wykonywania zawodu, w tym od ryzyka wykroczeń i zaniedbań.

2. Podmioty finansowe zapewniają, aby umowy zawarte z testerami zewnętrznymi wymagały należytego zarządzania wynikami testów penetracyjnych pod kątem wyszukiwania zagrożeń oraz aby żadne ich przetwarzanie, w tym generowanie, sporządzanie, przechowywanie, agregowanie, zgłaszanie, przekazywanie lub niszczenie, nie stwarzały ryzyka dla podmiotu finansowego.

ROZDZIAŁ V

ZARZĄDZANIE RYZYKIEM ZE STRONY ZEWNĘTRZNYCH DOSTAWCÓW USŁUG ICT

SEKCJA I

GŁÓWNE ZASADY NALEŻYTEGO ZARZĄDZANIA RYZYKIEM ZE STRONY ZEWNĘTRZNYCH DOSTAWCÓW USŁUG ICT

Artykuł 25

Zasady ogólne

Podmioty finansowe zarządzają ryzykiem ze strony zewnętrznych dostawców usług ICT jako integralnym elementem ryzyka związanego z ICT wchodzącym w zakres ich ram zarządzania ryzykiem związanym z ICT oraz zgodnie z opisanymi poniżej zasadami.

1. Podmioty finansowe, które zawarły ustalenia umowne dotyczące korzystania z usług ICT w celu prowadzenia działalności gospodarczej, pozostają przez cały czas w pełni odpowiedzialne za wypełnianie i wywiązywanie się z wszystkich obowiązków wynikających z niniejszego rozporządzenia i obowiązujących przepisów dotyczących usług finansowych.

2. Zarządzanie przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT odbywa się w świetle zasady proporcjonalności, z uwzględnieniem:

   a) skali, złożoności i znaczenia zależności w zakresie ICT;

   b) ryzyka wynikającego z ustaleń umownych dotyczących korzystania z usług ICT zawartych z zewnętrznymi dostawcami usług ICT, biorąc pod uwagę krytyczność lub znaczenie danej usługi, procesu lub funkcji oraz potencjalny wpływ na ciągłość i jakość usług finansowych i działalności finansowej, na poziomie indywidualnym i grupowym.

3. Jako część swoich ram zarządzania ryzykiem związanym z ICT podmioty finansowe przyjmują i regularnie weryfikują strategię dotyczącą ryzyka ze strony zewnętrznych

dostawców usług ICT, uwzględniając strategię obejmującą wielu dostawców, o której mowa w art. 5 ust. 9 lit. g). Strategia ta obejmuje politykę korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT i ma zastosowanie na zasadzie indywidualnej oraz, w stosownych przypadkach, na zasadzie subskonsolidowanej i skonsolidowanej. Organ zarządzający regularnie dokonuje przeglądu ryzyka zidentyfikowanego w odniesieniu do outsourcingu kluczowych lub ważnych funkcji.

4. W kontekście swoich ram zarządzania ryzykiem związanym z ICT podmioty finansowe prowadzą i aktualizują na poziomie podmiotu oraz na poziomie subskonsolidowanym i skonsolidowanym rejestr informacji w odniesieniu do wszystkich ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT.

   Ustalenia umowne, o których mowa w akapicie pierwszym, są odpowiednio udokumentowane, z rozróżnieniem na ustalenia, które obejmują kluczowe lub ważne funkcje, oraz ustalenia, które takich funkcji nie obejmują.

   Podmioty finansowe co najmniej raz w roku przedstawiają właściwym organom informacje na temat liczby nowych ustaleń dotyczących korzystania z usług ICT, kategorii zewnętrznych dostawców usług ICT, rodzaju ustaleń umownych oraz świadczonych usług i obsługiwanych funkcji.

   Podmioty finansowe udostępniają właściwemu organowi, na jego wniosek, pełny rejestr informacji lub, zgodnie z treścią takiego wniosku, określone sekcje tego rejestru wraz ze wszelkimi informacjami uznanymi za niezbędne, aby umożliwić skuteczny nadzór nad podmiotem finansowym.

   Podmioty finansowe informują w odpowiednim terminie właściwy organ o planowanym udzieleniu zamówienia obejmującego kluczowe lub ważne funkcje oraz o tym, że dana funkcja stała się kluczowa lub ważna.

5. Przed zawarciem ustalenia umownego dotyczącego korzystania z usług ICT podmioty finansowe są zobowiązane:

   a) ocenić, czy ustalenie umowne dotyczy kluczowej lub ważnej funkcji;

   b) ocenić, czy spełniono warunki nadzorcze dotyczące zawierania umów;

   c) określić i ocenić wszystkie rodzaje istotnego ryzyka związane z ustaleniem umownym, w tym możliwość, że takie ustalenie umowne może przyczynić się do zwiększenia ryzyka koncentracji w obszarze ICT;

   d) dołożyć należytej staranności w stosunku do potencjalnych zewnętrznych dostawców usług ICT i zapewnić, aby w trakcie całego procesu wyboru i oceny zewnętrzny dostawca usług ICT był odpowiedni;

   e) zidentyfikować i ocenić konflikty interesów, które mogą wynikać z ustalenia umownego.

6. Podmioty finansowe mogą zawierać ustalenia umowne wyłącznie z zewnętrznymi dostawcami usług ICT, którzy przestrzegają wysokich, odpowiednich i najnowszych standardów w zakresie bezpieczeństwa informacji.

7. Korzystając z praw dostępu, kontroli i audytu w odniesieniu do zewnętrznego dostawcy usług ICT, podmioty finansowe, stosując podejście oparte na analizie ryzyka, określają z góry częstotliwość audytów i kontroli oraz obszary, które mają podlegać kontroli, przestrzegając powszechnie przyjętych standardów audytu

zgodnie z wszelkimi instrukcjami nadzorczymi dotyczącymi stosowania i włączania takich standardów audytu.

W przypadku ustaleń umownych, które wiążą się z wysokim poziomem złożoności technologicznej, podmiot finansowy sprawdza, czy audytorzy – zarówno wewnętrzni, jak i grupy audytorów lub audytorzy zewnętrzni – posiadają odpowiednie umiejętności i wiedzę umożliwiające skuteczne przeprowadzanie odpowiednich kontroli i ocen.

8. Podmioty finansowe zapewniają, aby ustalenia umowne dotyczące korzystania z usług ICT wypowiadano co najmniej w następujących okolicznościach:

a) naruszenie przez zewnętrznego dostawcę usług ICT obowiązujących przepisów ustawowych, wykonawczych lub warunków umowy;

b) zidentyfikowanie okoliczności w trakcie monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT, w przypadku których to okoliczności uznano, że mogą one zmienić wykonywanie funkcji przewidzianych w ustaleniu umownym, w tym istotne zmiany mające wpływ na ustalenie umowne lub sytuację zewnętrznego dostawcy usług ICT;

c) wykazanie w przypadku zewnętrznego dostawcy usług ICT braków w ogólnym zarządzaniu ryzykiem związanym z ICT, a w szczególności w sposobie, w jaki zapewnia on bezpieczeństwo i integralność danych poufnych, osobowych lub w inny sposób wrażliwych lub danych nieosobowych;

d) wystąpienie okoliczności, w których właściwy organ wskutek odpowiednich ustaleń umownych nie może już skutecznie nadzorować podmiotu finansowego.

9. Podmioty finansowe wprowadzają strategie wyjścia w celu uwzględnienia ryzyka, które może pojawić się na poziomie zewnętrznego dostawcy usług ICT, w szczególności jego możliwej awarii, pogorszenia jakości obsługiwanych funkcji, wszelkich zakłóceń w działalności spowodowanych niewłaściwym lub nieudanym świadczeniem usług lub istotnego ryzyka związanego z odpowiednią i systematyczną realizacją funkcji.

Podmioty finansowe zapewniają sobie możliwość wycofania się z ustaleń umownych:

a) bez powodowania zakłóceń w swojej działalności;

b) bez ograniczania zgodności z wymogami regulacyjnymi;

c) bez szkody dla ciągłości i jakości usług świadczonych przez nie na rzecz klientów.

Plany wyjścia są kompleksowe, udokumentowane i, w stosownych przypadkach, wystarczająco przetestowane.

Podmioty finansowe określają rozwiązania alternatywne i opracowują plany przejściowe umożliwiające im odebranie funkcji będących przedmiotem umowy i odpowiednich danych zewnętrznemu dostawcy usług ICT oraz bezpieczne i integralne przekazanie ich dostawcom alternatywnym lub ponowne włączenie ich do struktury wewnętrznej.

Podmioty finansowe stosują odpowiednie środki awaryjne w celu utrzymania ciągłości działania we wszystkich okolicznościach, o których mowa w akapicie pierwszym.

10. Europejskie Urzędy Nadzoru – za pośrednictwem Wspólnego Komitetu – opracowują projekty wykonawczych standardów technicznych w celu ustanowienia standardowych wzorów na potrzeby rejestru informacji, o którym mowa w ust. 4.

Europejskie Urzędy Nadzoru przedstawiają Komisji te projekty wykonawczych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do przyjmowania wykonawczych standardów technicznych, o których mowa w akapicie pierwszym, zgodnie z art. 15 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

11. Za pośrednictwem Wspólnego Komitetu Europejskie Urzędy Nadzoru opracowują projekty regulacyjnych standardów technicznych w celu doprecyzowania:

a) szczegółowej treści polityki, o której mowa w ust. 3, w odniesieniu do ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT, poprzez odniesienie do głównych etapów cyklu życia odpowiednich ustaleń dotyczących korzystania z usług ICT;

b) rodzajów informacji, które mają być ujęte w rejestrze informacji, o którym mowa w ust. 4.

Europejskie Urzędy Nadzoru przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie drugim, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

Artykuł 26

Wstępna ocena ryzyka koncentracji w obszarze ICT i uzgodnień dotyczących dalszego podoutsourcingu

1. Dokonując identyfikacji i oceny ryzyka koncentracji w obszarze ICT, o którym mowa w art. 25 ust. 5 lit. c), podmioty finansowe biorą pod uwagę, czy zawarcie uzgodnienia umownego w związku z usługami ICT prowadziłoby do któregokolwiek z poniższych skutków:

a) zawarcia umowy z zewnętrznym dostawcą usług ICT, którego nie można łatwo zastąpić; lub

b) posiadania wielu ustaleń umownych dotyczących świadczenia usług ICT z tym samym zewnętrznym dostawcą usług ICT lub z blisko powiązanymi zewnętrznymi dostawcami usług ICT.

Podmioty finansowe rozważają korzyści i koszty rozwiązań alternatywnych, takich jak korzystanie z usług różnych zewnętrznych dostawców usług ICT, biorąc pod uwagę, czy i w jaki sposób przewidywane rozwiązania odpowiadają potrzebom i celom biznesowym określonym w ich strategii odporności cyfrowej.

2. W przypadku gdy ustalenia umowne dotyczące korzystania z usług ICT obejmują możliwość dalszego zlecania podwykonawstwa kluczowej lub ważnej funkcji przez zewnętrznego dostawcę usług ICT innym zewnętrznym dostawcom usług ICT, podmioty finansowe rozważają korzyści i ryzyko, które mogą wystąpić w związku z takim ewentualnym podwykonawstwem, w szczególności w przypadku podwykonawcy ICT mającego siedzibę w państwie trzecim.

W przypadku gdy ustalenia umowne dotyczące korzystania z usług ICT są zawierane z zewnętrznym dostawcą usług ICT mającym siedzibę w państwie trzecim, podmioty finansowe biorą pod uwagę istotne, co najmniej następujące czynniki:

a) przestrzeganie ochrony danych;

b) skuteczne egzekwowanie prawa;

c) przepisy prawa upadłościowego, które miałyby zastosowanie w przypadku upadłości zewnętrznego dostawcy usług ICT;

d) wszelkie ograniczenia, które mogą powstać w związku z pilnym odzyskiwaniem danych podmiotu finansowego.

Podmioty finansowe oceniają, czy i w jaki sposób potencjalnie długie lub złożone łańcuchy podwykonawstwa mogą wpływać na ich zdolność do pełnego monitorowania funkcji będących przedmiotem umowy oraz na zdolność właściwego organu do skutecznego nadzoru nad podmiotem finansowym w tym zakresie.

Artykuł 27

Kluczowe postanowienia umowne

1. Prawa i obowiązki podmiotu finansowego i zewnętrznego dostawcy usług ICT są wyraźnie przypisane i określone na piśmie. Całość umowy, która obejmuje klauzule o gwarantowanym poziomie usług, musi znaleźć się w jednym dokumencie mającym formę pisemną, dostępnym dla stron w wersji papierowej lub w formacie umożliwiającym pobieranie i dostęp.

2. Ustalenia umowne dotyczące korzystania z usług ICT obejmują co najmniej następujące elementy:

a) jasny i kompletny opis wszystkich funkcji i usług, które mają być świadczone przez zewnętrznego dostawcę usług ICT, ze wskazaniem, czy dozwolone jest podwykonawstwo kluczowej lub ważnej funkcji lub jej istotnych części, a jeżeli tak, to jakie warunki mają zastosowanie do takiego podwykonawstwa;

b) miejsca, w których mają być świadczone objęte umową lub podwykonawstwem funkcje i usługi oraz w których mają być przetwarzane dane, w tym miejsce przechowywania, oraz wymóg, aby zewnętrzny dostawca usług ICT powiadomił podmiot finansowy, jeżeli przewiduje zmianę tych miejsc;

c) postanowienia dotyczące dostępu, dostępności, integralności, bezpieczeństwa i ochrony danych osobowych oraz zapewnienia dostępu, odzyskiwania i zwrotu w łatwo dostępnym formacie danych osobowych i nieosobowych przetwarzanych przez podmiot finansowy w przypadku niewypłacalności lub rozwiązania zewnętrznego dostawcy usług ICT lub zaprzestania przez niego działalności gospodarczej;

d) pełne opisy poziomu usług, w tym ich aktualizacje i zmiany, oraz dokładne ilościowe i jakościowe cele w zakresie wyników w ramach uzgodnionych poziomów usług, aby umożliwić podmiotowi finansowemu skuteczne monitorowanie oraz umożliwić bezzwłoczne podjęcie odpowiednich działań naprawczych w przypadku nieosiągnięcia uzgodnionych poziomów usług;

e) okresy wypowiedzenia i obowiązki sprawozdawcze zewnętrznego dostawcy usług ICT w stosunku do podmiotu finansowego, w tym powiadamianie o każdej zmianie, która może mieć istotny wpływ na zdolność skutecznego wykonywania przez tego dostawcę kluczowych lub ważnych funkcji zgodnie z uzgodnionymi poziomami usług;

f) obowiązek zapewnienia przez zewnętrznego dostawcę usług ICT pomocy w przypadku incydentu związanego z ICT, bez dodatkowych opłat lub za opłatą określoną *ex ante*;

g) wymogi wobec zewnętrznego dostawcy usług ICT w zakresie wdrażania i testowania planów awaryjnych w związku z prowadzoną działalnością oraz posiadania środków, narzędzi i polityk w zakresie bezpieczeństwa ICT, które odpowiednio gwarantują bezpieczne świadczenie usług przez podmiot finansowy zgodnie z jego ramami regulacyjnymi;

h) prawo do monitorowania na bieżąco wyników osiąganych przez zewnętrznego dostawcę usług ICT, które obejmuje:

   (i) prawa dostępu, kontroli i audytu przez podmiot finansowy lub przez wyznaczoną osobę trzecią oraz prawo do sporządzania kopii odnośnej dokumentacji, przy czym skuteczne wykonywanie tych praw nie jest utrudnione lub ograniczone przez inne ustalenia umowne lub politykę w zakresie wdrażania;

   (ii) prawo do uzgodnienia alternatywnych poziomów zabezpieczenia w przypadku naruszenia praw innych klientów;

   (iii) zobowiązanie do pełnej współpracy podczas kontroli na miejscu przeprowadzanych przez podmiot finansowy oraz szczegółowe informacje na temat zakresu, warunków i częstotliwości zdalnego przeprowadzania audytów;

i) obowiązek pełnej współpracy zewnętrznego dostawcy usług ICT z właściwymi organami i organami ds. restrukturyzacji i uporządkowanej likwidacji podmiotu finansowego, w tym z osobami przez nie wyznaczonymi;

j) prawa do odstąpienia od umowy i związany z nimi minimalny okres wypowiedzenia umowy, zgodnie z oczekiwaniami właściwych organów;

k) strategie wyjścia, w szczególności ustanowienie obowiązkowego odpowiedniego okresu przejściowego:

   a) podczas którego zewnętrzny dostawca usług ICT będzie nadal świadczył odpowiednie funkcje lub usługi w celu zmniejszenia ryzyka wystąpienia zakłóceń w funkcjonowaniu podmiotu finansowego;

   b) który umożliwia podmiotowi finansowemu zmianę zewnętrznego dostawcy usług ICT na innego dostawcę lub przejście na rozwiązania dostępne na miejscu zgodnie ze złożonością świadczonej usługi.

3. Negocjując ustalenia umowne, podmioty finansowe i zewnętrzni dostawcy usług ICT rozważają zastosowanie standardowych klauzul umownych opracowanych dla określonych usług.

4. Europejskie Urzędy Nadzoru – za pośrednictwem Wspólnego Komitetu –opracowują projekty regulacyjnych standardów technicznych doprecyzowujących elementy, które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo kluczowych lub ważnych funkcji, w celu zapewnienia skuteczności przepisów ust. 2 lit. a).

Europejskie Urzędy Nadzoru przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie pierwszym, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010.

SEKCJA II

RAMY NADZORU NAD KLUCZOWYMI ZEWNĘTRZNYMI DOSTAWCAMI USŁUG ICT

Artykuł 28

Wyznaczenie kluczowych zewnętrznych dostawców usług ICT

1. Za pośrednictwem Wspólnego Komitetu i na podstawie zalecenia forum nadzoru ustanowionego zgodnie z art. 29 ust. 1 Europejskie Urzędy Nadzoru:

   a) wyznaczają zewnętrznych dostawców usług ICT, którzy mają dla podmiotów finansowych kluczowe znaczenie, uwzględniając kryteria określone w ust. 2;

   b) wyznaczają EUNB, ESMA albo EIOPA jako wiodący organ nadzorczy w odniesieniu do każdego z kluczowych zewnętrznych dostawców usług ICT, w zależności od tego, czy łączna wartość aktywów podmiotów finansowych korzystających z usług danego kluczowego zewnętrznego dostawcy usług ICT i objętych jednym z rozporządzeń, odpowiednio, (UE) nr 1093/2010 (UE), nr 1094/2010 lub (UE) nr 1095/2010, stanowi ponad połowę wartości łącznych aktywów wszystkich podmiotów finansowych korzystających z usług tego kluczowego zewnętrznego dostawcy usług ICT, wykazanych w bilansach skonsolidowanych lub w indywidualnych bilansach, jeżeli bilanse nie są skonsolidowane, tych podmiotów finansowych.

2. Wyznaczenie, o którym mowa w ust. 1 lit. a), opiera się na wszystkich następujących kryteriach:

   a) systemowym wpływie na stabilność, ciągłość lub jakość świadczenia usług finansowych, w przypadku gdy dany zewnętrzny dostawca usług ICT musiałby sprostać błędowi operacyjnemu na dużą skalę w zakresie świadczenia swoich usług, biorąc pod uwagę liczbę podmiotów finansowych, na rzecz których dany zewnętrzny dostawca usług ICT świadczy usługi;

   b) systemowym charakterze lub znaczeniu podmiotów finansowych, które korzystają z usług danego zewnętrznego dostawcy usług ICT, ocenianym zgodnie z poniższymi parametrami:

i) liczbą globalnych instytucji o znaczeniu systemowym lub innych instytucji o znaczeniu systemowym, które korzystają z usług danego zewnętrznego dostawcy usług ICT;

ii) wzajemną zależnością między globalnymi instytucjami o znaczeniu systemowym lub innymi instytucjami o znaczeniu systemowym, o których mowa w ppkt (i), a innymi podmiotami finansowymi, obejmującą sytuacje, w których globalne instytucje o znaczeniu systemowym lub inne instytucje o znaczeniu systemowym świadczą usługi w zakresie infrastruktury finansowej na rzecz innych podmiotów finansowych;

c) korzystaniu przez podmioty finansowe z usług świadczonych przez danego zewnętrznego dostawcę usług ICT w odniesieniu do kluczowych lub ważnych funkcji podmiotów finansowych, które ostatecznie obejmują tego samego zewnętrznego dostawcę usług ICT, niezależnie od tego, czy podmioty finansowe korzystają z tych usług bezpośrednio czy pośrednio, za pomocą lub w ramach umów dalszego podwykonawstwa;

d) stopniu substytucyjności zewnętrznego dostawcy usług ICT, biorąc pod uwagę następujące parametry:

(i) brak realnych alternatyw, nawet częściowych, ze względu na ograniczoną liczbę zewnętrznych dostawców usług ICT działających na określonym rynku lub udział w rynku danego zewnętrznego dostawcy usług ICT, bądź techniczną złożoność lub techniczny stopień zaawansowania, w tym w odniesieniu do jakiejkolwiek zastrzeżonej technologii, bądź szczególne cechy organizacji lub działalności tego dostawcy;

(ii) trudności z częściową lub całkowitą migracją stosownych danych i nakładów pracy od danego zewnętrznego dostawcy usług ICT do innego zewnętrznego dostawcy usług ICT, ze względu na znaczące koszty finansowe, czas lub inny rodzaj zasobów, które mogą wiązać się z procesem migracji, albo ze względu na zwiększone ryzyko związane z ICT lub inne ryzyko operacyjne, na które podmiot finansowy może być narażony w wyniku takiej migracji;

e) liczbie państw członkowskich, w których dany zewnętrzny dostawca usług ICT świadczy usługi;

f) liczbie państw członkowskich, w których działają podmioty finansowe korzystające z usług danego zewnętrznego dostawcy usług ICT.

3. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu uzupełnienia kryteriów, o których mowa w ust. 2.

4. Mechanizmu wyznaczania, o którym mowa w ust. 1 lit. a), nie można stosować do czasu przyjęcia przez Komisję aktu delegowanego zgodnie z ust. 3.

5. Mechanizm wyznaczania, o którym mowa w ust. 1 lit. a), nie ma zastosowania do zewnętrznych dostawców usług ICT, którzy podlegają ramom nadzoru ustanowionym na potrzeby wspierania realizacji zadań, o których mowa w art. 127 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej.

6. Za pośrednictwem Wspólnego Komitetu Europejskie Urzędy Nadzoru sporządzają, publikują i każdego roku aktualizują wykaz kluczowych zewnętrznych dostawców usług ICT na poziomie Unii.

7. Do celów ust. 1 lit. a) właściwe organy przekazują forum nadzoru ustanowionemu na podstawie art. 29 sprawozdania w ujęciu rocznym i zagregowanym, o których mowa w art. 25 ust. 4. Forum nadzoru ocenia zależności podmiotów finansowych od zewnętrznych dostawców usług ICT na podstawie informacji uzyskanych od właściwych organów.

8. Zewnętrzni dostawcy usług ICT, których nie uwzględniono w wykazie, o którym mowa w ust. 6, mogą zwrócić się z wnioskiem o umieszczenie ich w tym wykazie.

   Na potrzeby akapitu pierwszego zewnętrzni dostawcy usług ICT składają umotywowany wniosek do EUNB, ESMA lub EIOPA, które za pośrednictwem Wspólnego Komitetu podejmują decyzję, czy uwzględnić danego zewnętrznego dostawcę usług ICT w przedmiotowym wykazie zgodnie z ust. 1 lit. a).

   Decyzja, o której mowa w akapicie drugim, zostaje przyjęta i przekazana zewnętrznemu dostawcy usług ICT w terminie 6 miesięcy od otrzymania wniosku.

9. Podmioty finansowe nie korzystają z usług zewnętrznego dostawcy usług ICT z siedzibą w państwie trzecim, który na podstawie ust. 1 lit. a) zostałby wyznaczony jako jeden z kluczowych dostawców, gdyby miał siedzibę w Unii.

Artykuł 29

Struktura ram nadzoru

1. Zgodnie z art. 57 rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 Wspólny Komitet ustanawia forum nadzoru jako podkomitet na potrzeby wspierania prac Wspólnego Komitetu i wiodącego organu nadzorczego, o którym mowa w art. 28 ust. 1 lit. b), w obszarze ryzyka ze strony zewnętrznych dostawców usług ICT w całym sektorze finansowym. Forum nadzoru sporządza projekty wspólnych stanowisk i wspólnych aktów Wspólnego Komitetu w tym obszarze.

   Forum nadzoru regularnie omawia istotne zmiany dotyczące ryzyka i luk związanych z ICT oraz promuje spójne podejście przy monitorowaniu ryzyka ze strony zewnętrznych dostawców usług ICT w skali Unii.

2. Forum nadzoru co roku dokonuje zbiorowej oceny wyników i ustaleń z działań nadzorczych przeprowadzonych w odniesieniu do wszystkich kluczowych zewnętrznych dostawców usług ICT i promuje środki koordynacji mające na celu zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych, propagowanie najlepszych praktyk w zakresie eliminowania ryzyka koncentracji w obszarze ICT oraz analizę czynników łagodzących przenoszenie ryzyka między sektorami.

3. Forum nadzoru przedkłada kompleksowe wskaźniki referencyjne kluczowych zewnętrznych dostawców usług ICT, które mają zostać przyjęte przez Wspólny Komitet jako wspólne stanowiska Europejskich Urzędów Nadzoru zgodnie z art. 56 akapit pierwszy rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

4. W skład forum nadzoru wchodzą Przewodniczący każdego z Europejskich Urzędów Nadzoru oraz po jednym przedstawicielu wysokiego szczebla z aktualnego personelu stosownego właściwego organu z każdego państwa członkowskiego. W forum nadzoru jako obserwatorzy uczestniczą dyrektorzy wykonawczy każdego Europejskiego Urzędu Nadzoru oraz po jednym przedstawicielu z Komisji Europejskiej, ERRS, EBC i ENISA.

5. Zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 Europejskie Urzędy Nadzoru wydają wytyczne w zakresie współpracy między Europejskimi Urzędami Nadzoru i właściwymi organami na potrzeby niniejszej sekcji dotyczące szczegółowych procedur i warunków odnoszących się do wykonywania zadań między właściwymi organami i Europejskimi Urzędami Nadzoru oraz szczegółów wymiany informacji niezbędnych dla właściwych organów do zapewnienia działań następczych w związku z zaleceniami skierowanymi przez wiodący organ nadzorczy na podstawie art. 31 ust. 1 lit. d) do kluczowych zewnętrznych dostawców usług ICT.

6. Wymogi określone w niniejszej sekcji pozostają bez uszczerbku dla stosowania dyrektywy (UE) 2016/1148 i nie naruszają innych unijnych przepisów dotyczących nadzoru mających zastosowanie do dostawców usług w chmurze.

7. Za pośrednictwem Wspólnego Komitetu i na podstawie prac przygotowawczych przeprowadzonych przez forum nadzoru Europejskie Urzędy Nadzoru każdego roku przedstawiają Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie na temat stosowania przepisów niniejszej sekcji.

Artykuł 30

Zadania wiodącego organu nadzorczego

1. Wiodący organ nadzorczy ocenia, czy każdy z kluczowych zewnętrznych dostawców usług ICT wprowadził kompleksowe, rozsądne i skuteczne zasady, procedury, mechanizmy i ustalenia służące do zarządzania ryzykiem związanym z ICT, które dostawca ten może stanowić dla podmiotów finansowych.

2. Ocena, o której mowa w ust. 1, obejmuje:

   a) wymogi z zakresu ICT mające na celu zapewnienie w szczególności bezpieczeństwa, dostępności, ciągłości, skalowalności i jakości usług, które zewnętrzny dostawca usług ICT świadczy na rzecz podmiotów finansowych, jak również możliwości utrzymania przez cały czas wysokich standardów bezpieczeństwa, poufności i integralności danych;

   b) bezpieczeństwo fizyczne mające wpływ na zapewnienie bezpieczeństwa ICT, w tym bezpieczeństwo obiektów, urządzeń i ośrodków przetwarzania danych;

   c) procesy zarządzania ryzykiem, w tym strategie zarządzania ryzykiem związanym z ICT, ciągłość działania ICT oraz plany przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej w zakresie ICT;

   d) zasady zarządzania obejmujące strukturę organizacyjną z wyraźnymi, przejrzystymi i spójnymi obszarami odpowiedzialności i zasadami rozliczalności umożliwiającą skuteczne zarządzanie ryzykiem związanym z ICT;

e) identyfikację i monitorowanie incydentów związanych z ICT oraz ich szybkie zgłaszanie podmiotom finansowym, zarządzanie tymi incydentami i rozwiązywanie tych incydentów, w szczególności cyberataków;

f) mechanizmy przenoszenia danych oraz możliwości przenoszenia aplikacji i ich interoperacyjność, które zapewniają skuteczne wykonywanie praw do odstąpienia od umowy przez podmioty finansowe;

g) testowanie systemów, infrastruktury i kontroli ICT;

h) audyty ICT;

i) stosowanie odnośnych krajowych i międzynarodowych norm mających zastosowanie do świadczenia usług ICT na rzecz podmiotów finansowych.

3. Na podstawie oceny, o której mowa w ust. 1, wiodący organ nadzorczy przyjmuje jasny, szczegółowy i uzasadniony indywidualny plan nadzoru dla każdego kluczowego zewnętrznego dostawcy usług ICT. Każdego roku plan ten przekazuje się każdemu z kluczowych zewnętrznych dostawców usług ICT.

4. Po uzgodnieniu i przekazaniu rocznych planów nadzoru, o których mowa w ust. 3, kluczowym zewnętrznym dostawcom usług ICT właściwe organy mogą zastosować środki dotyczące kluczowych zewnętrznych dostawców usług ICT wyłącznie w porozumieniu z wiodącym organem nadzorczym.

Artykuł 31

Uprawnienia wiodącego organu nadzorczego

1. Na potrzeby wykonywania obowiązków określonych w niniejszej sekcji wiodący organ nadzorczy posiada uprawnienia do:

a) występowania z wnioskiem o przekazanie wszystkich stosownych informacji i dokumentów zgodnie z art. 32;

b) prowadzenia ogólnych dochodzeń i kontroli zgodnie z art. 33 i 34;

c) występowania z wnioskiem o złożenie sprawozdań po zakończeniu działań nadzorczych, w których omówiono działania podjęte lub środki zaradcze wdrożone przez kluczowych zewnętrznych dostawców usług ICT w związku z zaleceniami, o których mowa w lit. d) niniejszego ustępu;

d) kierowania zaleceń dotyczących obszarów, o których mowa w art. 30 ust. 2, odnoszących się w szczególności do:

(i) stosowania szczególnych wymogów lub procesów z zakresu bezpieczeństwa i jakości ICT, zwłaszcza w związku z wprowadzaniem poprawek, aktualizacji, szyfrowania i innych środków bezpieczeństwa, które wiodący organ nadzorczy uważa za istotne dla zapewnienia bezpieczeństwa ICT usług świadczonych na rzecz podmiotów finansowych;

(ii) korzystania z warunków i zasad, w tym ich technicznego wdrożenia, zgodnie z którymi kluczowi zewnętrzni dostawcy usług ICT świadczą usługi na rzecz podmiotów finansowych, które wiodący organ nadzorczy uważa za istotne dla zapobiegania powstawaniu pojedynczych punktów awarii lub ich nasileniu, lub dla minimalizowania potencjalnego wpływu

systemowego na cały sektor finansowy Unii w przypadku ryzyka koncentracji w obszarze ICT;

(iii) po przeprowadzeniu analizy zgodnie z art. 32 i 33 dotyczącej umów podwykonawstwa, w tym umów podoutsourcingu, które kluczowi zewnętrzni dostawcy usług ICT zamierzają zawrzeć z innymi zewnętrznymi dostawcami usług ICT lub z podwykonawcami usług ICT z siedzibą w państwie trzecim – wszelkiego planowanego podwykonawstwa, w tym podoutsourcingu, w przypadku którego wiodący organ nadzorczy uważa, że dalsze podwykonawstwo może wywołać ryzyko dla świadczenia usług przez podmiot finansowy lub ryzyko dla stabilności finansowej;

(iv) odstąpienia od zawarcia umowy dalszego podwykonawstwa, jeżeli spełnione są łącznie poniższe warunki:

– przewidzianym podwykonawcą jest zewnętrzny dostawca usług ICT lub podwykonawca usług ICT z siedzibą w państwie trzecim;

– podwykonawstwo dotyczy kluczowej lub ważnej funkcji podmiotu finansowego.

2. Przed wykonaniem uprawnień, o których mowa w ust. 1, wiodący organ nadzorczy konsultuje się z forum nadzoru.

3. Kluczowi zewnętrzni dostawcy usług ICT współpracują w dobrej wierze z wiodącym organem nadzorczym i pomagają mu w wykonywaniu jego zadań.

4. Wiodący organ nadzorczy może nałożyć okresową karę pieniężną, aby nakłonić kluczowego zewnętrznego dostawcę usług ICT do zachowania zgodności z ust. 1 lit. a), b) i c).

5. Okresowa kara pieniężna, o której mowa w ust. 4, jest nakładana za każdy dzień do czasu osiągnięcia zgodności i nie dłużej niż przez sześć miesięcy po powiadomieniu kluczowego zewnętrznego dostawcy usług ICT.

6. Kwota okresowej kary pieniężnej, naliczana od dnia określonego w decyzji nakładającej okresową karę pieniężną, wynosi 1 % średniego dziennego światowego obrotu kluczowego zewnętrznego dostawcy usług ICT w poprzedzającym roku obrotowym.

7. Okresowe kary pieniężne mają charakter administracyjny i podlegają egzekucji. Przebieg postępowania egzekucyjnego regulują przepisy dotyczące postępowania cywilnego obowiązujące w państwie członkowskim, na którego terytorium prowadzone są kontrole i dostęp. Do rozpatrywania skarg dotyczących nieprawidłowego przeprowadzania postępowania egzekucyjnego właściwe są sądy danego państwa członkowskiego. Kwoty okresowych kar pieniężnych przypisuje się do budżetu ogólnego Unii Europejskiej.

8. Europejskie Urzędy Nadzoru podają do wiadomości publicznej każdą nałożoną okresową karę pieniężną, chyba że takie publiczne ujawnienie zagrażałoby poważnie rynkom finansowym lub wyrządziłoby nieproporcjonalną szkodę stronom, których dotyczy.

9. Przed nałożeniem okresowej kary pieniężnej na podstawie ust. 4 wiodący organ nadzorczy musi zapewnić przedstawicielom kluczowego zewnętrznego dostawcy usług ICT, wobec którego toczy się postępowanie, możliwość bycia wysłuchanym

w sprawie ustaleń i musi oprzeć swoją decyzję wyłącznie na ustaleniach, do których kluczowy zewnętrzny dostawca usług ICT objęty postępowaniem miał szansę się odnieść. W postępowaniu w pełni przestrzega się prawa do obrony osób, których dotyczy postępowanie. Osobom tym przysługuje prawo dostępu do akt sprawy, z zastrzeżeniem prawnie uzasadnionego interesu innych osób w zakresie ochrony ich tajemnicy handlowej. Prawo dostępu do akt sprawy nie obejmuje dostępu do informacji poufnych ani wewnętrznych dokumentów przygotowawczych wiodącego organu nadzorczego.

Artykuł 32
Wniosek o informacje

1. Wiodący organ nadzorczy może w drodze zwykłego wniosku lub decyzji zobowiązać kluczowych zewnętrznych dostawców usług ICT do przekazania wszelkich informacji, które są niezbędne dla wiodącego organu nadzorczego do wykonywania jego obowiązków wynikających z niniejszego rozporządzenia, w tym wszystkich stosownych dokumentów przedsiębiorstwa lub dokumentów operacyjnych, umów, dokumentacji strategii, sprawozdań z audytu dotyczącego bezpieczeństwa ICT, sprawozdań z incydentów związanych z ICT, jak również wszelkich informacji na temat stron, którym kluczowy zewnętrzny dostawca usług ICT zlecał funkcje lub działania operacyjne.

2. Wysyłając zwykły wniosek o przekazanie informacji, o którym mowa w ust. 1, wiodący organ nadzorczy:

   a) odwołuje się do niniejszego artykułu jako podstawy prawnej wniosku;

   b) podaje cel tego wniosku;

   c) określa, jakie informacje są wymagane;

   d) wskazuje termin przekazania informacji;

   e) informuje przedstawiciela kluczowego zewnętrznego dostawcy usług ICT, do którego zwraca się z wnioskiem o informacje, że nie jest on zobowiązany do ich przekazania, lecz w przypadku dobrowolnej odpowiedzi na wniosek przekazane informacje nie mogą być niezgodne z prawdą ani mylące.

3. Wzywając w drodze decyzji do przekazania informacji zgodnie z ust. 1, wiodący organ nadzorczy:

   a) odwołuje się do niniejszego artykułu jako podstawy prawnej wniosku;

   b) podaje cel tego wniosku;

   c) określa, jakie informacje są wymagane;

   d) wskazuje termin przekazania informacji;

   e) wskazuje okresowe kary pieniężne przewidziane w art. 31 ust. 4, w przypadku gdy przekazane wymagane informacje są niekompletne;

   f) informuje o prawie do odwołania od decyzji do Komisji Odwoławczej Europejskiego Urzędu Nadzoru i prawie do zaskarżenia tej decyzji do Trybunału Sprawiedliwości Unii Europejskiej („Trybunał Sprawiedliwości”) zgodnie z art. 60 i 61 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

4. Przedstawiciele kluczowych zewnętrznych dostawców usług ICT muszą przekazać wymagane informacje. Prawnicy należycie upoważnieni do działania mogą przekazać informacje w imieniu swoich klientów. Kluczowy zewnętrzny dostawca usług ICT pozostaje w pełni odpowiedzialny, jeżeli przekazane informacje są niepełne, niezgodne z prawdą lub mylące.

5. Wiodący organ nadzorczy niezwłocznie przesyła kopię decyzji, w której wzywa do przekazania informacji, organom właściwym dla podmiotów finansowych, które korzystają z usług kluczowego zewnętrznego dostawcy usług ICT.

Artykuł 33
Dochodzenia ogólne

1. W celu wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia wiodący organ nadzorczy, przy wsparciu zespołu ds. kontroli, o którym mowa w art. 34 ust. 1, może prowadzić wszelkie niezbędne dochodzenia względem zewnętrznych dostawców usług ICT.

2. Wiodący organ nadzorczy jest uprawniony do:

   a) wglądu w dokumenty, dane, procedury i wszelkie inne materiały istotne z punktu widzenia realizacji swoich zadań, niezależnie od nośnika, na jakim są one przechowywane;

   b) wykonania lub uzyskania uwierzytelnionych kopii lub wyciągów z takich dokumentów, danych, procedur i innych materiałów;

   c) wzywania przedstawicieli zewnętrznego dostawcy usług ICT w celu złożenia przez nich ustnych lub pisemnych wyjaśnień na temat sytuacji faktycznej lub dokumentów związanych z przedmiotem i celem dochodzenia oraz do zaprotokołowania odpowiedzi;

   d) prowadzenia rozmów z wszelkimi innymi osobami fizycznymi lub prawnymi, które wyrażą na to zgodę, w celu pozyskania informacji dotyczących przedmiotu dochodzenia;

   e) żądania rejestrów połączeń telefonicznych i przesyłu danych.

3. Urzędnicy wiodącego organu nadzorczego i inne osoby upoważnione przez ten organ do prowadzenia dochodzeń, o których mowa w ust. 1, wykonują swoje uprawnienia po przedstawieniu pisemnego upoważnienia określającego przedmiot i cel dochodzenia.

   W upoważnieniu tym wskazuje się również okresowe kary pieniężne przewidziane w art. 31 ust. 4, nakładane w przypadku, gdy wymagane dokumenty, dane, procedury lub inne materiały lub odpowiedzi na pytania zadane przedstawicielom zewnętrznego dostawcy usług ICT nie zostaną przekazane bądź udzielone lub są niepełne.

4. Przedstawiciele zewnętrznego dostawcy usług ICT mają obowiązek poddać się dochodzeniom na mocy decyzji wiodącego organu nadzorczego. W decyzji określa się przedmiot i cel dochodzenia, okresowe kary pieniężne przewidziane w art. 31 ust. 4 i środki odwoławcze dostępne na mocy rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 oraz wskazuje się na prawo do zaskarżenia decyzji do Trybunału Sprawiedliwości.

5. Z odpowiednim wyprzedzeniem przed rozpoczęciem dochodzenia wiodący organ nadzorczy informuje organy właściwe dla podmiotów finansowych, które korzystają

z usług danego zewnętrznego dostawcy usług ICT, o samym dochodzeniu i o tożsamości upoważnionych osób.

Artykuł 34
Kontrole na miejscu

1. W celu wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia wiodący organ nadzorczy, przy wsparciu zespołów ds. kontroli, o których mowa w art. 35 ust. 1, może wejść do lokali, na grunty lub do nieruchomości stanowiących miejsce prowadzenia działalności gospodarczej zewnętrznych dostawców usług ICT, takich jak siedziby, centra operacyjne i lokale dodatkowe, oraz przeprowadzać w nich wszystkie niezbędne kontrole na miejscu, a także przeprowadzać kontrole poza godzinami prowadzenia działalności.

2. Urzędnicy wiodącego organu nadzorczego i inne osoby upoważnione przez ten organ do przeprowadzenia kontroli na miejscu mogą wejść do takich lokali, na grunty lub do nieruchomości stanowiących miejsce prowadzenia działalności gospodarczej i mają oni wszelkie prawa do pieczętowania wszelkich lokali stanowiących miejsce prowadzenia działalności gospodarczej oraz wszelkich ksiąg lub dokumentów na czas kontroli i w zakresie koniecznym do jej przeprowadzenia.

   Wykonują oni swoje uprawnienia po przedstawieniu pisemnego upoważnienia określającego przedmiot i cel kontroli oraz okresowe kary pieniężne przewidziane w art. 31 ust. 4, które podlegają nałożeniu w przypadku, gdy przedstawiciele odnośnych zewnętrznych dostawców usług ICT nie poddadzą się kontroli.

3. Z odpowiednim wyprzedzeniem przed rozpoczęciem kontroli wiodący organ nadzorczy informuje organy właściwe dla podmiotów finansowych, które korzystają z usług danego zewnętrznego dostawcy usług ICT.

4. Kontrole obejmują pełen zakres stosownych systemów, sieci, urządzeń, informacji i danych związanych z ICT wykorzystywanych do świadczenia usług na rzecz podmiotów finansowych albo mających wpływ na świadczenie tych usług.

5. Przed każdą planowaną kontrolą na miejscu wiodący organ nadzorczy powiadamia z odpowiednim wyprzedzeniem danego kluczowego zewnętrznego dostawcę usług ICT, chyba że takie powiadomienie jest niemożliwe ze względu na nadzwyczajną lub kryzysową sytuację, lub jeżeli prowadziłoby do sytuacji, w której kontrola lub audyt nie byłyby już skuteczne.

6. Kluczowy zewnętrzny dostawca usług ICT jest zobowiązany poddać się kontrolom na miejscu zarządzonym na mocy decyzji wiodącego organu nadzorczego. W decyzji tej określa się przedmiot i cel kontroli, datę jej rozpoczęcia oraz okresowe kary pieniężne przewidziane w art. 31 ust. 4, środki odwoławcze dostępne na mocy rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 oraz prawo do zaskarżenia decyzji do Trybunału Sprawiedliwości.

7. Jeżeli urzędnicy wiodącego organu nadzorczego i inne osoby upoważnione przez ten organ stwierdzą, że kluczowy zewnętrzny dostawca usług ICT sprzeciwia się kontroli zarządzonej na mocy niniejszego artykułu, wiodący organ nadzorczy informuje kluczowego zewnętrznego dostawcę usług ICT o konsekwencjach takiego sprzeciwu, w tym o możliwości wypowiedzenia przez organy właściwe dla odnośnych podmiotów finansowych ustaleń umownych zawartych z danym kluczowym zewnętrznym dostawcą usług ICT.

Artykuł 35

Bieżący nadzór

1. Przy przeprowadzaniu dochodzeń ogólnych lub kontroli na miejscu wiodące organy nadzorcze są wspierane przez zespół ds. kontroli ustanowiony dla każdego z kluczowych zewnętrznych dostawców usług ICT.

2. Wspólny zespół ds. kontroli, o którym mowa w ust. 1, składa się z pracowników zatrudnionych w wiodącym organie nadzorczym i w odpowiednich właściwych organach nadzorujących podmioty finansowe, ma rzecz których kluczowy zewnętrzny dostawca usług ICT świadczy usługi, którzy to pracownicy dołączą do przygotowywania i wykonywania działań nadzorczych, przy czym do zespołu może należeć maksymalnie 10 członków. Wszyscy członkowie wspólnego zespołu badawczego muszą posiadać wiedzę fachową z zakresu ICT i ryzyka operacyjnego. Prace wspólnego zespołu ds. kontroli podlegają koordynacji wyznaczonego pracownika Europejskiego Urzędu Nadzoru („koordynator ze strony wiodącego organu nadzorczego").

3. Za pośrednictwem Wspólnego Komitetu Europejskie Urzędy Nadzoru opracowują wspólne projekty regulacyjnych standardów technicznych, aby doprecyzować wyznaczenie członków wspólnego zespołu ds. kontroli z odpowiednich właściwych organów, jak również zadania i ustalenia robocze zespołu ds. kontroli. Europejskie Urzędy Nadzoru przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r.

   Komisja jest uprawniona do przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie pierwszym, zgodnie z art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

4. W terminie trzech miesięcy od zakończenia dochodzenia lub kontroli na miejscu wiodący organ nadzorczy, po konsultacji z forum nadzoru, przyjmuje zalecenia, które mają być skierowane przez wiodący organ nadzorczy do kluczowego zewnętrznego dostawcy usług ICT na podstawie uprawnień, o których mowa w art. 31.

5. Zalecenia, o których mowa w ust. 4, bezzwłocznie przekazuje się kluczowemu zewnętrznemu dostawcy usług ICT oraz organom właściwym dla podmiotów finansowych, na rzecz których dostawca ten świadczy swoje usługi.

   Do celów wykonania działań nadzorczych wiodący organ nadzorczy może uwzględnić wszelkie stosowne certyfikacje wydane przez stronę trzecią oraz sprawozdania z wewnętrznych lub zewnętrznych audytów dotyczących usług ICT świadczonych przez stronę trzecią udostępnione przez kluczowego zewnętrznego dostawcę usług ICT.

Artykuł 36

Harmonizacja warunków umożliwiających prowadzenie nadzoru

1. Za pośrednictwem Wspólnego Komitetu Europejskie Urzędy Nadzoru opracowują projekty regulacyjnych standardów technicznych określających:

a) informacje, które kluczowy zewnętrzny dostawca usług ICT musi zawrzeć we wniosku o dobrowolne przystąpienie określonym w art. 28 ust. 8;

b) treść i format sprawozdań, o które można się zwrócić do celów art. 31 ust. 1 lit. c);

c) przedstawienie informacji, w tym strukturę, formaty i metody, których przedłożenia, ujawnienia lub zgłoszenia wymaga się od kluczowego zewnętrznego dostawcy usług ICT na podstawie art. 31 ust. 1;

d) szczegóły przeprowadzonej przez właściwe organy oceny środków wprowadzonych przez kluczowego zewnętrznego dostawcę usług ICT w następstwie zaleceń wydanych przez wiodący organ nadzorczy na podstawie art. 37 ust. 2.

2. Europejskie Urzędy Nadzoru przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 1 stycznia 20xx r. [*Urząd Publikacji.: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*]

Komisji przekazuje się uprawnienia do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w akapicie pierwszym, zgodnie z procedurą określoną w art. 10–14 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010.

Artykuł 37

Działania następcze podejmowane przez właściwe organy

1. W terminie 30 dni kalendarzowych od otrzymania zaleceń wydanych przez wiodący organ nadzorczy na podstawie art. 31 ust. 1 lit. d) kluczowi zewnętrzni dostawcy usług ICT powiadamiają wiodący organ nadzorczy o tym, czy zamierzają zastosować się do tych zaleceń. Wiodące organy nadzorcze niezwłocznie przekazują tę informację właściwym organom.

2. Właściwe organy monitorują, czy podmioty finansowe uwzględniają ryzyko zidentyfikowane w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT przez wiodący organ nadzorczy zgodnie z art. 31 ust. 1 lit. d).

3. Zgodnie z art. 44 właściwe organy mogą zobowiązać podmioty finansowe do tymczasowego zawieszenia, w części albo w całości, korzystania z usługi świadczonej przez kluczowego zewnętrznego dostawcę usług ICT lub jej wdrażania do czasu wyeliminowania ryzyka zidentyfikowanego w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT Gdy zachodzi taka konieczność, właściwe organy mogą nakazać podmiotom finansowym wypowiedzenie, w części lub w całości, stosownych ustaleń umownych zawartych z kluczowymi zewnętrznymi dostawcami usług ICT.

4. Podejmując decyzje, o których mowa w ust. 3, właściwe organy biorą pod uwagę rodzaj i skalę ryzyka, które nie zostało wyeliminowane przez kluczowego zewnętrznego dostawcę usług ICT, a także istotność braku zgodności, uwzględniając następujące kryteria:

a) wagę braku zgodności i czas jego trwania;

b) kwestię, czy brak zgodności ujawnił poważne słabości w procedurach, systemach zarządzania, zarządzaniu ryzykiem i kontrolach wewnętrznych kluczowego zewnętrznego dostawcy usług ICT;

c) kwestię, czy brak zgodności doprowadził do przestępstwa finansowego lub ułatwił przestępstwo finansowe lub jest w inny sposób związany z takim przestępstwem;

d) kwestię, czy brak zgodności jest wynikiem działania umyślnego lub zaniedbania.

5. Właściwe organy regularnie informują wiodące organy nadzorcze o podejściach i środkach, które zastosowały w ramach swoich zadań nadzorczych w odniesieniu do podmiotów finansowych, jak również o środkach umownych zastosowanych przez te podmioty, w przypadku gdy kluczowy zewnętrzny dostawca usług ICT nie uznał, w części lub w całości, zaleceń skierowanych przez wiodące organy nadzorcze.

Artykuł 38
Opłaty nadzorcze

1. Europejskie Urzędy Nadzoru pobierają od kluczowych zewnętrznych dostawców usług ICT opłaty, które w pełni pokrywają niezbędne wydatki Europejskich Urzędów Nadzoru związane z wykonywaniem zadań nadzorczych na podstawie niniejszego rozporządzenia, w tym zwrot wszelkich kosztów, które mogą zostać poniesione w wyniku prac prowadzonych przez właściwe organy przystępujące do działań nadzorczych zgodnie z art. 35.

Wysokość opłaty pobieranej od kluczowego zewnętrznego dostawcy usług ICT pozwala na pokrycie wszystkich kosztów administracyjnych oraz jest proporcjonalna do jego obrotów.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 50 w celu uzupełnienia niniejszego rozporządzenia poprzez określenie wysokości opłat oraz sposobu ich uiszczania.

Artykuł 39
Współpraca międzynarodowa

1. EUNB, ESMA i EIOPA mogą zgodnie z art. 33 odpowiednio rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 zawrzeć porozumienia administracyjne z organami regulacyjnymi i organami nadzoru państw trzecich, aby wspierać współpracę międzynarodową w obszarze ryzyka ze strony zewnętrznych dostawców usług ICT w różnych sektorach finansowych, w szczególności przez opracowanie najlepszych praktyk dotyczących przeglądu praktyk zarządzania ryzykiem związanym z ICT i przeglądu kontroli takiego ryzyka, środków ograniczających takie ryzyko i reakcji na incydenty związane z takim ryzykiem.

2. Za pośrednictwem Wspólnego Komitetu Europejskie Urzędy Nadzoru co pięć lat przedkładają Parlamentowi Europejskiemu, Radzie i Komisji wspólne poufne sprawozdanie, w którym podsumowują ustalenia ze stosownych rozmów przeprowadzonych z organami państw trzecich, o których mowa w ust. 1, koncentrując się na rozwoju ryzyka ze strony zewnętrznych dostawców usług ICT

i następstwach dla stabilności finansowej, integralności rynku, ochrony inwestorów lub funkcjonowania jednolitego rynku.

ROZDZIAŁ VI

USTALENIA DOTYCZĄCE WYMIANY INFORMACJI

Artykuł 40

Ustalenia dotyczące wymiany informacji odnoszące się do informacji o cyberzagrożeniu i wyników analiz takiego cyberzagrożenia

1. Podmioty finansowe mogą wymieniać między sobą informacje o cyberzagrożeniu i wyniki analiz takiego cyberzagrożenia, w tym oznaki naruszenia integralności systemu, taktykę, techniki i procedury, ostrzeżenia dotyczące cyberbezpieczeństwa oraz narzędzia konfiguracji w zakresie, w jakim wymiana takich informacji i wyników analiz:

   a) ma na celu zwiększenie operacyjnej odporności cyfrowej podmiotów finansowych, w szczególności poprzez zwiększanie świadomości w odniesieniu do cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się zdolności do stwarzania cyberzagrożeń, wspieranie zakresu możliwości obronnych podmiotów finansowych, techniki wykrywania zagrożenia, strategie jego minimalizowania lub etapy reagowania i przywracania gotowości do pracy;

   b) odbywa się w zaufanych społecznościach podmiotów finansowych;

   c) jest realizowana za pośrednictwem ustaleń dotyczących wymiany informacji, które chronią potencjalnie poufny charakter wymienianych informacji i które są regulowane przez zasady prowadzenia działalności z pełnym poszanowaniem tajemnicy przedsiębiorstwa, ochrony danych osobowych[48] i wytycznych dotyczących polityki konkurencji[49].

2. Na potrzeby ust. 1 lit. c) ustalenia dotyczące wymiany informacji określają warunki przystąpienia i w stosownych przypadkach przewidują szczegóły uczestnictwa organów publicznych i możliwości włączenia ich do ustaleń dotyczących wymiany informacji, a także szczegóły elementów operacyjnych, w tym korzystania ze specjalnych platform informatycznych.

3. Podmioty finansowe powiadamiają właściwe organy o swoim przystąpieniu do ustaleń dotyczących wymiany informacji, o których mowa w ust. 1, po zatwierdzeniu ich członkostwa lub, w stosownych przypadkach, o ustaniu ich członkostwa, gdy stanie się ono skuteczne.

---

48 Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

49 Komunikat Komisji – Wytyczne w sprawie stosowania art. 101 Traktatu o funkcjonowaniu Unii Europejskiej do horyzontalnych porozumień kooperacyjnych, 2011/C 11/01.

ROZDZIAŁ VII

WŁAŚCIWE ORGANY

Artykuł 41

Właściwe organy

Nie naruszając przepisów dotyczących ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, o których mowa w rozdziale V sekcja II niniejszego rozporządzenia, zgodność z obowiązkami określonymi w niniejszym rozporządzeniu zapewniają następujące właściwe organy zgodnie z uprawnieniami przyznanymi im na mocy odnośnych aktów prawnych:

a) w odniesieniu do instytucji kredytowych – właściwy organ wyznaczony zgodnie z art. 4 dyrektywy 2013/36/UE, bez uszczerbku dla szczególnych zadań powierzonych EBC na mocy rozporządzenia (UE) nr 1024/2013;

b) w odniesieniu do dostawców usług płatniczych – właściwy organ wyznaczony zgodnie z art. 22 dyrektywy (UE) 2015/2366;

c) w odniesieniu do instytucji pieniądza elektronicznego – właściwy organ wyznaczony zgodnie z art. 37 dyrektywy 2009/110/WE;

d) w odniesieniu do firm inwestycyjnych – właściwy organ wyznaczony zgodnie z art. 4 dyrektywy (UE) 2019/2034;

e) w odniesieniu do dostawców usług w zakresie kryptoaktywów, emitentów kryptoaktywów, emitentów tokenów powiązanych z aktywami oraz emitentów znaczących tokenów powiązanych z aktywami – właściwy organ wyznaczony zgodnie z art. 3 ust. 1 lit. ee) tiret pierwsze [*rozporządzenia (UE) 20xx w sprawie rynków kryptoaktywów (MiCA)*];

f) w odniesieniu do centralnych depozytów papierów wartościowych – właściwy organ wyznaczony zgodnie z art. 11 rozporządzenia (UE) nr 909/2014;

g) w odniesieniu do kontrahentów centralnych – właściwy organ wyznaczony zgodnie z art. 22 rozporządzenia (UE) nr 648/2012;

h) w odniesieniu do systemów obrotu i dostawców usług w zakresie udostępniania informacji – właściwy organ wyznaczony zgodnie z art. 67 dyrektywy 2014/65/UE;

i) w odniesieniu do repozytoriów transakcji – właściwy organ wyznaczony zgodnie z art. 55 rozporządzenia (UE) nr 648/2012;

j) w odniesieniu do zarządzających alternatywnymi funduszami inwestycyjnymi – właściwy organ wyznaczony zgodnie z art. 44 dyrektywy 2011/61/UE;

k) w odniesieniu do spółek zarządzających – właściwy organ wyznaczony zgodnie z art. 97 dyrektywy 2009/65/WE;

l) w odniesieniu do zakładów ubezpieczeń i zakładów reasekuracji – właściwy organ wyznaczony zgodnie z art. 30 dyrektywy 2009/138/WE;

m) w odniesieniu do pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające – właściwy organ wyznaczony zgodnie z art. 12 dyrektywy (UE) 2016/97;

n) w odniesieniu do instytucji pracowniczych programów emerytalnych – właściwy organ wyznaczony zgodnie z art. 47 dyrektywy 2016/2341;

o) w odniesieniu do agencji ratingowych – właściwy organ wyznaczony zgodnie z art. 21 rozporządzenia (WE) nr 1060/2009;

p) w odniesieniu do biegłych rewidentów i firm audytorskich – właściwy organ wyznaczony zgodnie z art. 3 ust. 2 i art. 32 dyrektywy 2006/43/WE;

q) w odniesieniu do administratorów kluczowych wskaźników referencyjnych – właściwy organ wyznaczony zgodnie z art. 40 i 41 *rozporządzenia xx/202x*;

r) w odniesieniu do dostawców usług finansowania społecznościowego – właściwy organ wyznaczony zgodnie z *art. x rozporządzenia xx/202x*;

s) w odniesieniu do repozytoriów sekurytyzacji – właściwy organ wyznaczony zgodnie z art. 10 i art. 14 ust. 1 rozporządzenia (UE) 2017/2402.

Artykuł 42

Współpraca ze strukturami i organami ustanowionymi na mocy dyrektywy (UE) 2016/1148

1. Aby usprawnić współpracę i umożliwić wymianę informacji na temat nadzoru między właściwymi organami wyznaczonymi zgodnie z niniejszym rozporządzeniem i grupą współpracy ustanowioną na mocy art. 11 dyrektywy (UE) 2016/1148, Europejskie Urzędy Nadzoru i właściwe organy mogą zwrócić się o zaproszenie do udziału w pracach grupy współpracy.

2. W stosownych przypadkach właściwe organy mogą konsultować się z pojedynczym punktem kontaktowym i krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego, o których mowa odpowiednio w art. 8 i 9 dyrektywy (UE) 2016/1148.

Artykuł 43

Ćwiczenia wykonywane między sektorami finansowymi oraz komunikacja i współpraca między tymi sektorami

1. Europejskie Urzędy Nadzoru, za pośrednictwem Wspólnego Komitetu i we współpracy z właściwymi organami, EBC i ERRS, mogą ustanowić mechanizmy umożliwiające wymianę skutecznych praktyk między sektorami finansowymi, aby zwiększyć orientację sytuacyjną i zidentyfikować wspólne dla sektorów finansowych luki i rodzaje ryzyka w cyberprzestrzeni.

   Mogą one opracować ćwiczenia z zakresu zarządzania kryzysowego i sytuacji awaryjnych obejmujące scenariusze cyberataków w celu wypracowania kanałów komunikacyjnych i stopniowego umożliwiania skutecznej skoordynowanej reakcji na poziomie UE w przypadku poważnego transgranicznego incydentu związanego z ICT lub powiązanego zagrożenia mającego systemowy wpływ na cały sektor finansowy Unii.

   Ćwiczenia te mogą w stosownych przypadkach służyć również zbadaniu zależności sektora finansowego od innych sektorów gospodarki.

2. Właściwe organy, EUNB, ESMA lub EIOPA i EBC ściśle współpracują ze sobą i wymieniają się informacjami na potrzeby wykonywania swoich obowiązków na podstawie art. 42–48. Ściśle koordynują one prowadzony przez siebie nadzór w celu

identyfikowania naruszeń niniejszego rozporządzenia oraz stosowania wobec nich środków naprawczych, a także w celu opracowywania i promowania najlepszych praktyk, ułatwiania współpracy, promowania spójnej interpretacji oraz zapewniania ocen przekrojowych dotyczących odnośnych jurysdykcji w przypadku jakichkolwiek sporów.

Artykuł 44

Kary administracyjne i środki naprawcze

1. Właściwe organy posiadają wszelkie uprawnienia do sprawowania nadzoru, prowadzenia dochodzeń i nakładania sankcji niezbędne do wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia.

2. Uprawnienia, o których mowa w ust. 1, obejmują co najmniej uprawnienia do:

   a) uzyskania dostępu do wszelkich dokumentów lub danych przechowywanych w jakiejkolwiek formie, które właściwy organ uważa za istotne z punktu widzenia wykonywania swoich obowiązków oraz do otrzymywania lub sporządzania ich duplikatów;

   b) przeprowadzania kontroli na miejscu lub dochodzeń;

   c) wymagania zastosowania środków naprawczych w odniesieniu do naruszeń wymogów określonych w niniejszym rozporządzeniu.

3. Bez uszczerbku dla prawa państw członkowskich do nakładania sankcji karnych zgodnie z art. 46, państwa członkowskie określają przepisy ustanawiające właściwe kary administracyjne i środki naprawcze w odniesieniu do naruszeń przepisów niniejszego rozporządzenia i zapewniają ich skuteczne stosowanie.

   Te sankcje i środki muszą być skuteczne, proporcjonalne i odstraszające.

4. Państwa członkowskie powierzają właściwym organom uprawnienie do stosowania kar administracyjnych lub środków naprawczych w przypadku naruszeń przepisów niniejszego rozporządzenia, obejmujących co najmniej:

   a) wydanie nakazu zobowiązującego osobę fizyczną lub prawną do zaprzestania danego postępowania oraz do powstrzymania się od ponownego podejmowania tego postępowania;

   b) wymaganie tymczasowego lub stałego zaprzestania wszelkiej praktyki lub postępowania, które właściwy organ uważa za sprzeczne z przepisami niniejszego rozporządzenia, oraz niedopuszczenie do ponownego podejmowania takiej praktyki lub postępowania;

   c) przyjęcie wszelkiego rodzaju środków, w tym o charakterze pieniężnym, mających zapewnić dalsze przestrzeganie wymogów prawnych przez podmioty finansowe;

   d) wymaganie, w zakresie, w jakim zezwala na to prawo krajowe, udostępnienia istniejących rejestrów przesyłu danych będących w posiadaniu operatora telekomunikacyjnego, w przypadku gdy istnieje uzasadnione podejrzenie naruszenia przepisów niniejszego rozporządzenia oraz w przypadku gdy takie rejestry mogą mieć znaczenie dla dochodzenia w sprawie naruszeń przepisów niniejszego rozporządzenia; oraz

e) wydanie publicznych ogłoszeń, w tym podanie do wiadomości publicznej informacji wskazującej tożsamość osoby fizycznej lub prawnej oraz charakter naruszenia.

5. W przypadku gdy przepisy, o których mowa w ust. 2 lit. c) i ust. 4, mają zastosowanie do osób prawnych, państwa członkowskie powierzają właściwym organom uprawnienie do stosowania kar administracyjnych i środków naprawczych, z zastrzeżeniem warunków przewidzianych w prawie krajowym, wobec członków organu zarządzającego oraz innych osób fizycznych, które w świetle prawa krajowego ponoszą odpowiedzialność za naruszenie.

6. Państwa członkowskie zapewniają, aby każda decyzja nakładająca kary administracyjne lub środki naprawcze określone w ust. 2 lit. c) była właściwie uzasadniona i podlegała prawu do odwołania.

Artykuł 45

Wykonywanie uprawnień do nakładania kar administracyjnych i środków naprawczych

1. Właściwe organy wykonują uprawnienia do nakładania kar administracyjnych i środków naprawczych, o których mowa w art. 44, zgodnie ze swoimi krajowymi ramami prawnymi, stosownie do sytuacji:

   a) bezpośrednio;

   b) we współpracy z innymi organami;

   c) w drodze przekazania uprawnień innym organom, zachowując odpowiedzialność za wykonanie tych uprawnień;

   d) poprzez wnoszenie spraw do właściwych organów sądowych.

2. Ustalając rodzaj i poziom kary administracyjnej lub środka naprawczego, które mają zostać nałożone na mocy art. 44, właściwe organy biorą pod uwagę zakres, w jakim dane naruszenie ma charakter umyślny lub jest wynikiem zaniedbania, a także wszystkie inne stosowne okoliczności, w tym również, w stosownych przypadkach:

   a) istotność i wagę naruszenia oraz czas jego trwania;

   b) stopień odpowiedzialności osoby fizycznej lub prawnej odpowiedzialnej za dane naruszenie;

   c) sytuację finansową odpowiedzialnej osoby fizycznej lub prawnej;

   d) skalę korzyści uzyskanych lub strat unikniętych przez odpowiedzialną osobę fizyczną lub prawną, o ile można je ustalić;

   e) straty poniesione przez osoby trzecie w wyniku naruszenia, o ile można je ustalić;

   f) poziom współpracy odpowiedzialnej osoby fizycznej lub prawnej z właściwym organem, bez uszczerbku dla konieczności zapewnienia wydania uzyskanych korzyści lub wyrównania strat unikniętych przez tę osobę;

   g) uprzednie naruszenia popełnione przez odpowiedzialną osobę fizyczną lub prawną.

Artykuł 46

Sankcje karne

1. Państwa członkowskie mogą zadecydować o nieustanowieniu przepisów dotyczących kar administracyjnych lub środków naprawczych w odniesieniu do naruszeń, które podlegają sankcjom karnym na podstawie ich prawa krajowego.

2. W przypadku gdy państwa członkowskie postanowiły ustanowić sankcje karne za naruszenia przepisów niniejszego rozporządzenia, zapewniają one wprowadzenie odpowiednich środków, tak aby właściwe organy miały wszystkie niezbędne uprawnienia do współdziałania z organami sądowymi, organami ścigania lub organami wymiaru sprawiedliwości w sprawach karnych w ramach ich jurysdykcji na potrzeby otrzymywania szczegółowych informacji dotyczących dochodzeń lub postępowań karnych wszczętych w związku z naruszeniami przepisów niniejszego rozporządzenia oraz przekazywania takich informacji innym właściwym organom, a także EUNB, ESMA lub EIOPA w celu wypełnienia swojego obowiązku współpracy do celów niniejszego rozporządzenia.

Artykuł 47

Obowiązki w zakresie powiadamiania

Państwa członkowskie powiadamiają Komisję, ESMA, EUNB i EIOPA o przepisach ustawowych, wykonawczych i administracyjnych wdrażających przepisy niniejszego rozdziału, w tym o odpowiednich przepisach prawa karnego, do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 1 rok od dnia wejścia w życie niniejszego rozporządzenia*] r. Państwa członkowskie bez zbędnej zwłoki powiadamiają Komisję, ESMA, EUNB i EIOPA o wszelkich późniejszych zmianach tych przepisów.

Artykuł 48

Publikowanie informacji o nałożonych karach administracyjnych

1. Właściwe organy bez zbędnej zwłoki publikują na swojej oficjalnej stronie internetowej każdą decyzję nakładającą kary administracyjne, wobec której, po tym jak adresat sankcji został powiadomiony o tej decyzji, nie zostało wniesione odwołanie.

2. Publikacja, o której mowa w ust. 1, zawiera informacje na temat rodzaju i charakteru naruszenia oraz tożsamości osób odpowiedzialnych, a także informacje o nałożonych karach.

3. Jeżeli po przeprowadzeniu indywidualnej oceny właściwy organ uzna, że publikacja tożsamości, w przypadku osób prawnych, lub tożsamości i danych osobowych, w przypadku osób fizycznych, byłaby nieproporcjonalna, zagrażałaby stabilności rynków finansowych lub prowadzeniu toczącego się postępowania przygotowawczego w sprawie karnej lub wyrządziłaby nieproporcjonalną szkodę, o ile można ją ustalić, stronom, których dotyczy, przyjmuje on jedno z poniższych rozwiązań w stosunku do decyzji nakładającej karę administracyjną:

   a) odracza jej publikację do momentu, kiedy wszystkie powody uzasadniające nieopublikowanie przestaną być aktualne;

   b) publikuje ją w formie zanonimizowanej zgodnie z prawem krajowym; lub

c) odstępuje od jej opublikowania, jeżeli możliwości określone w lit. a) i b) zostaną uznane za niewystarczające, aby zagwarantować brak wszelkiego zagrożenia dla stabilności rynków finansowych, albo w przypadku gdy publikacja nie byłaby proporcjonalna do łagodnego wymiaru nałożonej kary.

4. W przypadku decyzji o publikacji informacji o karze administracyjnej w formie zanonimizowanej zgodnie z ust. 3 lit. b), opublikowanie odpowiednich danych może zostać odłożone w czasie.

5. W przypadku gdy właściwy organ publikuje decyzję o nałożeniu kary administracyjnej, od której złożono odwołanie do odpowiedniego organu sądowego, właściwe organy niezwłocznie publikują na swojej oficjalnej stronie internetowej odpowiednią informację, a na dalszych etapach wszelkie późniejsze powiązane informacje o wyniku takiego odwołania. Publikuje się również wszelkie orzeczenia sądowe unieważniające decyzję o nałożeniu kary administracyjnej.

6. Właściwe organy zapewniają, by publikacja, o której mowa w ust. 1–4, była dostępna na ich oficjalnej stronie internetowej przez co najmniej pięć lat po jej dokonaniu. Opublikowane dane osobowe pozostawia się na oficjalnej stronie internetowej właściwego organu jedynie przez okres, który jest niezbędny zgodnie z mającymi zastosowanie przepisami o ochronie danych.

Artykuł 49

Tajemnica zawodowa

1. Wszelkie poufne informacje otrzymywane, wymieniane lub przekazywane na mocy niniejszego rozporządzenia podlegają warunkom zachowania tajemnicy zawodowej ustanowionym w ust. 2.

2. Obowiązek zachowania tajemnicy zawodowej ma zastosowanie do wszystkich osób, które pracują lub pracowały dla właściwych organów zgodnie z niniejszym rozporządzeniem lub dla dowolnego organu lub przedsiębiorstwa rynkowego bądź osoby fizycznej lub prawnej, którym te właściwe organy przekazały swoje uprawnienia, włącznie z zatrudnionymi przez nie audytorami i ekspertami.

3. Informacje objęte tajemnicą zawodową nie mogą zostać ujawnione jakiejkolwiek innej osobie ani jakiemukolwiek innemu organowi, z wyjątkiem przypadków określonych w prawie Unii lub prawie krajowym.

4. Wszystkie informacje wymieniane między właściwymi organami na podstawie niniejszego rozporządzenia, które dotyczą warunków biznesowych lub operacyjnych oraz innych kwestii gospodarczych lub osobistych, uznaje się za informacje poufne oraz obejmuje obowiązkiem zachowania tajemnicy zawodowej, z wyjątkiem przypadków gdy w momencie ich przekazania właściwy organ stwierdzi, że informacje te mogą być ujawnione lub ich ujawnienie jest niezbędne do celów postępowania sądowego.

ROZDZIAŁ VIII

AKTY DELEGOWANE

Artykuł 50

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 28 ust. 3 i art. 38 ust. 2, powierza się Komisji na okres pięciu lat od dnia [Urząd Publikacji: należy wstawić datę przypadającą 5 lat od dnia wejścia w życie niniejszego rozporządzenia] r.

3. Parlament Europejski lub Rada mogą w dowolnym czasie odwołać przekazanie uprawnień, o którym mowa w art. 28 ust. 3 i art. 38 ust. 2. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 28 ust. 3 lub art. 38 ust. 2 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

ROZDZIAŁ IX

PRZEPISY PRZEJŚCIOWE I KOŃCOWE

SEKCJA I

Artykuł 51

Klauzula przeglądowa

Do dnia [*Urząd Publikacji: należy wstawić datę przypadającą 5 lat od dnia wejścia w życie niniejszego rozporządzenia*] r., po konsultacji z EUNB, ESMA, EIOPA i ERRS, stosownie do przypadku, Komisja przeprowadza przegląd i przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w stosownych przypadkach wraz z wnioskiem ustawodawczym,

dotyczące kryteriów wyznaczania kluczowych zewnętrznych dostawców usług ICT określonych w art. 28 ust. 2.

SEKCJA II

ZMIANY

Artykuł 52

Zmiany w rozporządzeniu (WE) nr 1060/2009

W załączniku I do rozporządzenia (WE) nr 1060/2009 sekcja A pkt 4 akapit pierwszy otrzymuje brzmienie:

„Agencja ratingowa posiada prawidłowe procedury administracyjne i księgowe, mechanizmy kontroli wewnętrznej, skuteczne procedury oceny ryzyka i skuteczne rozwiązania w zakresie kontroli i bezpieczeństwa zarządzania systemami ICT zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/xx* [DORA].

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/xx [...] (Dz.U. L XX z DD.MM.RRRR, s. X).”.

Artykuł 53

Zmiany w rozporządzeniu (UE) nr 648/2012

W rozporządzeniu (UE) nr 648/2012 wprowadza się następujące zmiany:

1) w art. 26 wprowadza się następujące zmiany:

   a) ust. 3 otrzymuje brzmienie:

      „3. CCP utrzymuje i stosuje strukturę organizacyjną zapewniającą ciągłość działania oraz prawidłowe funkcjonowanie w zakresie świadczenia usług i prowadzenia działalności. CCP stosuje odpowiednie i proporcjonalne systemy, zasoby i procedury, w tym systemy ICT zarządzane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/xx* [DORA].

      * Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/xx [...] (Dz.U. L XX z DD.MM.RRRR, s. X).”;

   b) uchyla się ust. 6;

2) w art. 34 wprowadza się następujące zmiany:

   a) ust. 1 otrzymuje brzmienie:

      „1. CCP ustanawia, wprowadza i utrzymuje odpowiednią strategię na rzecz ciągłości działania oraz plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, które obejmują ciągłość działania w zakresie ICT oraz plany przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej związanej z ICT opracowane zgodnie z rozporządzeniem (UE) 2021/xx [DORA], które służą

zachowaniu pełnionych funkcji, szybkiemu przywróceniu działalności i wywiązywaniu się z obowiązków.”;

b) ust. 3 akapit pierwszy otrzymuje brzmienie:

„W celu zapewnienia spójnego stosowania niniejszego artykułu ESMA, po konsultacji z członkami ESBC, opracowuje projekt regulacyjnych standardów technicznych określających minimalny zakres i minimalne wymogi dotyczące strategii na rzecz ciągłości działania oraz planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, z wyjątkiem ciągłości działania w zakresie ICT i planów przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej związanej z ICT.”;

3) art. 56 ust. 3 akapit pierwszy otrzymuje brzmienie:

„3. W celu zapewnienia spójnego stosowania niniejszego artykułu ESMA opracowuje projekty regulacyjnych standardów technicznych określających szczegółowe informacje, inne niż informacje w przypadku wymogów w zakresie zarządzania ryzykiem związanym z ICT, dotyczące wniosku o rejestrację, o którym mowa w ust. 1.”;

4) art. 79 ust. 1 i 2 otrzymują brzmienie:

„1. Repozytorium transakcji określa źródła ryzyka operacyjnego i ogranicza je również dzięki opracowaniu odpowiednich systemów, kontroli i procedur, w tym systemów ICT zarządzanych zgodnie z rozporządzeniem (UE) 2021/xx *[DORA*].

2. Repozytorium transakcji ustanawia, wprowadza i stosuje odpowiednią strategię na rzecz ciągłości działania oraz plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, które obejmują ciągłość działania w zakresie ICT i plany przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej związanej z ICT ustanowione zgodnie z rozporządzeniem (UE) 2021/xx*[DORA],* służące zachowaniu pełnionych funkcji, szybkiemu przywróceniu działalności i wywiązywaniu się z obowiązków repozytorium transakcji.”;

5) w art. 80 uchyla się ust. 1.

Artykuł 54

Zmiany w rozporządzeniu (UE) nr 909/2014

W art. 45 rozporządzenia (UE) nr 909/2014 wprowadza się następujące zmiany:

1) ust. 1 otrzymuje brzmienie:

„1. CDPW identyfikuje źródła ryzyka operacyjnego, zarówno wewnętrzne, jak i zewnętrzne, oraz ogranicza do minimum ich wpływ również poprzez stosowanie odpowiednich narzędzi i procesów ICT oraz strategii w zakresie ICT ustanowionych i zarządzanych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/xx*[*DORA*], a także stosując wszelkie inne stosowne narzędzia, środki kontroli i procedury w odniesieniu do innych rodzajów ryzyka operacyjnego, w tym dla wszystkich systemów rozrachunku papierów wartościowych, które prowadzi.

* Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/xx [...] (Dz.U. L XX z DD.MM.RRRR, s. X).”;

2) uchyla się ust. 2;

3) ust. 3 i 4 otrzymują brzmienie:

„3. W odniesieniu do świadczonych przez siebie usług oraz dla każdego prowadzonego przez siebie systemu rozrachunku papierów wartościowych CDPW ustanawia, wprowadza i utrzymuje odpowiednią strategię ciągłości działania oraz plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, które obejmują ciągłość działania w zakresie ICT i plany przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej związanej z ICT ustanowione zgodnie z rozporządzeniem (UE) 2021/xx [DORA], aby zapewnić zachowanie swoich usług, szybkie przywrócenie działalności i wywiązywanie się z obowiązków CDPW w przypadku zdarzeń stwarzających poważne ryzyko zakłócenia działalności.

4. Plan, o którym mowa w ust. 3, pozwala na przywrócenie wszystkich transakcji i pozycji uczestników istniejących w momencie wystąpienia zakłócenia, tak aby umożliwić uczestnikom CDPW dalsze działanie z zachowaniem pewności oraz ukończenie rozrachunku w wyznaczonym terminie, w tym poprzez zapewnienie, by najważniejsze systemy informatyczne mogły wznowić operacje od momentu wystąpienia zakłócenia, jak przewidziano w art. 11 ust. 5 i 7 rozporządzenia (UE) 2021/xx [DORA].”;

4) ust. 6 akapit pierwszy otrzymuje brzmienie*:*

„CDPW identyfikuje i monitoruje ryzyka dla jego działalności, które mogą stwarzać najważniejsi uczestnicy prowadzonych przez niego systemów rozrachunku papierów wartościowych oraz dostawcy usług i mediów, a także inne CDPW lub inne infrastruktury rynkowe, oraz zarządza tymi ryzykami. Na żądanie przedstawia on właściwym i odpowiednim organom informacje dotyczące wszelkich takich zidentyfikowanych ryzyk. Niezwłocznie informuje on także właściwy organ i odpowiednie organy o wszelkich zdarzeniach operacyjnych, innych niż w odniesieniu do ryzyka związanego z ICT, wynikających z takich ryzyk.”;

5) ust. 7 akapit pierwszy otrzymuje brzmienie*:*

„EUNGiPW opracowuje, w ścisłej współpracy z członkami ESBC, projekty regulacyjnych standardów technicznych w celu określenia ryzyk operacyjnych, o których mowa w ust. 1 i 6, innych niż ryzyka związane z ICT, metod testowania, usuwania lub ograniczania do minimum tych ryzyk, w tym strategii ciągłości działania i planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, o których mowa w ust. 3 i 4, oraz metod ich oceny.”.

Artykuł 55

Zmiany w rozporządzeniu (UE) nr 600/2014

W rozporządzeniu (UE) nr 600/2014 wprowadza się następujące zmiany:

1) w art. 27g wprowadza się następujące zmiany:

a) uchyla się ust. 4;

b) ust. 8 lit. c) otrzymuje brzmienie:

c) „c) konkretne wymogi organizacyjne określone w ust. 3 i 5.”;

2) w art. 27h wprowadza się następujące zmiany:

a) uchyla się ust. 5;

b) ust. 8 lit. e) otrzymuje brzmienie:

„e) konkretne wymogi organizacyjne określone w ust. 4.”;

3) w art. 27i wprowadza się następujące zmiany:

a) uchyla się ust. 3;

b) ust. 5 lit. b) otrzymuje brzmienie:

„b) konkretne wymogi organizacyjne określone w ust. 2 i 4.”.

Artykuł 56

Wejście w życie i stosowanie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie stosuje się od dnia [*Urząd Publikacji: należy wstawić datę przypadającą 12 miesięcy od dnia wejścia w życie niniejszego rozporządzenia*] r.

Art. 23 i 24 stosuje się jednak od dnia [*Urząd Publikacji: należy wstawić datę przypadającą 36 miesięcy od dnia wejścia w życie niniejszego rozporządzenia*] r.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodniczący	*Przewodniczący*

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

1.3. Charakter wniosku/inicjatywy

1.4. Cel(e)

1.5. Uzasadnienie wniosku/inicjatywy

1.6. Okres trwania i wpływ finansowy wniosku/inicjatywy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ na wydatki

3.2.1. Synteza szacunkowego wpływu na wydatki

3.2.2. Szacunkowy wpływ na środki

3.2.3. Szacunkowy wpływ na zasoby ludzkie

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

Załącznik

Założenia ogólne

Uprawnienia nadzorcze

OCENA SKUTKÓW FINANSOWYCH REGULACJI – „AGENCJE”

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie operacyjnej odporności cyfrowej sektora finansowego.

1.2. Dziedziny polityki, których dotyczy wniosek/inicjatywa

Dziedzina polityki: stabilność finansowa, usługi finansowe i unia rynków kapitałowych

Działanie: operacyjna odporność cyfrowa

1.3. Wniosek dotyczy:

☑ **nowego działania**

☐ **nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego**[50]

☐ **przedłużenia bieżącego działania**

☐ **połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania**

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

Ogólnym celem inicjatywy jest zwiększenie operacyjnej odporności cyfrowej podmiotów z sektora finansowego UE poprzez uproszczenie i udoskonalenie istniejących przepisów oraz wprowadzenie nowych wymogów w obszarach, w których odnotowano braki. Wzmocniłoby to również cyfrowy wymiar jednolitego zbioru przepisów.

Ogólny cel można podzielić na trzy główne cele: 1) ograniczenie ryzyka zakłóceń finansowych i niestabilności finansowej, 2) zmniejszenie obciążenia administracyjnego i zwiększenie skuteczności nadzoru oraz 3) wzmocnienie ochrony konsumentów i inwestorów.

1.4.2. Cel(e) szczegółowy(e)

Wniosek ma następujące cele szczegółowe:

radzenie sobie z ryzykiem związanym z technologiami informacyjno-komunikacyjnymi („ICT”) w bardziej kompleksowy sposób i zwiększenie ogólnego poziomu odporności cyfrowej sektora finansowego;

uproszczenie zgłaszania incydentów związanych z ICT i rozwiązanie problemu pokrywających się wymogów w zakresie zgłaszania;

umożliwienie organom nadzoru finansowego dostępu do informacji na temat incydentów związanych z ICT;

[50] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

zapewnienie podmiotom finansowym objętym zakresem niniejszego wniosku możliwości ocenienia skuteczności stosowanych przez siebie środków zabezpieczających i środków zwiększających odporność oraz zidentyfikowania luk związanych z ICT;

ograniczenie fragmentacji jednolitego rynku i umożliwienie transgranicznego uznawania wyników testów;

wzmocnienie zabezpieczeń umownych dla podmiotów finansowych przy korzystaniu z usług ICT, w tym dotyczących przepisów w zakresie outsourcingu (regulujących monitorowanie zewnętrznych dostawców usług ICT);

umożliwienie sprawowania nadzoru nad działalnością kluczowych zewnętrznych dostawców usług ICT;

zachęcanie do wymieniania się wynikami analiz zagrożeń przeprowadzanych w sektorze finansowym.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

Akt prawny w sprawie operacyjnej odporności cyfrowej sektora finansowego zapewniłby kompleksowe ramy obejmujące wszystkie aspekty operacyjnej odporności cyfrowej i byłby skuteczny w zwiększaniu ogólnej odporności operacyjnej w sektorze finansowym. Zapewniłby on czytelność i spójność jednolitego zbioru przepisów.

Przyczyniłby się on również do zapewnienia bardziej przejrzystego i spójnego powiązania z dyrektywą dotyczącą cyberbezpieczeństwa oraz jej przeglądem. Zapewniłby on również podmiotom finansowym przejrzystość w zakresie poszczególnych przepisów dotyczących operacyjnej odporności cyfrowej, z którymi muszą one zachować zgodność, w szczególności tym podmiotom finansowym, które posiadają kilka zezwoleń i prowadzą działalność na różnych rynkach w UE.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

Możliwe wskaźniki:

liczba incydentów związanych z ICT w sektorze finansowym UE i ich skutki;

liczba poważnych incydentów związanych z ICT zgłoszonych organom nadzoru ostrożnościowego;

liczba podmiotów finansowych, które byłyby zobowiązane do przeprowadzania testów penetracyjnych pod kątem wyszukiwania zagrożeń;

liczba podmiotów finansowych stosujących standardowe klauzule umowne do zawarcia ustaleń umownych z zewnętrznymi dostawcami usług ICT;

liczba kluczowych zewnętrznych dostawców usług ICT nadzorowanych przez Europejskie Urzędy Nadzoru/organy nadzoru ostrożnościowego;

liczba podmiotów finansowych uczestniczących w rozwiązaniach z zakresu wymiany wyników analizy zagrożeń;

liczba organów, które mają otrzymać sprawozdania z tego samego incydentu związanego z ICT;

liczba transgranicznych testów penetracyjnych pod kątem wyszukiwania zagrożeń.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Sektor finansowy w znacznym stopniu polega na technologiach informacyjno-komunikacyjnych (ICT). Pomimo znacznych postępów poczynionych dzięki krajowym i europejskim ukierunkowanym inicjatywom politycznym i ustawodawczym ryzyko związane z ICT nadal stanowi wyzwanie dla odporności operacyjnej, wydajności i stabilności systemu finansowego UE. Reforma, którą przeprowadzono po kryzysie finansowym z 2008 r., doprowadziła przede wszystkim do wzmocnienia odporności finansowej sektora finansowego UE, a także miała na celu zabezpieczenie konkurencyjności i stabilności UE z punktu widzenia gospodarki, standardów ostrożnościowych i zachowań rynkowych. Bezpieczeństwo ICT i ogólna operacyjna odporność cyfrowa są częścią ryzyka operacyjnego, ale elementy te

zajmowały mniej centralne miejsce w agendzie regulacyjnej po kryzysie i zostały opracowane tylko w niektórych obszarach polityki i przepisów UE w zakresie rynków finansowych lub jedynie w kilku państwach członkowskich. Przekłada się to na następujące wyzwania, którym należy sprostać za pośrednictwem niniejszego wniosku:

unijne ramy prawne obejmujące ryzyko związane z ICT i odporność operacyjną w zakresie ICT w sektorze finansowym są rozdrobnione i nie są w pełni spójne;

brak spójnych wymogów w zakresie zgłaszania incydentów związanych z ICT prowadzi do tego, że organy nadzoru mają niepełny obraz charakteru, częstotliwości, znaczenia i skutków incydentów;

niektóre podmioty finansowe napotykają złożone, pokrywające się i potencjalnie niespójne wymogi w zakresie zgłaszania w przypadku tego samego incydentu związanego z ICT;

niewystarczająca wymiana informacji i współpraca w zakresie analizy cyberzagrożeń na poziomie strategicznym, taktycznym i operacyjnym uniemożliwia pojedynczym podmiotom finansowym właściwą ocenę cyberzagrożeń, ich monitorowanie, obronę przed nimi i reagowanie na nie;

w niektórych podsektorach finansowych może istnieć wiele nieskoordynowanych ram testowania penetracyjnego i testowania odporności w połączeniu z brakiem transgranicznego uznawania wyników, natomiast inne sektory nie dysponują takimi ramami testowania;

brak wglądu organów nadzoru w działalność podmiotów finansowych wykonywaną przez zewnętrznych dostawców usług ICT naraża pojedyncze podmioty finansowe oraz cały system finansowy na ryzyko operacyjne;

organy nadzoru finansowego nie są wyposażone w wystarczające uprawnienia ani narzędzia do monitorowania ryzyka koncentracji i ryzyka systemowego wynikającego z zależności podmiotów finansowych od zewnętrznych dostawców usług ICT i zarządzania takim ryzykiem.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Przyczyny działania na poziomie europejskim (*ex ante*):

Operacyjna odporność cyfrowa jest przedmiotem wspólnego zainteresowania unijnych rynków finansowych. Działania na szczeblu UE przyniosłyby więcej korzyści i miałyby większą wartość niż działania podejmowane osobno na szczeblu krajowym. Bez dodania niniejszych przepisów operacyjnych dotyczących ryzyka związanego z ICT jednolity zbiór przepisów zapewniałby narzędzia do eliminowania wszystkich innych rodzajów ryzyka na poziomie europejskim, ale pomijałby aspekty operacyjnej odporności cyfrowej lub podporządkowywałby je rozdrobnionym i nieskoordynowanym inicjatywom na szczeblu krajowym. Niniejszy wniosek zapewniłby jasność prawa co do tego, czy i w jaki sposób przepisy w zakresie cyfrowych aspektów operacyjnych mają zastosowanie, w szczególności do transgranicznych podmiotów finansowych, i wyeliminowałby konieczność indywidualnego udoskonalania przez państwa członkowskie przepisów, norm i oczekiwań dotyczących odporności operacyjnej i cyberbezpieczeństwa w odpowiedzi na obecnie ograniczony zakres przepisów UE i ogólny charakter dyrektywy dotyczącej cyberbezpieczeństwa.

Oczekiwana wygenerowana unijna wartość dodana (*ex post*): Interwencja Unii znacząco zwiększyłaby skuteczność polityki, jednocześnie ograniczając również złożoność i zmniejszając obciążenie finansowe i administracyjne wszystkich podmiotów finansowych. Przyczyniłaby się ona do zharmonizowania obszaru gospodarki, w którym istnieją niezwykle głębokie wzajemne powiązania i który jest niezwykle głęboko zintegrowany i korzysta już z jednolitego zbioru przepisów i jednolitego nadzoru. Jeżeli chodzi o zgłaszanie incydentów związanych z ICT, wniosek ograniczyłby obciążenia związane ze zgłaszaniem – oraz dorozumiane koszty – wynikające ze zgłaszania tego samego incydentu związanego z ICT różnym organom unijnym lub krajowym. Ułatwi on również wzajemne uznawanie/akceptowanie wyników testów podmiotów prowadzących działalność transgraniczną, które podlegają wielu ramom testowania w różnych państwach członkowskich.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Nowa inicjatywa

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Cel niniejszego wniosku jest spójny z polityką UE w wielu innych dziedzinach oraz z bieżącymi inicjatywami, w szczególności z dyrektywą w sprawie bezpieczeństwa sieci i informacji (dyrektywą dotycząca cyberbezpieczeństwa) oraz dyrektywą w sprawie europejskiej infrastruktury krytycznej. Za pośrednictwem wniosku utrzymano by korzyści związane z horyzontalnymi ramami w zakresie cyberbezpieczeństwa dzięki utrzymaniu objęcia trzech podsektorów finansowych zakresem dyrektywy dotyczącej cyberbezpieczeństwa. Pozostając powiązanymi z ekosystemem dyrektywy dotyczącej cyberbezpieczeństwa, organy nadzoru finansowego byłyby w stanie wymieniać istotne informacje z organami ds. cyberbezpieczeństwa oraz uczestniczyć w pracach grupy współpracy w zakresie cyberbezpieczeństwa. Niniejszy wniosek nie miałby wpływu na dyrektywę dotyczącą cyberbezpieczeństwa, ale raczej opierałby się na niej i wyeliminował ewentualne przypadki powielania się przepisów za pośrednictwem zwolnienia *lex specialis*. Interakcję między regulacjami dotyczącymi usług finansowych i dyrektywą dotyczącą cyberbezpieczeństwa nadal regulowałaby klauzula *lex specialis*, tym samym zwalniając podmioty finansowe z zasadniczych wymogów przewidzianych w dyrektywie dotyczącej cyberbezpieczeństwa i zapobiegając pokrywaniu się tych dwóch aktów. Ponadto wniosek jest spójny z dyrektywą w sprawie europejskiej infrastruktury krytycznej, która jest obecnie poddawana przeglądowi w celu zwiększenia poziomu ochrony i odporności infrastruktur krytycznych na zagrożenia niezwiązane z cyberatakami.

Niniejszy wniosek nie miałby wpływu na wieloletnie ramy finansowe (WRF). Po pierwsze, ramy nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT będą w pełni finansowane z opłat pobieranych od tych dostawców; po drugie, realizację dodatkowych zadań regulacyjnych związanych z operacyjną odpornością cyfrową powierzonych Europejskim Urzędom Nadzoru zapewni wewnętrzne przeniesienie obecnych pracowników.

Przełoży się to na wniosek dotyczący zwiększenia liczby pracowników agencji podczas przyszłej rocznej procedury budżetowej. Agencja będzie nadal pracować nad maksymalizacją synergii i przyrostu wydajności (m.in. za pośrednictwem systemów informatycznych) oraz ściśle monitorować dodatkowe obciążenie pracą związane z niniejszym wnioskiem, co zostanie odzwierciedlone w liczbie pracowników, o których zatrudnienie agencja wystąpi w ramach rocznej procedury budżetowej.

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Rozważono kilka wariantów finansowania:

Po pierwsze, dodatkowe koszty mogłyby zostać pokryte w ramach zwykłego mechanizmu finansowania Europejskich Urzędów Nadzoru. Wiązałoby się to jednak ze znacznym wzrostem wkładu UE na rzecz zasobów finansowych Europejskich Urzędów Nadzoru.

Wariant ten wybiera się w odniesieniu do kosztów dotyczących zadań regulacyjnych związanych z niniejszym wnioskiem. W związku z tym Europejskie Urzędy Nadzoru zostaną poproszone o przeniesienie obecnych pracowników w celu wdrożenia szeregu standardów technicznych. Dodatkowych kosztów związanych z nadzorem nad kluczowymi zewnętrznymi dostawcami usług ICT nie można jednak pokryć w drodze przesunięcia zasobów wewnątrz Europejskich Urzędów Nadzoru, które oprócz zadań przewidzianych w niniejszym wniosku, a także w innych aktach prawnych Unii, mają inne zadania. Ponadto zadania nadzorcze z zakresu operacyjnej odporności cyfrowej wymagają specjalistycznej wiedzy technicznej

i fachowej. Ponieważ aktualnie poziom takich zasobów w Europejskich Urzędach Nadzoru jest niewystarczający, niezbędne są dodatkowe zasoby.

Co więcej, zgodnie z niniejszym wnioskiem pobierane będą opłaty od kluczowych zewnętrznych dostawców usług ICT podlegających nadzorowi. Zostaną one przeznaczone na pokrycie kosztów wszystkich dodatkowych zasobów niezbędnych dla Europejskich Urzędów Nadzoru do wykonywania swoich nowych zadań i uprawnień.

1.6. Okres trwania i wpływ finansowy wniosku/inicjatywy

☐ **Ograniczony okres trwania**

☐ Okres trwania wniosku/inicjatywy: od [DD/MM]RRRR r. do [DD/MM]RRRR r.

☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r.

☑ **Nieograniczony okres trwania**

Wprowadzenie w życie z okresem rozruchu od 2021 r.,

po którym następuje faza operacyjna.

1.7. Planowane tryby zarządzania[51]

Bezpośrednie zarządzanie przez Komisję za pośrednictwem

☐ agencji wykonawczych

☐ **Zarządzanie dzielone** z państwami członkowskimi

☑ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

☐EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

☑ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

☐ organom prawa publicznego;

☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

Uwagi

Nie dotyczy

[51] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Określić częstotliwość i warunki

Zgodnie z już istniejącymi ustaleniami Europejskie Urzędy Nadzoru regularnie opracowują sprawozdania ze swojej działalności (w tym sprawozdania wewnętrzne dla kadry kierowniczej wyższego szczebla, sprawozdania dla Rad oraz opracowanie sprawozdania rocznego) i podlegają audytom ze strony Trybunału Obrachunkowego i Służby Audytu Wewnętrznego Komisji, których przedmiotem jest wykorzystanie przez Europejskie Urzędy Nadzoru zasobów własnych oraz ich wyniki. Monitorowanie i sprawozdawczość w zakresie działań uwzględnionych we wniosku podlegać będą obecnie obowiązującym wymogom, a także wszelkim nowym wymogom wynikającym z niniejszego wniosku.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie proponowanych systemów zarządzania, mechanizmów wdrażania finansowania, sposobów płatności i strategii kontroli

Działania związane z zarządzaniem będą podejmowane w sposób pośredni za pośrednictwem Europejskich Urzędów Nadzoru. Mechanizm finansowania zostałby wdrożony przy wykorzystaniu opłat nałożonych na kluczowych zewnętrznych dostawców usług ICT.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

W odniesieniu do prawomocnego, gospodarnego, efektywnego i skutecznego wykorzystania środków udostępnionych w związku z niniejszym wnioskiem oczekuje się, że wniosek nie pociąga za sobą nowych rodzajów znacznego ryzyka, które nie byłyby już uwzględnione przez istniejące ramy kontroli wewnętrznej. Zapewnienie terminowego pobierania opłat od kluczowych zewnętrznych dostawców usług ICT może jednak stanowić nowe wyzwanie.

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Systemy zarządzania i kontroli przewidziane w rozporządzeniach w sprawie Europejskich Urzędów Nadzoru są już wdrożone. Europejskie Urzędy Nadzoru współpracują ściśle ze Służbą Audytu Wewnętrznego Komisji w celu zapewnienia spełnienia odpowiednich norm we wszystkich obszarach zasad ramowych kontroli wewnętrznej. Rozwiązania te będą również stosowane w odniesieniu do roli Europejskich Urzędów Nadzoru przewidzianej w niniejszym wniosku. Ponadto w każdym roku budżetowym Parlament Europejski na podstawie zalecenia Rady udziela każdemu Europejskiemu Urzędowi Nadzoru absolutorium budżetowego w związku z wykonaniem przez nie budżetu.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

Do celów zwalczania oszustw, korupcji oraz wszelkiej innej nielegalnej działalności do Europejskich Urzędów Nadzoru zastosowanie mają, bez żadnych ograniczeń, przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

Europejskie Urzędy Nadzoru dysponują specjalną strategią w zakresie zwalczania nadużyć finansowych i wynikającym z niej planem działania. Zintensyfikowane działania prowadzone przez Europejskie Urzędy Nadzoru w zakresie zwalczania nadużyć finansowych będą zgodne z zasadami i wytycznymi przewidzianymi w rozporządzeniu finansowym (środki zwalczania nadużyć finansowych jako część należytego zarządzania finansami), polityką OLAF w zakresie zapobiegania nadużyciom finansowym i postanowieniami zawartymi w strategii Komisji w zakresie zwalczania nadużyć finansowych (COM(2011) 376), jak również określonymi we wspólnym podejściu dotyczącym zdecentralizowanych agencji UE (lipiec 2012 r.) i powiązanym z nim planem działania.

Ponadto rozporządzenia w sprawie ustanowienia Europejskich Urzędów Nadzoru, a także regulacje finansowe Europejskich Urzędów Nadzoru zawierają przepisy dotyczące wykonania i kontroli budżetów Europejskich Urzędów Nadzoru oraz mające zastosowanie przepisy finansowe, w tym te ukierunkowane na zapobieganie nadużyciom finansowym i nieprawidłowościom.

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./niezróżn.[52]	państw EFTA[53]	krajów kandydujących[54]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego

Nowe linie budżetowe, o których utworzenie się wnioskuje

Według działów wieloletnich ram finansowych i linii budżetowych

Dział wieloletnic	Linia budżetowa	Type of środków	Wkład

[52] Środki zróżnicowane/środki niezróżnicowane

[53] EFTA: Europejskie Stowarzyszenie Wolnego Handlu.

[54] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

h ram finansowyc h	Numer	Zróżn./niez różn.	państw EFTA	krajów kandydując ych	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego

3.2. Szacunkowy wpływ na wydatki

3.3. Synteza szacunkowego wpływu na wydatki

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	Numer	Dział

DYREKCJA GENERALNA: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**OGÓŁEM**
	Środki na zobowiązania	(1)									
	Środki na płatności	(2)									
OGÓŁEM środki dla Dyrekcji Generalnej <>	Środki na zobowiązania										
	Środki na płatności										

Dział wieloletnich ram finansowych		

w mln EUR (do trzech miejsc po przecinku)

		2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Dyrekcje generalne:								
• Zasoby ludzkie								
• Pozostałe wydatki administracyjne <>								
OGÓŁEM dyrekcje generalne	Środki							

OGÓŁEM środki na DZIAŁ wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)							

w mln EUR (do trzech miejsc po przecinku) według cen stałych

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**OGÓŁEM**
OGÓŁEM środki na DZIAŁ 1 wieloletnich ram finansowych	Środki na zobowiązania							
	Środki na płatności							

3.3.1. Szacunkowy wpływ na środki

☑ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku) według cen stałych

Określić cele i produkty ⇩			2022		2023		2024		2025		2026		2027		**OGÓŁEM**	
	PRODUKT															
	Rodzaj[55]	Średni koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[56]																
– Produkt																
Cel szczegółowy nr 1 – suma cząstkowa																
CEL SZCZEGÓŁOWY nr 2																
– Produkt																
Cel szczegółowy nr 2 – suma cząstkowa																
KOSZT OGÓŁEM																

55 Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

56 Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

3.3.2. Szacunkowy wpływ na zasoby ludzkie

3.3.2.1. Streszczenie

☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku) według cen stałych

EUNB, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Pracownicy zatrudnieni na czas określony (grupy zaszeregowania AD)	1,188	2,381	2,381	2,381	2,381	2,381	13 093
Pracownicy zatrudnieni na czas określony (AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Personel kontraktowy							
Oddelegowani eksperci krajowi							
OGÓŁEM	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Wymagania dotyczące pracowników (EPC):

EUNB, EIOPA, ESMA i EEA	2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Pracownicy zatrudnieni na czas określony (grupy zaszeregowania AD) EUNB=5, EIOPA=5, ESMA=5	15	15	15	15	15	15	15
Pracownicy zatrudnieni na czas określony (AST) EUNB=1, EIOPA=1, EEA=1	3	3	3	3	3	3	3
Personel kontraktowy							
Oddelegowani eksperci krajowi							

OGÓŁEM	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Szacowane zapotrzebowanie na zasoby ludzkie (macierzystych) dyrekcji generalnych

☑ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

☐ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w pełnych kwotach (lub najwyżej z dokładnością do jednego miejsca po przecinku)

		2022	2023	2024	2025	2026	2027
• **Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)**							
• **Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)**[57]							
XX 01 02 01 (CA, SNE, INT z globalnej koperty finansowej)							
XX 01 02 02 (CA, LA, SNE, INT i JPD w delegaturach)							
XX 01 04 ***yy***[58]	– w centrali[59]						
	– w delegaturach						
XX 01 05 02 (CA, SNE, INT – pośrednie badania naukowe)							
10 01 05 02 (CA, INT, SNE – bezpośrednie badania naukowe)							
Inna linia budżetowa (określić)							
OGÓŁEM							

XX oznacza odpowiednią dziedzinę polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	

[57] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

[58] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

[59] Przede wszystkim fundusze strukturalne, Europejski Fundusz Rolny na rzecz Rozwoju Obszarów Wiejskich (EFRROW) oraz Europejski Fundusz Rybacki.

Personel zewnętrzny	

Opis metody obliczenia kosztów ekwiwalentów pełnego czasu pracy powinien zostać zamieszczony w załączniku V pkt 3.

3.3.3. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

☑ Wniosek/inicjatywa jest zgodny(-a) z obowiązującymi wieloletnimi ramami finansowymi.

☐ Wniosek/inicjatywa wymaga przeprogramowania odpowiedniego działu w wieloletnich ramach finansowych.

☐ Wniosek/inicjatywa wymaga zastosowania instrumentu elastyczności lub zmiany wieloletnich ram finansowych[60].

Należy wyjaśnić, który wariant jest konieczny, określając linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty. […]

3.3.4. Udział osób trzecich w finansowaniu

☐ Wniosek/inicjatywa nie przewiduje współfinansowania ze strony osób trzecich

☑ Wniosek/inicjatywa przewiduje współfinansowanie szacowane zgodnie z poniższym:

w mln EUR (do trzech miejsc po przecinku)

EUNB

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
OGÓŁEM środki objęte współfinansowaniem	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
OGÓŁEM środki objęte współfinansowaniem	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Zob. art. 11 i 17 rozporządzenia Rady (UE, Euratom) nr 1311/2013 określającego wieloletnie ramy finansowe na lata 2014–2020.

61 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

62 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

ESMA

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
OGÓŁEM środki objęte współfinansowaniem	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Szacunkowy wpływ na dochody

☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

☐ wpływ na zasoby własne

☐ wpływ na dochody inne

☐ Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[64]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł …….								

W przypadku wpływu na dochody różne „przeznaczone na określony cel” należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

[…]

Należy określić metodę obliczania wpływu na dochody.

[…]

63 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

64 W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.

ZAŁĄCZNIK

Założenia ogólne

Tytuł I – Wydatki na personel

Podczas obliczania wydatków na personel na podstawie zidentyfikowanych potrzeb kadrowych zastosowano następujące szczegółowe założenia wyjaśnione poniżej:

- koszty dodatkowego personelu zatrudnionego w 2022 r. wyceniono dla okresu sześciu miesięcy, biorąc pod uwagę zakładany czas konieczny, aby zatrudnić dodatkowy personel;
- średni roczny koszt pracownika zatrudnionego na czas określony wynosi 150 000 EUR, przy czym kwota ta obejmuje 25 000 EUR kosztów „dodatkowych” (budynki, IT itp.);
- współczynniki korekty mające zastosowanie do wynagrodzeń personelu w Paryżu (EUNB i ESMA) oraz we Frankfurcie (EIOPA) wynoszą, odpowiednio, 117,7 i 99,4;
- składki emerytalne pracodawcy w przypadku pracowników zatrudnionych na czas określony oparto na standardowym wynagrodzeniu podstawowym uwzględnionym w standardowych średnich kosztach rocznych, tj. 95 660 EUR;
- dodatkowi pracownicy zatrudnieni na czas określony należą do grup zaszeregowania AD5 i AST.

Tytuł II – Wydatki na infrastrukturę i działalność

Koszty określono dzięki pomnożeniu liczby pracowników przez część roku, podczas której są zatrudnieni, i przez standardowe koszty „dodatkowe”, tj. 25 000 EUR.

Tytuł III – Wydatki operacyjne

Koszty oszacowano przy zastosowaniu następujących założeń:

- koszty tłumaczenia określono na 350 000 EUR rocznie dla każdego Europejskiego Urzędu Nadzoru;
- przyjęto, że jednorazowe koszty IT wynoszące 500 000 EUR w przypadku każdego Europejskiego Urzędu Nadzoru zostaną poniesione w ciągu dwóch lat – 2022 i 2023 – według podziału 50–50 %. Szacuje się, że roczne koszty utrzymania począwszy od 2024 r. wyniosą 50 000 EUR dla każdego Europejskiego Urzędu Nadzoru;
- szacuje się, że roczne koszty nadzoru prowadzonego na miejscu dla każdego Europejskiego Urzędu Nadzoru wynoszą 200 000 EUR.

Przedstawione powyżej szacunki powodują następujące koszty ponoszone rocznie:

Dział wieloletnich ram finansowych	Numer	

Ceny stałe

EUNB:			2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Tytuł 1:	Środki na zobowiązania	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Środki na płatności	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Tytuł 2:	Środki na zobowiązania	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Środki na płatności	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Tytuł 3:	Środki na zobowiązania	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Środki na płatności	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
OGÓŁEM środki w przypadku EUNB	Środki na zobowiązania	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Środki na płatności	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Tytuł 1:	Środki na zobowiązania	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Środki na płatności	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Tytuł 2:	Środki na zobowiązania	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825

	Środki na płatności	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Tytuł 3:	Środki na zobowiązania	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Środki na płatności	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
OGÓŁEM środki w przypadku EIOPA	Środki na zobowiązania	=1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560
	Środki na płatności	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**OGÓŁEM**
Tytuł 1:	Środki na zobowiązania	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Środki na płatności	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Tytuł 2:	Środki na zobowiązania	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Środki na płatności	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Tytuł 3:	Środki na zobowiązania	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Środki na płatności	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
OGÓŁEM środki w przypadku ESMA	Środki na zobowiązania	=1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Środki na płatności	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

Wniosek wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku) według cen stałych

EUNB

Określić cele i produkty ⇩			2022		2023		2024		2025		2026		2027			
	PRODUKT															
	Rodzaj[65]	Średni koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[66] Bezpośredni nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT																
– Produkt				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Cel szczegółowy nr 1 – suma cząstkowa																
CEL SZCZEGÓŁOWY nr 2																
– Produkt																
Cel szczegółowy nr 2 – suma cząstkowa																
KOSZT OGÓŁEM				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Określić cele i produkty ⇩			2022		2023		2024		2025		2026		2027			
	PRODUKT															
	Rodzaj[67]	Średni koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[68] Bezpośredni nadzór nad kluczowymi zewnętrznymi dostawcami																

[65] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[66] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

[67] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[68] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

usług ICT																
– Produkt				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Cel szczegółowy nr 1 – suma cząstkowa																
CEL SZCZEGÓŁOWY nr 2																
– Produkt																
Cel szczegółowy nr 2 – suma cząstkowa																
KOSZT OGÓŁEM				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Określić cele i produkty ⇩			2022		2023		2024		2025		2026		2027			
	PRODUKT															
	Rodzaj[69]	Średni koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Nr	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[70] Bezpośredni nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT																
– Produkt				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Cel szczegółowy nr 1 – suma cząstkowa																
CEL SZCZEGÓŁOWY nr 2																
– Produkt																
Cel szczegółowy nr 2 – suma cząstkowa																
KOSZT OGÓŁEM				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[70] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

Działania nadzorcze są w pełni finansowane z następujących opłat pobieranych od podmiotów objętych nadzorem:

EUNB

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
OGÓŁEM środki objęte współfinansowaniem	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
OGÓŁEM środki objęte współfinansowaniem	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Ogółem
Koszty pokrywane są w 100 % z opłat pobieranych od podmiotów objętych nadzorem[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313

[71] 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

[72] 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

[73] 100 % łącznych szacunkowych kosztów powiększone o pełną kwotę składek emerytalnych odprowadzanych przez pracodawcę.

OGÓŁEM środki objęte współfinansowaniem	1,373	1,948	1,748	1,748	1,748	1,748	10,313

INFORMACJE SZCZEGÓŁOWE

Uprawnienia w zakresie bezpośredniego nadzoru

Tytułem wprowadzenia należy przypomnieć, że podmioty podlegające bezpośredniemu nadzorowi ESMA powinny uiszczać na rzecz ESMA opłaty (za jednorazowe koszty rejestracji i koszty stałe z tytułu bieżącego nadzoru). Jest tak w przypadku agencji ratingowych (zob. rozporządzenie delegowane Komisji (UE) nr 272/2012) i repozytoriów transakcji (rozporządzenie delegowane Komisji (UE) nr 1003/2013).

Zgodnie z niniejszym wnioskiem ustawodawczym Europejskim Urzędom Nadzoru powierzone zostaną nowe zadania mające na celu wspieranie konwergencji podejść nadzorczych do ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym poprzez objęcie kluczowych zewnętrznych dostawców usług ICT unijnymi ramami nadzoru.

Ramy nadzoru przewidziane w niniejszym wniosku opierają się na istniejącej strukturze instytucjonalnej w obszarze usług finansowych, w przypadku której Wspólny Komitet Europejskich Urzędów Nadzoru zapewnia międzysektorową koordynację w odniesieniu do wszystkich kwestii dotyczących ryzyka związanego z ICT, zgodnie z jego zadaniami w zakresie cyberbezpieczeństwa, przy wsparciu właściwego podkomitetu (forum nadzoru) przeprowadzającego prace przygotowawcze na potrzeby indywidualnych decyzji i wspólnych zaleceń skierowanych do kluczowych zewnętrznych dostawców usług ICT.

Za pośrednictwem tych ram Europejskie Urzędy Nadzoru wyznaczone jako wiodące organy nadzorcze dla każdego takiego kluczowego zewnętrznego dostawcy usług ICT otrzymują uprawnienia pozwalające zapewnić, by dostawcy usług technologicznych odgrywający kluczową rolę w funkcjonowaniu sektora finansowego byli objęci odpowiednim monitorowaniem na skalę ogólnoeuropejską. Obowiązki nadzorcze ustanowiono w niniejszym wniosku, a ich bardziej szczegółowe omówienie zawarto w uzasadnieniu. Obejmują one prawo do: występowania z wnioskiem o udostępnienie wszelkich stosownych informacji i dokumentów, przeprowadzania ogólnych dochodzeń i kontroli, kierowania zaleceń i późniejszego składania sprawozdań dotyczących działań podjętych lub środków zaradczych wdrożonych w celu zastosowania się do tych zaleceń.

Na potrzeby wykonywania nowych zadań przewidzianych w niniejszym wniosku Europejskie Urzędy Nadzoru są zobowiązane zatrudnić dodatkowy personel specjalizujący się w problematyce ryzyka związanego z ICT, ze szczególnym uwzględnieniem kwestii oceniania uzależnienia od zewnętrznych dostawców usług.

Potrzeby w zakresie zasobów ludzkich można oszacować na 6 EPC dla każdego Urzędu (5 pracowników należących do grupy zaszeregowania AD i 1 pracownik należący do grupy zaszeregowania AST udzielający wsparcia tym pracownikom AD). Europejskie Urzędy Nadzoru poniosą również dodatkowe koszty związane z IT, które szacuje się na 500 000 EUR (koszty jednorazowe) i 50 000 EUR rocznie dla każdego z trzech Europejskich Urzędów Nadzoru jako koszty utrzymania systemów IT. Istotnym elementem związanym z wykonywaniem nowych zadań są wizyty w celu przeprowadzania kontroli i audytów na miejscu – związane z nimi koszty można oszacować na 200 000 EUR rocznie dla każdego Europejskiego Urzędu Nadzoru. Koszty tłumaczenia dokumentów otrzymywanych przez Europejskie Urzędy Nadzoru od kluczowych zewnętrznych dostawców usług ICT są również uwzględnione w pozycji kosztów operacyjnych i wynoszą 350 000 EUR rocznie.

Wszystkie wspomniane powyżej koszty administracyjne zostaną w pełni pokryte z corocznych opłat pobieranych przez Europejskie Urzędy Nadzoru od objętych nadzorem kluczowych zewnętrznych dostawców usług ICT (brak wpływu na budżet UE).