I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/2554

z dnia 14 grudnia 2022 r.

w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011

(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 ([1]),

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) W epoce cyfrowej technologie informacyjno-komunikacyjne (ICT) stanowią wsparcie dla złożonych systemów wykorzystywanych w codziennych działaniach. ICT napędzają naszą gospodarkę w najważniejszych sektorach, w tym w sektorze finansowym, oraz wzmacniają funkcjonowanie rynku wewnętrznego. Większy zakres cyfryzacji i wzajemnych powiązań zwiększa również ryzyko związane z ICT, przez co całe społeczeństwo – i w szczególności system finansowy – staje się bardziej podatne na cyberzagrożenia lub zakłócenia w funkcjonowaniu ICT. Chociaż powszechne korzystanie z systemów ICT i wysoki stopień cyfryzacji oraz łączności to obecnie podstawowe cechy działań podmiotów finansowych w Unii, ich odporność cyfrowa nie jest jeszcze odpowiednio uwzględniona w ich szerszych ramach operacyjnych ani włączona do tych ram.

(2) W minionych dziesięcioleciach korzystanie z ICT zaczęło odgrywać zasadniczą rolę, jeżeli chodzi o świadczenie usług finansowych, do tego stopnia, że obecnie ICT mają krytyczne znaczenie dla wykonywania typowych codziennych funkcji wszystkich podmiotów finansowych. Cyfryzacja obejmuje teraz na przykład płatności, w przypadku których w coraz większym stopniu przechodzi się od metod gotówkowych i papierowych do 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, obsługę roszczeń i działalność *back–office*. Sektor ubezpieczeń również uległ przeobrażeniom w związku z korzystaniem z ICT, czego przykładem

([1]) Dz.U. C 343 z 26.8.2021, s. 1.
([2]) Dz.U. C 155 z 30.4.2021, s. 38.
([3]) Stanowisko Parlamentu Europejskiego z dnia 10 listopada 2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 28 listopada 2022 r.

jest pojawienie się pośredników ubezpieczeniowych oferujących swoje usługi przez internet i prowadzących działalność przy użyciu technologii ubezpieczeniowej (InsurTech) oraz zawieranie ubezpieczeń w formie cyfrowej. Finanse nie tylko stały się w dużej mierze cyfrowe w całym sektorze, ale cyfryzacja 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 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 współzależności między ich systemami ICT mogą stanowić podatność o charakterze systemowym, ponieważ lokalne cyberincydenty mogłyby szybko rozprzestrzenić się z każdego z około 22 000 unijnych podmiotów finansowych na cały system finansowy, bez żadnych przeszkód związanych z granicami geograficznymi. Poważne naruszenia związane z ICT występujące w sektorze finansowym nie dotyczą wyłącznie samych podmiotów finansowych. Naruszenia te zwiększają również ryzyko rozpowszechnienia lokalnych podatności we wszystkich kanałach oddziaływania finansowego oraz potencjalnie wywołują negatywne konsekwencje dla stabilności unijnego systemu finansowego, takie jak utrata płynności i ogólna utrata pewności i zaufania w odniesieniu do rynków finansowych.

(4) W ostatnich latach ryzyko związane z ICT przyciągnęło uwagę międzynarodowych, unijnych i krajowych decydentów, organów regulacyjnych i podmiotów normalizacyjnych, które starają się zwiększyć odporność cyfrową, 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 grupa G-7 i grupa G-20 dążą do zapewnienia właściwym organom i podmiotom gospodarczym z różnych jurysdykcji narzędzi mających na celu wzmocnienie odporności ich systemów finansowych. Prace te wynikały również z potrzeby należytego uwzględnienia ryzyka związanego z ICT w kontekście ściśle połączonego wzajemnie, globalnego systemu finansowego i dążenia do zapewnienia większej spójności odpowiednich najlepszych praktyk.

(5) Pomimo unijnych i krajowych ukierunkowanych polityk i inicjatyw ustawodawczych ryzyko związane z ICT nadal stanowi wyzwanie dla odporności operacyjnej, wydajności i stabilności unijnego systemu finansowego. Reformy, które przeprowadzono po kryzysie finansowym z 2008 r., doprowadziły przede wszystkim do wzmocnienia odporności finansowej unijnego sektora finansowego, a także miały na celu zabezpieczenie konkurencyjności i stabilności Unii z punktu widzenia gospodarki, standardów ostrożnościowych i zasad postępowania na rynku. Chociaż bezpieczeństwo ICT i odporność cyfrowa są częścią ryzyka operacyjnego, elementy te były w mniejszym stopniu przedmiotem agendy regulacyjnej po kryzysie finansowym i rozwijały się tylko w niektórych obszarach unijnej polityki dotyczącej usług finansowych oraz otoczenia regulacyjnego lub jedynie w niektórych państwach członkowskich.

(6) W swoim komunikacie z dnia 8 marca 2018 r. zatytułowanym „Plan działania w zakresie technologii finansowej: w kierunku bardziej konkurencyjnego i innowacyjnego europejskiego sektora finansowego" Komisja podkreśliła podstawowe znaczenie zwiększenia odporności unijnego sektora finansowego, w tym z operacyjnego punktu widzenia, dla zapewnienia jego bezpieczeństwa technologicznego oraz sprawnego funkcjonowania, szybkiego przywracania sprawności 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 utrzymaniu zaufania i pewności w odniesieniu do rynku.

(7) W kwietniu 2019 r. Europejski Urząd Nadzoru (Europejski Urząd Nadzoru Bankowego), (EUNB), ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([4]), *Europejski* Urząd Nadzoru (Europejski Urząd Nadzoru Ubezpieczeń *i* Pracowniczych Programów Emerytalnych), (EIOPA), ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE)
nr 1094/2010 ([5]), oraz Europejski Urząd Nadzoru (Europejski Urząd Nadzoru Giełd i Papierów Wartościowych), (ESMA) ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([6]), (wspólnie znane

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.U. L 331 z 15.12.2010, s. 48).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE (Dz.U. L 331 z 15.12.2010, s. 84).

jako „Europejskie Urzędy Nadzoru" lub „EUN") opublikowały wspólnie 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 pomocą unijnej inicjatywy sektorowej.

(8) Unijny sektor finansowy jest regulowany za pomocą 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 zasady postępowania na rynku. Należy zatem rozbudować jednolity zbiór przepisów i system nadzoru, tak aby uwzględniały również operacyjną odporność cyfrową, poprzez wzmocnienie mandatów właściwych organów w celu umożliwienia im sprawowania nadzoru w zakresie zarządzania ryzykiem ICT w sektorze finansowym w celu ochrony integralności i efektywności rynku wewnętrznego oraz ułatwieniu jego należytego funkcjonowania.

(9) Rozbieżności legislacyjne i niejednolite krajowe podejścia regulacyjne lub nadzorcze do ryzyka związanego z ICT powodują powstanie przeszkód dla funkcjonowania rynku wewnętrznego usług finansowych, utrudniając sprawne korzystanie ze swobody przedsiębiorczości i swobody świadczenia usług podmiotom finansowym prowadzącym działalność transgraniczną. Może zostać również zakłócona konkurencja między tego samego rodzaju podmiotami finansowymi działającymi w różnych państwach członkowskich. Dzieje się tak 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 rynku wewnętrznego ze szkodą dla uczestników rynku i dla stabilności finansowej.

(10) Dotychczasowe częściowe tylko uwzględnienie przepisów dotyczących ryzyka związanego z ICT na szczeblu Unii powoduje braki lub nakładanie się przepisów w istotnych obszarach, takich jak zgłaszanie incydentów związanych z ICT i testowanie operacyjnej odporności cyfrowej, oraz niespójności wynikające z wprowadzanych rozbieżnych przepisów krajowych lub nieefektywnego kosztowo stosowania nakładających się przepisów. Ma to szczególnie szkodliwy wpływ na użytkowników intensywnie wykorzystujących ICT, takich jak w sektorze finansowym, 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 każde z nich może 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 negatywnego wpływu 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 w zakresie ICT i ogólna odporność, rozwijane przez podmioty finansowe – na podstawie tych najważniejszych wymogów – 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 rynku wewnętrznego, powinno ono opierać się na przepisach art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) zgodnie z jego wykładnią przyjętą w świetle utrwalonego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości").

(12) Niniejsze rozporządzenie ma na celu konsolidację i aktualizację wymogów dotyczących ryzyka związanego z ICT jako części wymogów dotyczących ryzyka operacyjnego zawartych dotychczas osobno w różnych unijnych aktach prawnych. Chociaż te akty prawne obejmowały główne kategorie ryzyka finansowego (np. ryzyko kredytowe, ryzyko rynkowe, ryzyko kredytowe kontrahenta i ryzyko płynności, ryzyko związane z postępowaniem na rynku), nie uwzględniono w nich – w momencie ich przyjęcia – w sposób kompleksowy wszystkich elementów odporności operacyjnej. Przepisy dotyczące ryzyka operacyjnego, jeżeli zostały szerzej rozwinięte w tych unijnych aktach prawnych, często sprzyjały tradycyjnemu ilościowemu podejściu do zwalczania ryzyka (polegającemu na określeniu wymogu kapitałowego na potrzeby pokrycia ryzyka związanego z ICT), a nie ukierunkowanym przepisom jakościo-

wym dotyczącym zdolności w zakresie ochrony, wykrywania, powstrzymywania, przywracania sprawności i odbudowy w odniesieniu do incydentów związanych z ICT lub zdolności w zakresie sprawozdawczości i testowania cyfrowego. Te akty prawne miały przede wszystkim obejmować i aktualizować podstawowe przepisy dotyczące nadzoru ostrożnościowego, integralności rynku lub postępowania na rynku. Poprzez konsolidację i aktualizację różnych przepisów dotyczących ryzyka związanego z ICT, wszystkie przepisy dotyczące ryzyka cyfrowego w sektorze finansowym powinny zostać po raz pierwszy zebrane w spójny sposób w jednym akcie ustawodawczym. Niniejsze rozporządzenie wypełnia braki lub eliminuje niespójności w niektórych z poprzednich aktów prawnych, w tym związane ze stosowaną w nich terminologią, oraz wyraźnie odnosi się do ryzyka związanego z ICT za pośrednictwem ukierunkowanych przepisów w sprawie zdolności w zakresie zarządzania ryzykiem związanym z ICT, zgłaszania incydentów, testowania odporności operacyjnej oraz monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT. Zatem niniejsze rozporządzenie powinno również zwiększyć świadomość na temat ryzyka związanego z ICT i potwierdzić, że incydenty związane z ICT i brak odporności operacyjnej mogą zagrozić dobrej kondycji finansowej podmiotów finansowych.

(13) Podmioty finansowe powinny przyjąć to samo podejście i stosować się do tych samych, opartych na zasadach przepisów podczas zwalczania ryzyka związanego z ICT, uwzględniając przy tym swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności realizowanych usług, działań i operacji. Spójność przyczynia się do wzmocnienia zaufania do systemu finansowego oraz ochrony jego stabilności, zwłaszcza w czasach dużej zależności od 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) Rozporządzenie pomaga ograniczyć stopień złożoności regulacyjnej, wspiera spójność w zakresie nadzoru, zwiększa pewność prawa, a także przyczynia się do ograniczenia kosztów przestrzegania przepisów, zwłaszcza dla podmiotów finansowych prowadzących działalność transgraniczną, i do zmniejszenia zakłóceń konkurencji. W związku z tym wybór rozporządzenia na potrzeby ustanowienia wspólnych ram operacyjnej odporności cyfrowej podmiotów finansowych wydaje się najbardziej odpowiednim sposobem zagwarantowania jednolitego i spójnego stosowania wszystkich elementów zarządzania ryzykiem związanym z ICT przez unijny sektor finansowy.

(15) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 ([7]) stanowiła pierwsze horyzontalne ramy w zakresie cyberbezpieczeństwa obowiązujące na szczeblu Unii, mające też zastosowanie do trzech rodzajów podmiotów finansowych, a mianowicie instytucji kredytowych, systemów 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 zidentyfikowani przez państwa członkowskie są w praktyce objęci jej zakresem stosowania, a zatem mają obowiązek spełniać określone w niej wymogi w zakresie bezpieczeństwa ICT i zgłaszania incydentów. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 ([8]) ustanawia jednolite kryterium określania podmiotów objętych jej zakresem stosowania (zasada limitu wielkości), przy czym obejmuje nim też wspomniane trzy rodzaje podmiotów finansowych.

(16) Niemniej jednak biorąc pod uwagę, że niniejsze rozporządzenie zwiększa poziom harmonizacji różnych elementów odporności cyfrowej poprzez wprowadzenie wymogów w zakresie zarządzania ryzykiem związanym z ICT i zgłaszania incydentów związanych z ICT, które to wymogi są bardziej rygorystyczne w porównaniu z wymogami określonymi w obecnych unijnych przepisach dotyczących usług finansowych, ten wyższy poziom zapewnia zwiększoną harmonizację również w porównaniu z wymogami określonymi w dyrektywie (UE) 2022/2555. W związku z tym niniejsze rozporządzenie stanowi *lex specialis* względem dyrektywy (UE) 2022/2555. Jednocześnie, utrzymanie silnego związku między sektorem finansowym a unijnymi horyzontalnymi ramami w zakresie cyberbezpieczeństwa, określonymi obecnie w dyrektywie (UE) 2022/2555, ma zasadnicze znaczenie dla zapewnienia spójności z przyjętymi przez państwa członkowskie strategiami w zakresie cyberbezpieczeństwa oraz umożliwienia organom nadzoru finansowego uzyskania informacji na temat cyberincydentów wpływających na inne sektory objęte tą dyrektywą.

([7]) 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).

([8]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (zob. s. 80 niniejszego Dziennika Urzędowego).

(17) Zgodnie z art. 4 ust. 2 Traktatu o Unii Europejskiej i bez uszczerbku dla kontroli sądowej sprawowanej przez Trybunał Sprawiedliwości niniejsze rozporządzenie nie powinno mieć wpływu na odpowiedzialność państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i ochrony bezpieczeństwa narodowego, np. jeżeli chodzi o przekazywanie informacji stojących w sprzeczności z ochroną bezpieczeństwa narodowego.

(18) 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) 2022/2555, powinny pozostać częścią „ekosystemu" tej dyrektywy (np. Grupa Współpracy i zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)). EUN i właściwe organy krajowe powinny być w stanie uczestniczyć w dyskusjach na temat strategicznej polityki i technicznych pracach grupy współpracy na mocy tej dyrektywy oraz wymieniać informacje i dalej współpracować z pojedynczymi punktami kontaktowymi wyznaczonymi lub ustanowionymi zgodnie z tą dyrektywą. Właściwe organy zgodnie z niniejszym rozporządzeniem powinny również prowadzić konsultacje i współpracować z CSIRT. Właściwe organy powinny też mieć możliwość zwrócenia się o zalecenia techniczne do właściwych organów wyznaczonych lub ustanowionych zgodnie dyrektywą (UE) 2022/2555 i opracowania ustaleń dotyczących współpracy, służących zapewnieniu skutecznych i szybkich mechanizmów koordynacji działań.

(19) Ze względu na silne powiązania między cyfrową i fizyczną odpornością podmiotów finansowych, w niniejszym rozporządzeniu i w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557 ([9]) należy zastosować spójne podejście do kwestii odporności podmiotów krytycznych. Z uwagi na to, że w przewidzianych w niniejszym rozporządzeniu obowiązkach w zakresie zarządzania ryzykiem związanym z ICT i w zakresie zgłaszania incydentów kompleksowo zajęto się kwestią fizycznej odporności podmiotów finansowych, obowiązki ustanowione w rozdziałach III i IV dyrektywy (UE) 2022/2557 nie powinny mieć zastosowania do podmiotów finansowych objętych zakresem stosowania tej dyrektywy.

(20) Dostawcy usług chmurowych stanowią jedną z kategorii infrastruktury cyfrowej objętej dyrektywą (UE) 2022/2555. Unijne ramy nadzoru (zwane dalej „ramami nadzoru") ustanowione niniejszym rozporządzeniem mają zastosowanie do wszystkich kluczowych zewnętrznych dostawców usług ICT, w tym dostawców usług chmurowych, jeżeli świadczą oni usługi ICT na rzecz podmiotów finansowych; należy zatem uznać, że stanowią one uzupełnienie nadzoru sprawowanego zgodnie z dyrektywą (UE) 2022/2555. Ponadto, wobec braku unijnych horyzontalnych ram ustanawiających organ nadzoru cyfrowego, ramy nadzoru ustanowione w niniejszym rozporządzeniu powinny obejmować dostawców usług chmurowych.

(21) 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 obsługi wszystkich incydentów związanych z ICT oraz zgłaszania najpoważniejszych z nich. Podmioty finansowe powinny również dysponować strategiami na potrzeby testowania systemów, kontroli i procesów ICT, a także zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT. Należy podwyższyć podstawowy poziom operacyjnej odporności cyfrowej w odniesieniu do podmiotów finansowych, umożliwiając jednocześnie proporcjonalne stosowanie wymogów w odniesieniu do niektórych podmiotów finansowych, zwłaszcza mikroprzedsiębiorstw, a także podmiotów finansowych objętych uproszczonymi ramami zarządzania ryzykiem związanym z ICT. Aby ułatwić skuteczny nadzór nad instytucjami pracowniczych programów emerytalnych, który jest proporcjonalny i uwzględnia potrzebę zmniejszenia obciążeń administracyjnych dla właściwych organów, w odniesieniu do takich podmiotów finansowych w odpowiednich krajowych mechanizmach nadzoru należy uwzględnić wielkość tych podmiotów i ich ogólny profil ryzyka oraz charakter, skalę i stopień złożoności realizowanych usług, działań i operacji, nawet w przypadku gdy przekroczone zostały odpowiednie progi określone w art. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2341 ([10]). W szczególności działania nadzorcze powinny się koncentrować przede wszystkim na konieczności zwalczania poważnych zagrożeń w kontekście zarządzania ryzykiem związanym z ICT w odniesieniu do poszczególnych podmiotów.

([9]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylenia dyrektywy Rady 2008/114/WE (zob. s. 164 niniejszego Dziennika Urzędowego)..

([10]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2341 z dnia 14 grudnia 2016 r. w sprawie działalności instytucji pracowniczych programów emerytalnych oraz nadzoru nad takimi instytucjami (IORP) (Dz.U. L 354 z 23.12.2016, s. 37).

Właściwe organy powinny również zachować ostrożne, lecz proporcjonalnego podejście w kwestii nadzoru nad instytucjami pracowniczych programów emerytalnych, które – zgodnie z art. 31 dyrektywy (UE) 2016/2341 – zlecają usługodawcom w drodze outsourcingu znaczną część swojej podstawowej działalności, m.in. zarządzanie aktywami, obliczenia aktuarialne, księgowość i zarządzanie danymi.

(22) Progi i taksonomie dotyczące zgłaszania incydentów związanych z ICT różnią się znacznie na szczeblu krajowym. Chociaż płaszczyznę porozumienia można osiągnąć dzięki odpowiednim pracom podejmowanym przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) ustanowioną rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 ([11]) i grupę współpracy zgodnie z dyrektywą (UE) 2022/2555, rozbieżne podejścia do ustalania progów i stosowania taksonomii nadal istnieją lub mogą pojawić się w przypadku pozostałych podmiotów finansowych. Ze względu na te rozbieżności wprowadzono liczne wymogi, które podmioty finansowe muszą spełnić, zwłaszcza w sytuacji, gdy prowadzą działalność w kilku unijnych państwach członkowskich i gdy są częścią grupy finansowej. Ponadto takie rozbieżności mogą utrudniać tworzenie dalszych jednolitych lub scentralizowanych unijnych mechanizmów przyspieszających proces zgłaszania oraz wspierających szybką i sprawną wymianę informacji między właściwymi organami, co ma zasadnicze znaczenie dla zwalczania ryzyka związanego z ICT w przypadku ataków na wielką skalę, które mogą mieć konsekwencje systemowe.

(23) Aby zmniejszyć obciążenie administracyjne i potencjalnie powielające się obowiązki w zakresie zgłaszania incydentów w odniesieniu do niektórych podmiotów finansowych, obowiązek zgłaszania incydentów zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2015/2366 ([12]) nie powinien mieć zastosowania do dostawców usług płatniczych, którzy są objęci zakresem stosowania niniejszego rozporządzenia. W związku z tym instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje płatnicze i dostawcy świadczący usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 tej dyrektywy, powinni zgłaszać od daty stosowania niniejszego rozporządzenia – zgodnie z niniejszym rozporządzeniem – wszelkie incydenty operacyjne lub incydenty w zakresie bezpieczeństwa związane z płatnościami, które wcześniej były zgłaszane zgodnie z tą dyrektywą, niezależnie od tego, czy są one związane z ICT.

(24) Aby umożliwić właściwym organom wykonywanie 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, w niniejszym rozporządzeniu należy ustanowić solidny system zgłaszania incydentów związanych z ICT przewidujący odpowiednie wymogi, które wyeliminowałyby obecne luki w przepisach dotyczących usług finansowych, oraz usunąć istniejące pokrywające się i dublujące przepisy w celu obniżenia kosztów. Podstawowe znaczenie ma harmonizacja systemu zgłaszania incydentów związanych z ICT poprzez zobowiązanie wszystkich podmiotów finansowych do zgłaszania ich właściwym organom za pomocą jednolitych usprawnionych ram, zgodnie z niniejszym rozporządzeniem. Ponadto należy przyznać EUN uprawnienia do doprecyzowania istotnych elementów na potrzeby ram zgłaszania incydentów związanych z ICT, takich jak taksonomia, ramy czasowe, zbiory danych, wzory i mające zastosowanie progi. Aby zapewnić pełną zgodność z dyrektywą (UE) 2022/2555, podmioty finansowe powinny mieć możliwość dobrowolnego zgłaszania znaczących cyberzagrożeń odpowiedniemu właściwemu organowi, jeżeli uznają dane cyberzagrożenie za istotne dla systemu finansowego, użytkowników usług lub klientów.

(25) Wymogi w zakresie testowania operacyjnej odporności cyfrowej zostały opracowane w niektórych podsektorach finansowych i określają ramy, które nie zawsze są w pełni dostosowane. Prowadzi to do potencjalnego dublowania kosztów transgranicznych podmiotów finansowych i komplikuje wzajemne uznawanie wyników testowania operacyjnej odporności cyfrowej, co z kolei może spowodować fragmentację rynku wewnętrznego.

([11]) 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).

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

(26) Dodatkowo, w przypadku braku wymogu testowania w zakresie ICT, podatności pozostają niewykryte i powodują narażenie podmiotów finansowych na ryzyko związane z ICT, a ostatecznie stwarzają większe ryzyko dla stabilności i integralności sektora finansowego. Bez interwencji Unii testowanie operacyjnej odporności cyfrowej pozostałoby niejednolite i nie istniałby system wzajemnego uznawania wyników testowania w zakresie ICT między różnymi jurysdykcjami. Ponadto, biorąc pod uwagę, że prawdopodobieństwo przyjęcia przez inne podsektory finansowe systemów testowania na szeroką skalę jest niewielkie, ominęłyby je potencjalne korzyści wynikające z ram testowania, takie jak ujawnianie podatności i zagrożeń w zakresie ICT oraz testowanie zdolności obronnych i ciągłości działania, co przyczynia się do zwiększenia zaufania konsumentów, dostawców i partnerów biznesowych. Aby zlikwidować te pokrywające się przepisy oraz rozbieżności i luki w przepisach, należy wprowadzić przepisy dotyczące skoordynowanego systemu testowania, ułatwiając tym samym wzajemne uznawanie zaawansowanego testowania w odniesieniu do podmiotów finansowych, które spełniają kryteria określone w niniejszym rozporządzeniu.

(27) Zależność podmiotów finansowych od korzystania z 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.

(28) O takim 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, nawet jeżeli te ostatnie są zapisane w umowach. Ponadto w wielu tych ustaleniach umownych nie przewidziano wystarczających gwarancji umożliwiających pełnoprawne monitorowanie procesów podwykonawstwa, pozbawiając tym samym podmioty finansowe możliwości oceny powiązanych zagrożeń. Ponadto biorąc pod uwagę, że zewnętrzni dostawcy usług ICT często świadczą wystandaryzowane usługi na rzecz różnego rodzaju klientów, takie ustalenia umowne nie zawsze odpowiednio uwzględniają indywidualne lub szczególne potrzeby podmiotów sektora finansowego.

(29) Chociaż unijne przepisy dotyczące usług finansowych zawierają kilka ogólnych przepisów dotyczących outsourcingu, 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, które to zasady mają szczególne znaczenie w przypadku, gdy podmioty finansowe korzystają z zewnętrznych dostawców usług ICT w celu wspierania ich krytycznych lub istotnych funkcji. Zasadom tym powinien towarzyszyć zestaw podstawowych praw umownych związanych z kilkoma elementami związanymi z wykonywaniem i wypowiadaniem ustaleń umownych w celu zapisania pewnych minimalnych zabezpieczeń w celu wzmocnienia zdolności podmiotów finansowych do skutecznego monitorowania wszystkich zagrożeń w zakresie ICT powstających na poziomie zewnętrznych dostawców usług. Zasady te stanowią uzupełnienie przepisów sektorowych mających zastosowanie do outsourcingu.

(30) Obecnie oczywiste jest, że nie ma wystarczającej jednorodności i spójności w monitorowaniu ryzyka ze strony zewnętrznych dostawców usług ICT oraz zależności od zewnętrznych dostawców usług ICT. Pomimo działań odnoszących się do outsourcingu, m.in. w postaci wytycznych EUNB w sprawie outsourcingu z 2019 r. oraz zaleceń ESMA w sprawie outsourcingu zlecanego dostawcom usług chmurowych z 2021 r., w unijnych przepisach niewystarczającą uwagę poświęca się szerszemu problemowi przeciwdziałania ryzyku systemowemu, które może powstać w wyniku kontaktu sektora finansowego z ograniczoną liczbą kluczowych zewnętrznych dostawców usług ICT. Ten brak przepisów na szczeblu unijnym jest spotęgowany brakiem krajowych przepisów dotyczących kompetencji i narzędzi umożliwiających organom nadzoru finansowego osiągnięcie właściwego zrozumienia zależności od zewnętrznych dostawców usług ICT i odpowiednie monitorowanie zagrożeń wynikających z koncentracji zależności od zewnętrznych dostawców usług ICT.

(31) 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, by zapewnić organom nadzoru finansowego odpowiednie narzędzia umożliwiające 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 ram nadzoru umożliwiających stałe monitorowanie działań zewnętrznych dostawców usług ICT będących kluczowymi zewnętrznymi dostawcami usług ICT dla podmiotów finansowych, z zapewnieniem poufności i bezpieczeństwa klientom innym niż podmioty finansowe. Choć świadczenie usług ICT wewnątrz grupy wiąże się z konkretnym ryzykiem i konkretnymi korzyściami, nie należy go automatycznie uznawać za mniej ryzykowne niż świadczenie usług ICT przez dostawców spoza grupy finansowej, a tym samym powinno ono być objęte tymi samymi ramami regulacyjnymi. Niemniej jednak w przypadku gdy usługi ICT są świadczone w ramach tej samej grupy finansowej, podmioty finansowe mogą mieć większą kontrolę nad dostawcami wewnątrz grupy, co należy uwzględnić w ogólnej ocenie ryzyka.

(32) W związku z tym, że ryzyka związane z ICT stają się coraz bardziej złożone i zaawansowane, solidne środki wykrywania ryzyka w zakresie ICT i zapobiegania mu zależą w dużej mierze od regularnej wymiany analiz zagrożeń i podatności między podmiotami finansowymi. Wymiana informacji przyczynia się do zwiększania świadomości na temat cyberzagrożeń. To z kolei wzmacnia zdolność podmiotów finansowych do zapobiegania przekształcaniu się cyberzagrożeń w realne incydenty związane z ICT oraz umożliwia podmiotom finansowym skuteczniejsze ograniczanie skutków incydentów związanych z ICT oraz szybsze przywracanie sprawności. Wydaje się, że wobec braku wytycznych na szczeblu Unii szereg czynników ogranicza taką wymianę analiz, zwłaszcza niepewność co do zgodności z ochroną danych osobowych, przepisami antymonopolowymi i zasadami dotyczącymi odpowiedzialności.

(33) Ponadto wątpliwości 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 celu egzekwowania prawa), skutkują wstrzymaniem przekazywania przydatnych informacji. W związku z tym obecnie 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 systemu finansowego. Trzeba zatem wzmocnić te kanały komunikacyjne.

(34) Należy zachęcać podmioty finansowe, by wymieniały między sobą informacje i analizy na temat cyberzagrożeń oraz by wspólnie wykorzystywały swoją indywidualną wiedzę i praktyczne doświadczenie 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 poprzez udział w rozwiązaniach mających na celu wymianę informacji. 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 sektora finansowego zapobiegać cyberzagrożeniom i wspólnie na nie reagować poprzez szybkie ograniczenie rozpowszechnienia ryzyka związanego z ICT i utrudnienie wystąpienia potencjalnego efektu domina we wszystkich kanałach finansowych. Mechanizmy te powinny być zgodne z mającymi zastosowanie unijnymi zasadami prawa konkurencji określonymi w komunikacie Komisji z dnia 14 stycznia 2011 r. zatytułowanym „Wytyczne w sprawie stosowania art. 101 Traktatu o funkcjonowaniu Unii Europejskiej do horyzontalnych porozumień kooperacyjnych", a także z unijnymi przepisami o ochronie danych, w szczególności z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 ([13]). Powinny one działać w oparciu o co najmniej jedną z podstaw prawnych ustanowionych w art. 6 tego rozporządzenia, np. 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, a także w kontekście przetwarzania danych osobowych niezbędnych do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędnych do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, o czym mowa, odpowiednio, w art. 6 ust. 1 lit. c) i e) tego rozporządzenia.

([13]) 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).

(35) Aby utrzymać wysoki poziom operacyjnej odporności cyfrowej całego sektora finansowego, a jednocześnie dotrzymać kroku rozwojowi technologicznemu, niniejsze rozporządzenie powinno zwalczać ryzyko wynikające ze wszystkich rodzajów usług ICT. W tym celu definicję usług ICT w kontekście niniejszego rozporządzenia należy rozumieć szeroko jako obejmującą usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego. Definicja ta powinna na przykład obejmować tzw. usługi OTT, które należą do kategorii usług łączności elektronicznej. Powinna wyłączać jedynie ograniczoną kategorię tradycyjnych usług telefonii analogowej kwalifikujących się jako usługi publicznej komutowanej sieci telefonicznej (PSTN), usługi z wykorzystaniem linii naziemnej, podstawowej usługi telefonicznej (POTS) lub usługi telefonii stacjonarnej.

(36) Niezależnie od szerokiego zakresu stosowania przewidzianego w niniejszym rozporządzeniu, stosując zasady dotyczące operacyjnej odporności cyfrowej, należy uwzględniać istotne różnice między podmiotami finansowymi pod względem ich wielkości i ogólnego profilu ryzyka. Co do zasady, rozdzielając zasoby i zdolności na wdrażanie ram zarządzania ryzykiem związanym z ICT, podmioty finansowe powinny należycie dostosować swoje potrzeby związane z ICT do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności realizowanych usług, działań i operacji, natomiast właściwe organy powinny nadal oceniać i weryfikować podejście do takiego rozdziału.

(37) Dostawcy świadczący usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366, są wyraźnie włączeni do zakresu stosowania niniejszego rozporządzenia, z uwzględnieniem szczególnego charakteru ich działalności i wynikającego z niej ryzyka. Dodatkowo instytucje pieniądza elektronicznego i instytucje płatnicze, zwolnione zgodnie z art. 9 ust. 1 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE ([14]) oraz art. 32 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366, zostają włączone do zakresu stosowania niniejszego rozporządzenia, nawet jeżeli nie udzielono im zezwolenia na emisję pieniądza elektronicznego lub nie udzielono im zezwolenia na świadczenie i wykonywanie usług płatniczych zgodnie z dyrektywą (UE) 2015/2366. Niemniej jednak instytucje świadczące żyro pocztowe, o których mowa w art. 2 ust. 5 pkt 3) dyrektywy Parlamentu Europejskiego i Rady 2013/36/UE ([15]), są wyłączone z zakresu stosowania niniejszego rozporządzenia. Właściwymi organami instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366, instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE i dostawców świadczących usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366, są właściwe organy wyznaczone zgodnie z art. 22 dyrektywy (UE) 2015/2366.

(38) Ponieważ większe podmioty finansowe mogą korzystać z większych zasobów i są w stanie szybko przeznaczyć środki finansowe na opracowanie struktur zarządzania i stworzenie szeregu strategii korporacyjnych, wymóg tworzenia bardziej złożonych rozwiązań w zakresie zarządzania należy nałożyć wyłącznie na podmioty finansowe, które nie są mikroprzedsiębiorstwami w rozumieniu niniejszego rozporządzenia. 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, do organizowania zarządzania w zakresie ryzyka związanego z ICT zgodnie z modelem trzech linii obrony lub do ustanowienia wewnętrznego modelu zarządzania ryzykiem i kontroli ryzyka oraz do poddania swoich ram zarządzania ryzykiem związanym z ICT audytowi wewnętrznemu.

(39) Niektóre podmioty finansowe korzystają ze zwolnień lub są objęte bardzo łagodnymi ramami regulacyjnymi na mocy odpowiednich przepisów sektorowych prawa Unii. Takie podmioty finansowe obejmują zarządzających alternatywnymi funduszami inwestycyjnymi, o których mowa w art. 3 ust. 2 dyrektywy Parlamentu Europejskiego i Rady 2011/61/UE ([16]), zakłady ubezpieczeń i zakłady reasekuracji, o których mowa w art. 4 dyrektywy Parlamentu Europejskiego i Rady 2009/138/WE ([17]), oraz instytucje pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników. W świetle tych zwolnień włączenie takich podmio-

([14]) 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).

([15]) Dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE (Dz.U. L 176 z 27.6.2013, s. 338).

([16]) Dyrektywa Parlamentu Europejskiego i Rady 2011/61/UE z dnia 8 czerwca 2011 r. w sprawie zarządzających alternatywnymi funduszami inwestycyjnymi i zmiany dyrektyw 2003/41/WE i 2009/65/WE oraz rozporządzeń (WE) nr 1060/2009 i (UE) nr 1095/2010 (Dz.U. L 174 z 1.7.2011, s. 1).

([17]) Dyrektywa Parlamentu Europejskiego i Rady 2009/138/WE z dnia 25 listopada 2009 r. w sprawie podejmowania i prowadzenia działalności ubezpieczeniowej i reasekuracyjnej (Wypłacalność II) (Dz.U. L 335 z 17.12.2009, s. 1).

tów finansowych do zakresu stosowania niniejszego rozporządzenia nie byłoby proporcjonalne. Dodatkowo w niniejszym rozporządzeniu uznaje się specyfikę struktury rynku pośrednictwa ubezpieczeniowego, w związku z czym pośrednicy ubezpieczeniowi, pośrednicy reasekuracyjni i pośrednicy oferujący ubezpieczenia uzupełniające kwalifikujący się jako mikroprzedsiębiorstwa, czy małe lub średnie przedsiębiorstwa, nie powinni podlegać niniejszemu rozporządzeniu.

(40) Ponieważ podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE, są wyłączone z zakresu stosowania tej dyrektywy, państwa członkowskie powinny w związku z tym mieć możliwość podjęcia decyzji o zwolnieniu takich podmiotów mających siedzibę na ich odpowiednich terytoriach z zakresu stosowania niniejszego rozporządzenia.

(41) Analogicznie, aby dostosować niniejsze rozporządzenie do zakresu stosowania dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE ([18]), z zakresu stosowania niniejszego rozporządzenia należy wyłączyć osoby fizyczne i prawne, o których mowa w art. 2 i 3 tej dyrektywy, które posiadają zezwolenie na świadczenie usług inwestycyjnych bez konieczności uzyskiwania zezwolenia na mocy dyrektywy 2014/65/UE. Niemniej jednak w art. 2 dyrektywy 2014/65/UE wyłącza się z zakresu stosowania tej dyrektywy podmioty, które kwalifikują się jako podmioty finansowe do celów niniejszego rozporządzenia, takie jak centralne depozyty papierów wartościowych, przedsiębiorstwa zbiorowego inwestowania lub zakłady ubezpieczeń i zakłady reasekuracji. Wyłączenie osób i podmiotów, o których mowa w art. 2 i 3 tej dyrektywy, z zakresu stosowania niniejszego rozporządzenia nie powinno obejmować tych centralnych depozytów papierów wartościowych, przedsiębiorstw zbiorowego inwestowania ani zakładów ubezpieczeń czy reasekuracji.

(42) Na mocy przepisów sektorowych prawa Unii niektóre podmioty finansowe – ze względu na ich wielkość lub świadczone usługi – są objęte łagodniejszymi wymogami lub zwolnieniami. Ta kategoria podmiotów finansowych obejmuje małe i niepowiązane wzajemnie firmy inwestycyjne oraz małe instytucje pracowniczych programów emerytalnych, które mogą być wyłączone z zakresu stosowania dyrektywy (UE) 2016/2341 na warunkach określonych w art. 5 tej dyrektywy przez odnośne państwa członkowskie i które obsługują programy emerytalne liczące łącznie nie więcej niż 100 uczestników, a także instytucje zwolnionych na mocy dyrektywy 2013/36/UE. W związku z tym zgodnie z zasadą proporcjonalności oraz w celu zachowania ducha przepisów sektorowych prawa Unii te podmioty finansowe również należy objąć uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia. Regulacyjne standardy techniczne, które mają zostać opracowane przez EUN, nie powinny zmieniać proporcjonalnego charakteru ram zarządzania ryzykiem związanym z ICT obejmujących te podmioty finansowe. Ponadto, zgodnie z zasadą proporcjonalności, uproszczone ramy zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny też obejmować instytucje płatnicze, o których mowa w art. 32 ust. 1 dyrektywy (UE) 2015/2366, i instytucje pieniądza elektronicznego, o których mowa w art. 9 dyrektywy 2009/110/WE, zwolnione zgodnie z krajowymi przepisami transponującymi te unijne akty prawne, przy czym instytucje płatnicze i instytucje pieniądza elektronicznego, które nie zostały zwolnione zgodnie z odpowiednimi krajowymi przepisami transponującymi przepisy sektorowe prawa Unii, powinny przestrzegać ogólnych ram ustanowionych w niniejszym rozporządzeniu.

(43) Analogicznie podmioty finansowe, które kwalifikują się jako mikroprzedsiębiorstwa lub są objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia, nie powinny być zobowiązane do ustanowienia funkcji polegającej na monitorowaniu uzgodnień zawartych z zewnętrznymi dostawcami usług ICT w sprawie korzystania z usług ICT; do wyznaczenia członka kadry kierowniczej wyższego szczebla jako odpowiedzialnego za nadzorowanie związanej z tym ekspozycji na ryzyko i odpowiedniej dokumentacji; do powierzenia obowiązku zarządzania ryzykiem związanym z ICT i sprawowania nadzoru nad nim przez funkcję kontroli i zapewnienia odpowiedniego stopnia niezależności takiej funkcji kontroli w celu uniknięcia konfliktów interesów; do dokumentowania uproszczonych ram zarządzania ryzykiem związanym z ICT; poddawania ich przeglądowi co najmniej raz w roku; do ich regularnego poddawania audytowi wewnętrznemu; do przeprowadzania dogłębnych ocen po istotnych zmianach w ich infrastrukturze sieci i systemów informatycznych oraz powiązanych procedurach, do regularnego przeprowadzania analiz ryzyka w odniesieniu do dotychczasowych systemów ICT, do poddawania wdrażania planów reagowania i przywracania sprawności ICT niezależnym wewnętrznym przeglądom audytowym, do posiadania funkcji zarządzania w sytuacji kryzysowej, do rozszerzenia zakresu testowania ciągłości działania oraz planów reagowania i przywracania sprawności w celu uwzględnienia scenariuszy pracy awaryjnej obejmujących przełączanie się z podstawowej infrastruktury ICT na urządzenia redundantne, do zgłaszania właści-

([18]) Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE (Dz.U. L 173 z 12.6.2014, s. 349).

wym organom, na ich żądanie, szacunkowych łącznych rocznych kosztów i strat spowodowanych poważnymi incydentami związanymi z ICT, do utrzymywania nadmiarowych zdolności w zakresie ICT, do informowania właściwych organów krajowych o zmianach wdrożonych w następstwie przeglądów przeprowadzonych po wystąpieniu incydentu związanego z ICT, do ciągłego monitorowania odpowiednich zmian technologicznych, do ustanowienia kompleksowego programu testowania operacyjnej odporności cyfrowej stanowiącego integralną część ram zarządzania ryzykiem związanym z ICT przewidzianych w niniejszym rozporządzeniu ani do przyjęcia strategii dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT i dokonywania jej regularnego przeglądu. Dodatkowo mikroprzedsiębiorstwa powinny być zobowiązane do oceny potrzeby utrzymywania takich nadmiarowych zdolności w zakresie ICT wyłącznie w oparciu o ich profil ryzyka. Mikroprzedsiębiorstwa powinny korzystać z bardziej elastycznego systemu w odniesieniu do programów testowania operacyjnej odporności cyfrowej. Rozważając rodzaj i częstotliwość przeprowadzanych testów, mikroprzedsiębiorstwa powinny odpowiednio wyważyć cel polegający na utrzymaniu wysokiej operacyjnej odporności cyfrowej, dostępne zasoby i ich ogólny profil ryzyka. Mikroprzedsiębiorstwa i podmioty finansowe objęte uproszczonymi ramami zarządzania ryzykiem związanym z ICT na mocy niniejszego rozporządzenia powinny być zwolnione z obowiązku przeprowadzania zaawansowanego testowania narzędzi, systemów i procesów ICT z wykorzystaniem testów penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT), jako że taki obowiązek powinien dotyczyć wyłącznie podmiotów finansowych spełniających kryteria określone w niniejszym rozporządzeniu. Ze względu na swoje ograniczone możliwości mikroprzedsiębiorstwa powinny mieć możliwość uzgodnienia z zewnętrznym dostawcą usług ICT, że przysługujące danemu podmiotowi finansowemu prawa dostępu, kontroli i audytu zostaną przekazane niezależnemu podmiotowi trzeciemu, który zostanie wyznaczony przez zewnętrznego dostawcę usług ICT, pod warunkiem że dany podmiot finansowy będzie mógł w dowolnym momencie zwrócić się do odpowiedniego niezależnego podmiotu trzeciego o wszystkie istotne informacje na temat wyników zewnętrznego dostawcy usług ICT i o poświadczenie tych wyników.

(44) Ponieważ jedynie od podmiotów finansowych objętych zaawansowanym testowaniem odporności cyfrowej powinno wymagać się przeprowadzenia testów penetracyjnych pod kątem wyszukiwania zagrożeń, procesy administracyjne i koszty finansowe związane z przeprowadzeniem takich testów powinny być ponoszone przez niewielki odsetek podmiotów finansowych.

(45) Aby zapewnić pełną zgodność i ogólną spójność między strategiami biznesowymi poszczególnych podmiotów finansowych a zarządzaniem ryzykiem związanym z ICT, należy zobowiązać organy zarządzające tych podmiotów finansowych do utrzymania kluczowej i aktywnej roli w kierowaniu i dostosowywaniu ram zarządzania ryzykiem związanym z ICT oraz ogólnej strategii w zakresie operacyjnej odporności cyfrowej. W podejściu, które przyjmą organy zarządzające, 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.

(46) Co więcej, zasada pełnej i ostatecznej odpowiedzialności organu zarządzającego za zarządzanie ryzykiem związanym z ICT podmiotu finansowego idzie w parze z koniecznością zabezpieczenia poziomu inwestycji związanych z ICT oraz ogólnego budżetu podmiotu finansowego, tak aby podmiot ten mógł osiągnąć wysoki poziom operacyjnej odporności cyfrowej.

(47) W niniejszym rozporządzeniu, inspirowanym odpowiednimi międzynarodowymi, krajowymi i sektorowymi najlepszymi praktykami, wytycznymi, zaleceniami i podejściami w zakresie zarządzania ryzykiem w cyberprzestrzeni, promuje się zestaw zasad ułatwiających ustanowienie ogólnej struktury zarządzania ryzykiem związanym z ICT. Tym samym, dopóki podstawowe możliwości wprowadzane przez podmioty finansowe odpowiadają różnym funkcjom w ramach zarządzania ryzykiem związanym z ICT (identyfikacja, ochrona i zapobieganie, wykrywanie, reagowanie i przywracanie sprawności, uczenie się i rozwój oraz komunikacja) określonym w niniejszym rozporządzeniu, podmioty finansowe powinny zachować swobodę korzystania z modeli zarządzania ryzykiem związanym z ICT, dla których opracowano inne ramy lub kategorie.

(48) Aby nadążyć za zmieniającym się krajobrazem cyberzagrożeń, podmioty finansowe powinny na bieżąco aktualizować systemy ICT, które muszą być niezawodne i posiadać zdolność nie tylko do zagwarantowania przetwarzania danych niezbędnych do świadczenia ich usług, ale również do zapewnienia wystarczającej 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.

(49) 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 przywracania sprawności zgodnie z ich politykami tworzenia kopii zapasowych. Takie wznowienie działalności nie powinno jednak w żaden sposób zagrażać integralności i bezpieczeństwu sieci i systemów informatycznych lub dostępności, autentyczności, integralności czy poufności danych.

(50) Choć niniejsze rozporządzenie pozwala podmiotom finansowym na określenie w sposób elastyczny zakładanego czasu przywrócenia systemów i akceptowalny poziom utraty danych, a tym samym na wyznaczanie go poprzez pełne uwzględnienie charakteru i krytyczności danych funkcji oraz wszelkich szczególnych potrzeb biznesowych, powinno jednak nakładać na te podmioty wymóg przeprowadzenia oceny potencjalnego ogólnego wpływu na efektywność rynku przy określaniu takich celów.

(51) Inicjatorzy cyberataków zwykle dążą do osiągnięcia zysków finansowych bezpośrednio u źródła, narażając tym samym podmioty finansowe na poważne konsekwencje. Aby zapobiec niedostępności lub utracie integralności systemów ICT, a tym samym by uniknąć naruszeń poufnych danych i uszkodzeń fizycznej infrastruktury ICT, należy znacznie usprawnić i uprościć procedurę zgłaszania przez podmioty finansowe poważnych incydentów związanych z ICT. Procedurę zgłaszania incydentów związanych z ICT należy ujednolicić: wszystkie podmioty finansowe powinny być zobowiązane do zgłaszania tych incydentów bezpośrednio do swoich odpowiednich właściwych organów. W przypadku gdy nadzór nad podmiotem finansowym sprawuje więcej niż jeden właściwy organ krajowy, państwa członkowskie powinny wyznaczyć jeden właściwy organ do celów takich zgłoszeń. Instytucje kredytowe sklasyfikowane jako istotne zgodnie z art. 6 ust. 4 rozporządzenia Rady (UE) nr 1024/2013 ([19]) powinny przekazywać takie zgłoszenia właściwym organom krajowym, które następnie powinny przekazać stosowne sprawozdanie Europejskiemu Bankowi |Centralnemu (EBC).

(52) Bezpośrednie zgłaszanie incydentów powinno umożliwić organom nadzoru finansowego natychmiastowy dostęp do informacji na temat poważnych incydentów związanych z ICT. Organy nadzoru finansowego powinny z kolei przekazywać szczegółowe informacje na temat takich poważnych incydentów związanych z ICT organom publicznym spoza sektora finansowego (takim jak właściwe organy i pojedyncze punkty kontaktowe na mocy dyrektywy (UE) 2022/2555, krajowe organy ochrony danych i organom ścigania w przypadku poważnych incydentów o charakterze przestępczym związanych z ICT), aby zwiększyć wiedzę takich organów o takich incydentach oraz – w przypadku CSIRT – ułatwić szybką pomoc, której można udzielić podmiotom finansowym, stosownie do przypadku. Dodatkowo państwa członkowskie powinny mieć możliwość określenia, że to same podmioty finansowe powinny przekazywać takie informacje organom publicznym spoza obszaru usług finansowych. Te przepływy informacji powinny umożliwić podmiotom finansowym szybkie korzystanie z wszelkich istotnych informacji technicznych, porad dotyczących środków zaradczych oraz działań następczych ze strony takich organów. Informacje na temat poważnych incydentów związanych z ICT powinny być wzajemnie przekazywane: organy sprawujące nadzór finansowy powinny przekazywać podmiotowi finansowemu wszelkie niezbędne informacje zwrotne lub wytyczne, natomiast EUN powinny udostępniać zanonimizowane dane na temat cyberzagrożeń i podatności związanych z danym incydentem, aby wspomóc szerzej pojętą zbiorową obronę.

(53) Chociaż wszystkie podmioty finansowe powinny być objęte wymogiem zgłaszania incydentów, przewiduje się, że wymóg ten nie będzie wszystkich ich obciążać w ten sam sposób. Odpowiednie progi w zakresie istotności i ramy czasowe zgłaszania incydentów powinny być należycie dostosowane, w kontekście aktów delegowanych opartych na regulacyjnych standardach technicznych, które mają zostać opracowane przez EUN, tak by uwzględniać jedynie poważne incydenty związane z ICT. Dodatkowo przy określaniu ram czasowych do celów obowiązków w zakresie zgłaszania incydentów należy uwzględnić specyfikę podmiotów finansowych.

(54) Niniejsze rozporządzenie powinno nakładać na instytucje kredytowe, instytucje płatnicze, dostawców świadczących usługę dostępu do informacji o rachunku i instytucje pieniądza elektronicznego wymóg zgłaszania wszelkich incydentów operacyjnych lub w zakresie bezpieczeństwa związanych z płatnościami, które wcześniej były zgłaszane na mocy dyrektywy (UE) 2015/2366, niezależnie od tego, czy są one związane z ICT.

([19]) 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).

(55) EUN należy powierzyć zadanie polegające na ocenie możliwości i warunków ewentualnej centralizacji zgłoszeń dotyczących incydentów związanych z ICT na szczeblu Unii. Taka centralizacja mogłaby obejmować jeden unijny węzeł informacyjny na potrzeby zgłaszania poważnych incydentów związanych z ICT, który by otrzymywał odpowiednie zgłoszenia bezpośrednio i automatycznie powiadamiał właściwe organy krajowe albo który by służył jedynie jako centralne miejsce do przekazywania odpowiednich zgłoszeń przez właściwe organy krajowe i tym samym pełnił funkcję koordynującą. EUN należy powierzyć zadanie polegające na przygotowaniu, w porozumieniu z EBC i ENISA, wspólnego sprawozdania badającego możliwość ustanowienia takiego jednego unijnego węzła informacyjnego.

(56) W celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej oraz zgodnie zarówno z odpowiednimi standardami międzynarodowymi (np. określonymi przez G-7 podstawowymi elementami dotyczącymi testów penetracyjnych pod kątem wyszukiwania zagrożeń), jak i ramami stosowanymi w Unii, takimi jak TIBER–EU, podmioty finansowe powinny regularnie testować swoje systemy ICT i personel wykonujący obowiązki związane z ICT pod kątem skuteczności ich zdolności w zakresie zapobiegania, wykrywania, reagowania i przywracania sprawności, aby wykrywać i eliminować potencjalne podatności w zakresie ICT. Aby odzwierciedlić różnice istniejące między różnymi podsektorami finansowymi i w ramach tych podsektorów w zakresie gotowości podmiotów finansowych do reagowania w obszarze cyberbezpieczeństwa, testowanie powinno obejmować szeroki zakres narzędzi i działań, począwszy od oceny podstawowych wymogów (np. oceny podatności 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 kompleksowe) aż po bardziej zaawansowane testowanie przy użyciu TLPT. Takie zaawansowane testowanie powinno być wymagane jedynie w przypadku podmiotów finansowych wystarczająco zaawansowanych z punktu widzenia ICT, aby były w stanie przeprowadzić takie testy. Wymagane w niniejszym rozporządzeniu testowanie operacyjnej odporności cyfrowej powinno być zatem bardziej rygorystyczne dla podmiotów finansowych spełniających kryteria określone w niniejszym rozporządzeniu (np. dużych systemowych i zaawansowanych z punktu widzenia ICT instytucji kredytowych, giełd papierów wartościowych, centralnych depozytów papierów wartościowych oraz kontrahentów centralnych) niż dla innych podmiotów finansowych. Jednocześnie testowanie operacyjnej odporności cyfrowej przy użyciu TLPT powinno mieć większe znaczenie w przypadku podmiotów finansowych prowadzących działalność w podstawowych podsektorach usług finansowych i odgrywających rolę systemową (np. płatności, bankowość oraz systemy rozliczeń i rozrachunku), a mniejsze w przypadku innych podsektorów (np. podmiotów zarządzających aktywami oraz agencji ratingowych itp.).

(57) Podmioty finansowe prowadzące działalność transgraniczną i korzystające ze swobody przedsiębiorczości lub swobody świadczenia usług w Unii powinny spełniać jeden zestaw wymogów w zakresie zaawansowanego testowania (np. TLPT) w swoim macierzystym państwie członkowskim, a testowanie to powinno obejmować infrastrukturę ICT we wszystkich jurysdykcjach, w których dana transgraniczna grupa finansowa prowadzi działalność w Unii, co pozwoli takim transgranicznym grupom finansowym ponosić koszty przeprowadzenia testów związanych z ICT tylko w jednej jurysdykcji.

(58) Aby wykorzystać wiedzę fachową zdobytą już przez niektóre właściwe organy, w szczególności w odniesieniu do wdrażania ram TIBER–EU, niniejsze rozporządzenie powinno umożliwiać państwom członkowskim wyznaczenie jednego organu publicznego jako odpowiedzialnego w sektorze finansowym na szczeblu krajowym za wszelkie kwestie dotyczące TLPT lub powinno umożliwiać właściwym organom – w przypadku braku takiego wyznaczenia – przekazanie wykonywania zadań związanych z TLPT innemu krajowemu właściwemu organowi finansowemu.

(59) Z uwagi na to, że niniejsze rozporządzenie nie nakłada na podmioty finansowe wymogu objęcia wszystkich krytycznych lub istotnych funkcji pojedynczym testem penetracyjnym pod kątem wyszukiwania zagrożeń, podmioty te powinny mieć możliwość określenia, które z tych funkcji i jaką ich liczbę należy objąć zakresem takiego testu.

(60) Testowanie zbiorcze w rozumieniu niniejszego rozporządzenia – z udziałem kilku podmiotów finansowych w TLPT i w odniesieniu do którego zewnętrzny dostawca usług ICT może zawrzeć ustalenia umowne bezpośrednio z testerem zewnętrznym – powinno być dozwolone jedynie w przypadku, gdy można racjonalnie przewidywać, że jakość lub bezpieczeństwo usług świadczonych przez zewnętrznego dostawcę usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia lub poufność danych związanych z takimi usługami będą zagrożone. Testowanie zbiorcze powinno też podlegać zabezpieczeniom (kierowanie przez jeden wyznaczony podmiot finansowy, określenie liczby uczestniczących podmiotów finansowych), aby zapewnić poddanie uczestniczących podmiotów finansowych rygorystycznym testom spełniającym cele TLPT zgodnie z niniejszym rozporządzeniem.

(61) Aby wykorzystać zasoby wewnętrzne dostępne na poziomie przedsiębiorstwa, niniejsze rozporządzenie powinno umożliwiać korzystanie z wewnętrznych testerów do celów przeprowadzania TLPT, pod warunkiem że uzyskano zgodę od organu nadzoru, nie występuje konflikt interesów i że TLTP są przeprowadzane naprzemiennie przez testerów wewnętrznych i zewnętrznych (okresowo – zmiana co trzy testy), przy czym dostawcy analiz zagrożeń wykorzystywanych w ramach TLPT zawsze muszą być podmiotem zewnętrznym względem danego podmiotu finansowego. Pełną odpowiedzialność za prowadzenie TLPT powinien ponosić podmiot finansowy. Potwierdzenia wydawane przez odpowiednie organy powinny służyć wyłącznie do celów wzajemnego uznawania i nie powinny wykluczać działań następczych niezbędnych, by wyeliminować ryzyko związane z ICT, na które dany podmiot finansowy jest narażony, nie powinny też być postrzegane jako potwierdzenie przez organ nadzoru zdolności podmiotu finansowego w zakresie zarządzania ryzykiem związanym z ICT i jego łagodzenia.

(62) Aby zapewnić należyte monitorowanie ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym, konieczne jest ustanowienie zbioru opartych na zasadach przepisów regulujących monitorowanie przez podmioty finansowe ryzyka występującego w kontekście funkcji zlecanych zewnętrznym dostawcom usług ICT, zwłaszcza w odniesieniu do usług ICT wspierających krytyczne lub istotne funkcje, oraz, w bardziej ogólnym zakresie, w kontekście wszelkich zależności od zewnętrznych dostawców usług ICT.

(63) Aby sprostać stopniowi złożoności różnych źródeł ryzyka związanego z ICT, uwzględniając przy tym dużą liczbę i różnorodność dostawców rozwiązań technologicznych umożliwiających sprawne świadczenie usług finansowych, niniejsze rozporządzenie powinno obejmować wielu różnych zewnętrznych dostawców usług ICT, w tym dostawców usług chmurowych, oprogramowania, usług analizy danych i dostawców usług przetwarzania danych. Analogicznie, z uwagi na to, że podmioty finansowe powinny skutecznie i spójnie określać wszystkie rodzaje ryzyka i nimi zarządzać, m.in. w kontekście usług ICT zamawianych w ramach grupy finansowej, należy doprecyzować, że przedsiębiorstwa, które są częścią grupy finansowej i świadczą usługi ICT głównie na rzecz swojej jednostki dominującej lub na rzecz jednostek zależnych lub oddziałów swojej jednostki dominującej, jak również podmioty finansowe świadczące usługi ICT na rzecz innych podmiotów finansowych także powinny być uznawane za zewnętrznych dostawców usług ICT na mocy niniejszego rozporządzenia. Ponadto w związku ze zmieniającym się rynkiem usług płatniczych, który jest coraz bardziej zależny od złożonych rozwiązań technicznych, oraz w świetle pojawiających się rodzajów usług płatniczych i rozwiązań związanych z płatnościami, uczestnicy ekosystemu usług płatniczych prowadzący działania przetwarzania płatności lub obsługujący infrastrukturę płatniczą również powinni być uznawani za zewnętrznych dostawców usług ICT na mocy niniejszego rozporządzenia, z wyjątkiem banków centralnych prowadzących systemy płatności lub systemy rozrachunku papierów wartościowych oraz organów publicznych świadczących usługi związane z ICT w kontekście pełnienia funkcji państwa.

(64) Podmiot finansowy powinien przez cały czas ponosić pełną odpowiedzialność za wypełnianie swoich obowiązków określonych w niniejszym rozporządzeniu. Podmioty finansowe powinny stosować proporcjonalne podejście do monitorowania zagrożeń występujących na poziomie zewnętrznego dostawcy usług ICT i odpowiednio uwzględnić charakter, skalę, stopień złożoności i znaczenie swoich zależności w zakresie ICT, krytyczność lub znaczenie usług, procesów lub funkcji objętych ustaleniami umownymi, a ostatecznie na podstawie starannej oceny wszelkiego potencjalnego wpływu na ciągłość i jakość usług finansowych na szczeblu indywidualnym i grupowym, w zależności od przypadku.

(65) 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 dotyczącej ryzyka ze strony zewnętrznych dostawców usług ICT, opartej na ciągłym badaniu wszystkich takich zależności od zewnętrznych dostawców usług ICT. Aby zwiększyć świadomość organów sprawujących nadzór co do zależności od zewnętrznych dostawców usług ICT, a także w celu dalszego wspierania prac prowadzonych w kontekście ram nadzoru ustanowionych w niniejszym rozporządzeniu, wszystkie podmioty finansowe powinny być zobowiązane do prowadzenia rejestru informacji obejmującego wszystkie ustalenia umowne dotyczące korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT. Organy sprawujące nadzór finansowy powinny mieć możliwość żądania dostępu do pełnego rejestru lub określonych jego części, i tym samym uzyskania podstawowych informacji umożliwiających lepsze zrozumienie zależności podmiotów finansowych w obszarze ICT.

(66) Gruntowna analiza poprzedzająca zawarcie umowy powinna mieć miejsce przed formalnym dokonaniem ustaleń umownych i powinna się koncentrować w szczególności na takich elementach, jak krytyczność lub znaczenie usług wspieranych w ramach planowanej umowy w zakresie ICT, niezbędne zgody organów nadzoru lub inne warunki, możliwe powiązane ryzyko koncentracji; należy ją przeprowadzić z zastosowaniem należytej staranności w procesie selekcji i oceny zewnętrznych dostawców usług ICT oraz dokonać oceny potencjalnych konfliktów interesów. W przypadku ustaleń umownych dotyczących krytycznych lub istotnych funkcji podmioty finansowe powinny brać pod uwagę fakt, czy zewnętrzni dostawcy usług ICT stosują najbardziej aktualne i najwyższe standardy bezpieczeństwa informacji. Wypowiedzenie ustaleń umownych mogłoby być spowodowane wystąpieniem co najmniej szeregu okoliczności wskazujących na braki po stronie zewnętrznego dostawcy usług ICT, w szczególności poważnych naru-

szeń przepisów lub warunków umownych, okoliczności ujawniających potencjalne zmiany w wykonywaniu funkcji przewidzianych w warunkach umownych, dowodów na słabości danego zewnętrznego dostawcy usług ICT w ogólnym zarządzaniu ryzykiem związanym z ICT, lub okoliczności wskazujących na niezdolność odpowiedniego właściwego organu do sprawowania nadzoru nad danym podmiotem finansowym.

(67) Aby zaradzić skutkom systemowym koncentracji ryzyka ze strony zewnętrznych dostawców usług ICT, niniejsze rozporządzenie promuje zrównoważone rozwiązania poprzez elastyczne i stopniowe podejście do takiego ryzyka koncentracji, ponieważ nałożenie jakichkolwiek sztywnych limitów lub ścisłych ograniczeń może utrudniać prowadzenie działalności gospodarczej i ograniczać swobodę zawierania umów. Podmioty finansowe powinny dokładnie oceniać swoje planowane ustalenia umowne w celu określenia prawdopodobieństwa wystąpienia takiego ryzyka, w tym poprzez dogłębną analizę ustaleń dotyczących podwykonawstwa, 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 określenia zasad w odniesieniu do sztywnych limitów i ograniczeń dotyczących ekspozycji wobec zewnętrznych dostawców usług ICT. W kontekście ram nadzoru wiodący organ nadzorczy wyznaczony zgodnie z niniejszym rozporządzeniem powinien – w odniesieniu do kluczowych zewnętrznych dostawców usług ICT zwracać szczególną uwagę na pełne zrozumienie skali współzależności, wykrywać konkretne przypadki, w których wysoki poziom koncentracji kluczowych zewnętrznych dostawców usług ICT w Unii może stanowić zagrożenie dla stabilności i integralności systemu finansowego Unii, i utrzymywać dialog z kluczowymi zewnętrznymi dostawcami usług ICT w przypadku stwierdzenia takiego konkretnego zagrożenia.

(68) Aby regularnie oceniać i monitorować zdolność zewnętrznego dostawcy usług ICT do bezpiecznego świadczenia usług na rzecz podmiotu finansowego bez negatywnego wpływu na operacyjną odporność cyfrową tego podmiotu, należy ujednolicić kilka najważniejszych elementów umownych z zewnętrznymi dostawcami usług ICT. Takie ujednolicenie powinno obejmować minimum obszarów mających kluczowe znaczenie dla umożliwienia pełnego monitorowania zagrożeń, które mogłyby się pojawić ze strony zewnętrznego dostawcy usług ICT, przez podmiot finansowy w kontekście konieczności zapewnienia odporności cyfrowej tego podmiotu finansowego ze względu na jego głębokie uzależnienie od stabilności, funkcjonalności, dostępności i bezpieczeństwa otrzymywanych usług ICT.

(69) Renegocjując ustalenia umowne w celu dostosowania ich do wymogów niniejszego rozporządzenia, podmioty finansowe i zewnętrzni dostawcy usług ICT powinni zapewnić, by ustalenia te obejmowały najważniejsze postanowienia umowne, jak przewidziano w niniejszym rozporządzeniu.

(70) Określona w niniejszym rozporządzeniu definicja „krytycznej lub istotnej funkcji" obejmuje definicję „funkcji krytycznych" określoną w art. 2 ust. 1 pkt 35 dyrektywy Parlamentu Europejskiego i Rady 2014/59/UE ([20]). W związku z tym funkcje uznawane za krytyczne zgodnie z dyrektywą 2014/59/UE są ujęte w definicji funkcji krytycznych w rozumieniu niniejszego rozporządzenia.

(71) Niezależnie od tego czy funkcje wspierane przez usługi ICT mają charakter krytyczny lub istotny, 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 mają być przetwarzane dane, jak również wskazanie opisów gwarantowanych poziomów usług. Innymi elementami o podstawowym znaczeniu dla umożliwienia podmiotowi finansowemu monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT są: postanowienia umowne określające sposób, w jaki zewnętrzny dostawca usług ICT zapewnia dostęp, dostępność, integralność, bezpieczeństwo i ochronę danych osobowych, przepisy ustanawiające odpowiednie gwarancje umożliwiające dostęp do danych, ich odzyskiwanie i zwrot w przypadku niewypłacalności, rozwiązania, zaprzestania działalności gospodarczej zewnętrznego dostawcy usług ICT, a także przepisy nakładające na zewnętrznych dostawców usług ICT wymóg udzielania pomocy w przypadku incydentów związanych ze świadczonymi usługami ICT bez dodatkowych kosztów lub za opłatą określoną *ex ante*; przepisy dotyczące obowiązku pełnej współpracy zewnętrznego dostawcy usług ICT z właś-

([20]) Dyrektywa Parlamentu Europejskiego i Rady 2014/59/UE z dnia 15 maja 2014 r. ustanawiająca ramy na potrzeby prowadzenia działań naprawczych oraz restrukturyzacji i uporządkowanej likwidacji w odniesieniu do instytucji kredytowych i firm inwestycyjnych oraz zmieniająca dyrektywę Rady 82/891/EWG i dyrektywy Parlamentu Europejskiego i Rady 2001/24/WE, 2002/47/WE, 2004/25/WE, 2005/56/WE, 2007/36/WE, 2011/35/UE, 2012/30/UE i 2013/36/EU oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 i (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 190).

ciwymi organami i organami ds. restrukturyzacji i uporządkowanej likwidacji podmiotu finansowego; oraz przepisy dotyczące praw do wypowiedzenia umowy i związane z tym minimalne okresy wypowiedzenia ustaleń umownych, zgodnie oczekiwaniami właściwych organów i organów ds. restrukturyzacji i uporządkowanej likwidacji.

(72) W uzupełnieniu takich postanowień umownych i z myślą o zapewnieniu, aby podmioty finansowe zachowały pełną kontrolę nad wszelkimi wydarzeniami ze strony podmiotu zewnętrznego, które mogą mieć negatywny wpływ na ich bezpieczeństwo w obszarze ICT, w umowach na świadczenie usług ICT wspierających krytyczne lub istotne funkcje należy również przewidzieć następujące elementy: specyfikację pełnych opisów gwarantowanych poziomów usług wraz z dokładnymi ilościowymi i jakościowymi celami w zakresie wyników, aby umożliwić bez zbędnej zwłoki odpowiednie działania naprawcze w przypadku nieosiągnięcia uzgodnionych gwarantowanych poziomów usług; odpowiednie okresy wypowiedzenia i obowiązki zewnętrznego dostawcy usług ICT w zakresie zgłaszania incydentów w przypadku wydarzeń, które mogą mieć istotny wpływ na zdolność skutecznego świadczenia przez tego dostawcę odnośnych usług ICT; wymóg wobec zewnętrznego dostawcy usług ICT, by wdrażał i testował plany awaryjne w związku z prowadzoną działalnością oraz posiadał środki, narzędzia i polityki w zakresie bezpieczeństwa ICT, które umożliwiają bezpieczne świadczenie usług, oraz by uczestniczył w przeprowadzanych przez podmiot finansowy TLPT i w pełni współpracował w tym zakresie.

(73) Umowy na świadczenie usług ICT wspierających krytyczne lub istotne funkcje powinny również zawierać przepisy umożliwiające korzystanie z praw dostępu kontroli i audytu przez podmiot finansowy lub wyznaczoną osobę trzecią oraz prawa do sporządzania kopii jako kluczowych instrumentów bieżącego monitorowania przez podmioty finansowe wyników zewnętrznego dostawcy usług ICT w połączeniu z pełną współpracą tego ostatniego podczas kontroli. Analogicznie właściwemu organowi podmiotu finansowego powinno przysługiwać, na podstawie otrzymanych zawiadomień, podobne prawo do kontroli i audytu zewnętrznego dostawcy usług ICT, z zastrzeżeniem ochrony informacji poufnych.

(74) W takich ustaleniach umownych należy również przewidzieć specjalne strategie wyjścia umożliwiające w szczególności obowiązkowe okresy przejściowe, w których zewnętrzni dostawcy usług ICT powinni nadal świadczyć odpowiednie usługi, aby zmniejszyć ryzyko zakłóceń na poziomie podmiotu finansowego lub umożliwić temu ostatniemu skuteczne przejście do korzystania z innych zewnętrznych dostawców usług ICT lub, alternatywnie, skorzystanie z rozwiązań dostępnych w ramach struktury wewnętrznej, stosownie do stopnia złożoności świadczonej usługi ICT. Co więcej, podmioty finansowe objęte zakresem stosowania dyrektywy 2014/59/UE powinny zapewnić, by odpowiednie umowy na usługi ICT były solidne i w pełni egzekwowalne w przypadku restrukturyzacji i uporządkowanej likwidacji tych podmiotów finansowych. W związku z tym zgodnie z oczekiwaniami organów ds. restrukturyzacji i uporządkowanej likwidacji te podmioty finansowe powinny zapewnić, by odpowiednie umowy na usługi ICT wykazywały się odpornością na wypadek restrukturyzacji i uporządkowanej likwidacji. Dopóki te podmioty finansowe wypełniają swoje zobowiązania płatnicze, powinny zapewnić, by odpowiednie umowy dotyczące usług ITC – oprócz innych wymogów – zawierały też klauzule o niemożności ich wypowiedzenia, zawieszenia i modyfikacji z powodu restrukturyzacji lub uporządkowanej likwidacji.

(75) Ponadto dobrowolne stosowanie standardowych klauzul umownych opracowanych przez organy publiczne lub instytucje unijne, w szczególności stosowanie klauzul umownych opracowanych przez Komisję na potrzeby usług chmurowych może zapewnić dodatkowy komfort podmiotom finansowym i zewnętrznym dostawcom usług ICT poprzez zwiększenie poziomu pewności prawa w zakresie korzystania z usług chmurowych przez sektor finansowy, z zachowaniem pełnej zgodności z wymogami i oczekiwaniami określonymi w unijnych przepisach dotyczących usług finansowych. Prace służące opracowaniu standardowych klauzul umownych 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 chmurowych na zasadzie outsourcingu przez podmioty finansowe, czerpiąc z międzysektorowych wysiłków zainteresowanych podmiotów świadczących usługi chmurowe, które Komisja ułatwiła dzięki zaangażowaniu sektora finansowego.

(76) Aby wesprzeć ujednolicenie i poprawę efektywności podejść w zakresie nadzoru w odniesieniu do ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym oraz wzmocnić operacyjną odporność cyfrową podmiotów finansowych, które w przypadku usług ICT wspierających świadczenie usług finansowych polegają na kluczowych zewnętrznych dostawcach usług ICT, a tym samym przyczynić się do utrzymania stabilności systemu finansowego Unii oraz integralności wewnętrznego rynku usług finansowych, kluczowi zewnętrzni dostawcy usług ICT powinni być objęci unijnymi ramami nadzoru. Choć ustanowienie ram nadzoru jest uzasadnione z uwagi na wartość dodaną działań na szczeblu Unii oraz nieodłączną rolę i specyfikę korzystania z usług ICT w świadczeniu usług finansowych, należy jednocześnie przypomnieć, że rozwiązanie to wydaje się odpowiednie jedynie w kontekś-

cie niniejszego rozporządzenia, które dotyczy konkretnie operacyjnej odporności cyfrowej w sektorze finansowym. Niemniej jednak takich ram nadzoru nie należy uznawać za nowy model unijnego nadzoru w innych obszarach usług i działań finansowych.

(77) Ramy nadzoru powinny mieć zastosowanie wyłącznie do kluczowych zewnętrznych dostawców usług ICT. Należy zatem wprowadzić mechanizm wyznaczania, aby uwzględnić wymiar i charakter zależności sektora finansowego od takich zewnętrznych dostawców usług ICT. Mechanizm ten powinien obejmować zestaw kryteriów ilościowych i jakościowych, które określałyby parametry krytyczności jako podstawę do objęcia ramami nadzoru. Aby zapewnić dokładność tej oceny i niezależnie od struktury organizacyjnej zewnętrznego dostawcy usług ICT, takie kryteria powinny – w przypadku zewnętrznego dostawcy usług ICT będącego częścią szerszej grupy – uwzględniać całą strukturę grupy tego zewnętrznego dostawcy usług ICT. Z jednej strony kluczowi zewnętrzni dostawcy usług ICT, którzy nie zostali automatycznie wyznaczeni na podstawie wspomnianych wyżej kryteriów, powinni mieć możliwość dobrowolnego przystąpienia do ram nadzoru, natomiast z drugiej strony ci zewnętrzni dostawcy usług ICT, których objęto już ramami mechanizmu nadzoru wspierającymi realizację zadań Europejskiego Systemu Banków Centralnych, o których mowa w art. 127 ust. 2 TFUE, powinni zostać zwolnieni.

(78) Analogicznie podmioty finansowe, które świadczą usługi ICT na rzecz innych podmiotów finansowych, powinny być zwolnione z ram nadzoru – choć należą do kategorii zewnętrznych dostawców usług ICT na mocy niniejszego rozporządzenia – ponieważ podlegają już mechanizmom nadzorczym ustanowionym przez odpowiednie unijne przepisy dotyczące usług finansowych. W stosownych przypadkach w kontekście działań nadzorczych właściwe organy powinny też uwzględniać ryzyko związane z ICT dla podmiotów finansowych, które jest stwarzane przez podmioty finansowe świadczące usługi ICT. Podobnie ze względu na mechanizmy monitorowania ryzyka istniejące na poziomie grupy to samo zwolnienie powinno zostać wprowadzone względem zewnętrznych dostawców usług ICT świadczących usługi głównie na rzecz podmiotów w ramach swojej grupy. Zewnętrzni dostawcy usług ICT świadczący usługi wyłącznie w jednym państwie członkowskim na rzecz podmiotów finansowych działających tylko w tym państwie członkowskim również powinni zostać zwolnieni z mechanizmu wyznaczania ze względu na ich ograniczoną działalność i brak skutków transgranicznych.

(79) Transformacja cyfrowa zachodząca w usługach finansowych doprowadziła do bezprecedensowego poziomu wykorzystania usług ICT i uzależnienia się od nich. Ponieważ świadczenie usług finansowych bez korzystania z usług chmurowych, rozwiązań w zakresie oprogramowania i usług związanych z danymi nie jest już możliwe, unijny ekosystem finansowy stał się wewnętrznie współzależny od pewnych usług ICT świadczonych przez dostawców usług ICT. Niektórzy z tych dostawców, innowacyjni w opracowywaniu i stosowaniu technologii opartych na ICT, odgrywają znaczącą rolę w świadczeniu usług finansowych lub zostali włączeni do łańcucha wartości usług finansowych. Tym samym mają teraz kluczowe znaczenie dla stabilności i integralności unijnego systemu finansowego. Ta powszechna zależność od usług świadczonych przez kluczowych zewnętrznych dostawców usług ICT, w połączeniu ze współzależnością systemów informacyjnych różnych podmiotów gospodarczych, tworzy bezpośrednie i potencjalnie poważne ryzyko dla unijnego systemu usług finansowych i dla ciągłości świadczenia usług finansowych, gdyby kluczowych zewnętrznych dostawców usług ICT dotknęły zakłócenia operacyjne lub poważne cyberincydenty. Cyberincydenty charakteryzują się wyjątkową zdolnością do zwielokrotniania i rozprzestrzeniania się w całym systemie finansowym w znacznie szybszym tempie niż inne rodzaje ryzyka monitorowane w sektorze finansowym oraz mogą mieć zasięg międzysektorowy i wykraczać poza granice geograficzne. Mogą przekształcić się w kryzys systemowy, w którym zaufanie do systemu finansowego zostanie podkopane w wyniku zakłócenia funkcji wspierających gospodarkę realną lub w związku ze znacznymi stratami finansowymi, i osiągnąć poziom, na którym system finansowy nie będzie w stanie przetrwać lub będzie wymagać uruchomienia poważnych środków amortyzacji wstrząsów. Aby zapobiec urzeczywistnieniu tych scenariuszy, a przez to zagrożeniu stabilności finansowej i integralności Unii, należy zapewnić spójność praktyk nadzorczych dotyczących ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansów, w szczególności poprzez nowe przepisy umożliwiające unijny nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT.

(80) Ramy nadzoru w dużej mierze zależą od stopnia współpracy między wiodącym organem nadzorczym i kluczowym zewnętrznym dostawcą usług ICT, który dostarcza podmiotom finansowym usługi mające wpływ na świadczenie usług finansowych. Skuteczny nadzór opiera się m.in. na zdolności wiodącego organu nadzorczego do skutecznego przeprowadzania misji monitorujących i kontroli w celu oceny zasad, mechanizmów kontroli i procesów stosowanych przez kluczowych zewnętrznych dostawców usług ICT, a także potencjalnego skumulowanego wpływu ich działań na stabilność finansową i integralność systemu finansowego. Jednocześnie podstawowe znaczenie ma to, by kluczowi zewnętrzni dostawcy usług ICT stosowali się do zaleceń wiodącego organu nadzorczego i reagowali na jego uwagi. Ponieważ brak współpracy ze strony kluczowych zewnętrznych dostawców usług ICT dostarczających usługi mające wpływ na świadczenie usług finansowych, np. odmowa udzielenia dostępu do ich pomieszczeń lub przedłożenia informacji, ostatecznie skutkowałby sytuacją, w której wiodący organ nadzorczy zostałby pozbawiony podstawowych narzędzi umożliwiających ocenę ryzyka ze strony zewnętrznych dostawców usług ICT, i mógłby mieć negatywny wpływ na stabilność finansową i integralność systemu finansowego, należy też przewidzieć adekwatny system kar.

(81) W tym kontekście trudności związane z egzekwowaniem tych kar pieniężnych od kluczowych zewnętrznych dostawców usług ICT mających siedzibę w państwach trzecich nie mogą uniemożliwiać nałożenia przez wiodący organ nadzorczy kar pieniężnych w celu zmuszenia kluczowych zewnętrznych dostawców usług ICT do wypełnienia obowiązków w zakresie przejrzystości i dostępu określonych w niniejszym rozporządzeniu. Aby zapewnić możliwość wyegzekwowania takich kar oraz umożliwić szybkie uruchomienie procedur gwarantujących prawa kluczowych zewnętrznych dostawców usług ICT do obrony w kontekście mechanizmu wyznaczania i wydawania zaleceń, kluczowi zewnętrzni dostawcy usług ICT świadczący usługi podmiotom finansowym mające wpływ na świadczenie usług finansowych powinni być zobowiązani do utrzymywania odpowiedniej obecności biznesowej w Unii. Ze względu na charakter nadzoru i brak porównywalnych ustaleń w innych jurysdykcjach nie istnieją odpowiednie alternatywne mechanizmy zapewniające osiągnięcie tego celu poprzez skuteczną współpracę z organami nadzoru finansowego w państwach trzecich w odniesieniu do monitorowania wpływu cyfrowego ryzyka operacyjnego ze strony systemowych zewnętrznych dostawców usług ICT kwalifikujących się jako kluczowi zewnętrzni dostawcy usług ICT mający siedzibę w państwach trzecich. W związku z tym, aby móc dalej świadczyć usługi ICT na rzecz podmiotów finansowych w Unii, zewnętrzni dostawcy usług ICT mający siedzibę w państwach trzecich, wyznaczeni jako kluczowi zgodnie z niniejszym rozporządzeniem powinni w ciągu 12 miesięcy od takiego wyznaczenia podjąć wszelkie działania niezbędne do uzyskania zdolności prawnej wewnątrz Unii w drodze ustanowienia jednostki zależnej, zgodnie z definicją zawartą w unijnym dorobku prawnym, a mianowicie w dyrektywie Parlamentu Europejskiego i Rady 2013/34/UE ([21]).

(82) Wymóg utworzenia jednostki zależnej w Unii nie powinien uniemożliwiać kluczowemu zewnętrznemu dostawcy usług ICT świadczenia usług ICT i powiązanego wsparcia technicznego z obiektów i infrastruktury znajdującej się poza Unią. Niniejsze rozporządzenie nie nakłada obowiązku lokalizacji danych, ponieważ nie nakłada wymogu, by czynności przechowywania i przetwarzania danych były przeprowadzane w Unii.

(83) Kluczowi zewnętrzni dostawcy usług ICT powinni mieć możliwość świadczenia usług ICT z dowolnego miejsca na świecie, niekoniecznie lub nie tylko z obiektów znajdujących się w Unii. Działania nadzorcze powinny być prowadzone w pierwszej kolejności w obiektach znajdujących się w Unii i poprzez kontakty z podmiotami znajdującymi się w Unii, w tym w jednostkach zależnych ustanowionych przez kluczowych zewnętrznych dostawców usług ICT zgodnie z niniejszym rozporządzeniem. Niemniej jednak takie działania wewnątrz Unii mogą być niewystarczające, by wiodący organ nadzorczy mógł w pełni i skutecznie wykonywać swoje obowiązki wynikające z niniejszego rozporządzenia. Wiodący organ nadzorczy powinien zatem mieć również możliwość wykonywania swoich odpowiednich uprawnień nadzorczych w państwach trzecich. Wykonywanie tych uprawnień w państwach trzecich powinno umożliwić wiodącemu organowi nadzorczemu zbadanie obiektów, z których kluczowy zewnętrzny dostawca usług ICT faktycznie świadczy usługi ICT lub usługi wsparcia technicznego lub nimi zarządza, i powinno pozwolić wiodącemu organowi nadzorczemu na kompleksowy ogląd i zrozumienie – pod kątem operacyjnym – sposobu, w jaki dany dostawca usług ICT zarządza ryzykiem związanym z ICT. Możliwość wykonywania przez wiodący organ nadzorczy – jako agencję unijną – uprawnień poza terytorium Unii powinna być należycie ustrukturyzowana i obwarowana stosownymi warunkami, w szczególności chodzi tu o zgodę ze strony danego kluczowego zewnętrznego dostawcy usług ICT. Podobnie odpowiednie organy państwa trzeciego powinny być poinformowane i nie wyrażać sprzeciwu w odniesieniu do działań wiodącego organu nadzorczego wykonywanych na ich terytorium. Aby jednak zapewnić skuteczne wdrożenie i bez uszczerbku dla odpowiednich kompetencji instytucji Unii i państw członkow-

([21]) Dyrektywa Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniająca dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylająca dyrektywy Rady 78/660/EWG i 83/349/EWG (Dz.U. L 182 z 29.6.2013, s. 19).

skich, takie uprawnienia muszą też być w pełni zakorzenione w porozumieniach o współpracy administracyjnej zawartych z odpowiednimi organami danego państwa trzeciego. Niniejsze rozporządzenie powinno zatem umożliwić EUN zawieranie porozumień o współpracy administracyjnej z odpowiednimi organami państw trzecich, które w żaden sposób nie powinny tworzyć zobowiązań prawnych w odniesieniu do Unii i jej państw członkowskich.

(84) Aby ułatwić komunikację z wiodącym organem nadzorczym i zapewnić odpowiednią reprezentację, kluczowi zewnętrzni dostawcy usług ICT będący częścią grupy powinni wyznaczyć jedną osobę prawną jako swój punkt koordynacyjny.

(85) Ramy nadzoru powinny pozostawać bez uszczerbku dla kompetencji państw członkowskich, jeżeli chodzi o prowadzenie własnych misji w zakresie sprawowania nadzoru lub monitorowania w odniesieniu do zewnętrznych dostawców usług ICT, których nie wyznaczono jako kluczowych na mocy niniejszego rozporządzenia, ale którzy są uznawani za istotnych na szczeblu krajowym.

(86) Aby wykorzystać wielowarstwową strukturę instytucjonalną w obszarze usług finansowych, Wspólny Komitet EUN powinien nadal zapewniać ogólną międzysektorową koordynację w odniesieniu do wszystkich kwestii dotyczących ryzyka związanego z ICT, zgodnie ze swoimi zadaniami w zakresie cyberbezpieczeństwa. Powinien być wspierany przez nowy podkomitet (zwany dalej „forum nadzoru"), który będzie prowadził prace przygotowawcze zarówno w zakresie indywidualnych decyzji skierowanych do kluczowych zewnętrznych dostawców usług ICT, jak i wydawania zbiorowych zaleceń, w szczególności w odniesieniu do 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.

(87) Aby zapewnić odpowiedni i skuteczny nadzór nad kluczowymi zewnętrznymi dostawcami usług ICT na szczeblu Unii, w niniejszym rozporządzeniu przewidziano, że dowolny z trzech EUN może zostać wyznaczony jako wiodący organ nadzorczy. Przypisanie poszczególnych kluczowych zewnętrznych dostawców usług ICT jednemu z trzech EUN powinno być oparte na ocenie tego, w którym sektorze finansowym dane podmioty finansowe przeważają i któremu z EUN sektor ten podlega. Podejście to powinno prowadzić do zrównoważonego podziału zadań i obowiązków między trzema EUN w kontekście sprawowania funkcji nadzorczych oraz powinno możliwie najlepiej wykorzystywać zasoby kadrowe i specjalistyczną wiedzę techniczną dostępne w każdym z trzech EUN.

(88) Wiodącym organom nadzorczym należy powierzyć niezbędne uprawnienia do prowadzenia dochodzeń, przeprowadzania kontroli na miejscu i kontroli zdalnych w obiektach i lokalizacjach kluczowych zewnętrznych dostawców usług ICT oraz uzyskiwania pełnych i aktualnych informacji. Uprawnienia te powinny umożliwić wiodącym organom nadzorczym 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 EUN roli wiodących organów nadzorczych jest jednym z warunków wstępnych do zrozumienia i wyeliminowania systemowego wymiaru ryzyka związanego z ICT w sektorze finansów. Wpływ kluczowych zewnętrznych dostawców usług ICT na unijny sektor finansowy oraz potencjalne problemy wynikające z powiązanym ryzykiem koncentracji w obszarze ICT wymagają przyjęcia wspólnego podejścia na szczeblu Unii. Jednoczesne przeprowadzanie licznych audytów i korzystanie z praw dostępu, wykonywane osobno przez szereg właściwych organów, przy niewielkiej lub braku jakiejkolwiek koordynacji pomiędzy nimi, uniemożliwiłoby organom nadzoru finansowego uzyskanie pełnego i kompleksowego przeglądu ryzyka ze strony zewnętrznych dostawców usług ICT w Unii, powodując też przy tym redundancję, obciążenie i złożoność na poziomie kluczowych zewnętrznych dostawców usług ICT, gdyby zostali oni objęci dużą liczbą wniosków o monitorowanie i kontrolę.

(89) Ze względu na to, że dla konkretnego dostawcy fakt bycia wyznaczonym jako kluczowy zewnętrzny dostawca usług ICT niesie za sobą poważne konsekwencje, niniejsze rozporządzenie powinno zapewniać przestrzeganie praw kluczowych zewnętrznych dostawców usług ICT w całym okresie wdrażania ram nadzoru. Zanim dostawcy zostaną wyznaczeni jako kluczowi, powinni oni przykładowo mieć prawo przedłożyć wiodącemu organowi nadzorczemu uzasadnione oświadczenie zawierające wszelkie istotne informacje na potrzeby oceny związanej z ich wyznaczeniem. W związku z tym, że wiodący organ nadzorczy powinien być uprawniony do przedstawiania zaleceń w zakresie ryzyka związanego z ICT oraz odpowiednich środków zaradczych, w tym prawa do sprzeciwiania się określonym ustaleniom umownym, które ostatecznie wpływają na stabilność podmiotu finansowego lub systemu finansowego, przed finalizacją tych zaleceń kluczowi dostawcy usług ICT również powinni mieć możliwość przedstawienia wyjaśnień dotyczących spodziewanego wpływu rozwiązań proponowanych w tych zaleceniach na klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia i zaproponowania rozwiązań służących

łagodzeniu ryzyka. Kluczowi dostawcy usług ICT, którzy nie zgadzają się z zaleceniami, również przedstawić uzasadnione wyjaśnienie powodów, dla których nie zamierzają przyjąć danego zalecenia. W przypadku gdy nieprzedstawienia takiego uzasadnienia lub uznania przedstawionego uzasadnienia za niewystarczające, wiodący organ nadzorczy powinien wydać publiczne ogłoszenie opisujące zwięźle kwestię niezgodności.

(90) Właściwe organy powinny mieć za zadanie sprawdzenie tego, czy zalecenia wydane przez wiodący organ nadzorczy w ramach jego funkcji dotyczących nadzoru ostrożnościowego nad podmiotami finansowymi są przestrzegane pod kątem merytorycznym. Właściwe organy powinny mieć możliwość wymagania od podmiotów finansowych, by te podjęły dodatkowe środki w celu zwalczania ryzyka stwierdzonego w zaleceniach wiodącego organu nadzorczego, oraz we właściwym czasie powinny wydać stosowne zawiadomienia. W przypadku gdy wiodący organ nadzorczy kieruje zalecenia do kluczowych zewnętrznych dostawców usług ICT, którzy podlegają nadzorowi na mocy dyrektywy (UE) 2022/2555, właściwe organy powinny mieć możliwość skonsultowania się, na zasadzie dobrowolności i przed przyjęciem dodatkowych środków, z właściwymi organami na mocy tej dyrektywy w celu przyjęcia skoordynowanego podejścia do danych kluczowych zewnętrznych dostawców usług ICT.

(91) Sprawowanie nadzoru powinno opierać się na trzech zasadach operacyjnych mających na celu zapewnienie: a) ścisłej koordynacji pomiędzy EUN działającymi jako wiodący organ nadzorczy, poprzez wspólną sieć nadzoru, b) spójności z ramami ustanowionymi dyrektywą (UE) 2022/2555 (poprzez dobrowolne konsultacje z organami na mocy tej dyrektywy w celu uniknięcia powielania środków ukierunkowanych na kluczowych zewnętrznych dostawców usług ICT), oraz c) staranności w celu zminimalizowania potencjalnego ryzyka zakłócenia usług świadczonych przez kluczowych dostawców usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia.

(92) Ramy nadzoru nie powinny zastępować, ani w żaden sposób lub w żadnej części stanowić zamiennika obowiązku 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. Analogicznie ramy nadzoru nie powinny mieć wpływu na pełną odpowiedzialność podmiotów finansowych za przestrzeganie i wywiązywanie się ze wszystkich zobowiązań prawnych ustanowionych w niniejszym rozporządzeniu i w odpowiednich przepisach dotyczących usług finansowych.

(93) Aby uniknąć powielania i nakładania się działań, właściwe organy powinny powstrzymać się od samodzielnego podejmowania jakichkolwiek środków mających na celu monitorowanie ryzyka ze strony kluczowych zewnętrznych dostawców usług ICT i w tym względzie powinny opierać się na ocenie odpowiednich wiodących organów nadzorczych. W każdym przypadku wszelkie środki należy uprzednio skoordynować i uzgodnić z danymi wiodącymi organami nadzorczymi *w kontekście* wykonywania zadań objętych ramami nadzoru.

(94) Aby wspierać ujednolicenie na szczeblu międzynarodowym stosowania najlepszych praktyk, które mają być stosowane przy dokonywaniu przeglądu i monitorowaniu cyfrowego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT, należy zachęcać EUN do zawierania porozumień o współpracy z odpowiednimi organami nadzoru i organami regulacyjnymi państw trzecich.

(95) Aby wykorzystać szczególne kompetencje, umiejętności techniczne i wiedzę pracowników specjalizujących się w ryzyku operacyjnym i ryzyku związanym z ICT w ramach właściwych organów, trzy EUN oraz – na zasadzie dobrowolności – właściwe organy na mocy dyrektywy (UE) 2022/2555 i wiodący organ nadzorczy powinny korzystać z umiejętności i wiedzy 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 realizacji działań nadzorczych, w tym dochodzeń ogólnych i kontroli u kluczowych zewnętrznych dostawców usług ICT, a także z myślą o wszelkich niezbędnych działaniach następczych.

(96) Choć koszty wynikające z zadań nadzorczych byłyby w pełni finansowane z opłat pobieranych od kluczowych zewnętrznych dostawców usług ICT, EUN prawdopodobnie poniosą, przed rozpoczęciem obowiązywania ram nadzoru, koszty wdrożenia specjalnych systemów ICT wspierających przyszły nadzór, ponieważ specjalne systemy ICT musiałyby zostać wcześniej opracowane i wdrożone. W związku z tym niniejsze rozporządzenie przewiduje model finansowania hybrydowego, w ramach którego ramy nadzoru jako takie byłyby w całości finansowane z opłat, a opracowywanie systemów ICT w EUN byłoby finansowane ze środków unijnych i wkładów wnoszonych przez właściwe organy krajowe.

(97) Właściwe organy powinny posiadać wszelkie wymagane uprawnienia w zakresie sprawowania nadzoru, prowadzenia dochodzeń i nakładania kar, aby zapewnić prawidłowe wykonywanie obowiązków spoczywających na nich na mocy niniejszego rozporządzenia. Powinny one co do zasady publikować zawiadomienia o nakładanych karach administracyjnych. Ponieważ podmioty finansowe i zewnętrzni dostawcy usług ICT mogą mieć siedziby w różnych państwach członkowskich oraz podlegać nadzorowi różnych właściwych organów, należy ułatwić stosowanie niniejszego rozporządzenia, z jednej strony, poprzez ścisłą współpracę pomiędzy odpowiednimi właściwymi organami, w tym EBC w zakresie zadań szczególnych powierzonych mu na mocy rozporządzenia Rady (UE) nr 1024/2013, oraz, z drugiej strony, poprzez konsultacje z EUN w drodze wzajemnej wymiany informacji i dzięki zapewnieniu pomocy w kontekście odpowiedniej działalności nadzorczej.

(98) 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 przyjmowania aktów zgodnie z art. 290 TFUE, aby uzupełnić niniejsze rozporządzenie w odniesieniu do bardziej szczegółowego określenia skutków systemowych, jakie awaria lub przestój operacyjny zewnętrznego dostawcy usług ICT mogłyby mieć dla podmiotów finansowych, na rzecz których świadczy usługi, 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 danym rynku, kosztów migracji danych i nakładów pracy w zakresie ICT do innych zewnętrznych dostawców usług ICT, 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 były one prowadzone zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([22]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te powinny otrzymywać wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji powinni systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(99) Regulacyjne standardy techniczne powinny zapewniać spójną harmonizację wymogów ustanowionych w niniejszym rozporządzeniu. Opracowanie projektów regulacyjnych standardów technicznych, które nie wymagają podejmowania decyzji politycznych, w celu przedłożenia Komisji, należy powierzyć EUN działającym jako organy dysponujące wysokim poziomem wiedzy specjalistycznej. Należy opracować regulacyjne standardy techniczne w dziedzinie zarządzania ryzykiem związanym z ICT, zgłaszania poważnych incydentów związanych z ICT, testowania i w odniesieniu do najważniejszych wymogów dotyczących należytego monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT. Komisja i EUN powinny zapewnić, aby wspomniane standardy i wymogi mogły być stosowane przez wszystkie podmioty finansowe w sposób proporcjonalny do ich wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności ich usług, działań i operacji. Komisja powinna być uprawniona do przyjmowania tych regulacyjnych standardów technicznych w drodze aktów delegowanych zgodnie z art. 290 TFUE oraz zgodnie z art. 10–14 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

(100) W celu ułatwienia porównywalności sprawozdań dotyczących poważnych incydentów związanych z ICT i poważnych incydentów operacyjnych lub poważnych incydentów w zakresie bezpieczeństwa związanych z płatnościami oraz w celu zapewnienia przejrzystości w zakresie ustaleń umownych dotyczących korzystania z usług ICT świadczonych przez zewnętrznych dostawców usług ICT, EUN powinny opracować projekty wykonawczych standardów technicznych ustanawiających standardowe wzory, formularze i procedury dla podmiotów finansowych na potrzeby zgłaszania poważnych incydentów związanych z ICT i poważnych incydentów operacyjnych lub poważnych incydentów w zakresie bezpieczeństwa związanych z płatnościami, jak również standardowych wzorów na potrzeby rejestrowania informacji. Przy opracowywaniu tych standardów EUN powinny brać pod uwagę wielkość i ogólny profil ryzyka danego podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji. Komisja powinna być uprawniona do przyjmowania tych wykonawczych standardów technicznych w drodze aktów wykonawczych zgodnie z art. 291 TFUE oraz zgodnie z art. 15 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 oraz (UE) nr 1095/2010.

([22]) Dz.U. L 123 z 12.5.2016, s. 1.

(101) Ponieważ dalsze wymogi określono już w aktach delegowanych i wykonawczych opartych na regulacyjnych i wykonawczych standardach technicznych w rozporządzeniach Parlamentu Europejskiego i Rady (WE) nr 1060/2009 ([23]), (UE) nr 648/2012 ([24]), (UE) nr 600/2014 ([25]) i (UE) nr 909/2014 ([26]), należy upoważnić EUN, 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.

(102) Ponieważ niniejsze rozporządzenie, wraz z dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2556 ([27]), pociąga za sobą konsolidację przepisów dotyczących zarządzania ryzykiem związanym z ICT obejmujących wiele rozporządzeń i dyrektyw z unijnego dorobku prawnego w zakresie usług finansowych, w tym rozporządzeń (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) nr 909/2014 oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/1011 ([28]), w celu zapewnienia pełnej spójności należy zmienić te rozporządzenia, aby wyjaśnić, że mające zastosowanie przepisy dotyczące ryzyka związanego z ICT ustanowiono w niniejszym rozporządzeniu.

(103) W związku z tym zakres odpowiednich artykułów związanych z ryzykiem operacyjnym, na mocy których powierzono uprawnienia ustanowione w rozporządzeniach (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 (UE) nr 909/2014 oraz (UE) 2016/1011 do przyjmowania aktów delegowanych i wykonawczych, należy zawęzić z myślą o przeniesieniu do niniejszego rozporządzenia wszystkich przepisów obejmujących aspekty operacyjnej odporności cyfrowej stanowiących obecnie część tych rozporządzeń.

(104) Potencjalne systemowe ryzyko w cyberprzestrzeni związane z wykorzystywaniem infrastruktury ICT umożliwiającej funkcjonowanie systemów płatniczych i prowadzenie działań w zakresie przetwarzania płatności powinno być należycie uwzględnione na szczeblu Unii poprzez zharmonizowane przepisy dotyczące odporności cyfrowej. W tym celu Komisja powinna szybko ocenić potrzebę dokonania przeglądu zakresu stosowania niniejszego rozporządzenia, dostosowując taki przegląd do wyniku kompleksowego przeglądu przewidzianego na mocy dyrektywy (UE) 2015/2366. Liczne ataki na wielką skalę w ostatnim dziesięcioleciu pokazują, że systemy płatności są narażone na cyberzagrożenia. Systemy płatnicze i działania w zakresie przetwarzania płatności, które zostały umieszczone w centrum łańcucha usług płatniczych i wykazują silne powiązania z ogólnym systemem finansowym, mają obecnie podstawowe znaczenie dla funkcjonowania unijnych rynków finansowych. Cyberataki na takie systemy mogą powodować poważne zakłócenia w działalności operacyjnej i mieć bezpośredni wpływ na najważniejsze funkcje gospodarcze, takie jak uproszczenie płatności, oraz pośrednie skutki dla powiązanych procesów gospodarczych. Do czasu wprowadzenia na szczeblu Unii zharmonizowanego systemu oraz nadzoru nad operatorami systemów płatniczych i podmiotami prowadzącymi czynności przetwarzania, państwa członkowskie mogą, przy stosowaniu przepisów wobec operatorów systemów płatniczych i podmiotów prowadzących czynności przetwarzania podlegających nadzorowi w ramach ich jurysdykcji – z myślą o stosowaniu podobnych praktyk rynkowych – inspirować się wymogami w zakresie operacyjnej odporności cyfrowej ustanowionymi w niniejszym rozporządzeniu.

([23]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 z dnia 16 września 2009 r. w sprawie agencji ratingowych (Dz.U. L 302 z 17.11.2009, s. 1).

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

([25]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 84).

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

([27]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2556 z dnia 14 grudnia 2022 r. zmieniająca dyrektywy 2009/65/WE, 2009/138/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 oraz (UE) 2016/2341 w odniesieniu do operacyjnej odporności cyfrowej sektora finansowego (zob. s. 153 niniejszego Dziennika Urzędowego).

([28]) 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).

(105) Ponieważ cel niniejszego rozporządzenia, a mianowicie osiągnięcie wysokiego poziomu operacyjnej odporności cyfrowej w odniesieniu do regulowanych podmiotów finansowych, nie może zostać w wystarczającym stopniu osiągnięty przez państwa członkowskie, gdyż wymaga harmonizacji wielu różnych przepisów w prawie Unii i prawie krajowym, natomiast ze względu na skalę i skutki osiągnięcie tego celu 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 artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(106) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([29]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia 10 maja 2021 r. ([30]),

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot

1. W celu osiągnięcia wysokiego wspólnego poziomu operacyjnej odporności cyfrowej w niniejszym rozporządzeniu ustanawia się następujące jednolite wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych wspierających procesy biznesowe podmiotów finansowych:

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

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

   (ii) zgłaszania poważnych incydentów związanych z ICT właściwym organom oraz dobrowolnego informowania ich o znaczących cyberzagrożeniach;

   (iii) zgłaszania właściwym organom przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)–d), poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami;

   (iv) testowania operacyjnej odporności cyfrowej;

   (v) wymiany informacji i analiz w związku z cyberzagrożeniami i podatnościami w tym obszarze;

   (vi) środków na rzecz należytego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT;

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

c) zasady dotyczące ustanowienia i funkcjonowania ram 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 podmioty kluczowe lub ważne zgodnie z przepisami krajowymi transponującymi art. 3 dyrektywy (UE) 2022/2555 niniejsze rozporządzenie uznaje się za sektorowy akt prawny Unii do celów art. 4 tej dyrektywy.

3. Niniejsze rozporządzenie pozostaje bez uszczerbku dla odpowiedzialności państw członkowskich w zakresie podstawowych funkcji państwa dotyczących bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego zgodnie prawem Unii.

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

([30]) Dz.U. C 229 z 15.6.2021, s. 16.

Artykuł 2

Zakres stosowania

1. Bez uszczerbku dla ust. 3 i 4 niniejsze rozporządzenie ma zastosowanie do następujących podmiotów:

a) instytucji kredytowych;

b) instytucji płatniczych, w tym instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366;

c) dostawców świadczących usługę dostępu do informacji o rachunku;

d) instytucji pieniądza elektronicznego, w tym instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE;

e) firm inwestycyjnych;

f) dostawców usług w zakresie kryptoaktywów, którzy uzyskali zezwolenie na mocy rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptoaktywów oraz zmieniającego rozporządzenia (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektywy 2013/36/UE i (UE) 2019/1937 (zwanego dalej „rozporządzeniem w sprawie rynków kryptoaktywów") i emitentów tokenów powiązanych z aktywami;

g) centralnych depozytów papierów wartościowych;

h) kontrahentów centralnych;

i) systemów obrotu;

j) repozytoriów transakcji;

k) zarządzających alternatywnymi funduszami inwestycyjnymi;

l) spółek zarządzających;

m) dostawców usług w zakresie udostępniania informacji;

n) zakładów ubezpieczeń i zakładów reasekuracji;

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

p) instytucji pracowniczych programów emerytalnych;

q) agencji ratingowych;

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 ust. 1 lit. a)–t), są wspólnie określane jako „podmioty finansowe".

3. Niniejsze rozporządzenie nie ma zastosowania do:

a) zarządzających alternatywnymi funduszami inwestycyjnymi, o których mowa w art. 3 ust. 2 dyrektywy 2011/61/UE;

b) zakładów ubezpieczeń i zakładów reasekuracji, o których mowa w art. 4 dyrektywy 2009/138/WE;

c) instytucji pracowniczych programów emerytalnych, które obsługują programy emerytalne liczące łącznie nie więcej niż 15 uczestników;

d) osób fizycznych lub prawnych zwolnionych zgodnie z art. 2 i 3 dyrektywy 2014/65/UE;

e) pośredników ubezpieczeniowych, pośredników reasekuracyjnych i pośredników oferujących ubezpieczenia uzupełniające będących mikroprzedsiębiorstwami, małymi lub średnimi przedsiębiorstwami;

f) instytucji świadczących żyro pocztowe, o których mowa w art. 2 ust. 5 pkt 3 dyrektywy 2013/36/UE.

4. Państwa członkowskie mogą wyłączyć z zakresu stosowania niniejszego rozporządzenia podmioty, o których mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE, mające siedzibę na ich odpowiednich terytoriach. Jeżeli państwo członkowskie korzysta z takiej możliwości, informuje o tym Komisję oraz o wszelkich późniejszych zmianach w tym względzie. Komisja podaje te informacje do wiadomości publicznej na swojej stronie internetowej lub za pomocą innych łatwo dostępnych środków.

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 operacyjnej integralności i niezawodności 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, w tym w trakcie zakłóceń;

2) „sieci i systemy informatyczne" oznaczają sieci i systemy informatyczne zdefiniowane w art. 6 pkt 1 dyrektywy (UE) 2022/2555;

3) „dotychczasowy system ICT" oznacza system ICT, którego cykl życia dobiegł końca (koniec okresu użytkowania), którego ze względów technologicznych i komercyjnych nie można zmodernizować ani naprawić, lub który nie jest już obsługiwany przez dostawcę lub zewnętrznego dostawcę usług ICT, ale który nadal jest wykorzystywany i wspiera funkcje danego podmiotu finansowego;

4) „bezpieczeństwo sieci i systemów informatycznych" oznacza bezpieczeństwo sieci i systemów informatycznych zdefiniowane w art. 6 pkt 2 dyrektywy (UE) 2022/2555;

5) „ryzyko związane z ICT" oznacza każdą dającą się racjonalnie określić okoliczność związaną z użytkowaniem sieci i systemów informatycznych, która – jeżeli dojdzie do jej urzeczywistnienia – może zagrozić bezpieczeństwu sieci i systemów informatycznych, dowolnego narzędzia lub procesu zależnego od technologii, bezpieczeństwu operacji i procesów lub świadczeniu usług poprzez wywoływanie negatywnych skutków w środowisku cyfrowym lub fizycznym;

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

7) „zasób ICT" oznacza oprogramowanie lub zasoby komputerowe w sieci i systemach informatycznych wykorzystywanych przez dany podmiot finansowy;

8) „incydent związany z ICT" oznacza pojedyncze zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez dany podmiot finansowy, które zagrażają bezpieczeństwu sieci i systemów informatycznych i mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych lub na usługi świadczone przez ten podmiot finansowy;

9) „incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami" oznacza zdarzenie lub serię powiązanych ze sobą zdarzeń, nieplanowanych przez podmioty finansowe, o których mowa w art. 2 ust. 1 lit. a)–d), związanych z ICT lub nie, które mają negatywny wpływ na dostępność, autentyczność, integralność lub poufność danych związanych z płatnościami lub świadczonych usług związanych z płatnościami realizowanymi przez dany podmiot finansowy;

10) „poważny incydent związany z ICT" oznacza incydent związany z ICT o dużym negatywnym wpływie na sieci i systemy informatyczne, które wspierają krytyczne lub istotne funkcje podmiotu finansowego;

11) „poważny incydent operacyjny lub poważny incydent w zakresie bezpieczeństwa związany z płatnościami" oznacza incydent operacyjny lub incydent w zakresie bezpieczeństwa związany z płatnościami o dużym negatywnym wpływie na świadczone usługi związane z płatnościami;

12) „cyberzagrożenie" oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

13) „znaczące cyberzagrożenie" oznacza cyberzagrożenie, którego charakterystyka techniczna wskazuje, że potencjalnie może spowodować poważny incydent związany z ICT lub poważny incydent operacyjny lub poważny incydent w zakresie bezpieczeństwa związany z płatnościami;

14) „cyberatak" oznacza złośliwy incydent związany z ICT wywołany przez próbę zniszczenia, ujawnienia, zmiany, dezaktywacji, kradzieży lub uzyskania nieuprawnionego dostępu do składnika aktywów lub jego nieuprawnionego wykorzystania przez jakiegokolwiek agresora;

15) „analiza zagrożeń" oznacza informacje, które zostały zagregowane, przekształcone, przeanalizowane, zinterpretowane lub wzbogacone w celu zapewnienia niezbędnego kontekstu na potrzeby podejmowania decyzji i umożliwienia odpowiedniego i wystarczającego zrozumienia 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;

16) „podatność" oznacza słabość, wrażliwość lub wadę zasobu, systemu, procesu lub kontroli, które można wykorzystać;

17) „testy penetracyjne pod kątem wyszukiwania zagrożeń (TLPT)" oznaczają ramy naśladujące taktykę, techniki i procedury stosowane w rzeczywistości przez agresorów uznanych za stanowiących rzeczywiste cyberzagrożenie, które zapewniają kontrolowane, dostosowane do konkretnych zagrożeń, oparte na analizie zagrożeń (*red team*) testy działających na bieżąco krytycznych systemów produkcji podmiotu finansowego;

18) „ryzyko ze strony zewnętrznych dostawców usług ICT" oznacza ryzyko związane z ICT, które może wystąpić w przypadku podmiotu finansowego w związku z korzystaniem przez niego z usług ICT świadczonych przez zewnętrznych dostawców usług ICT lub przez ich podwykonawców, w tym w drodze uzgodnień dotyczących outsourcingu;

19) „zewnętrzny dostawca usług ICT" oznacza przedsiębiorstwo świadczące usługi ICT;

20) „dostawca usług ICT wewnątrz grupy" oznacza przedsiębiorstwo, które jest częścią grupy finansowej i które świadczy głównie usługi ICT na rzecz podmiotów finansowych należących do tej samej grupy lub podmiotów finansowych należących do tego samego systemu ochrony instytucjonalnej, w tym ich jednostek dominujących, jednostek zależnych, oddziałów lub innych podmiotów będących wspólną własnością lub pod wspólną kontrolą;

21) „usługi ICT" oznaczają usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej;

22) „krytyczna lub istotna funkcja" oznacza funkcję, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu lub której zaprzestanie lub wadliwe lub zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych;

23) „kluczowy zewnętrzny dostawca usług ICT" oznacza zewnętrznego dostawcę usług ICT wyznaczonego zgodnie z art. 31;

24) „zewnętrzny dostawca usług ICT z siedzibą w państwie trzecim" oznacza zewnętrznego dostawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim i który zawarł z podmiotem finansowym ustalenie umowne o świadczenie usług ICT;

25) „jednostka zależna" oznacza jednostkę zależną w rozumieniu art. 2 pkt 10 i art. 22 dyrektywy 2013/34/UE;

26) „grupa" oznacza grupę zdefiniowaną w art. 2 pkt 11 dyrektywy 2013/34/UE;

27) „jednostka dominująca" oznacza jednostkę dominującą w rozumieniu art. 2 pkt 9 i art. 22 dyrektywy 2013/34/UE;

(28) „podwykonawca usług ICT z siedzibą w państwie trzecim" oznacza podwykonawcę usług ICT, który jest osobą prawną mającą siedzibę w państwie trzecim i który zawarł ustalenie umowne z zewnętrznym dostawcą usług ICT albo z zewnętrznym dostawcą usług ICT mającym siedzibę w państwie trzecim;

29) „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 braki po stronie tych ostatnich mogą potencjalnie zagrozić zdolności podmiotu finansowego do wypełniania krytycznych lub istotnych funkcji lub przyczynić się do poniesienia przez ten podmiot innego rodzaju negatywnych skutków, w tym dużych strat, lub zagrozić stabilności finansowej Unii jako całości;

30) „organ zarządzający" oznacza organ zarządzający zdefiniowany w 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 ([31]), art. 2 ust. 1 pkt 45 rozporządzenia (UE) nr 909/2014, art. 3 ust. 1 pkt 20 rozporządzenia (UE) 2016/1011, oraz w odpowiednim przepisie rozporządzenia w sprawie rynków kryptoaktywów lub równorzędne osoby, które faktycznie zarządzają podmiotem lub pełnią kluczowe funkcje zgodnie z odpowiednimi przepisami unijnymi lub krajowymi;

31) „instytucja kredytowa" oznacza instytucję kredytową zdefiniowaną w art. 4 ust. 1 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 ([32]);

32) „instytucja zwolniona zgodnie z dyrektywą 2013/36/UE" oznacza podmiot, o którym mowa w art. 2 ust. 5 pkt 4–23 dyrektywy 2013/36/UE;

33) „firma inwestycyjna" oznacza firmę inwestycyjną zdefiniowaną w art. 4 ust. 1 pkt 1 dyrektywy 2014/65/UE;

34) „mała i niepowiązana wzajemnie firma inwestycyjna" oznacza firmę inwestycyjną, która spełnia warunki określone w art. 12 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/2033 ([33]);

35) „instytucja płatnicza" oznacza instytucję płatniczą zdefiniowaną w art. 4 pkt 4 dyrektywy (UE) 2015/2366;

36) „instytucja płatnicza zwolniona zgodnie z dyrektywą (UE) 2015/2366" oznacza instytucję płatniczą zwolnioną zgodnie z art. 32 ust. 1 dyrektywy (UE) 2015/2366;

37) „dostawca świadczący usługę dostępu do informacji o rachunku" oznacza dostawcę świadczącego usługę dostępu do informacji o rachunku, o którym mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366;

38) „instytucja pieniądza elektronicznego" oznacza instytucję pieniądza elektronicznego zdefiniowaną w art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady 2009/110/WE;

39) „instytucja pieniądza elektronicznego zwolniona zgodnie z dyrektywą 2009/110/WE" oznacza instytucję pieniądza elektronicznego korzystającą z wyłączenia, o którym mowa w art. 9 ust. 1 dyrektywy 2009/110/WE;

40) „kontrahent centralny" oznacza CCP zdefiniowanego w art. 2 pkt 1 rozporządzenia (UE) nr 648/2012;

41) „repozytorium transakcji" oznacza repozytorium transakcji zdefiniowane w art. 2 pkt 2 rozporządzenia (UE) nr 648/2012;

42) „centralny depozyt papierów wartościowych" oznacza centralny depozyt papierów wartościowych zdefiniowany w art. 2 ust. 1 pkt 1 rozporządzenia (UE) nr 909/2014;

43) „system obrotu" oznacza system obrotu zdefiniowany w art. 4 ust. 1 pkt 24 dyrektywy 2014/65/UE;

44) „zarządzający alternatywnymi funduszami inwestycyjnymi" oznacza zarządzającego alternatywnymi funduszami inwestycyjnymi zdefiniowanego w art. 4 ust. 1 lit. b) dyrektywy 2011/61/UE;

45) „spółka zarządzająca" oznacza spółkę zarządzającą zdefiniowaną w art. 2 ust. 1 lit. b) dyrektywy 2009/65/WE;

46) „dostawca usług w zakresie udostępniania informacji" oznacza dostawcę usług w zakresie udostępniania informacji w rozumieniu rozporządzenia (UE) nr 600/2014, zgodnie z art. 2 ust. 1 pkt 34–36 tego rozporządzenia;

47) „zakład ubezpieczeń" oznacza zakład ubezpieczeń zdefiniowany w art. 13 pkt 1 dyrektywy 2009/138/WE;

48) „zakład reasekuracji" oznacza zakład reasekuracji zdefiniowany w art. 13 pkt 4 dyrektywy 2009/138/WE;

([31]) Dyrektywa Parlamentu Europejskiego i Rady 2009/65/WE z dnia 13 lipca 2009 r. w sprawie koordynacji przepisów ustawowych, wykonawczych i administracyjnych odnoszących się do przedsiębiorstw zbiorowego inwestowania w zbywalne papiery wartościowe (UCITS) (Dz.U. L 302 z 17.11.2009, s. 32).

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

([33]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/2033 z dnia 27 listopada 2019 r. w sprawie wymogów ostrożnościowych dla firm inwestycyjnych oraz zmieniające rozporządzenia (UE) nr 1093/2010, (UE) nr 575/2013, (UE) nr 600/2014 i (UE) nr 806/2014 (Dz.U. L 314 z 5.12.2019, s. 1).

49) „pośrednik ubezpieczeniowy" oznacza pośrednika ubezpieczeniowego zdefiniowanego w art. 2 ust. 1 pkt 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/97 ([34]);

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

51) „pośrednik reasekuracyjny" oznacza pośrednika reasekuracyjnego zdefiniowanego w art. 2 ust. 1 pkt 5 dyrektywy (UE) 2016/97;

52) „instytucja pracowniczych programów emerytalnych" oznacza instytucję pracowniczych programów emerytalnych zdefiniowaną w art. 6 pkt 1 dyrektywy (UE) 2016/2341;

53) „mała instytucja pracowniczych programów emerytalnych" oznacza instytucję pracowniczych programów emerytalnych, która obsługuje programy emerytalne liczące łącznie nie więcej niż 100 uczestników;

54) „agencja ratingowa" oznacza agencję ratingową zdefiniowaną w art. 3 ust. 1 lit. b) rozporządzenia (WE) nr 1060/2009;

55) „dostawca usług w zakresie kryptoaktywów" oznacza dostawcę usług w zakresie kryptoaktywów zdefiniowanego w odpowiednim przepisie rozporządzenia w sprawie rynków kryptoaktywów;

56) „emitent tokenów powiązanych z aktywami" oznacza emitenta tokenów powiązanych z aktywami zdefiniowanego w odpowiednim przepisie rozporządzenia w sprawie rynków kryptoaktywów;

57) „administrator kluczowych wskaźników referencyjnych" oznacza administratora kluczowych wskaźników referencyjnych zdefiniowanych w art. 3 pkt 25 rozporządzenia (UE) 2016/1011;

58) „dostawca usług finansowania społecznościowego" oznacza dostawcę usług finansowania społecznościowego zdefiniowanego w art. 2 ust. 1 lit. e) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2020/1503 ([35]);

59) „repozytorium sekurytyzacji" oznacza repozytorium sekurytyzacji zdefiniowane w art. 2 pkt 23 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2402 ([36]);

60) „mikroprzedsiębiorstwo" oznacza podmiot finansowy inny niż system obrotu, kontrahent centralny, repozytorium transakcji lub centralny depozyt papierów wartościowych, który zatrudnia mniej niż 10 osób i którego roczny obrót lub bilans roczny nie przekracza 2 mln EUR;

61) „wiodący organ nadzorczy" oznacza Europejski Urząd Nadzoru wyznaczony zgodnie z art. 31 ust. 1 lit. b) niniejszego rozporządzenia;

62) „Wspólny Komitet" oznacza komitet, o którym mowa w art. 54 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 oraz (UE) nr 1095/2010;

63) „małe przedsiębiorstwo" oznacza podmiot finansowy zatrudniający co najmniej 10 osób, ale mniej niż 50 osób, którego roczny obrót lub bilans roczny przekracza 2 mln EUR, ale nie przekracza 10 mln EUR;

64) „średnie przedsiębiorstwo" oznacza podmiot finansowy niebędący małym przedsiębiorstwem, zatrudniający mniej niż 250 osób i którego roczny obrót nie przekracza 50 mln EUR lub którego bilans roczny nie przekracza 43 mln EUR;

65) „organ publiczny" oznacza każdy rząd lub inny podmiot administracji publicznej, w tym krajowe banki centralne.

([34]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/97 z dnia 20 stycznia 2016 r. w sprawie dystrybucji ubezpieczeń (Dz.U. L 26 z 2.2.2016, s. 19).

([35]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/1503 z dnia 7 października 2020 r. w sprawie europejskich dostawców usług finansowania społecznościowego dla przedsięwzięć gospodarczych oraz zmieniające rozporządzenie (UE) 2017/1129 i dyrektywę (UE) 2019/1937 (Dz.U. L 347 z 20.10.2020, s. 1).

([36]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2402 z dnia 12 grudnia 2017 r. w sprawie ustanowienia ogólnych ram dla sekurytyzacji oraz utworzenia szczególnych ram dla prostych, przejrzystych i standardowych sekurytyzacji, a także zmieniające dyrektywy 2009/65/WE, 2009/138/WE i 2011/61/UE oraz rozporządzenia (WE) nr 1060/2009 i (UE) nr 648/2012 (Dz.U. L 347 z 28.12.2017, s. 35).

Artykuł 4

Zasada proporcjonalności

1. Podmioty finansowe stosują przepisy ustanowione w rozdziale II zgodnie z zasadą proporcjonalności, biorąc pod uwagę swoją wielkość i ogólny profil ryzyka oraz charakter, skalę i stopień złożoności swoich usług, działań i operacji.

2. Dodatkowo podmioty finansowe stosują rozdział III, IV i rozdział V sekcja I w sposób proporcjonalny do swojej wielkości i ogólnego profilu ryzyka oraz charakteru, skali i stopnia złożoności swoich usług, działań i operacji, jak szczegółowo przewidziano w odpowiednich przepisach tych rozdziałów.

3. Właściwe organy analizują stosowanie zasady proporcjonalności przez podmioty finansowe przy dokonywaniu przeglądu spójności ram zarządzania ryzykiem związanym z ICT na podstawie sprawozdań przedkładanych na żądanie właściwych organów zgodnie z art. 6 ust. 5 i art. 16 ust. 2.

ROZDZIAŁ II

Zarządzanie ryzykiem związanym z ICT

Sekcja I

Artykuł 5

Zarządzanie i organizacja

1. Podmioty finansowe posiadają wewnętrzne ramy zarządzania i kontroli, które zapewniają skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka związanego z ICT, zgodnie z art. 6 ust. 4, w celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej.

2. Organ zarządzający podmiotu finansowego określa, zatwierdza i nadzoruje wdrażanie wszystkich ustaleń dotyczących ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 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) wprowadza polityki mające zapewnić utrzymanie wysokich standardów dostępności, autentyczności, integralności i poufności danych;

c) ustala wyraźne role i obowiązki w odniesieniu do wszystkich funkcji związanych z ICT i ustanawia odpowiednie rozwiązania w zakresie zarządzania, aby zapewnić skuteczną i terminową komunikację, współpracę i koordynację przy wykonywaniu tych funkcji;

d) ponosi pełną odpowiedzialność za określenie i zatwierdzenie strategii operacyjnej odporności cyfrowej, o czym mowa w art. 6 ust. 8, w tym za określenie odpowiedniego poziomu tolerancji ryzyka związanego z ICT danego podmiotu finansowego, o czym mowa w art. 6 ust. 8 lit. b);

e) zatwierdza i nadzoruje wdrażanie strategii na rzecz ciągłości działania podmiotu finansowego w zakresie ICT oraz planów reagowania i przywracania sprawności ICT, o których mowa odpowiednio w art. 11 ust. 1 i 3 i które mogą być przyjmowane jako specjalna strategia szczegółowa stanowiąca integralną część ogólnej strategii na rzecz ciągłości działania oraz planu reagowania i przywracania sprawności danego podmiotu finansowego, oraz okresowo dokonuje przeglądu wdrażania tej strategii i tych planów;

f) zatwierdza plany podmiotu finansowego dotyczące wewnętrznych audytów ICT, audyty ICT i ich istotne zmiany i okresowo dokonuje ich przeglądu;

g) przydziela odpowiedni budżet w celu zaspokojenia potrzeb podmiotu finansowego w zakresie operacyjnej odporności cyfrowej w odniesieniu do wszystkich rodzajów zasobów, w tym odpowiednich programów zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkoleń w zakresie operacyjnej odporności cyfrowej, o których mowa w art. 13 ust. 6, i umiejętności ICT dla wszystkich pracowników, i okresowo dokonuje jego przeglądu;

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

i) wprowadza na szczeblu przedsiębiorstwa kanały dokonywania zgłoszeń umożliwiające uzyskiwanie odpowiednich informacji na temat:

(i) ustaleń zawartych z zewnętrznymi dostawcami usług ICT w sprawie korzystania z usług ICT,

(ii) wszelkich planowanych istotnych zmian dotyczących zewnętrznych dostawców usług ICT,

(iii) potencjalnego wpływu takich zmian na krytyczne lub istotne funkcje objęte tymi ustaleniami, w tym streszczenia analizy ryzyka w celu oceny wpływu tych zmian, oraz co najmniej na temat poważnych incydentów związanych z ICT i ich wpływu jak również na temat środków reagowania, środków przywracania sprawności i środków naprawczych.

3. Podmioty finansowe inne niż mikroprzedsiębiorstwa ustanawiają funkcję w celu monitorowania 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 podmiotu finansowego aktywnie aktualizują wiedzę i umiejętności wystarczające do zrozumienia i oceny ryzyka związanego z ICT i jego wpływu na operacje podmiotu finansowego, w tym poprzez regularny udział w specjalnych szkoleniach, współmiernych do zarządzanego ryzyka związanego z ICT.

Sekcja II

Artykuł 6

Ramy zarządzania ryzykiem związanym z ICT

1. Podmioty finansowe dysponują – jako częścią swojego ogólnego systemu zarządzania ryzykiem – 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.

2. Ramy zarządzania ryzykiem związanym z ICT obejmują co najmniej strategie, polityki, procedury, protokoły i narzędzia ICT niezbędne do należytej i odpowiedniej ochrony wszystkich odpowiednich zasobów informacyjnych i zasobów ICT, w tym oprogramowania i sprzętu komputerowego, serwerów, a także wszystkich odpowiednich elementów fizycznych i infrastruktury, takich jak obiekty, ośrodki przetwarzania danych i wyznaczone obszary wrażliwe, w celu zapewnienia odpowiedniej ochrony wszystkich zasobów informacyjnych i zasobów ICT 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 ICT, zgodnie ze swoimi ramami zarządzania ryzykiem związanym z ICT. Dostarczają one właściwym organom, na ich żądanie, pełnych i aktualnych informacji na temat ryzyka związanego z ICT oraz swoich ram zarządzania ryzykiem związanym z ICT.

4. Podmioty finansowe inne niż mikroprzedsiębiorstwa powierzają obowiązek zarządzania ryzykiem związanym z ICT i nadzór nad nim funkcji kontroli oraz zapewniają odpowiedni poziom niezależności takiej funkcji kontroli w celu uniknięcia konfliktów interesów. Podmioty finansowe zapewniają odpowiednie rozdzielenie i niezależność funkcji zarządzania ryzykiem związanym z ICT, funkcji kontroli oraz funkcji audytu wewnętrznego, zgodnie z modelem trzech linii obrony lub wewnętrznym modelem zarządzania ryzykiem i kontroli ryzyka.

5. Ramy zarządzania ryzykiem związanym z ICT są dokumentowane i poddawane przeglądowi co najmniej raz w roku, lub okresowo w przypadku mikroprzedsiębiorstw, 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. Sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT przedkłada się właściwemu organowi na jego żądanie.

6. Ramy zarządzania ryzykiem związanym z ICT podmiotów finansowych innych niż mikroprzedsiębiorstwa są regularnie poddawane audytowi wewnętrznemu przeprowadzanemu przez audytorów zgodnie z planami tych podmiotów finansowych dotyczącymi audytów. Audytorzy ci posiadają wystarczającą wiedzę, umiejętności i wiedzę fachową w zakresie ryzyka związanego z ICT oraz mają odpowiednią niezależność. Częstotliwość i przedmiot audytów ICT są współmierne do ryzyka związanego z ICT danego podmiotu finansowego.

7. W oparciu o wnioski z przeglądu audytowego, podmioty finansowe ustanawiają formalny proces działań następczych, w tym zasady terminowej weryfikacji oraz wdrażania środków zaradczych w następstwie krytycznych ustaleń audytu ICT.

8. Ramy zarządzania ryzykiem związanym z ICT obejmują strategię operacyjnej odporności cyfrowej, w której określono sposób wdrażania tych ram. W tym celu strategia operacyjnej odporności cyfrowej zawiera metody przeciwdziałania ryzyku związanemu z ICT i osiągania szczególnych celów w dziedzinie ICT poprzez:

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

b) ustalenie limitu tolerancji ryzyka w odniesieniu do ryzyka związanego z ICT, zgodnie z gotowością podmiotu finansowego do podejmowania ryzyka, oraz analizę tolerancji wpływu zakłóceń w funkcjonowaniu ICT;

c) określenie jasnych celów w zakresie bezpieczeństwa informacji, w tym najważniejszych wskaźników efektywności i kluczowych wskaźników ryzyka;

d) objaśnienie referencyjnej architektury ICT oraz wszelkich zmian niezbędnych do osiągnięcia konkretnych celów biznesowych;

e) przedstawienie poszczególnych mechanizmów wprowadzonych w celu wykrywania incydentów związanych z ICT, zapobiegania ich skutkom i ochrony przed nimi;

f) dokumentowanie obecnej sytuacji w zakresie operacyjnej odporności cyfrowej na podstawie liczby zgłoszonych poważnych incydentów związanych z ICT oraz skuteczności środków zapobiegawczych;

g) wdrożenie testowania operacyjnej odporności cyfrowej, zgodnie z rozdziałem IV niniejszego rozporządzenia;

h) przedstawienie strategii komunikacji w przypadku incydentów związanych z ICT, których ujawnienie jest wymagane zgodnie z art. 14.

9. Podmioty finansowe mogą, w kontekście strategii operacyjnej odporności cyfrowej, o której mowa w ust. 8, określić całościową strategię obejmującą wielu dostawców ICT, na poziomie grupy lub podmiotu, przedstawiając w niej kluczowe zależności od zewnętrznych dostawców usług ICT i wyjaśniając przesłanki łączenia zamówień u różnych zewnętrznych dostawców usług ICT.

10. Podmioty finansowe mogą, zgodnie z unijnym i krajowym prawem sektorowym, zlecić w drodze outsourcingu zadania związane ze sprawdzaniem zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT przedsiębiorstwom wewnątrz grupy lub przedsiębiorstwom zewnętrznym. W przypadku takiego outsourcingu podmiot finansowy pozostaje w pełni odpowiedzialny za sprawdzanie zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT.

Artykuł 7

Systemy, protokoły i narzędzia ICT

Aby wyeliminować ryzyko związane z ICT i nim zarządzać, podmioty finansowe wykorzystują i utrzymują zaktualizowane systemy, protokoły i narzędzia ICT, które:

a) są odpowiednie do skali operacji wspierających prowadzenie ich działalności, zgodnie z zasadą proporcjonalności, o której mowa w art. 4;

b) są wiarygodne;

c) mają wystarczającą zdolność do dokładnego przetwarzania danych niezbędnych do prowadzenia działalności i terminowego świadczenia usług 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 wymaganymi w skrajnych warunkach rynkowych lub w innych niekorzystnych sytuacjach.

Artykuł 8

Identyfikacja

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe identyfikują, klasyfikują i odpowiednio dokumentują wszystkie wspierane przez ICT funkcje biznesowe, zadania i obowiązki, zasoby informacyjne i zasoby ICT wspierające te funkcje oraz ich zadania i zależności w odniesieniu do ryzyka związanego z ICT. Podmioty finansowe dokonują w miarę potrzeb, a co najmniej raz w roku, przeglądu adekwatności tej klasyfikacji 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 podatności w obszarze ICT istotne dla ich funkcji biznesowych wspieranych przez ICT, zasobów informacyjnych i zasobów 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 biznesowe wspierane przez ICT, zasoby informacyjne lub zasoby ICT.

4. Podmioty finansowe wskazują wszystkie zasoby informacyjne i zasoby ICT, w tym zasoby zdalne, zasoby sieciowe i sprzęt komputerowy, oraz ewidencjonują te z nich, które są uznawane za krytyczne. Podmioty finansowe ewidencjonują konfigurację zasobów informacyjnych i zasobów ICT oraz powiązania i współzależności między poszczególnymi zasobami informacyjnymi i zasobami ICT.

5. Podmioty finansowe wskazują i dokumentują wszystkie procesy, które zależą od zewnętrznych dostawców usług ICT, oraz wskazują wzajemne powiązania z zewnętrznymi dostawcami usług ICT, którzy świadczą usługi wspierające krytyczne lub istotne funkcje.

6. Do celów ust. 1, 4 i 5 podmioty finansowe utrzymują odpowiednie wykazy, które są aktualizowane okresowo i przy każdej większej zmianie, o której mowa w ust. 3.

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

Artykuł 9

Ochrona i zapobieganie

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

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

3. Aby osiągnąć cele, o których mowa w ust. 2, podmioty finansowe stosują rozwiązania i procesy ICT, które są odpowiednie, zgodnie z art. 4. Te rozwiązania i procesy ICT:

a) zapewniają bezpieczeństwo środków przekazywania danych;

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

c) zapobiegają brakowi dostępności, osłabianiu autentyczności i integralności, naruszeniom poufności i utracie danych;

d) zapewniają ochronę danych przed ryzykiem związanym z zarządzaniem danymi, w tym ryzykiem związanym z niewłaściwym administrowaniem, przetwarzaniem i błędem ludzkim.

4. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe:

a) opracowują i dokumentują politykę bezpieczeństwa informacji określającą zasady ochrony dostępności, autentyczności, integralności oraz poufności danych, zasobów informacyjnych i zasobów ICT, w tym, w stosownych przypadkach danych, zasobów informacyjnych i zasobów ICT swoich klientów;

b) zgodnie z podejściem opartym na analizie ryzyka ustalają należyte zarządzanie siecią i infrastrukturą z wykorzystaniem odpowiednich technik, metod i protokołów, które mogą obejmować wdrażanie zautomatyzowanych mechanizmów izolowania zasobów informacyjnych na wypadek cyberataków;

c) wdrażają polityki ograniczające fizyczny lub logiczny dostęp do zasobów informacyjnych i zasobów 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 praw zarządzania dostępem i zapewniających należyte zarządzanie tymi prawami;

d) wdrażają polityki i protokoły dotyczące silnych mechanizmów uwierzytelniania, oparte na odpowiednich standardach i specjalnych systemach kontroli oraz środkach ochrony kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka związanego z ICT;

e) wdrażają udokumentowane polityki, procedury i kontrole w zakresie zarządzania zmianą w systemach ICT, w tym zmianami w oprogramowaniu, sprzęcie komputerowym, komponentach oprogramowania sprzętowego, parametrach systemowych lub parametrach 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 udokumentowaną politykę dotyczącą poprawek i aktualizacji.

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

Do celów akapitu pierwszego lit. e) proces zarządzania zmianami ICT jest zatwierdzany przez właściwe struktury kierownicze i opiera się na specjalnych protokołach.

Artykuł 10

Wykrywanie

1. Podmioty finansowe dysponują mechanizmami pozwalającymi na szybkie wykrywanie nietypowych działań, zgodnie z art. 17, w tym problemów związanych z wydajnością sieci ICT i incydentów związanych z ICT, oraz na identyfikację potencjalnych istotnych pojedynczych punktów awarii.

Wszystkie mechanizmy wykrywania, o których mowa w akapicie pierwszym, są regularnie testowane zgodnie z art. 25.

2. Mechanizmy wykrywania, o których mowa w ust. 1, umożliwiają wielopoziomową kontrolę, określają progi alarmowe i kryteria uruchamiania i inicjowania procesów reagowania na incydenty związane z ICT, łącznie z automatycznymi mechanizmami ostrzegawczymi dla odpowiednich pracowników odpowiedzialnych za reagowanie na incydenty związane z ICT.

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

4. Dostawcy usług w zakresie udostępniania informacji dodatkowo posiadają systemy umożliwiające skuteczną kontrolę raportów z transakcji pod kątem kompletności, wykrywanie przeoczeń i oczywistych błędów oraz żądanie ponownego przesłania takich sprawozdań.

Artykuł 11

Reagowanie i przywracania sprawności

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, oraz w oparciu o wymogi dotyczące identyfikacji określone w art. 8, podmioty finansowe wprowadzają kompleksową strategię na rzecz ciągłości działania w zakresie ICT, która może zostać przyjęta jako specjalna odrębna strategia stanowiąca integralną część ogólnej strategii na rzecz operacyjnej ciągłości działania podmiotu finansowego.

2. Podmioty finansowe realizują strategię na rzecz ciągłości działania w zakresie ICT poprzez specjalne, odpowiednie i udokumentowane ustalenia, plany, procedury i mechanizmy, których celem jest:

a) zapewnienie ciągłości pełnienia przez podmiot finansowy jego krytycznych lub istotnych funkcji;

b) szybkie, właściwe i skuteczne reagowanie na wszystkie incydenty związane z ICT i ich rozwiązywanie w sposób ograniczający szkody i nadający priorytet wznowieniu działań i działaniom mającym na celu przywrócenie systemów;

c) 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 sprawności, które to procedury zostały ustanowione zgodnie z art. 12;

d) szacowanie wstępnych skutków, szkód i strat;

e) określanie działań w zakresie komunikacji i zarządzania kryzysowego, które zapewniają przekazywanie aktualnych informacji wszystkim odpowiednim pracownikom wewnętrznym i zewnętrznym interesariuszom zgodnie z art. 14 i zgłaszanie ich właściwym organom zgodnie z art. 19.

3. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe wdrażają powiązane z ich działalnością plany reagowania i przywracania sprawności ICT, które w przypadku podmiotów finansowych innych niż mikroprzedsiębiorstwa podlegają niezależnym wewnętrznym przeglądom audytowym.

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

5. Jako część ogólnej strategii na rzecz ciągłości działania podmioty finansowe przeprowadzają analizę wpływu na działalność (BIA) swojego narażenia na poważne zakłócenia działalności gospodarczej. W ramach BIA podmioty finansowe oceniają potencjalny wpływ poważnych zakłóceń w działalności gospodarczej przy użyciu kryteriów ilościowych i jakościowych, z wykorzystaniem danych wewnętrznych i zewnętrznych oraz analizy scenariuszowej, stosownie do przypadku. BIA uwzględnia krytyczność zidentyfikowanych i zgrupowanych funkcji biznesowych, procesów wsparcia, zależności od zewnętrznych dostawców usług i zasobów informacyjnych, oraz ich współzależności. Podmioty finansowe zapewniają, by zasoby ICT i usługi ICT były projektowane i wykorzystywane z zachowaniem pełnej zgodności z BIA, w szczególności jeśli chodzi o odpowiednie zapewnienie redundancji wszystkich krytycznych komponentów.

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

a) co najmniej raz w roku oraz po wprowadzeniu istotnych zmian w systemach ICT wspierających krytyczne lub istotne funkcje testują plany ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT w odniesieniu do systemów ICT wspierających wszystkie funkcje;

b) testują plany działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej ustanowione zgodnie z art. 14.

Do celów akapitu pierwszego lit. a) podmioty finansowe inne niż mikroprzedsiębiorstwa uwzględniają w planach testowania scenariusze cyberataków i pracy awaryjnej w trakcie przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności w zakresie ICT, kopie zapasowe i urządzenia redundantne, które są konieczne do wypełniania obowiązków określonych w art. 12.

Podmioty finansowe dokonują regularnych przeglądów swojej strategii na rzecz ciągłości działania w zakresie ICT oraz planów przywracania sprawności ICT, uwzględniając wyniki testów przeprowadzonych zgodnie z akapitem pierwszym oraz zalecenia wynikające z kontroli audytowych lub przeglądów nadzorczych.

7. Podmioty finansowe inne niż mikroprzedsiębiorstwa posiadają funkcję zarządzania w sytuacji kryzysowej, w której – w przypadku uruchomienia ich planów ciągłości działania w zakresie ICT lub planów reagowania i przywracania sprawności ICT – określono między innymi. jasne procedury zarządzania wewnętrznymi i zewnętrznymi działaniami informacyjnymi na wypadek wystąpienia sytuacji kryzysowej zgodnie z art. 14.

8. W przypadku uruchomienia planów ciągłości działania w zakresie ICT i planów reagowania i przywracania sprawności ICT podmioty finansowe prowadzą łatwo dostępną ewidencję działań prowadzonych przed wystąpieniem zakłóceń i w trakcie ich wystąpienia.

9. Centralne depozyty papierów wartościowych dostarczają właściwym organom kopie wyników testów ciągłości działania w zakresie ICT lub podobnych testów.

10. Podmioty finansowe inne niż mikroprzedsiębiorstwa zgłaszają właściwym organom, na żądanie, szacunkowe łączne roczne koszty i straty spowodowane poważnymi incydentami związanymi z ICT.

11. Zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 do dnia 17 lipca 2024 r. EUN, za pośrednictwem Wspólnego Komitetu, opracowują wspólne wytyczne w sprawie szacowania łącznych rocznych kosztów i strat, o których mowa w ust. 10.

Artykuł 12

Polityki i procedury tworzenia kopii zapasowych oraz metody i procedury przywracania i odzyskiwania danych

1. W celu zapewnienia przywrócenia systemów ICT i danych przy minimalnej przerwie, ograniczonych zakłóceniach i stratach, w kontekście ram zarządzania ryzykiem związanym z ICT podmioty finansowe opracowują i dokumentują:

a) polityki i procedury tworzenia kopii zapasowych, w których określono zakres danych, które obejmuje kopia zapasowa, oraz minimalną częstotliwość tworzenia kopii zapasowej, w oparciu o krytyczność informacji lub poziom poufności danych;

b) procedury i metody przywracania i odzyskiwania danych.

2. Podmioty finansowe ustanawiają systemy tworzenia kopii zapasowych, które mogą być uruchamiane zgodnie z politykami i procedurami tworzenia kopii zapasowych oraz procedurami i metodami przywracania i odzyskiwania danych. Uruchomienie systemów tworzenia kopii zapasowych nie może zagrażać bezpieczeństwu sieci i systemów informatycznych ani dostępności, autentyczności, integralności ani poufności danych. Procedury tworzenia kopii zapasowych a także procedury i metody przywracania i odzyskiwania danych są testowane okresowo.

3. Przywracając dane z kopii zapasowych przy użyciu własnych systemów, podmioty finansowe korzystają z systemów ICT, które są oddzielone fizycznie i logicznie od ich głównego systemu ICT. Systemy ICT są zabezpieczone przed wszelkim nieupoważnionym dostępem lub uszkodzeniem w zakresie ICT i umożliwiają terminowe przywrócenie usług w razie potrzeby przy wykorzystaniu kopii zapasowych danych i systemów.

W przypadku kontrahentów centralnych plany przywracania sprawności umożliwiają odzyskanie wszystkich transakcji realizowanych w chwili wystąpienia zakłócenia, tak aby umożliwić kontrahentowi centralnemu dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie.

Dostawcy usług w zakresie udostępniania informacji dodatkowo utrzymują odpowiednie zasoby i dysponują urządzeniami służącymi do tworzenia kopii zapasowych i przywracania danych, by móc przez cały czas oferować i utrzymywać swoje usługi.

4. Podmioty finansowe inne niż mikroprzedsiębiorstwa utrzymują nadmiarowe zdolności w zakresie ICT posiadające zasoby, zdolności i funkcje, które są odpowiednie do zaspokojenia potrzeb biznesowych. Mikroprzedsiębiorstwa oceniają potrzebę utrzymywania takich nadmiarowych zdolności w zakresie ICT wyłącznie w oparciu o swój profil ryzyka.

5. Centralne depozyty papierów wartościowych utrzymują co najmniej jedną zapasową lokalizację przetwarzania danych, wyposażoną w odpowiednie zasoby, zdolności, funkcje i personel do zaspokojenia potrzeb biznesowych.

Zapasowa 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 krytycznych lub istotnych funkcji identycznie jak w przypadku głównego miejsca przetwarzania danych lub świadczyć usługi na poziomie niezbędnym do zapewnienia realizacji przez podmiot finansowy operacji krytycznych w ramach celów związanych z przywracaniem sprawności;

c) jest niezwłocznie dostępna dla personelu podmiotu finansowego, aby zapewnić ciągłość krytycznych lub istotnych funkcji, w przypadku gdy główne miejsce przetwarzania danych stanie się niedostępne.

6. Określając zakładany czas przywrócenia systemów oraz akceptowalny poziom utraty danych w odniesieniu do każdej funkcji, podmioty finansowe biorą pod uwagę, czy jest to krytyczna lub istotna funkcja, oraz potencjalny ogólny wpływ na efektywność rynku. Takie zakładane czasy przywrócenia systemów zapewniają osiągnięcie uzgodnionych gwarantowanych poziomów usług w scenariuszach warunków skrajnych.

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

Artykuł 13

Uczenie się i rozwój

1. Podmioty finansowe dysponują zdolnościami i personelem umożliwiającymi im gromadzenie informacji na temat podatności 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 przeprowadzonych po ich wystąpieniu, gdy taki poważny incydent związany z ICT spowoduje zakłócenia w ich głównej działalności, analizując przyczyny zakłócenia i identyfikując wymagane ulepszenia operacji ICT lub strategii na rzecz ciągłości działania w zakresie ICT, o której mowa w art. 11.

Podmioty finansowe inne niż mikroprzedsiębiorstwa informują właściwe organy, na żądanie, o zmianach wprowadzonych w następstwie przeglądów incydentów związanych z ICT przeprowadzonych po ich wystąpieniu, o których mowa w akapicie pierwszym.

W ramach przeglądów incydentów związanych z ICT, przeprowadzanych po ich wystąpieniu, o których mowa w akapicie pierwszym, 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 dotkliwości;

b) jakości i szybkości przeprowadzania analizy śledczej, w stosownych przypadkach;

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. 26 i 27 oraz z rzeczywistych incydentów związanych z ICT, w szczególności cyberataków, wraz z wyzwaniami związanymi z uruchomieniem planów ciągłości działania w zakresie ICT oraz planów reagowania i przywracania sprawności ICT, a także z odpowiednimi informacjami wymienianymi z kontrahentami i ocenianymi podczas przeglądów nadzorczych. Ustalenia te stanowią podstawę stosownych przeglądów odpowiednich elementów ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1.

4. Podmioty finansowe monitorują skuteczność wdrażania swojej strategii operacyjnej odporności cyfrowej określonej w art. 6 ust. 8. 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, w szczególności w odniesieniu do krytycznych lub istotnych funkcji, oraz zwiększenia dojrzałości i gotowości danego 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, a ich poziom złożoności jest współmierny do funkcji pełnionych przez te osoby. W stosownych przypadkach podmioty finansowe obejmują też zewnętrznych dostawców usług ICT swoimi odnośnymi systemami szkoleń zgodnie z art. 30 ust. 2 lit. i).

7. Podmioty finansowe inne niż mikroprzedsiębiorstwa 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, aby skutecznie przeciwdziałać dotychczasowym lub nowym formom cyberataków.

Artykuł 14

Komunikacja

1. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, podmioty finansowe posiadają plany działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej umożliwiające odpowiedzialne ujawnianie, co najmniej, poważnych incydentów związanych z ICT lub podatności klientom i kontrahentom, a także, w stosownych przypadkach, opinii publicznej.

2. W kontekście ram zarządzania ryzykiem związanym z ICT podmioty finansowe realizują politykę komunikacyjną dla pracowników wewnętrznych i interesariuszy zewnętrznych. W polityce komunikacyjnej skierowanej do pracowników uwzględnia się potrzebę rozróżnienia między pracownikami zaangażowanymi w zarządzanie ryzykiem związanym z ICT, w szczególności pracownikami odpowiedzialnymi za reagowanie i przywracanie sprawności, a pracownikami, których należy informować.

3. Co najmniej jednej osobie w podmiocie finansowym powierza się zadanie wdrożenia strategii komunikacyjnej w zakresie incydentów związanych z ICT i w tym celu pełni ona funkcję osoby ds. kontaktów z opinią publiczną i mediami.

Artykuł 15

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

EUN, za pośrednictwem Wspólnego Komitetu i w porozumieniu z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), opracowują wspólne projekty regulacyjnych standardów technicznych w celu:

a) doprecyzowania elementów, które należy uwzględnić w politykach, procedurach, protokołach i narzędziach w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2, w celu zapewnienia bezpieczeństwa sieci, odpowiednich zabezpieczeń przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem, zachowania dostępności, autentyczności, integralności oraz poufności danych, w tym technik kryptograficznych, oraz zagwarantowania dokładnego i szybkiego przesyłania danych bez poważnych zakłóceń i zbędnych opóźnień;

b) doprecyzowania elementów kontroli praw zarządzania dostępem, o których mowa w art. 9 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;

c) doprecyzowania elementów określonych w art. 10 ust. 1 umożliwiających szybkie wykrywanie nietypowych działań oraz określonych w art. 10 ust. 2 kryteriów uruchamiania procesów wykrywania incydentów związanych z ICT i reagowania na nie;

d) doprecyzowania elementów strategii na rzecz ciągłości działania w zakresie ICT, o której mowa w art. 11 ust. 1;

e) doprecyzowania testowania planów ciągłości działania w zakresie ICT, o których mowa w art. 11 ust. 6, aby zapewnić, by w ramach takiego testowania w należyty sposób uwzględniono scenariusze, w których jakość pełnienia krytycznej lub istotnej funkcji pogarsza się do niedopuszczalnego poziomu lub funkcja ta przestaje być pełniona, a także w należyty sposób uwzględniono potencjalny wpływ niewypłacalności lub innych rodzajów awarii któregokolwiek z odnośnych zewnętrznych dostawców usług ICT oraz, w stosownych przypadkach, ryzyko polityczne w jurysdykcjach odnośnych dostawców;

f) doprecyzowania elementów planów reagowania i przywracania sprawności ICT, o których mowa w art. 11 ust. 3;

g) doprecyzowania treści i formatu sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT, o którym mowa w art. 6 ust. 5.

Opracowując te projekty regulacyjnych standardów technicznych, EUN biorą pod uwagę wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji, a jednocześnie należycie uwzględniają szczególne cechy wynikające z wyjątkowego charakteru działalności w różnych sektorach usług finansowych.

EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 stycznia 2024 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 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

Artykuł 16

Uproszczone ramy zarządzania ryzykiem związanym z ICT

1. Art. 5–15 niniejszego rozporządzenia nie mają zastosowania do małych i niepowiązanych wzajemnie firm inwestycyjnych, instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366; instytucji zwolnionych zgodnie z dyrektywą 2013/36/UE, w odniesieniu do których państwa członkowskie podjęły decyzję o niewykorzystywaniu możliwości, o której mowa w art. 2 ust. 4 niniejszego rozporządzenia; instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE; oraz małych instytucji pracowniczych programów emerytalnych.

Bez uszczerbku dla akapitu pierwszego, podmioty finansowe wymienione w akapicie pierwszym:

a) wprowadzają i utrzymują prawidłowe i udokumentowane ramy zarządzania ryzykiem związanym z ICT, które wyszczególniają mechanizmy i środki mające na celu szybkie, skuteczne i kompleksowe zarządzanie ryzykiem związanym z ICT, w tym w celu ochrony odpowiednich elementów fizycznych i infrastruktury;

b) stale monitorują bezpieczeństwo i funkcjonowanie wszystkich systemów ICT;

c) minimalizują wpływ ryzyka związanego z ICT poprzez stosowanie prawidłowych, odpornych i zaktualizowanych systemów, protokołów i narzędzi ICT, które są odpowiednie do wspierania realizacji ich działań i świadczenia usług i odpowiednio chronią dostępność, autentyczność, integralność oraz poufność danych w sieci i systemach informatycznych;

d) umożliwiają szybką identyfikację i wykrywanie źródeł ryzyka związanego z ICT i nieprawidłowości w sieci i systemach informatycznych oraz szybkie reagowanie na incydenty związane z ICT;

e) określają najważniejsze zależności od zewnętrznych dostawców usług ICT;

f) zapewniają ciągłość krytycznych lub istotnych funkcji poprzez plany ciągłości działania oraz środki reagowania i przywracania sprawności, które obejmują co najmniej środki tworzenia kopii zapasowych i środki przywracania danych;

g) regularnie testują plany i środki, o których mowa w lit. f), a także skuteczność działań wdrożonych zgodnie z lit. a) i c);

h) wdrażają, stosownie do przypadku, odpowiednie wnioski operacyjne wynikające z testów, o których mowa w lit. g), oraz wnioski z analiz przeprowadzonych po wystąpieniu incydentu do procesu oceny ryzyka związanego z ICT i opracowują, stosownie do potrzeb i profilu ryzyka związanego z ICT, programy zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkoleń w zakresie operacyjnej odporności cyfrowej dla pracowników i kadry zarządzającej.

2. Ramy zarządzania ryzykiem związanym z ICT, o których mowa w ust. 1 akapit drugi lit. a), są udokumentowane oraz poddawane przeglądowi okresowo i po wystąpieniu poważnych incydentów związanych z ICT, zgodnie z instrukcjami nadzorczymi. Są one stale ulepszane na podstawie wniosków płynących z wdrażania i monitorowania. Sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT przedkłada się właściwemu organowi na jego żądanie.

3. EUN, za pośrednictwem Wspólnego Komitetu i w porozumieniu z ENISA, opracowują wspólne projekty regulacyjnych standardów technicznych w celu:

a) doprecyzowania elementów, jakie należy ująć w ramach zarządzania ryzykiem związanym z ICT, o którym mowa w ust. 1 akapit drugi lit. a);

b) doprecyzowania elementów związanych z systemami, protokołami i narzędziami, aby zminimalizować wpływ ryzyka związanego z ICT, o którym mowa w ust. 1 akapit drugi lit. c), w celu zapewnienia bezpieczeństwa sieci, odpowiednim zabezpieczeniu przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem oraz zachowania dostępności, autentyczności, integralności i poufności danych;

c) doprecyzowania elementów planów ciągłości działania w zakresie ICT, o których mowa w ust. 1 akapit drugi lit. f);

d) doprecyzowania przepisów dotyczących testowania planów ciągłości działania oraz zapewnienia skuteczności kontroli, o których mowa w ust. 1 akapit drugi lit. g) oraz zapewnienia, by w ramach takiego testowania w należyty sposób uwzględniono scenariusze, w których jakość pełnienia krytycznej lub istotnej funkcji pogarsza się do niedopuszczalnego poziomu lub funkcja ta przestaje być pełniona;

e) doprecyzowania treści i formatu sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT, o którym mowa w ust. 2.

Opracowując te projekty regulacyjnych standardów technicznych, EUN biorą pod uwagę wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji.

EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 stycznia 2024 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 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

ROZDZIAŁ III

Zarządzanie incydentami związanymi z ICT, ich klasyfikacja i zgłaszanie

Artykuł 17

Proces zarządzania incydentami związanymi z ICT

1. Podmioty finansowe określają, ustanawiają i wdrażają proces zarządzania incydentami związanymi z ICT w celu wykrywania incydentów związanych z ICT, zarządzania nimi i ich zgłaszania.

2. Podmioty finansowe rejestrują wszystkie incydenty związane z ICT i znaczące cyberzagrożenia. Podmioty finansowe ustanawiają odpowiednie procedury i procesy mające zapewnić spójne i zintegrowane monitorowanie incydentów związanych z ICT i obsługa takich incydentów oraz działania następcze w związku z takimi incydentami, aby zapewnić zidentyfikowanie, udokumentowanie 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) wprowadzenie wskaźników wczesnego ostrzegania;

b) ustanowienie procedur identyfikowania, śledzenia, rejestrowania, kategoryzowania i klasyfikowania incydentów związanych z ICT według ich priorytetu i dotkliwości oraz krytyczności usług, na które incydenty te mają wpływ, zgodnie z kryteriami określonymi w art. 18 ust. 1;

c) przydzielenie ról i obowiązków, które należy wprowadzić w przypadku różnych rodzajów incydentów związanych z ICT i odnośnych scenariuszy;

d) określenie planów działań informacyjnych skierowanych do pracowników, interesariuszy zewnętrznych i mediów zgodnie z art. 14 oraz planów powiadamiania klientów, planów dotyczących wewnętrznych procedur eskalacji, w tym skarg klientów związanych z ICT, jak również, w stosownych przypadkach, dostarczania informacji podmiotom finansowym działającym jako kontrahenci;

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

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

Artykuł 18

Klasyfikacja incydentów związanych z ICT i cyberzagrożeń

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

a) liczba lub znaczenie klientów lub kontrahentów finansowych oraz, w stosownych przypadkach, kwota lub liczba transakcji, których dotyczy incydent związany z ICT, oraz to, czy taki incydent spowodował skutki reputacyjne;

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

c) zasięg geograficzny incydentu związanego z ICT, w szczególności jeżeli dotyczy on więcej niż dwóch państw członkowskich;

d) utrata danych w wyniku incydentu związanego z ICT w kontekście dostępności, autentyczności, integralności lub poufności danych;

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

f) skutki gospodarcze incydentu związanego z ICT, w szczególności bezpośrednie i pośrednie koszty i straty, zarówno w kategoriach bezwzględnych, jak i względnych.

2. Podmioty finansowe klasyfikują cyberzagrożenia jako znaczące na podstawie krytyczności usług zagrożonych, w tym narażonych transakcji i operacji podmiotu finansowego, liczby lub znaczenia klientów lub kontrahentów finansowych oraz zasięgu geograficznego zagrożonych obszarów.

3. EUN, za pośrednictwem Wspólnego Komitetu i w porozumieniu z EBC i ENISA, opracowują wspólne projekty regulacyjnych standardów technicznych określające następujące elementy:

a) kryteria określone w ust. 1, w tym progi istotności do celów ustalania poważnych incydentów związanych z ICT lub, stosownie do przypadku, poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami, które podlegają obowiązkowi zgłaszania określonemu w art. 19 ust. 1;

b) kryteria, które mają być stosowane przez właściwe organy do celów oceny znaczenia poważnych incydentów związanych z ICT lub, stosownie do przypadku, poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami dla właściwych organów w innych państwach członkowskich, oraz szczegółowe informacje dotyczące zgłaszania poważnych incydentów związanych z ICT lub, stosownie do przypadku, poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami, które mają być udostępniane innym właściwym organom zgodnie z art. 19 ust. 6 lub 7;

c) kryteria określone w ust. 2 niniejszego artykułu, w tym wysokie progi istotności do celów ustalania znaczących cyberzagrożeń.

4. Opracowując wspólne projekty regulacyjnych standardów technicznych, o których mowa w ust. 3 niniejszego artykułu, EUN biorą pod uwagę kryteria określone w art. 4 ust. 2, a także standardy międzynarodowe, wytyczne i specyfikacje opracowane i opublikowane przez ENISA, w tym, w stosownych przypadkach, specyfikacje dotyczące innych sektorów gospodarki. Do celów stosowania kryteriów określonych w art. 4 ust. 2 EUN należycie uwzględniają konieczność zaangażowania przez mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa wystarczających zasobów i zdolności, by zapewnić sprawne zarządzanie incydentami związanymi z ICT.

EUN przedkładają Komisji te wspólne projekty regulacyjnych standardów technicznych do dnia 17 stycznia 2024 r.

Komisja jest uprawniona do uzupełnienia niniejszego rozporządzenia w drodze przyjmowania regulacyjnych standardów technicznych, o których mowa w ust. 3, zgodnie z art. 10–14 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

Artykuł 19

Zgłaszanie poważnych incydentów związanych z ICT i dobrowolne powiadamianie o znaczących cyberzagrożeniach

1. Podmioty finansowe zgłaszają poważne incydenty związane z ICT odpowiedniemu właściwemu organowi, o którym mowa w art. 46, zgodnie z ust. 4 niniejszego artykułu.

W przypadku gdy nadzór nad podmiotem finansowym sprawuje więcej niż jeden właściwy organ krajowy, o którym mowa w art. 46, państwa członkowskie wyznaczają jeden właściwy organ jako odpowiedni właściwy organ odpowiedzialny za wykonywanie funkcji i obowiązków przewidzianych w tym artykule.

Instytucje kredytowe sklasyfikowane jako istotne zgodnie z art. 6 ust. 4 rozporządzenia (UE) nr 1024/2013 zgłaszają poważne incydenty związane z ICT odpowiedniemu właściwemu organowi krajowemu wyznaczonemu zgodnie z art. 4 dyrektywy 2013/36/UE, który niezwłocznie przekazuje EBC takie sprawozdania.

Do celów akapitu pierwszego podmioty finansowe – po zebraniu i przeanalizowaniu wszystkich istotnych informacji – sporządzają wstępne powiadomienia i sprawozdania, o których mowa w ust. 4 niniejszego artykułu, wykorzystując wzory, o których mowa w art. 20, i przedkładają je właściwemu organowi. W przypadku gdy brak technicznej możliwości nie pozwala na przedłożenie wstępnego powiadomienia z wykorzystaniem wzoru, podmioty finansowe powiadamiają o tym właściwy organ za pomocą alternatywnych środków.

Wstępne powiadomienie i sprawozdania, o których mowa w ust. 4, zawierają wszystkie informacje niezbędne właściwemu organowi do określenia znaczenia poważnego incydentu związanego z ICT oraz do oceny ewentualnych skutków transgranicznych.

Bez uszczerbku dla dokonywania przez podmioty finansowe zgłoszenia zgodnie z akapitem pierwszym do odpowiedniego właściwego organu, państwa członkowskie mogą dodatkowo postanowić, że niektóre lub wszystkie podmioty finansowe mają również przekazywać wstępne powiadomienie i poszczególne sprawozdania, o których mowa w ust. 4 niniejszego artykułu, z wykorzystaniem wzorów, o których mowa w art. 20, właściwym organom lub zespołom reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) wyznaczonym lub ustanowionym zgodnie z dyrektywą (UE) 2022/2555.

2. Podmioty finansowe mogą dobrowolnie powiadomić odpowiedni właściwy organ o znaczących cyberzagrożeniach, jeżeli uznają dane zagrożenie za istotne dla systemu finansowego, użytkowników usług lub klientów. Odpowiedni właściwy organ może przekazać takie informacje innym odpowiednim organom, o których mowa w ust. 6.

Instytucje kredytowe sklasyfikowane jako istotne zgodnie z art. 6 ust. 4 rozporządzenia (UE) nr 1024/2013 mogą dobrowolnie powiadomić o znaczących cyberzagrożeniach odpowiedni właściwy organ krajowy wyznaczony zgodnie z art. 4 dyrektywy 2013/36/UE, który niezwłocznie przekazuje EBC takie powiadomienia.

Państwa członkowskie mogą postanowić, że te podmioty finansowe, które dobrowolnie przekazują takie powiadomienie zgodnie z akapitem pierwszym, mogą je również przekazać CSIRT wyznaczonym lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555

3. W przypadku gdy wystąpi poważny incydent związany z ICT, który ma istotny wpływ na interesy finansowe klientów, podmioty finansowe bez zbędnej zwłoki, gdy tylko się o nim dowiedzą, informują swoich klientów o poważnym incydencie związanym z ICT oraz o środkach, które podjęto w celu złagodzenia negatywnych skutków takiego incydentu.

W przypadku znaczącego cyberzagrożenia podmioty finansowe, w stosownych przypadkach, informują swoich klientów, których może ono dotyczyć, o wszelkich odpowiednich środkach ochrony, których podjęcie klienci ci mogą rozważyć.

4. W terminach, które zostaną określone zgodnie z art. 20 akapit pierwszy lit. a) ppkt (ii), podmioty finansowe przedkładają odpowiedniemu właściwemu organowi następujące dokumenty:

a) wstępne powiadomienie;

b) sprawozdanie śródokresowe po wstępnym powiadomieniu, o którym mowa w lit. a), jak tylko status pierwotnego incydentu ulegnie istotnej zmianie lub gdy w oparciu o nowe informacje zmienia się obsługa danego poważnego incydentu związanego z ICT; po tym sprawozdaniu, 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 łagodzące skutki incydentu, oraz po udostępnieniu danych dotyczących rzeczywistego wpływu zastępujących dane szacunkowe.

5. Podmioty finansowe mogą zlecić w drodze outsourcingu, zgodnie z unijnym i krajowym prawem sektorowym, zadania związane z obowiązkami sprawozdawczymi na mocy niniejszego artykułu zewnętrznemu dostawcy usług. W przypadku takiego outsourcingu podmiot finansowy pozostaje w pełni odpowiedzialny za spełnienie wymogów dotyczących zgłaszania incydentów.

6. Po otrzymaniu wstępnego powiadomienia i poszczególnych sprawozdań, o których mowa w ust. 4, właściwy organ w odpowiednim czasie przekazuje szczegółowe informacje na temat danego poważnego incydentu związanego z ICT następującym odbiorcom, z uwzględnieniem, stosownie do przypadku, ich odnośnych kompetencji:

a) EUNB, ESMA lub EIOPA;

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

c) właściwym organom, pojedynczym punktom kontaktowym lub CSIRT wyznaczonym lub ustanowionym zgodnie z dyrektywą (UE) 2022/2555;

d) organom ds. restrukturyzacji i uporządkowanej likwidacji, o których mowa w art. 3 dyrektywy 2014/59/UE, oraz Jednolitej Radzie ds. Restrukturyzacji i Uporządkowanej Likwidacji (SRB) w odniesieniu do podmiotów, o których mowa w art. 7 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 806/2014 ([37]), i w odniesieniu do podmiotów i grup, o których mowa w art. 7 ust. 4 lit. b) i ust. 5 tego rozporządzenia, jeżeli takie szczegółowe informacje dotyczą incydentów, które mogą zagrażać zapewnieniu funkcji krytycznych w rozumieniu art. 2 ust. 1 pkt 35 dyrektywy 2014/59/UE; oraz

e) innym odpowiednim organom publicznym zgodnie z prawem krajowym.

7. Po otrzymaniu informacji zgodnie z ust. 6 EUNB, ESMA lub EIOPA i EBC, w porozumieniu z ENISA i we współpracy z odpowiednim właściwym organem, oceniają, czy dany poważny incydent związany z ICT jest istotny dla właściwych organów w innych państwach członkowskich. Po dokonaniu tej oceny EUNB, ESMA lub EIOPA jak najszybciej powiadamiają o jej wynikach odpowiednie właściwe organy w innych państwach członkowskich. 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.

([37]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 806/2014 z dnia 15 lipca 2014 r. ustanawiające jednolite zasady i jednolitą procedurę restrukturyzacji i uporządkowanej likwidacji instytucji kredytowych i niektórych firm inwestycyjnych w ramach jednolitego mechanizmu restrukturyzacji i uporządkowanej likwidacji oraz jednolitego funduszu restrukturyzacji i uporządkowanej likwidacji oraz zmieniające rozporządzenie (UE) nr 1093/2010 (Dz.U. L 225 z 30.7.2014, s. 1).

8. Powiadomienie, które ma zostać przekazane przez ESMA zgodnie z ust. 7 niniejszego artykułu, pozostaje bez uszczerbku dla spoczywającego na odnośnym właściwym organie obowiązku pilnego przekazania szczegółowych informacji na temat danego poważnego incydentu związanego z ICT odpowiedniemu organowi w przyjmującym państwie członkowskim, w którym centralny depozyt papierów wartościowych prowadzi znaczącą działalność transgraniczną, w którym incydent ten prawdopodobnie spowoduje poważne konsekwencje dla jego rynków finansowych i w którym istnieją ustalenia dotyczące współpracy między właściwymi organami w zakresie nadzoru nad podmiotami finansowymi.

Artykuł 20

Harmonizacja treści i wzorów zgłoszeń

EUN, za pośrednictwem Wspólnego Komitetu i w porozumieniu z ENISA i EBC, opracowują:

a) wspólne projekty regulacyjnych standardów technicznych w celu:

   (i) ustalenia treści zgłoszeń dotyczących poważnych incydentów związanych z ICT, aby odzwierciedlić kryteria określone w art. 18 ust. 1 i włączyć dodatkowe elementy, takie jak szczegółowe informacje służące ustaleniu, czy zgłoszone zdarzenie jest istotne dla innych państw członkowskich i czy stanowi poważny incydent operacyjny lub poważny incydent w zakresie bezpieczeństwa związany z płatnościami;

   (ii) określenia terminów dotyczących wstępnego powiadomienia i poszczególnych sprawozdań, o których mowa w art. 19 ust. 4;

   (iii) ustalenia treści powiadomienia o znaczących cyberzagrożeniach.

   Opracowując te projekty regulacyjnych standardów technicznych, EUN biorą pod uwagę wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji, w szczególności z myślą o zapewnieniu, by – do celów lit. a) ppkt (ii) niniejszego akapitu – różne terminy mogły odzwierciedlać, stosownie do przypadku, specyfikę poszczególnych sektorów finansowych, bez uszczerbku dla utrzymania spójnego podejścia do kwestii zgłaszania poważnych incydentów związanych z ICT zgodnie z niniejszym rozporządzeniem i dyrektywą (UE) 2022/2555. W stosownych przypadkach EUN przedstawiają uzasadnienie odstąpienia od podejścia przyjętego w kontekście tej dyrektywy;

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 i powiadamiania o znaczących cyberzagrożeniach.

EUN przedkładają Komisji wspólne projekty regulacyjnych standardów technicznych, o których mowa w akapicie pierwszym lit. a), oraz wspólne projekty wykonawczych standardów technicznych, o których mowa w akapicie pierwszym lit. b), do dnia 17 lipca 2024 r.

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

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

Artykuł 21

Centralizacja zgłaszania poważnych incydentów związanych z ICT

1. EUN, 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. We wspólnym 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. Wspólne sprawozdanie, o którym mowa w ust. 1, obejmuje co najmniej:

a) warunki wstępne do utworzenia jednego unijnego węzła informacyjnego;

b) korzyści, ograniczenia i rodzaje ryzyka, w tym ryzyko związane z dużą koncentracją informacji szczególnie chronionych;

c) zdolności niezbędne do zapewnienia interoperacyjności w odniesieniu do innych istotnych systemów sprawozdawczości;

d) elementy zarządzania operacyjnego;

e) warunki członkostwa;

f) ustalenia techniczne umożliwiające dostęp podmiotów finansowych i właściwych organów krajowych do jednego unijnego węzła informacyjnego;

g) wstępną ocenę kosztów finansowych poniesionych w związku z utworzeniem platformy operacyjnej wspierającej pojedynczy unijny węzeł informacyjny, w tym wymaganą wiedzę fachową.

3. EUN przedkładają Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie, o którym mowa w ust. 1, do dnia 17 stycznia 2025 r.

Artykuł 22

Informacje zwrotne od organów nadzoru

1. Bez uszczerbku dla informacji technicznych, porad lub środków zaradczych oraz działań następczych, które w stosownych przypadkach zgodnie z prawem krajowym CSIRT mogą zapewnić na mocy dyrektywy (UE) 2022/2555, właściwy organ – po otrzymaniu wstępnego powiadomienia i poszczególnych sprawozdań, o których mowa w art. 19 ust. 4 – potwierdza otrzymanie i, gdy jest to wykonalne, może w odpowiednim czasie przekazać danemu podmiotowi finansowemu odpowiednie i proporcjonalne informacje zwrotne lub wskazówki wysokiego poziomu w szczególności poprzez udostępnienie wszelkich istotnych zanonimizowanych informacji i analiz na temat podobnych zagrożeń, oraz może omówić środki zaradcze zastosowane na poziomie danego podmiotu finansowego oraz sposoby zminimalizowania i złagodzenia negatywnego wpływu we wszystkich sektorach finansowych. Bez uszczerbku dla otrzymanych informacji zwrotnych podmioty finansowe pozostają w pełni odpowiedzialne za obsługę incydentów związanych z ICT zgłoszonych zgodnie z art. 19 ust. 1 i za konsekwencje tych incydentów.

2. EUN, za pośrednictwem Wspólnego Komitetu, składają corocznie, na podstawie zanonimizowanych i zbiorczych danych, sprawozdanie na temat poważnych incydentów związanych z ICT, na podstawie szczegółowych informacji przekazanych przez właściwe organy zgodnie z art. 19 ust. 6, określając co najmniej liczbę poważnych incydentów związanych z ICT, ich charakter i wpływ na operacje podmiotów finansowych lub klientów, podjęte działania naprawcze i poniesione koszty.

EUN wydają ostrzeżenia i opracowują dane statystyczne wysokiego poziomu w celu wsparcia oceny zagrożeń i podatności w obszarze ICT.

Artykuł 23

Incydenty operacyjne lub incydenty bezpieczeństwa związane z płatnościami dotyczące instytucji kredytowych, instytucji płatniczych, dostawców świadczących usługę dostępu do informacji o rachunku i instytucji pieniądza elektronicznego

Wymogi określone w niniejszym rozdziale mają również zastosowanie do incydentów operacyjnych lub incydentów bezpieczeństwa związanych z płatnościami oraz do poważnych incydentów operacyjnych lub poważnych incydentów bezpieczeństwa związanych z płatnościami, w przypadku gdy dotyczą one instytucji kredytowych, instytucji płatniczych, dostawców świadczących usługę dostępu do informacji o rachunku i instytucji pieniądza elektronicznego.

ROZDZIAŁ IV

Testowanie operacyjnej odporności cyfrowej

Artykuł 24

Ogólne wymogi dotyczące testowania operacyjnej odporności cyfrowej

1. Do celów oceny gotowości do obsługi incydentów związanych z ICT, określania słabości, niedoskonałości i luk w zakresie operacyjnej odporności cyfrowej oraz niezwłocznego wdrażania środków naprawczych podmioty finansowe inne niż mikroprzedsiębiorstwa – biorąc pod uwagę kryteria określone w art. 4 ust. 2 – ustanawiają i utrzymują prawidłowy i kompleksowy program testowania operacyjnej odporności cyfrowej stanowiący integralną część ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6, oraz dokonują przeglądu tego programu.

2. Program testowania operacyjnej odporności cyfrowej obejmuje szereg ocen, testów, metodyk, praktyk i narzędzi, które należy stosować zgodnie z art. 25 i 26.

3. Podczas realizacji programu testowania operacyjnej odporności cyfrowej, o którym mowa w ust. 1 niniejszego artykułu, podmioty finansowe inne niż mikroprzedsiębiorstwa stosują podejście oparte na analizie ryzyka i biorą pod uwagę kryteria określone w art. 4 ust. 2, należycie uwzględniając zmieniające się środowisko ryzyka związanego z ICT, wszelkie szczególne rodzaje ryzyka, na które dany 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 inne niż mikroprzedsiębiorstwa zapewniają, aby testy były przeprowadzane przez niezależne strony wewnętrzne lub zewnętrzne. W przypadku gdy testy są przeprowadzane przez testera wewnętrznego, podmioty finansowe przeznaczają wystarczające zasoby i zapewniają unikanie konfliktów interesów na wszystkich etapach projektowania i wykonywania testu.

5. Podmioty finansowe inne niż mikroprzedsiębiorstwa ustanawiają procedury i zasady ustalania hierarchii, klasyfikowania i rozwiązywania wszystkich problemów ujawnionych w trakcie przeprowadzania testów oraz ustanawiają wewnętrzne metody zatwierdzania w celu dopilnowania, aby w pełni usunięto wszystkie stwierdzone słabości, niedoskonałości lub luki.

6. Podmioty finansowe inne niż mikroprzedsiębiorstwa zapewniają, co najmniej raz w roku, przeprowadzenie odpowiednich testów wszystkich systemów i aplikacji ICT wspierających krytyczne lub istotne funkcje.

Artykuł 25

Testowanie narzędzi i systemów ICT

1. Program testowania operacyjnej odporności cyfrowej, o którym mowa w art. 24, przewiduje, zgodnie z kryteriami określonymi w art. 4 ust. 2, przeprowadzenie odpowiednich testów, takich jak oceny podatności i skanowanie pod tym kątem, analizy otwartego oprogramowania, oceny bezpieczeństwa sieci, analizy braków, fizycznych kontroli bezpieczeństwa, kwestionariusze i rozwiązania w zakresie oprogramowania skanującego, przeglądy kodu źródłowego, gdy jest to wykonalne, testy scenariuszowe, testy kompatybilności, testy wydajności, testy kompleksowe i testy penetracyjne.

2. Centralne depozyty papierów wartościowych i kontrahenci centralni przeprowadzają oceny podatności przed każdym wdrożeniem lub przeniesieniem nowych lub istniejących aplikacji i elementów infrastruktury oraz usług ICT wspierających krytyczne lub istotne funkcje danego podmiotu finansowego.

3. Mikroprzedsiębiorstwa przeprowadzają testy, o których mowa w ust. 1, łącząc podejście oparte na analizie ryzyka ze strategicznym planowaniem testowania związanego z ICT i należycie uwzględniając potrzebę utrzymania równowagi między skalą zasobów i czasem, który należy przeznaczyć na testowanie związane z ICT przewidziane w niniejszym artykule, z jednej strony, a pilnością, rodzajem ryzyka, krytycznością zasobów informacyjnych i świadczonych usług, a także wszelkimi innymi istotnymi czynnikami, w tym zdolnością danego podmiotu finansowego do podejmowania świadomego ryzyka, z drugiej strony.

Artykuł 26

Zaawansowane testowanie narzędzi, systemów i procesów ICT z wykorzystaniem TLPT

1. Podmioty finansowe inne niż podmioty, o których mowa w art. 16 ust. 1 akapit pierwszy, i inne niż mikroprzedsiębiorstwa, które określono zgodnie z ust. 8 akapit trzeci niniejszego artykułu, przeprowadzają nie rzadziej niż co trzy lata zaawansowane testy za pomocą TLPT. W oparciu o profil ryzyka danego podmiotu finansowego i z uwzględnieniem okoliczności operacyjnych właściwy organ może, w razie potrzeby, zwrócić się do tego podmiotu finansowego o zmniejszenie lub zwiększenie częstotliwości przeprowadzania tych testów.

2. Każdy test penetracyjny pod kątem wyszukiwania zagrożeń obejmuje kilka krytycznych lub istotnych funkcji podmiotu finansowego lub wszystkie te funkcje i jest przeprowadzany na działających systemach produkcyjnych wspierających takie funkcje.

Podmioty finansowe określają wszystkie istotne bazowe systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcje oraz wszystkie usługi ICT, w tym systemy, procesy i technologie ICT wspierające krytyczne lub istotne funkcje i usługi zlecone w drodze outsourcingu zewnętrznym dostawcom usług ICT lub będące przedmiotem umowy z takimi dostawcami.

Podmioty finansowe oceniają, które krytyczne lub istotne funkcje należy objąć TLPT. Wynik tej oceny określa dokładny zakres TLPT i podlega zatwierdzeniu przez właściwe organy.

3. W przypadku gdy zakres TLPT obejmuje zewnętrznych dostawców usług ICT, podmiot finansowy stosuje niezbędne środki i zabezpieczenia w celu zapewnienia udziału takich zewnętrznych dostawców usług ICT w TLPT i przez cały czas ponosi pełną odpowiedzialność za zapewnianie zgodności z niniejszym rozporządzeniem.

4. Bez uszczerbku dla ust. 2 akapity pierwszy i drugi, w przypadku gdy można racjonalnie przewidywać, że udział zewnętrznego dostawcy usług ICT w TLPT, o czym mowa w ust. 3, będzie miał negatywny wpływ na jakość lub bezpieczeństwo usług świadczonych przez tego zewnętrznego dostawcę usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia lub na poufność danych związanych z takimi usługami, dany podmiot finansowy i dany zewnętrzny dostawca usług ICT mogą uzgodnić na piśmie, że ten zewnętrzny dostawca usług ICT zawrze ustalenia umowne bezpośrednio z testerem zewnętrznym w celu przeprowadzenia – pod kierownictwem jednego wyznaczonego podmiotu finansowego – zbiorczych TLPT z udziałem kilku podmiotów finansowych (testowania zbiorczego), na rzecz których dany zewnętrzny dostawca usług ICT świadczy usługi ICT.

Takie testowanie zbiorcze obejmuje odpowiedni zakres usług ICT wspierających krytyczne lub istotne funkcje będące przedmiotem zawartej przez te podmioty finansowe umowy z tym zewnętrznym dostawcą usług ICT. Testowanie zbiorcze uznaje się za TLPT przeprowadzone przez podmioty finansowe biorące udział w tym testowaniu zbiorczym.

Liczba podmiotów finansowych uczestniczących w testowaniu zbiorczym jest należycie dostosowana i uwzględnia stopień złożoności i rodzaj objętych nim usług.

5. Podmioty finansowe – we współpracy z zewnętrznymi dostawcami usług ICT i innymi zaangażowanymi stronami, w tym testerami, ale z wyłączeniem właściwych organów – stosują skuteczne środki kontroli zarządzania ryzykiem w celu złagodzenia ryzyka potencjalnego wpływu na dane, szkód dla zasobów i zakłócenia krytycznych lub istotnych funkcji, usług lub operacji samego podmiotu finansowego, jego kontrahentów lub sektora finansowego.

6. Na koniec testowania, po uzgodnieniu sprawozdań i planów naprawczych, podmiot finansowy i, w stosownych przypadkach, testerzy zewnętrzni przedstawiają organowi wyznaczonemu zgodnie z ust. 9 lub 10 podsumowanie najbardziej istotnych ustaleń, plany naprawcze i dokumentację wykazującą, że TLPT przeprowadzono zgodnie z wymogami.

7. Organy przekazują podmiotom finansowym poświadczenie, że test został przeprowadzony zgodnie z wymogami potwierdzonymi w dokumentacji, aby umożliwić właściwym organom wzajemne uznawanie testów penetracyjnych pod kątem wyszukiwania zagrożeń. Podmiot finansowy powiadamia odpowiedni właściwy organ o poświadczeniu, podsumowaniu najbardziej istotnych ustaleń i planach naprawczych.

Bez uszczerbku dla takiego poświadczenia podmioty finansowe przez cały czas ponoszą pełną odpowiedzialność za skutki testów, o których mowa w ust. 4.

8. Podmioty finansowe zawierają z testerami umowy, których przedmiotem jest przeprowadzenie TLPT, zgodnie z art. 27. W przypadku gdy podmioty finansowe korzystają z testerów wewnętrznych w celu przeprowadzenia TLPT, co trzy testy zlecają to zadanie testerom zewnętrznym.

Instytucje kredytowe sklasyfikowane jako istotne zgodnie z art. 6 ust. 4 rozporządzenia (UE) nr 1024/2013, korzystają wyłącznie z testerów zewnętrznych zgodnie z art. 27 ust. 1 lit. a)–e).

Właściwe organy określają podmioty finansowe, od których wymaga się, by przeprowadzały TLPT z uwzględnieniem kryteriów określonych w art. 4 ust. 2, w oparciu o ocenę następujących elementów:

a) czynników związanych z wpływem, w szczególności zakresu, w jakim świadczone usługi i działaniami podejmowane przez podmiot finansowy mają wpływ na sektor finansowy;

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

c) specyficznego profilu ryzyka związanego z ICT, poziomu zaawansowania podmiotu finansowego pod względem ICT lub zastosowanych rozwiązań technologicznych.

9. Państwa członkowskie mogą wyznaczyć jeden organ publiczny w sektorze finansowym, który będzie odpowiedzialny za kwestie związane z TLPT w sektorze finansowym na szczeblu krajowym, i powierzają mu wszelkie kompetencje i zadania w tym zakresie.

10. W przypadku niewyznaczenia takiego organu zgodnie z ust. 9 niniejszego artykułu i bez uszczerbku dla uprawnienia do określenia podmiotów finansowych, które są zobowiązane do przeprowadzania TLPT, właściwy organ może przekazać wykonywanie niektórych lub wszystkich zadań, o których mowa w niniejszym artykule i w art. 26 i 27, innemu organowi krajowemu w sektorze finansowym.

11. EUN, w porozumieniu z EBC, opracowują wspólne projekty regulacyjnych standardów technicznych zgodnie z ramami TIBER–EU, aby doprecyzować następujące elementy:

a) kryteria wykorzystywane do celów stosowania ust. 8 akapit drugi;

b) wymogi i standardy regulujące korzystanie z testerów wewnętrznych;

c) wymogi dotyczące:

   (i) zakresu TLPT, o których mowa w ust. 2;

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

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

d) rodzaj współpracy w zakresie nadzoru i inne odpowiednie rodzaje współpracy potrzebne do przeprowadzenia TLPT i do ułatwienia wzajemnego uznawania takiego testowania 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.

Opracowując te projekty regulacyjnych standardów technicznych, EUN należycie uwzględniają szczególne cechy wynikające z wyjątkowego charakteru działalności w różnych sektorach usług finansowych.

EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 lipca 2024 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 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

Artykuł 27

Wymogi dotyczące testerów na potrzeby przeprowadzania TLPT

1. W celu przeprowadzania TLPT 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 i testów z udziałem zespołów typu *red team*;

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

d) przedstawiają niezależne zapewnienie lub sprawozdanie z audytu dotyczące należytego zarządzania ryzykiem związanym z przeprowadzaniem TLPT, w tym należytej ochrony poufnych informacji podmiotu finansowego i dochodzenia roszczeń z tytułu ryzyka biznesowego podmiotu finansowego;

e) są należycie i w pełni objęci odpowiednimi ubezpieczeniami od odpowiedzialności cywilnej z tytułu wykonywania zawodu, w tym od ryzyka uchybień i zaniedbań.

2. Korzystając z testerów wewnętrznych podmioty finansowe zapewniają, by poza wymogami ust. 1, spełnione były następujące warunki:

a) takie korzystanie z testerów wewnętrznych zostało zatwierdzone przez odpowiedni właściwy organ lub przez jeden organ publiczny wyznaczony zgodnie z art. 26 ust. 9 i 10;

b) odpowiedni właściwy organ sprawdził, że dany podmiot finansowy dysponuje wystarczającymi zasobami przeznaczonymi na ten cel i że zapewnił unikanie konfliktów interesów na wszystkich etapach projektowania i wykonywania testu; oraz

c) dostawca analizy zagrożeń jest podmiotem zewnętrznym względem danego podmiotu finansowego.

3. Podmioty finansowe zapewniają, aby umowy zawarte z testerami zewnętrznymi wymagały należytego zarządzania wynikami TLPT oraz aby żadne przetwarzanie danych pochodzących z tych wyników, w tym generowanie, przechowywanie, agregowanie, sporządzanie, zgłaszanie, przekazywanie lub niszczenie, nie stwarzały ryzyka dla podmiotu finansowego.

ROZDZIAŁ V

Zarządzanie ryzykiem ze strony zewnętrznych dostawców usług ICT

Sekcja I

Najważniejsze zasady prawidłowego zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT

Artykuł 28

Zasady ogólne

1. Podmioty finansowe zarządzają ryzykiem ze strony zewnętrznych dostawców usług ICT integralnym elementem ryzyka związanego z ICT wchodzącym w zakres ich ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 ust. 1, oraz zgodnie z opisanymi poniżej zasadami:

a) podmioty finansowe, które zawarły ustalenia umowne dotyczące korzystania z usług ICT w celu prowadzenia działalności gospodarczej, przez cały czas ponoszą pełną odpowiedzialność za wypełnianie i wywiązywanie się ze wszystkich obowiązków wynikających z niniejszego rozporządzenia i mających zastosowanie przepisów dotyczących usług finansowych;

b) zarządzanie przez podmioty finansowe ryzykiem ze strony zewnętrznych dostawców usług ICT odbywa się w świetle zasady proporcjonalności, z uwzględnieniem:

(i) charakteru, skali, stopnia złożoności i znaczenia zależności w zakresie ICT;

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

2. Jako część swoich ram zarządzania ryzykiem związanym z ICT podmioty finansowe inne niż podmioty, o których mowa w art. 16 ust. 1 akapit pierwszy, i inne niż mikroprzedsiębiorstwa przyjmują strategię dotyczącą ryzyka ze strony zewnętrznych dostawców usług ICT i regularnie dokonują jej przeglądu, uwzględniając, stosownie do przypadku, strategię obejmującą wielu dostawców, o której mowa w art. 6 ust. 9. Strategia dotycząca ryzyka ze strony zewnętrznych dostawców usług ICT obejmuje politykę korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT i ma zastosowanie na zasadzie indywidualnej oraz, w stosownych przypadkach, na zasadzie subskonsolidowanej i skonsolidowanej. Na podstawie oceny ogólnego profilu ryzyka danego podmiotu finansowego oraz skali i stopnia złożoności usług biznesowych organ zarządzający regularnie dokonuje przeglądu ryzyk zidentyfikowanych w odniesieniu do ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje.

3. W kontekście swoich ram zarządzania ryzykiem związanym z ICT podmioty finansowe utrzymują 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 usługi ICT wspierające krytyczne lub istotne funkcje, oraz ustalenia, które takich funkcji nie wspierają.

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 ICT i obsługiwanych funkcji.

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

Podmioty finansowe informują w odpowiednim terminie właściwy organ o wszelkich planowanych ustaleniach umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje oraz o tym, że dana funkcja stała się krytyczna lub istotna.

4. Przed zawarciem ustalenia umownego dotyczącego korzystania z usług ICT podmioty finansowe:

a) oceniają, czy dane ustalenie umowne dotyczy korzystania z usług ICT wspierających krytyczną lub istotną funkcję;

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

c) określają i oceniają 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, o czym mowa w art. 29;

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

e) identyfikują i oceniają konflikty interesów, które mogą wynikać z ustalenia umownego.

5. Podmioty finansowe mogą zawierać ustalenia umowne wyłącznie z zewnętrznymi dostawcami usług ICT, którzy przestrzegają odpowiednich standardów w zakresie bezpieczeństwa informacji. W przypadku gdy te ustalenia umowne dotyczą krytycznych lub istotnych funkcji, podmioty finansowe – przed zawarciem takich ustaleń umownych – należycie uwzględniają, czy zewnętrzni dostawcy usług ICT stosują najbardziej aktualne i najwyższe standardy bezpieczeństwa informacji.

6. 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 gdy ustalenia umowne dotyczące korzystania z usług ICT zawarte z zewnętrznymi dostawcami usług ICT wiążą się z wysokim stopniem złożoności technicznej, podmiot finansowy sprawdza, czy audytorzy – zarówno wewnętrzni, jak i zewnętrzni lub grupa audytorów – posiadają odpowiednie umiejętności i wiedzę umożliwiające skuteczne przeprowadzanie odpowiednich audytów i ocen.

7. Podmioty finansowe zapewniają, aby ustalenia umowne dotyczące korzystania z usług ICT mogły być wypowiadane w którejkolwiek z następujących sytuacji:

a) poważne 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 jego słabych stron w zakresie jego ogólnego zarządzania ryzykiem związanym z ICT, a w szczególności, jeżeli chodzi o sposób, w jaki zapewnia on dostępność, autentyczność, integralność i poufność danych, niezależnie od tego, czy chodzi o dane osobowe lub w inny sposób wrażliwe, czy też o dane nieosobowe;

d) gdy w wyniku warunków lub okoliczności związanych z danym ustaleniem umownym właściwy organ nie może już skutecznie nadzorować podmiotu finansowego.

8. W odniesieniu do usług ICT wspierających krytyczne lub istotne funkcje podmioty finansowe wprowadzają strategie wyjścia. Strategie wyjścia uwzględniają ryzyko, które może pojawić się na poziomie zewnętrznych dostawców usług ICT, w szczególności ich możliwej awarii, pogorszenia jakości świadczonych usług ICT, wszelkich zakłóceń w działalności spowodowanych niewłaściwym lub nieudanym świadczeniem usług ICT lub jakiegokolwiek istotnego ryzyka związanego z odpowiednią i ciągłą realizacją danej usługi ICT lub w razie wypowiedzenia ustaleń umownych z zewnętrznymi dostawcami usług w związku z wystąpieniem którejkolwiek z okoliczności wymienionych w ust. 7.

Podmioty finansowe zapewniają sobie możliwość wycofania się z ustaleń umownych bez:

a) powodowania zakłóceń w swojej działalności;

b) ograniczania zgodności z wymogami regulacyjnymi;

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

Plany wyjścia są kompleksowe, udokumentowane i, zgodnie z kryteriami określonymi w art. 4 ust. 2, wystarczająco przetestowane oraz podlegają okresowym przeglądom.

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

Podmioty finansowe wprowadzają odpowiednie środki awaryjne w celu utrzymania ciągłości działania na wypadek okoliczności, o których mowa w akapicie pierwszym.

9. EUN, za pośrednictwem Wspólnego Komitetu, opracowują projekty wykonawczych standardów technicznych w celu ustanowienia standardowych wzorów na potrzeby rejestru informacji, o którym mowa w ust. 3, w tym informacji wspólnych dla wszystkich ustaleń umownych dotyczących korzystania z usług ICT. EUN przedkładają Komisji te projekty wykonawczych standardów technicznych do dnia 17 stycznia 2024 r.

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

10. EUN, za pośrednictwem Wspólnego Komitetu, opracowują projekty regulacyjnych standardów technicznych w celu doprecyzowania szczegółowej treści polityki, o której mowa w ust. 2, w odniesieniu do ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT.

Opracowując te projekty regulacyjnych standardów technicznych, EUN biorą pod uwagę wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji. EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 stycznia 2024 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 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

Artykuł 29

Wstępna ocena ryzyka koncentracji w obszarze ICT

1. Dokonując identyfikacji i oceny ryzyka, o czym mowa w art. 28 ust. 4 lit. c), podmioty finansowe biorą również pod uwagę, czy zawarcie planowanego ustalenia umownego w związku z usługami ICT wspierającymi krytyczne lub istotne funkcje 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 wspierających krytyczne lub istotne funkcje 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 wspierających krytyczne lub istotne funkcje obejmują możliwość dalszego zlecania podwykonawstwa usług ICT wspierających krytyczne lub istotne funkcje przez zewnętrznego dostawcę usług ICT innym zewnętrznym dostawcom usług ICT, podmioty finansowe rozważają korzyści i ryzyka, które mogą wystąpić w związku z takim podwykonawstwem, w szczególności w przypadku podwykonawcy ICT mającego siedzibę w państwie trzecim.

W przypadku gdy ustalenia umowne dotyczą usług ICT wspierających krytyczne lub istotne funkcje, podmioty finansowe należycie uwzględniają przepisy prawa upadłościowego, które miałyby zastosowanie w przypadku upadłości zewnętrznego dostawcy usług ICT, a także wszelkie ograniczenia, które mogą powstać w związku z pilnym odzyskiwaniem danych podmiotu finansowego.

W przypadku gdy ustalenia umowne dotyczące korzystania z usług ICT wspierających krytyczne lub istotne funkcje są zawierane z zewnętrznym dostawcą usług ICT mającym siedzibę w państwie trzecim, podmioty finansowe – oprócz kwestii wymienionych w akapicie drugim – biorą pod uwagę również, czy w tym państwie trzecim przestrzega się unijnych przepisów o ochronie danych i skutecznie się je egzekwuje.

W przypadku gdy ustalenia umowne dotyczące korzystania z usług ICT wspierających krytyczne lub istotne funkcje przewidują zlecanie tych usług podwykonawcom, 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 30

Najważniejsze postanowienia umowne

1. Prawa i obowiązki podmiotu finansowego i zewnętrznego dostawcy usług ICT są wyraźnie przypisane i określone na piśmie. Całość umowy obejmuje klauzule o gwarantowanym poziomie usług i jest zawarta w jednym dokumencie mającym formę pisemną, który jest dostępny dla stron w wersji papierowej, lub w dokumencie w innym formacie umożliwiającym pobieranie, zapewniającym trwałość i dostęp.

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

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

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

c) postanowienia dotyczące dostępności, autentyczności, integralności i poufności w związku z ochroną danych, w tym danych osobowych;

d) postanowienia dotyczące 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 lub w przypadku wypowiedzenia ustaleń umownych;

e) opisy gwarantowanych poziomów usług, w tym ich aktualizacje i zmiany;

f) obowiązek zapewnienia przez zewnętrznego dostawcę usług ICT pomocy podmiotowi finansowemu, bez dodatkowych opłat lub za opłatą określoną *ex ante*, w przypadku wystąpienia incydentu związanego z ICT dotyczącego usług ICT świadczonych na rzecz tego podmiotu finansowego;

g) obowiązek zewnętrznego dostawcy usług ICT do pełnej współpracy z właściwymi organami oraz organami przymusowej restrukturyzacji podmiotu finansowego, w tym z osobami przez nie wyznaczonymi;

h) prawa do wypowiedzenia umowy i związane z tym minimalne okresy wypowiedzenia ustaleń umownych, zgodnie z oczekiwaniami właściwych organów i organów ds. restrukturyzacji i uporządkowanej likwidacji;

i) warunki uczestnictwa zewnętrznych dostawców usług ICT w opracowanych przez podmioty finansowe programach zwiększania świadomości w zakresie bezpieczeństwa ICT i szkoleniach w zakresie operacyjnej odporności cyfrowej zgodnie z art. 13 ust. 6.

3. Ustalenia umowne dotyczące korzystania z usług ICT wspierających krytyczne lub istotne funkcje zawierają, oprócz elementów, o których mowa w ust. 2, co najmniej następujące elementy:

a) pełne opisy gwarantowanych poziomów usług, w tym ich aktualizacje i zmiany, wraz z dokładnymi ilościowymi i jakościowymi celami w zakresie wyników w ramach uzgodnionych gwarantowanych poziomów usług, aby umożliwić podmiotowi finansowemu skuteczne monitorowanie usług ICT oraz umożliwić bezzwłoczne podjęcie odpowiednich działań naprawczych w przypadku nieosiągnięcia uzgodnionych gwarantowanych poziomów usług;

b) 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 usług ICT wspierających krytyczne lub istotne funkcje z zachowaniem uzgodnionych gwarantowanych poziomów usług;

c) 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 zapewniających odpowiedni poziom bezpieczeństwa świadczenia usług przez podmiot finansowy zgodnie z jego ramami regulacyjnymi;

d) obowiązek uczestnictwa zewnętrznych dostawców usług ICT w TLPT danego podmiotu finansowego i ich pełnej współpracy w tym zakresie, o czym mowa w art. 26 i 27;

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

(i) nieograniczone prawa dostępu, kontroli i audytu przez podmiot finansowy lub wyznaczoną osobę trzecią i przez właściwy organ oraz prawo sporządzania kopii odnośnej dokumentacji na miejscu, jeżeli mają one kluczowe znaczenie dla operacji zewnętrznego dostawcy usług ICT, przy czym skutecznego wykonywania tych praw nie utrudniają ani nie ograniczają inne ustalenia umowne ani polityka w zakresie wdrażania;

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

(iii) obowiązek zewnętrznego dostawcy usług ICT do pełnej współpracy podczas kontroli i audytów na miejscu przeprowadzanych przez właściwe organy, wiodący organ nadzorczy, podmiot finansowy lub wyznaczoną osobę trzecią; oraz

(iv) obowiązek przekazywania szczegółowych informacji na temat zakresu, mających zastosowanie procedur i częstotliwości takich kontroli i audytów;

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

(i) podczas którego zewnętrzny dostawca usług ICT będzie nadal zapewniał odpowiednie funkcje lub usługi ICT w celu zmniejszenia ryzyka wystąpienia zakłóceń w funkcjonowaniu podmiotu finansowego lub w celu zapewnienia jego skutecznej uporządkowanej likwidacji i restrukturyzacji;

(ii) który umożliwi podmiotowi finansowemu migrację do innego zewnętrznego dostawcy usług ICT lub przejście na rozwiązania dostępne w ramach struktury wewnętrznej stosownie do stopnia złożoności świadczonej usługi.

Na zasadzie odstępstwa od lit. e) zewnętrzny dostawca usług ICT i podmiot finansowy będący mikroprzedsiębiorstwem mogą uzgodnić, że przysługujące podmiotowi finansowemu prawa dostępu, kontroli i audytu mogą zostać przekazane niezależnej osobie trzeciej, wyznaczonej przez zewnętrznego dostawcę usług ICT, oraz że podmiot finansowy może w dowolnym momencie zażądać od tej osoby trzeciej informacji o wynikach zewnętrznego dostawcy usług ICT i poświadczenia tych wyników.

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

5. EUN, za pośrednictwem Wspólnego Komitetu, opracowują projekty regulacyjnych standardów technicznych doprecyzowujących elementy, o których mowa w ust. 2 lit. a), które podmiot finansowy musi określić i ocenić, zlecając podwykonawstwo usług ICT wspierających krytyczne lub istotne funkcje.

Opracowując te projekty regulacyjnych standardów technicznych, EUN biorą pod uwagę wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i stopień złożoności jego usług, działań i operacji.

EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 lipca 2024 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 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

Sekcja II

Ramy nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT

Artykuł 31

Wyznaczenie kluczowych zewnętrznych dostawców usług ICT

1. Za pośrednictwem Wspólnego Komitetu i na podstawie zalecenia forum nadzoru ustanowionego zgodnie z art. 32 ust. 1 EUN:

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

b) wyznaczają – jako wiodący organ nadzorczy w odniesieniu do każdego z kluczowych zewnętrznych dostawców usług ICT – EUN, który jest odpowiedzialny, zgodnie z rozporządzeniem (UE) nr 1093/2010, rozporządzeniem (UE) nr 1094/2010 lub rozporządzeniem (UE) nr 1095/2010, za podmioty finansowe mające wspólnie największą część łącznych aktywów wszystkich podmiotów finansowych korzystających z usług danego kluczowego zewnętrznego dostawcy usług ICT, wykazanych jako suma indywidualnych bilansów tych podmiotów finansowych.

2. Wyznaczenie, o którym mowa w ust. 1 lit. a), w odniesieniu do usług ICT świadczonych przez zewnętrznego dostawcę usług ICT 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 awarii operacyjnej na dużą skalę w zakresie świadczenia swoich usług, biorąc pod uwagę liczbę podmiotów finansowych i łączną wartość aktywów 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) współzależnością 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) zależności podmiotów finansowych od usług świadczonych przez danego zewnętrznego dostawcę usług ICT w odniesieniu do krytycznych lub istotnych 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, 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 stopień złożoności technicznej lub zaawansowania technicznego, 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 inne zasoby, 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.

3. W przypadku gdy zewnętrzny dostawca usług ICT należy do grupy, kryteria, o których mowa w ust. 2, są uwzględniane w kontekście usług ICT świadczonych przez grupę jako całość.

4. Kluczowi zewnętrzni dostawcy usług ICT będący częścią grupy wyznaczają jedną osobę prawną jako punkt koordynacyjny w celu zapewnienia odpowiedniej reprezentacji i komunikacji z wiodącym organem nadzorczym.

5. Wiodący organ nadzorczy powiadamia zewnętrznego dostawcę usług ICT o wyniku oceny do celów wyznaczenia, o którym mowa w ust. 1 lit. a). W terminie 6 tygodni od daty powiadomienia zewnętrzny dostawca usług ICT może przedłożyć wiodącemu organowi nadzorczemu uzasadnione oświadczenie zawierające wszelkie istotne informacje na potrzeby tej oceny. Wiodący organ nadzorczy analizuje uzasadnione oświadczenie i może zażądać przedłożenia dodatkowych informacji w terminie 30 dni kalendarzowych od otrzymania takiego oświadczenia.

Po wyznaczeniu zewnętrznego dostawcy usług ICT jako kluczowego, EUN, za pośrednictwem Wspólnego Komitetu, powiadamia tego zewnętrznego dostawcę usług ICT o takim wyznaczeniu i o dacie, od której będzie on faktycznie podlegać działaniom nadzorczym. Data ta nie może być późniejsza niż miesiąc po powiadomieniu. Ten zewnętrzny dostawca usług ICT powiadamia o takim wyznaczeniu podmioty finansowe, na rzecz których świadczy usługi.

6. Komisja jest uprawniona do przyjmowania aktu delegowanego zgodnie z art. 57 w celu uzupełnienia niniejszego rozporządzenia poprzez doprecyzowanie kryteriów, o których mowa w ust. 2 niniejszego artykułu do dnia 17 lipca 2024 r.

7. Wyznaczenie, o którym mowa w ust. 1 lit. a), nie może być dokonane do czasu przyjęcia przez Komisję aktu delegowanego zgodnie z ust. 6.

8. Wyznaczenie, o którym mowa w ust. 1 lit. a), nie ma zastosowania do:

(i) podmiotów finansowych świadczących usługi ICT na rzecz innych podmiotów finansowych;

(ii) 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;

(iii) dostawców usług ICT wewnątrz grupy;

(iv) zewnętrznych dostawców usług ICT świadczących usługi ICT wyłącznie w jednym państwie członkowskim na rzecz podmiotów finansowych działających tylko w tym państwie członkowskim.

9. EUN, za pośrednictwem Wspólnego Komitetu, sporządzają, publikują i co roku aktualizują wykaz kluczowych zewnętrznych dostawców usług ICT na szczeblu Unii.

10. Do celów ust. 1 lit. a) właściwe organy przekazują forum nadzoru ustanowionemu zgodnie z art. 32 sprawozdania w ujęciu rocznym i zagregowanym, o których mowa w art. 28 ust. 3 akapit trzeci. Forum nadzoru ocenia zależności podmiotów finansowych od zewnętrznych dostawców usług ICT na podstawie informacji uzyskanych od właściwych organów.

11. Zewnętrzni dostawcy usług ICT, których nie uwzględniono w wykazie, o którym mowa w ust. 9, mogą zwrócić się z wnioskiem o wyznaczenie ich jako kluczowych zgodnie z ust. 1 lit. a).

Do celów akapitu pierwszego zewnętrzni dostawcy usług ICT składają umotywowany wniosek do EUNB, ESMA lub EIOPA, które, za pośrednictwem Wspólnego Komitetu, podejmują decyzję, czy wyznaczyć danego zewnętrznego dostawcę usług ICT jako kluczowego 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.

12. Podmioty finansowe mogą korzystać z usług zewnętrznych dostawców usług ICT mających siedzibę w państwie trzecim i wyznaczonych jako kluczowi zgodnie z ust. 1 lit. a) wyłącznie wtedy, gdy ci zewnętrzni dostawcy usług ICT ustanowili w Unii swoją jednostkę zależną w ciągu 12 miesięcy od wyznaczenia.

13. Kluczowy zewnętrzny dostawca usług ICT, o którym mowa w ust. 12, powiadamia wiodący organ nadzorczy o wszelkich zmianach w strukturze zarządzania jednostki zależnej ustanowionej w Unii.

Artykuł 32

Struktura ram nadzoru

1. Zgodnie z art. 57 ust. 1 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. 31 ust. 1 lit. b), w obszarze ryzyka ze strony zewnętrznych dostawców usług ICT we wszystkich sektorach finansowych. Forum nadzoru sporządza projekty wspólnych stanowisk i projekty wspólnych aktów Wspólnego Komitetu w tym obszarze.

Forum nadzoru regularnie omawia istotne zmiany dotyczące ryzyka i podatności związanych z ICT oraz promuje spójne podejście przy monitorowaniu ryzyka ze strony zewnętrznych dostawców usług ICT na szczeblu 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 EUN 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:

a) przewodniczący poszczególnych EUN;

b) po jednym przedstawicielu wysokiego szczebla z aktualnego personelu odpowiedniego właściwego organu, o którym mowa w art. 46, z każdego państwa członkowskiego;

c) jako obserwatorzy – dyrektorzy wykonawczy każdego z EUN oraz po jednym przedstawicielu z Komisji, ERRS, EBC i ENISA;

d) w stosownych przypadkach, jako obserwatorzy – po jednym dodatkowym przedstawicielu właściwego organu, o którym mowa w art. 46, z każdego państwa członkowskiego;

e) w stosownych przypadkach, jako obserwatorzy – po jednym przedstawicielu właściwych organów wyznaczonych lub ustanowionych na mocy dyrektywy (UE) 2022/2555 jako odpowiedzialne za nadzór nad kluczowym lub ważnym podmiotem objętym zakresem stosowania tej dyrektywy, który został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT.

W stosownych przypadkach forum nadzoru może zwrócić się o poradę do niezależnych ekspertów wyznaczonych zgodnie z ust. 6.

5. Każde państwo członkowskie wyznacza odpowiedni właściwy organ, którego członkiem personelu jest przedstawiciel wysokiego szczebla, o którym mowa w ust. 4 akapit pierwszy lit. b), i informuje o tym wiodący organ nadzorczy.

EUN publikują na swoich stronach internetowych wykaz przedstawicieli wysokiego szczebla będących członkami personelu odpowiedniego właściwego organu wyznaczonych przez państwa członkowskie.

6. Niezależni eksperci, o których mowa w ust. 4 akapit drugi, są wyznaczani przez forum nadzoru spośród grupy ekspertów wybranych po przeprowadzeniu publicznej i przejrzystej procedury składania wniosków.

Niezależni eksperci są wyznaczani na podstawie posiadanej wiedzy fachowej w dziedzinie stabilności finansowej, operacyjnej odporności cyfrowej i bezpieczeństwa ICT. Działają oni niezależnie i obiektywnie w wyłącznym interesie Unii jako całości i nie zwracają się o instrukcje do instytucji lub organów unijnych, rządu żadnego z państw członkowskich lub do innego podmiotu publicznego lub prywatnego ani nie przyjmują takich instrukcji.

7. Zgodnie z art. 16 rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1094/2010 i rozporządzenia (UE) nr 1095/2010 EUN wydają – do celów niniejszej sekcji – wytyczne do dnia 17 lipca 2024 r. w zakresie współpracy między EUN i właściwymi organami dotyczące szczegółowych procedur i warunków podziału i wykonywania zadań między właściwymi organami i EUN oraz szczegółów wymiany informacji niezbędnych właściwym organom do zapewnienia działań następczych w związku z zaleceniami zgodnie z art. 35 ust. 1 lit. d) skierowanymi do kluczowych zewnętrznych dostawców usług ICT.

8. Wymogi określone w niniejszej sekcji pozostają bez uszczerbku dla stosowania dyrektywy (UE) 2022/2555 i nie naruszają innych unijnych przepisów dotyczących nadzoru mających zastosowanie do dostawców usług chmurowych.

9. EUN, za pośrednictwem Wspólnego Komitetu i na podstawie prac przygotowawczych przeprowadzonych przez forum nadzoru, co roku przedstawiają Parlamentowi Europejskiemu, Radzie i Komisji sprawozdanie na temat stosowania niniejszej sekcji.

Artykuł 33

Zadania wiodącego organu nadzorczego

1. Wiodący organ nadzorczy, wyznaczony zgodnie z art. 31 ust. 1 lit. b), sprawuje nadzór nad przypisanymi mu kluczowymi zewnętrznymi dostawcami usług ICT i do celów wszelkich kwestii związanych z nadzorem jest głównym punktem kontaktowym dla tych kluczowych zewnętrznych dostawców usług ICT.

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

Ocena, o której mowa w akapicie pierwszym, koncentruje się głównie na usługach ICT świadczonych przez kluczowego zewnętrznego dostawcę usług ICT wspierających krytyczne lub istotne funkcje podmiotów finansowych. Gdy istnieje potrzeba oceny wszystkich istotnych rodzajów ryzyka, ocena ta obejmuje usługi ICT wspierające funkcje inne niż krytyczne lub istotne.

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

a) wymogi z zakresu ICT mające na celu zapewnienie w szczególności bezpieczeństwa, dostępności, ciągłości, skalowalności i jakości usług, które kluczowy zewnętrzny dostawca usług ICT świadczy na rzecz podmiotów finansowych, jak również możliwości utrzymania przez cały czas wysokich standardów dostępności, autentyczności, integralności lub poufności 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, strategię na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT;

d) rozwiązania w zakresie 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 istotnych incydentów związanych z ICT oraz ich szybkie zgłaszanie podmiotom finansowym, zarządzanie tymi incydentami i zaradzanie tym incydentom, w szczególności cyberatakom;

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 standardów mających zastosowanie do świadczenia usług ICT na rzecz podmiotów finansowych.

4. Na podstawie oceny, o której mowa w ust. 2, i w koordynacji ze wspólną siecią nadzoru, o której mowa w art. 34 ust. 1, wiodący organ nadzorczy przyjmuje jasny, szczegółowy i uzasadniony indywidualny plan nadzoru dla każdego kluczowego zewnętrznego dostawcy usług ICT opisujący roczne cele w zakresie nadzoru i główne planowane działania nadzorcze. Co roku plan ten przekazuje się każdemu z kluczowych zewnętrznych dostawców usług ICT.

Przed przyjęciem planu nadzoru wiodący organ nadzorczy przekazuje projekt tego planu odnośnemu kluczowemu zewnętrznemu dostawcy usług ICT.

Po otrzymaniu projektu planu nadzoru kluczowy zewnętrzny dostawca usług ICT może w ciągu 15 dni kalendarzowych przedłożyć uzasadnione oświadczenie dokumentujące spodziewany wpływ na klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia i w stosownych przypadkach przedstawiające rozwiązania w celu złagodzenia ryzyka.

5. Po przyjęciu rocznych planów nadzoru, o których mowa w ust. 4, i po powiadomieniu o nich kluczowych zewnętrznych dostawców usług ICT właściwe organy mogą stosować środki dotyczące kluczowych zewnętrznych dostawców usług ICT wyłącznie w porozumieniu z wiodącym organem nadzorczym.

Artykuł 34

Koordynacja operacyjna wiodących organów nadzorczych

1. Aby zapewnić spójne podejście do działań nadzorczych i umożliwić stosowanie skoordynowanych ogólnych strategii nadzoru oraz spójnych podejść operacyjnych i metod pracy, trzy wiodące organy nadzorcze, wyznaczone zgodnie z art. 31 ust. 1 lit. b), ustanawiają wspólną sieć nadzoru w celu koordynacji swoich działań na etapach przygotowawczych i koordynacji prowadzenia działań nadzorczych nad odpowiednimi nadzorowanymi kluczowymi zewnętrznymi dostawcami usług ICT, a także w celu koordynacji kierunków działań, jakie mogą być konieczne zgodnie z art. 42.

2. Do celów ust. 1 wiodący organ nadzorczy sporządza wspólny protokół nadzoru określający szczegółowe procedury, które należy stosować w celu prowadzenia bieżącej koordynacji oraz zapewnienia szybkiej wymiany informacji i szybkich reakcji. Protokół jest okresowo zmieniany w celu odzwierciedlenia potrzeb operacyjnych, w szczególności ewolucji praktycznych ustaleń nadzorczych.

3. Wiodące organy nadzorcze mogą na zasadzie ad hoc zwrócić się do EBC i ENISA o zapewnienie doradztwa technicznego, podzielenie się praktycznymi doświadczeniami lub uczestnictwo w konkretnych posiedzeniach koordynacyjnych wspólnej sieci nadzoru.

Artykuł 35

Uprawnienia wiodącego organu nadzorczego

1. Do celów wykonywania obowiązków określonych w niniejszej sekcji wiodący organ nadzorczy posiada w odniesieniu do kluczowych zewnętrznych dostawców usług ICT uprawnienia do:

a) występowania z wnioskiem o przekazanie wszystkich stosownych informacji i dokumentów zgodnie z art. 37;

b) prowadzenia ogólnych dochodzeń i kontroli zgodni, odpowiednio, z art. 38 i 39;

c) występowania z wnioskiem o złożenie sprawozdań po zakończeniu działań nadzorczych, w których omówione są 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) wydawania zaleceń dotyczących obszarów, o których mowa w art. 33 ust. 3, odnoszących się w szczególności do:

   (i) stosowania szczególnych wymogów lub procesów z zakresu bezpieczeństwa i jakości ICT, w szczególności 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 ICT 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) wszelkiego planowanego podwykonawstwa, w przypadku którego wiodący organ nadzorczy uważa – po przeprowadzeniu analizy informacji zebranych zgodnie z art. 37 i 38 – że dalsze podwykonawstwo, w tym umowy podwykonawstwa, które kluczowi zewnętrzni dostawcy usług ICT zamierzają zawrzeć z innymi zewnętrznymi dostawcami usług ICT lub z podwykonawcami usług ICT z siedzibą w państwie trzecim, 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 krytycznej lub istotnej funkcji podmiotu finansowego, oraz

— wiodący organ nadzorczy uważa, że korzystanie z takiego podwykonawstwa stwarza wyraźne i poważne ryzyko dla stabilności finansowej Unii lub podmiotów finansowych, w tym dla zdolności podmiotów finansowych do spełnienia wymogów w zakresie nadzoru.

Do celów ppkt (iv) niniejszej litery zewnętrzni dostawcy usług ICT przekazują wiodącemu organowi nadzorczemu informacje dotyczące podwykonawstwa, wykorzystując wzór, o którym mowa w art. 41 ust. 1 lit. b).

2. Wykonując uprawnienia, o których mowa w niniejszym artykule, wiodący organ nadzorczy:

a) zapewnia regularną koordynację działań w ramach wspólnej sieci nadzoru, a w szczególności dąży do stosowania spójnych podejść, stosownie do przypadku, w odniesieniu do nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT;

b) należycie uwzględnia ramy ustanowione dyrektywą (UE) 2022/2555 oraz, w razie potrzeby, konsultuje się z odpowiednimi właściwymi organami wyznaczonymi lub ustanowionymi zgodnie z tą dyrektywą, aby uniknąć powielania środków technicznych i organizacyjnych, które mogą mieć zastosowanie do kluczowych zewnętrznych dostawców usług ICT zgodnie z tą dyrektywą;

c) dążą do zminimalizowania, na ile to możliwe, ryzyka zakłócenia usług świadczonych przez kluczowych dostawców usług ICT na rzecz klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia.

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

Przed wydaniem zaleceń zgodnie z ust. 1 lit. d) wiodący organ nadzorczy daje zewnętrznemu dostawcy usług ICT możliwość dostarczenia w terminie 30 dni kalendarzowych istotnych informacji dokumentujących spodziewany wpływ na klientów będących podmiotami nieobjętymi zakresem stosowania niniejszego rozporządzenia i w stosownych przypadkach przedstawiających rozwiązania w celu złagodzenia ryzyka.

4. Wiodący organ nadzorczy informuje wspólną sieć nadzoru o wynikach wykonania uprawnień, o których mowa w ust. 1 lit. a) i b). Wiodący organ nadzorczy bez zbędnej zwłoki przekazuje sprawozdania, o których mowa w ust. 1 lit. c), wspólnej sieci nadzoru i właściwym organom podmiotów finansowych korzystających z usług ICT świadczonych przez tego kluczowego zewnętrznego dostawcę usług ICT.

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

6. W przypadku całkowitego lub częściowego niezastosowania się do środków, które należy podjąć w związku z wykonaniem uprawnień na mocy ust. 1 lit. a), b) i c), oraz po upływie co najmniej 30 dni kalendarzowych od dnia, w którym kluczowy zewnętrzny dostawca usług ICT otrzymał powiadomienie o odpowiednich środkach, wiodący organ nadzorczy przyjmuje decyzję nakładającą okresową karę pieniężną, aby nakłonić kluczowego zewnętrznego dostawcę usług ICT do zastosowania się do tych środków.

7. Okresowa kara pieniężna, o której mowa w ust. 6, jest nakładana za każdy dzień do czasu zastosowania się do środków i nie dłużej niż przez sześć miesięcy po powiadomieniu kluczowego zewnętrznego dostawcy usług ICT o decyzji nakładającej tę karę.

8. Kwota okresowej kary pieniężnej, naliczana od dnia określonego w decyzji nakładającej okresową karę pieniężną, wynosi maksymalnie 1 % średniego dziennego światowego obrotu kluczowego zewnętrznego dostawcy usług ICT w poprzedzającym roku obrotowym. Ustalając kwoty okresowej kary pieniężnej, wiodący organ nadzorczy bierze pod uwagę następujące kryteria dotyczące niezastosowania się do środków, o których mowa w ust. 6:

a) wagę tego niezastosowania się i czas jego trwania;

b) kwestię, czy niezastosowanie się jest wynikiem działania umyślnego lub zaniedbania;

c) poziom współpracy zewnętrznego dostawcy usług z wiodącym organem nadzorczym.

Do celów akapitu pierwszego, aby zapewnić spójne podejście, wiodący organ nadzorczy podejmuje konsultacje ze wspólną siecią nadzoru.

9. 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 udzielany jest dostęp. Do rozpatrywania skarg dotyczących nieprawidłowego przeprowadzania postępowania egzekucyjnego właściwe są sądy danego państwa członkowskiego. Kwoty okresowych kar pieniężnych stanowi przychód budżetu ogólnego Unii Europejskiej.

10. Wiodący organ nadzorczy podaje do wiadomości publicznej każdą nałożoną okresową karę pieniężną, chyba że takie ujawnienie zagrażałoby poważnie rynkom finansowym lub wyrządziłoby nieproporcjonalną szkodę stronom, których dotyczy.

11. Przed nałożeniem okresowej kary pieniężnej na podstawie ust. 6 wiodący organ nadzorczy zapewnia przedstawicielom kluczowego zewnętrznego dostawcy usług ICT, wobec którego toczy się postępowanie, możliwość bycia wysłuchanym w sprawie ustaleń i opiera 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. Kluczowemu zewnętrznemu dostawcy usług ICT objętemu postępowaniem 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 36

Wykonywanie uprawnień wiodącego organu nadzorczego poza Unią

1. W przypadku gdy cele w zakresie nadzoru nie mogą zostać osiągnięte poprzez kontakty z jednostką zależną utworzoną do celów art. 31 ust. 12 lub poprzez działania nadzorcze prowadzone w obiektach znajdujących się w Unii, wiodący organ nadzorczy może – we wszystkich obiektach znajdujących się w państwie trzecim, które są własnością kluczowego zewnętrznego dostawcy usług ICT lub są wykorzystywane w dowolny sposób w celu świadczenia przez tego dostawcę usług na rzecz unijnych podmiotów finansowych w związku z jego działalnością gospodarczą, funkcjami lub usługami, w tym we wszystkich biurach ds. administracyjnych, biznesowych czy operacyjnych, odnośnych obiektach, terenach, budynkach lub innych nieruchomościach – wykonywać uprawnienia przewidziane w następujących przepisach:

a) w art. 35 ust. 1 lit. a); oraz

b) w art. 35 ust. 1 lit. b), zgodnie z art. 38 ust. 2 lit. a), b) i d) oraz, odpowiednio, w art. 39 ust. 1 i ust. 2 lit. a).

Uprawnienia, o których mowa w akapicie pierwszym, mogą być wykonywane, o ile spełnione są wszystkie następujące warunki:

(i) wiodący organ nadzorczy uznaje przeprowadzenie kontroli w państwie trzecim za konieczne, by umożliwić mu pełne i skuteczne wykonywanie obowiązków wynikających z niniejszego rozporządzenia;

(ii) kontrola w państwie trzecim jest bezpośrednio związana ze świadczeniem usług ICT na rzecz podmiotów finansowych w Unii;

(iii) dany kluczowy dostawca usług ICT wyraża zgodę na przeprowadzenie kontroli w państwie trzecim; oraz

(iv) odpowiedni organ danego państwa trzeciego został o tym oficjalnie powiadomiony przez wiodący organ nadzorczy i nie zgłosił sprzeciwu.

2. Bez uszczerbku dla odpowiednich kompetencji instytucji unijnych oraz państw członkowskich, do celów ust. 1 EUNB, ESMA lub EIOPA zawierają porozumienia o współpracy administracyjnej z odpowiednimi organami państw trzecich, aby umożliwić sprawne przeprowadzenie w danym państwie trzecim kontroli przez wiodący organ nadzorczy i jego zespół wyznaczony do tego zadania w tym państwie trzecim. Te porozumienia o współpracy nie tworzą zobowiązań prawnych w odniesieniu do Unii i jej państw członkowskich ani nie uniemożliwiają państwom członkowskim i ich właściwym organom zawierania dwustronnych lub wielostronnych porozumień z tymi państwami trzecimi i ich odpowiednimi organami.

W tych porozumieniach o współpracy określa się co najmniej następujące elementy:

a) procedury koordynacji działań nadzorczych prowadzonych na mocy niniejszego rozporządzenia oraz wszelkich analogicznych działań w zakresie monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT w sektorze finansowym wykonywanych przez odpowiedni organ danego państwa trzeciego, w tym szczegółowe informacje dotyczące przekazywania zgody tego organu na prowadzenie przez wiodący organ nadzorczy i jego wyznaczony zespół na terytorium objętym jego jurysdykcją ogólnych dochodzeń i kontroli na miejscu, o których mowa w ust. 1 akapit pierwszy;

b) mechanizm przekazywania wszelkich istotnych informacji między EUNB, ESMA lub EIOPA oraz odpowiednim organem danego państwa trzeciego, w szczególności w związku z informacjami, o które wiodący organ nadzorczy może się zwrócić zgodnie z art. 37;

c) mechanizmy szybkiego powiadamiania przez odpowiedni organ danego państwa trzeciego EUNB, ESMA lub EIOPA o przypadkach, w których uznaje się, że zewnętrzny dostawca usług ICT mający siedzibę w państwie trzecim i wyznaczony jako krytyczny zgodnie z art. 31 ust. 1 lit. a), naruszył mające zastosowanie przepisy tego państwa trzeciego podczas świadczenia usług na rzecz podmiotów finansowych w tym państwie trzecim, a także o podjętych środkach zaradczych i zastosowanych sankcjach;

d) regularne przekazywanie aktualnych informacji na temat zmian regulacyjnych lub nadzorczych w zakresie monitorowania ryzyka ze strony zewnętrznych dostawców usług ICT dla instytucji finansowych w danym państwie trzecim;

e) szczegółowe informacje umożliwiające, w razie potrzeby, udział jednego przedstawiciela odpowiedniego organu państwa trzeciego w kontrolach prowadzonych przez wiodący organ nadzorczy i wyznaczony zespół.

3. W przypadku gdy wiodący organ nadzorczy nie jest w stanie przeprowadzić działań nadzorczych poza Unią, o czym mowa w ust. 1 i 2, organ ten:

a) wykonuje swoje uprawnienia na mocy art. 35 w oparciu o wszystkie dostępne mu fakty i dokumenty;

b) dokumentuje i wyjaśnia wszelkie konsekwencje niemożności przeprowadzenia planowanych działań nadzorczych, o których mowa w niniejszym artykule.

Potencjalne konsekwencje, o których mowa w lit. b) niniejszego ustępu, są uwzględniane w zaleceniach wydawanych przez wiodący organ nadzorczy zgodnie z art. 35 ust. 1 lit. d).

Artykuł 37

Wniosek o udzielenie informacji

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 w drodze outsourcingu 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 myląće.

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. 35 ust. 6, w przypadku gdy przekazane wymagane informacje są niekompletne lub jeżeli takie informacje nie zostaną dostarczone w terminie, o którym mowa w lit. d) niniejszego ustępu;

f) informuje o prawie do odwołania od decyzji do Komisji Odwoławczej EUN i prawie do zaskarżenia tej decyzji do Trybunału Sprawiedliwości Unii Europejskiej (Trybunał Sprawiedliwości) zgodnie z art. 60 i 61 rozporządzeń (UE) nr 1093/2010, (UE) nr 1094/2010 i (UE) nr 1095/2010.

4. Przedstawiciele kluczowych zewnętrznych dostawców usług ICT przekazują 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 myląće.

5. Wiodący organ nadzorczy niezwłocznie przekazuje kopię decyzji, w której wzywa do przekazania informacji, organom właściwym dla podmiotów finansowych, które korzystają z usług danych kluczowych zewnętrznych dostawców usług ICT, oraz wspólnej sieci nadzoru.

Artykuł 38

Dochodzenia ogólne

1. W celu wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia wiodący organ nadzorczy, przy wsparciu wspólnego zespołu ds. kontroli, o którym mowa w art. 40 ust. 1, może, w razie potrzeby, prowadzić dochodzenia względem kluczowych 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, udokumentowanych procedur i z wszelkich innych materiałów;

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

d) przesłuchiwania wszelkich innych osób fizycznych lub prawnych, które wyrażą na to zgodę, w celu zebrania 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. 35 ust. 6, nakładane w przypadku, gdy wymagane dokumenty, dane, udokumentowane procedury lub inne materiały lub odpowiedzi na pytania zadane przedstawicielom zewnętrznego dostawcy usług ICT nie zostaną przekazane bądź udzielone lub są niepełne.

4. Przedstawiciele kluczowego 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. 35 ust. 6 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 kluczowego zewnętrznego dostawcy usług ICT, o planowanym dochodzeniu i o tożsamości upoważnionych osób.

Wiodący organ nadzorczy przekazuje wspólnej sieci nadzoru wszystkie informacje otrzymane zgodnie z akapitem pierwszym.

Artykuł 39

Kontrole

1. W celu wykonywania swoich obowiązków wynikających z niniejszego rozporządzenia wiodący organ nadzorczy, przy wsparciu wspólnych zespołów ds. kontroli, o których mowa w art. 40 ust. 1, może wejść do obiektów, na tereny lub do nieruchomości, które stanowią 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 zdalne.

Do celów wykonywania uprawnień, o których mowa w akapicie pierwszym, wiodący organ nadzorczy konsultuje się ze wspólną siecią nadzoru.

2. Urzędnicy i inne osoby upoważnione przez wiodący organ nadzorczy do przeprowadzania kontroli na miejscu są uprawnieni do:

a) wejścia do wszelkich takich lokali, na teren lub do nieruchomości; oraz

b) opieczętowania wszelkich takich lokali, ksiąg lub rejestrów na czas i w zakresie koniecznym do przeprowadzenia kontroli.

Urzędnicy i inne osoby upoważnione przez wiodący organ nadzorczy wykonują swoje uprawnienia po przedstawieniu pisemnego upoważnienia określającego przedmiot i cel kontroli oraz okresowe kary pieniężne przewidziane w art. 35 ust. 6, które podlegają nałożeniu w przypadku, gdy przedstawiciele odnośnych kluczowych zewnętrznych dostawców usług ICT nie poddadzą się kontroli.

3. Z odpowiednim wyprzedzeniem przed rozpoczęciem kontroli wiodący organ nadzorczy informuje o niej 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 ICT 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 określonym w decyzji wiodącego organu nadzorczego. W decyzji tej określa się przedmiot i cel kontroli, datę jej rozpoczęcia oraz okresowe kary pieniężne przewidziane w art. 35 ust. 6, 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 tego kluczowego zewnętrznego dostawcę usług ICT o konsekwencjach takiego sprzeciwu, w tym o możliwości żądania przez właściwe organy, by podmioty finansowe zakończyły stosunki umowne z tym kluczowym zewnętrznym dostawcą usług ICT.

Artykuł 40

Bieżący nadzór

1. Przy przeprowadzaniu działań nadzorczych, w szczególności dochodzeń ogólnych lub kontroli, wiodący organ nadzorczy jest wspierany przez wspólny 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:

a) EUN;

b) odpowiednich właściwych organów nadzorujących podmioty finansowe, na rzecz których kluczowy zewnętrzny dostawca usług ICT świadczy usługi;

c) na zasadzie dobrowolności – krajowego właściwego organu, o którym mowa w art. 32 ust. 4 lit. e);

d) na zasadzie dobrowolności – jednego z krajowych właściwych organów państwa członkowskiego, w którym dany kluczowy zewnętrzny dostawca usług ICT ma siedzibę.

Członkowie wspólnego zespołu badawczego mają wiedzę fachową z zakresu ICT i ryzyka operacyjnego. Prace wspólnego zespołu ds. kontroli podlegają koordynacji wyznaczonego pracownika wiodącego organu nadzorczego („koordynator wiodącego organu nadzorczego").

3. W terminie trzech miesięcy od zakończenia dochodzenia lub kontroli wiodący organ nadzorczy, po konsultacji z forum nadzoru, przyjmuje zalecenia, które mają być skierowane do kluczowego zewnętrznego dostawcy usług ICT zgodnie z uprawnieniami, o których mowa w art. 35.

4. Zalecenia, o których mowa w ust. 3, bezzwłocznie przekazuje się kluczowemu zewnętrznemu dostawcy usług ICT oraz organom właściwym dla podmiotów finansowych, na rzecz których dostawca ten świadczy usługi ICT.

Do celów wykonania działań nadzorczych wiodący organ nadzorczy może uwzględnić wszelkie stosowne certyfikaty 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 41

Harmonizacja warunków umożliwiających prowadzenie działań nadzorczych

1. Za pośrednictwem Wspólnego Komitetu EUN opracowują projekty regulacyjnych standardów technicznych określających:

a) informacje, które zewnętrzny dostawca usług ICT ma zawrzeć w dobrowolnym wniosku o wyznaczenie go jako kluczowego na mocy art. 31 ust. 11;

b) zakres, strukturę i format informacji, które zewnętrzni dostawcy usług ICT mają przedłożyć, ujawnić lub zgłosić zgodnie z art. 35 ust. 1, w tym wzór do celów przekazywania informacji na temat umów dalszego podwykonawstwa;

c) kryteria ustalania składu wspólnego zespołu ds. kontroli zapewniające zrównoważony udział pracowników EUN i odpowiednich właściwych organów, a także sposób ich wyznaczenia, zadania i ustalenia robocze;

d) szczegóły przeprowadzonej przez właściwe organy oceny środków wprowadzonych przez kluczowych zewnętrznych dostawców usług ICT w następstwie zaleceń wydanych przez wiodący organ nadzorczy zgodnie z art. 42 ust. 3.

2. EUN przedkładają Komisji te projekty regulacyjnych standardów technicznych do dnia 17 lipca 2024 r.

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

Artykuł 42

Działania następcze podejmowane przez właściwe organy

1. W terminie 60 dni kalendarzowych od otrzymania zaleceń wydanych przez wiodący organ nadzorczy zgodnie z art. 31 ust. 1 lit. d) kluczowi zewnętrzni dostawcy usług ICT powiadamiają wiodący organ nadzorczy o tym, czy zamierzają zastosować się do tych zaleceń, albo przedstawiają uzasadnione wyjaśnienie powodów, dla których nie zamierzają przyjąć takich zaleceń. Wiodący organ nadzorczy niezwłocznie przekazuje tę informację właściwym organom dla odpowiednich podmiotów finansowych.

2. Wiodący organ nadzorczy podaje do wiadomości publicznej informację o tym, że dany kluczowy zewnętrzny dostawca usług ICT nie przekazał mu powiadomienia zgodnie z ust. 1 lub że wyjaśnienie przekazane przez danego kluczowego dostawcę usług ICT nie zostało uznane za wystarczające. W informacji tej ujawnia się tożsamość kluczowego zewnętrznego dostawcy usług ICT oraz opisuje rodzaj i charakter niezgodności. Taka informacja ogranicza się do tego, co jest istotne i proporcjonalne do celów zapewnienia powszechnej wiedzy w tym zakresie, chyba że taka publikacja wyrządziłaby nieproporcjonalną szkodę zaangażowanym stronom lub poważnie zagroziła uporządkowanemu funkcjonowaniu i integralności rynków finansowych lub stabilności całego sytemu finansowego Unii lub jego części.

Wiodący organ nadzorczy powiadamia zewnętrznego dostawcę usług ICT o upublicznieniu tych informacji.

3. Właściwe organy informują odpowiednie podmioty finansowe o ryzyku zidentyfikowanym w zaleceniach skierowanych do kluczowych zewnętrznych dostawców usług ICT zgodnie z art. 35 ust. 1 lit. d).

Zarządzając ryzykiem zewnętrznych dostawców usług ICT, podmioty finansowe uwzględniają ryzyka, o których mowa w akapicie pierwszym.

4. W przypadku gdy właściwy organ uzna, że w ramach zarządzania ryzykiem zewnętrznych dostawców usług ICT podmiot finansowy nie uwzględnia szczególnych rodzajów ryzyka zidentyfikowanych w zaleceniach lub uwzględnia je w niewystarczający sposób, powiadamia ten podmiot finansowy o możliwości podjęcia decyzji w ciągu 60 dni kalendarzowych od otrzymania takiego powiadomienia, zgodnie z ust. 6, w związku z brakiem odpowiednich ustaleń umownych mających na celu zwalczanie takich rodzajów ryzyka.

5. Po otrzymaniu sprawozdań, o których mowa w art. 35 ust. 1 lit. c), i przed podjęciem decyzji, o której mowa w ust. 6 niniejszego artykułu, właściwe organy mogą, na zasadzie dobrowolności, skonsultować się z właściwymi organami wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555 odpowiedzialnymi za nadzór nad kluczowym lub ważnym podmiotem objętym zakresem stosowania tej dyrektywy, który został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT.

6. Jako środek ostateczny, po powiadomieniu i, w stosownych przypadkach, konsultacjach w myśl ust. 4 i 5 niniejszego artykułu, zgodnie z art. 50 właściwe organy mogą podjąć decyzję nakazującą podmiotom finansowym tymczasowe zawieszenie, 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. W razie potrzeby, właściwe organy mogą nakazać podmiotom finansowym wypowiedzenie, w części lub w całości, stosownych ustaleń umownych zawartych z kluczowymi zewnętrznymi dostawcami usług ICT.

7. W przypadku gdy kluczowy zewnętrzny dostawca usług odmówi zatwierdzenia zaleceń, w oparciu o podejście odmienne od podejścia zalecanego przez wiodący organ nadzorczy, a takie odmienne podejście może mieć negatywny wpływ na dużą liczbę podmiotów finansowych lub znaczną część sektora finansowego, i gdy indywidualne ostrzeżenia wydane przez właściwe organy nie doprowadziły do przyjęcia spójnego podejścia łagodzącego potencjalne ryzyko dla stabilności finansowej, w stosownych przypadkach wiodący organ nadzorczy – po konsultacji z forum nadzoru – może wydać niewiążące i niejawne opinie na potrzeby właściwych organów w celu promowania spójnych i zbieżnych środków następczych w zakresie nadzoru.

8. Po otrzymania sprawozdań, o których mowa w art. 35 ust. 1 lit. c), właściwe organy – podejmując decyzję, o której mowa w ust. 6 niniejszego artykułu, 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;

e) kwestię, czy zawieszenie lub wypowiedzenie ustaleń umownych wprowadza ryzyko dla ciągłości działalności gospodarczej danego podmiotu finansowego pomimo wysiłków podejmowanych przez ten podmiot finansowy, by uniknąć zakłócenia w świadczeniu przez niego usług;

f) w stosownych przypadkach opinię właściwych organów wyznaczonych lub ustanowionych zgodnie z dyrektywą (UE) 2022/2555 jako odpowiedzialne za nadzór nad kluczowym lub ważnym podmiotem objętym zakresem stosowania tej dyrektywy, którzy zostali wyznaczeni jako kluczowy zewnętrzny dostawca usług ICT, o którą zwrócono się na zasadzie dobrowolności zgodnie z ust. 5 niniejszego artykułu.

Właściwe organy dają podmiotom finansowym odpowiednio dużo czasu na dostosowanie ustaleń umownych z kluczowymi zewnętrznymi dostawcami usług ICT, aby uniknąć szkodliwych skutków dla ich operacyjnej odporności cyfrowej i umożliwić im wdrożenie strategii wyjścia i planów przejściowych, o których mowa w art. 28.

9. O decyzji określonej w ust. 6 niniejszego artykułu powiadamia się członków forum nadzoru, o którym mowa w art. 32 ust. 4 lit. a), b) i c), i wspólną sieć nadzoru.

Kluczowi zewnętrzni dostawcy usług ICT, których dotyczą decyzje przewidziane w ust. 6, w pełni współpracują z podmiotami finansowymi, na które decyzje te mają wpływ, w szczególności w kontekście procesu zawieszenia lub wypowiedzenia ich ustaleń umownych.

10. Właściwe organy regularnie informują wiodący odpowiedni organ nadzorczy o podejściach i środkach, które zastosowały w ramach swoich zadań nadzorczych w odniesieniu do podmiotów finansowych, jak również o ustaleniach umownych zawartych z tymi podmiotami finansowymi, w przypadku gdy kluczowi zewnętrzni dostawcy usług ICT nie uznali, w części lub w całości, zaleceń skierowanych do nich przez dany wiodący organ nadzorczy.

11. Wiodący organ nadzorczy może, na wniosek, przedstawić dalsze wyjaśnienia dotyczące wydanych zaleceń, aby ukierunkować właściwe organy w kwestii działań następczych.

Artykuł 43

Opłaty nadzorcze

1. Zgodnie z aktem delegowanym, o którym mowa w ust. 2 niniejszego artykułu, wiodący organ nadzorczy pobiera od kluczowych zewnętrznych dostawców usług ICT opłaty, które w pełni pokrywają jego niezbędne wydatki związane z wykonywaniem zadań nadzorczych zgodnie z niniejszym rozporządzeniem, w tym zwrot wszelkich kosztów, które mogą zostać poniesione w wyniku prac prowadzonych przez wspólny zespół ds. kontroli, o którym mowa w art. 40, a także kosztów porad udzielanych przez niezależnych ekspertów, o czym mowa w art. 32 ust. 4 akapit drugi, w odniesieniu do kwestii objętych bezpośrednim nadzorem.

Wysokość opłaty pobieranej od kluczowego zewnętrznego dostawcy usług ICT pozwala na pokrycie wszystkich kosztów związanych z wypełnianiem obowiązków określonych w niniejszej sekcji oraz jest proporcjonalna do jego obrotów.

2. Komisja jest uprawniona do przyjmowania aktów delegowanych zgodnie z art. 57 w celu uzupełnienia niniejszego rozporządzenia poprzez określenie wysokości opłat oraz sposobu ich uiszczania do dnia 17 lipca 2024 r.

Artykuł 44

Współpraca międzynarodowa

1. Bez uszczerbku dla art. 36, EUNB, ESMA i EIOPA mogą zgodnie z art. 33, odpowiednio, rozporządzenia (UE) nr 1093/2010, rozporządzenia (UE) nr 1095/2010 i rozporządzenia (UE) nr 1094/2010 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 łagodzących takie ryzyko i reakcji na incydenty związane z takim ryzykiem.

2. EUN, za pośrednictwem Wspólnego Komitetu, 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 ewolucji ryzyka ze strony zewnętrznych dostawców usług ICT i następstwach dla stabilności finansowej, integralności rynku, ochrony inwestorów i funkcjonowania rynku wewnętrznego.

ROZDZIAŁ VI

Ustalenia dotyczące wymiany informacji

Artykuł 45

Ustalenia dotyczące wymiany 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 możliwości obronnych, technik wykrywania zagrożenia, strategii jego minimalizowania lub etapów reagowania i przywracania sprawności;

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 zgodnie z rozporządzeniem (UE) 2016/679 i wytycznych dotyczących polityki konkurencji.

2. Do celów 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, szczegóły uczestnictwa zewnętrznych dostawców usług ICT, 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.

ROZDZIAŁ VII

Właściwe organy

Artykuł 46

Właściwe organy

Bez uszczerbku dla przepisów dotyczących ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT, o których mowa w rozdziale V sekcja II niniejszego rozporządzenia, następujące właściwe organy zgodnie z uprawnieniami przyznanymi im na mocy odpowiednich aktów prawnych zapewniają przestrzeganie niniejszego rozporządzenia:

a) w odniesieniu do instytucji kredytowych i instytucji zwolnionych zgodnie z dyrektywą 2013/36/UE – właściwy organ wyznaczony zgodnie z art. 4 tej dyrektywy, a dla instytucji kredytowych sklasyfikowanych jako istotne zgodnie z art. 6 ust. 4 rozporządzenia (UE) nr 1024/2013 – EBC zgodnie z uprawnieniami i zadaniami przyznanymi na mocy tego rozporządzenia;

b) w odniesieniu do instytucji płatniczych, w tym instytucji płatniczych zwolnionych zgodnie z dyrektywą (UE) 2015/2366, instytucji pieniądza elektronicznego, w tym instytucji pieniądza elektronicznego zwolnionych zgodnie z dyrektywą 2009/110/WE i dostawców świadczących usługę dostępu do informacji o rachunku, o których mowa w art. 33 ust. 1 dyrektywy (UE) 2015/2366 – właściwy organ wyznaczony zgodnie z art. 22 dyrektywy (UE) 2015/2366;

c) w odniesieniu do firm inwestycyjnych – właściwy organ wyznaczony zgodnie z art. 4 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/2034 ([38]);

d) w odniesieniu do dostawców usług w zakresie kryptoaktywów, którzy uzyskali zezwolenie na mocy rozporządzenia w sprawie rynków kryptoaktywów i emitentów tokenów powiązanych z aktywami – właściwy organ wyznaczony zgodnie z odpowiednim przepisem tego rozporządzenia;

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

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

g) w odniesieniu do systemów obrotu i dostawców usług w zakresie udostępniania informacji – właściwy organ wyznaczony zgodnie z art. 67 dyrektywy 2014/65/UE i właściwy organ zdefiniowany w art. 2 ust. 1 pkt 18 rozporządzenia (UE) nr 600/2014;

h) w odniesieniu do repozytoriów transakcji – właściwy organ wyznaczony zgodnie z art. 22 rozporządzenia (UE) nr 648/2012;

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

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

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

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

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

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

o) w odniesieniu do administratorów kluczowych wskaźników referencyjnych – właściwy organ wyznaczony zgodnie z art. 40 i 41 rozporządzenia (UE) 2016/1011;

([38]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/2034 z dnia 27 listopada 2019 r. w sprawie nadzoru ostrożnościowego nad firmami inwestycyjnymi oraz zmieniająca dyrektywy 2002/87/WE, 2009/65/WE, 2011/61/UE, 2013/36/UE, 2014/59/UE i 2014/65/UE (Dz.U. L 314 z 5.12.2019, s. 64).

p) w odniesieniu do dostawców usług finansowania społecznościowego – właściwy organ wyznaczony zgodnie z art. 29 rozporządzenia (UE) 2020/1503;

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

Artykuł 47

Współpraca ze strukturami i organami ustanowionymi na mocy dyrektywy (UE) 2022/2555

1. Aby usprawnić współpracę i umożliwić wymianę informacji na temat nadzoru między właściwymi organami wyznaczonymi na mocy niniejszego rozporządzenia i grupą współpracy ustanowioną na mocy art. 14 dyrektywy (UE) 2022/2555 EUN i właściwe organy mogą uczestniczyć w czynnościach tej grupy w kwestiach, które dotyczą ich działań nadzorczych w odniesieniu do podmiotów finansowych. EUN i właściwe organy mogą zwrócić się o zaproszenie do udziału w czynnościach grupy współpracy w kwestiach, które dotyczą kluczowych lub ważnych podmiotów objętych zakresem stosowania dyrektywy (UE) 2022/2555 i które zostały wyznaczone jako kluczowi zewnętrzni dostawcy usług ICT zgodnie z art. 31 niniejszego rozporządzenia.

2. W stosownych przypadkach właściwe organy mogą konsultować się i wymieniać informacje z pojedynczymi punktami kontaktowymi i CSIRT wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555.

3. W stosownych przypadkach właściwe organy mogą zwrócić się o wszelkie istotne zalecenia techniczne i pomoc techniczną do właściwych organów wyznaczonych lub ustanowionych zgodnie z dyrektywą (UE) 2022/2555 i ustalić zasady dotyczące współpracy umożliwiające utworzenie skutecznych i szybkich mechanizmów koordynacji działań.

4. Ustalenia, o których mowa w ust. 3 niniejszego artykułu, mogą m.in. określać procedury koordynacji działań nadzorczych i nadzoru prowadzonych w odniesieniu do kluczowego lub ważnego podmiotu objętego zakresem stosowania dyrektywy (UE) 2022/2555, który został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT zgodnie z art. 31 niniejszego rozporządzenia, w tym na potrzeby prowadzenia – zgodnie z prawem krajowym – dochodzeń i kontroli na miejscu, a także na potrzeby mechanizmów wymiany informacji między właściwymi organami na mocy niniejszego rozporządzenia i właściwymi organami wyznaczonymi lub ustanowionymi zgodnie z tą dyrektywą, co obejmuje dostęp do informacji żądanych przez te organy.

Artykuł 48

Współpraca między organami

1. Właściwe organy ściśle współpracują ze sobą oraz, w stosownych przypadkach, z wiodącym organem nadzorczym.

2. Właściwe organy i wiodący organ nadzorczy wzajemnie wymieniają w sposób terminowy wszelkie istotne informacje dotyczące kluczowych zewnętrznych dostawców usług ICT, które to informacje są im niezbędne do wykonywania ich odpowiednich obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do zidentyfikowanych rodzajów ryzyka, podejść i środków podjętych w ramach zadań nadzorczych wiodącego organu nadzorczego.

Artykuł 49

Ćwiczenia, komunikacja i współpraca między sektorami finansowymi

1. EUN, za pośrednictwem Wspólnego Komitetu i we współpracy z właściwymi organami, krajowymi organami ds. restrukturyzacji i uporządkowanej likwidacji, o których mowa w art. 3 dyrektywy 2014/59/UE, EBC, Jednolitą Radą ds. Restrukturyzacji i Uporządkowanej Likwidacji na potrzeby uzyskiwania informacji dotyczących podmiotów objętych zakresem stosowania rozporządzenia (UE) nr 806/2014, ERRS i ENISA, stosownie do przypadku, mogą ustanowić mechanizmy umożliwiające wymianę skutecznych praktyk między sektorami finansowymi, aby zwiększyć świadomość o określonych sytuacjach i zidentyfikować wspólne dla sektorów finansowych podatności i rodzaje ryzyka w cyberprzestrzeni.

Mogą one przygotować ćwiczenia z zakresu zarządzania kryzysowego i sytuacji awaryjnych obejmujące scenariusze cyberataków w celu wypracowania kanałów komunikacyjnych i stopniowego umożliwiania skutecznej skoordynowanej reakcji na poziomie Unii 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, EUN i EBC ściśle współpracują ze sobą i wymieniają się informacjami na potrzeby wykonywania swoich obowiązków zgodnie z art. 47–54. 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 50

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) 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 kopii;

b) przeprowadzania kontroli na miejscu lub dochodzeń, które obejmują m.in.:

   (i) wzywanie przedstawicieli podmiotów finansowych w celu złożenia przez nich ustnych lub pisemnych wyjaśnień na temat faktów lub dokumentów związanych z przedmiotem i celem dochodzenia oraz do zaprotokołowania odpowiedzi;

   (ii) przesłuchiwanie wszelkich innych osób fizycznych lub prawnych, które wyrażą na to zgodę, w celu zebrania informacji dotyczących przedmiotu dochodzenia;

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. 52, państwa członkowskie określają przepisy ustanawiające właściwe kary administracyjne i środki naprawcze w odniesieniu do naruszeń 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 niniejszego rozporządzenia, obejmujących co najmniej:

a) wydanie nakazu zobowiązującego osobę fizyczną lub prawną do zaprzestania postępowania naruszającego niniejsze rozporządzenie 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) podejmowanie 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 niniejszego rozporządzenia oraz w przypadku gdy takie rejestry mogą mieć znaczenie dla dochodzenia w sprawie naruszeń 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 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 51

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. 50, 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; lub

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. 50, 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 przyczynienia się osoby fizycznej lub prawnej do naruszenia;

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 fizyczną lub prawną;

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

Artykuł 52

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 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 w celu otrzymywania szczegółowych informacji dotyczących dochodzeń lub postępowań karnych wszczętych w związku z naruszeniami niniejszego rozporządzenia oraz przekazywania takich informacji innym właściwym organom, a także EUNB, ESMA lub EIOPA w celu wypełnienia swoich obowiązków w zakresie współpracy do celów niniejszego rozporządzenia.

Artykuł 53

Obowiązki dotyczące powiadamiania

Państwa członkowskie powiadamiają Komisję, ESMA, EUNB oraz EIOPA o przepisach ustawowych, wykonawczych i administracyjnych wykonujących przepisy niniejszego rozdziału, w tym o wszelkich odpowiednich przepisach prawa karnego, do dnia 17 stycznia 2025 r. Państwa członkowskie bez zbędnej zwłoki powiadamiają Komisję, ESMA, EUNB i EIOPA o wszelkich późniejszych zmianach tych przepisów.

Artykuł 54

Publikowanie kar administracyjnych

1. Właściwe organy bez zbędnej zwłoki publikują na swojej oficjalnej stronie internetowej każdą decyzję nakładającą kary administracyjne, wobec której, po tym jak adresat kary 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 i m.in. rodziła ryzyko w zakresie ochrony danych osobowych, 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 istnieć;

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 jakiegokolwiek 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 wniesiono 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 jedynie przez okres, który jest konieczny do wdrożenia niniejszego artykułu. Okres ten nie może przekraczać pięciu lat po dokonaniu tej publikacji.

Artykuł 55

Tajemnica zawodowa

1. Wszelkie poufne informacje otrzymywane, wymieniane lub przekazywane zgodnie z niniejszym rozporządzeniem 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, w tym wymiana informacji pomiędzy właściwymi organami na mocy niniejszego rozporządzenia i właściwymi organami wyznaczonymi lub ustanowionymi zgodnie z dyrektywą (UE) 2022/2555, 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 zgodnie z niniejszym rozporządzeniem, które dotyczą warunków biznesowych lub operacyjnych oraz innych kwestii gospodarczych lub osobistych, uznaje się za informacje poufne i obejmuje się 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.

Artykuł 56

Ochrona danych

1. EUN i właściwe organy mogą przetwarzać dane osobowe wyłącznie wtedy, gdy jest to konieczne do celów wykonywania ich odpowiednich obowiązków i zadań zgodnie z niniejszym rozporządzeniem, w szczególności w zakresie dochodzeń, kontroli, wniosków o udzielenie informacji, komunikacji, publikacji, ewaluacji, weryfikacji, oceny i sporządzania planów nadzoru. Dane osobowe są przetwarzane zgodnie z rozporządzeniem (UE) 2016/679 lub rozporządzeniem (UE) 2018/1725, w zależności od tego, które z nich ma zastosowanie.

2. O ile inne akty sektorowe nie stanowią inaczej, dane osobowe, o których mowa w ust. 1, są zatrzymywane do czasu wywiązania się z mających zastosowanie obowiązków nadzorczych i w każdym przypadku przez maksymalnie 15 lat, z wyjątkiem sytuacji, gdy toczy się postępowanie sądowe wymagające dalszego zatrzymania takich danych.

ROZDZIAŁ VIII

Akty delegowane

Artykuł 57

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 31 ust. 6 i art. 43 ust. 2, powierza się Komisji na okres pięciu lat od dnia 17 stycznia 2024 r. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem tego pięcioletniego okresu. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.

3. Parlament Europejski lub Rada mogą w dowolnym czasie odwołać przekazanie uprawnień, o którym mowa w art. 31 ust. 6 i art. 43 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 zgodnie z art. 31 ust. 6 lub art. 43 ust. 2 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech 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 trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

ROZDZIAŁ IX

Przepisy przejściowe i końcowe

Sekcja I

Artykuł 58

Klauzula przeglądowa

1. Do dnia 17 stycznia 2028 r., po konsultacji z EUN i ERRS, stosownie do przypadku, Komisja przeprowadza przegląd i przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w stosownych przypadkach wraz z wnioskiem ustawodawczym. Przegląd ten obejmuje co najmniej:

a) kryteria wyznaczania kluczowych zewnętrznych dostawców usług ICT określonych zgodnie z art. 31 ust. 2;

b) dobrowolny charakter powiadamiania o znaczących cyberzagrożeniach, o których mowa w art. 19;

c) system, o którym mowa w art. 31 ust. 12, i uprawnienia wiodącego organu nadzorczego przewidziane w art. 35 ust. 1 lit. d) ppkt (iv) tiret pierwsze z myślą o ocenie skuteczności tych przepisów, jeżeli chodzi o zapewnienie skutecznego nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT mającymi siedzibę w państwie trzecim oraz konieczności ustanowienia jednostki zależnej w Unii.

   Do celów akapitu pierwszego niniejszej litery przegląd obejmuje analizę systemu, o którym mowa w art. 31 ust. 12, w tym warunków dostępu unijnych podmiotów finansowych do usług z państw trzecich oraz dostępności takich usług na rynku unijnym, i uwzględnia dalsze zmiany na rynkach usług objętych niniejszym rozporządzeniem, praktyczne doświadczenia podmiotów finansowych i organów nadzoru finansowego w zakresie, odpowiednio, stosowania tego systemu i nadzoru nad nim oraz wszelkie istotne zmiany regulacyjne i nadzorcze zachodzące na poziomie międzynarodowym;

d) zasadność włączenia do zakresu stosowania niniejszego rozporządzenia podmiotów finansowych, o których mowa w art. 2 ust. 3 lit. e), wykorzystujących zautomatyzowane systemy sprzedaży, w świetle zmian dotyczących stosowania takich systemów, jakie mogą zajść na rynku w przyszłości;

e) funkcjonowanie i skuteczność wspólnej sieci nadzoru, jeżeli chodzi o wspieranie spójności nadzoru i efektywności wymiany informacji w kontekście ram nadzoru.

2. W związku z przeglądem dyrektywy (UE) 2015/2366 Komisja ocenia potrzebę zwiększenia cyberodporności systemów płatniczych i działań przetwarzania płatności oraz zasadność rozszerzenia zakresu stosowania niniejszego rozporządzenia na operatorów systemów płatniczych i podmioty prowadzące czynności przetwarzania. W świetle tej oceny, w ramach przeglądu dyrektywy (UE) 2015/2366, Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie nie później niż do dnia 17 lipca 2023 r.

Na podstawie tego sprawozdania z przeglądu i po konsultacji z EUN, EBC i ERRS Komisja może przedłożyć, w stosownych przypadkach i w ramach wniosku ustawodawczego, który może przyjąć zgodnie z art. 108 akapit drugi dyrektywy (UE) 2015/2366, propozycję służącą zapewnieniu, by wszyscy operatorzy systemów płatniczych i podmioty prowadzące czynności przetwarzania płatności byli objęci odpowiednim nadzorem, uwzględniając przy tym istniejący nadzór sprawowany przez bank centralny.

3. Do dnia 17 stycznia 2026 r., po konsultacji z EUN i Komitetem Europejskich Organów Nadzoru Audytowego, Komisja przeprowadza przegląd i przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w stosownych przypadkach wraz z wnioskiem ustawodawczym, w sprawie zasadności wprowadzenia wzmocnionych wymogów dla biegłych rewidentów i firm audytorskich, jeżeli chodzi o operacyjną odporność cyfrową, poprzez włączenie biegłych rewidentów i firm audytorskich do zakresu stosowania niniejszego rozporządzenia lub poprzez zmiany w dyrektywie Parlamentu Europejskiego i Rady 2006/43/WE ([39]).

Sekcja II

Zmiany

Artykuł 59

Zmiany w rozporządzeniu (WE) nr 1060/2009

W rozporządzeniu (WE) nr 1060/2009 wprowadza się następujące zmiany:

1) załącznik I sekcja A pkt 4 akapit pierwszy otrzymuje brzmienie:

„Agencja ratingowa posiada solidne 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) 2022/2554 (*).

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

2) załącznik III pkt 12 otrzymuje brzmienie:

„12. Agencja ratingowa narusza art. 6 ust. 2, w związku z przepisami załącznika I sekcja A pkt 4, jeżeli nie posiada solidnych procedur administracyjnych lub księgowych, mechanizmów kontroli wewnętrznej, skutecznych procedur oceny ryzyka lub skutecznych rozwiązań w zakresie kontroli lub bezpieczeństwa do celów zarządzania systemami ICT zgodnie z rozporządzeniem (UE) 2022/2554; lub nie wdrożyła lub nie utrzymuje procedur decyzyjnych lub struktur organizacyjnych wymaganych w tym ustępie.".

Artykuł 60

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. Stosuje odpowiednie i proporcjonalne systemy, zasoby i procedury, w tym systemy ICT zarządzane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2022/2554 (*)

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

([39]) Dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca dyrektywę Rady 84/253/EWG (Dz.U. L 157 z 9.6.2006, s. 87).

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 przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej, które obejmują strategię na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT wprowadzone i wdrożone zgodnie z rozporządzeniem (UE) 2022/2554, służące zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenie działalności i wywiązywanie się z obowiązków CCP.";

b) ust. 3 akapit pierwszy otrzymuje brzmienie:

„3. 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 przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej, z wyjątkiem strategii na rzecz ciągłości działania w zakresie ICT i planów przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej w zakresie 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 minimalizuje je również dzięki opracowaniu odpowiednich systemów, kontroli i procedur, w tym systemów ICT zarządzanych zgodnie z rozporządzeniem (UE) 2022/2554.

2. Repozytorium transakcji ustanawia, wprowadza i utrzymuje odpowiednią strategię na rzecz ciągłości działania oraz plan przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej, które obejmują strategię na rzecz ciągłości działania w zakresie ICT i plany reagowania i przywracania sprawności ICT ustanowione zgodnie z rozporządzeniem (UE) 2022/2554, służące zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenia działalności i wywiązywania się z obowiązków repozytorium transakcji.";

5) w art. 80 uchyla się ust. 1.

6) w załączniku I sekcja II wprowadza się następujące zmiany:

a) lit. a) i b) otrzymują brzmienie:

„a) repozytorium transakcji narusza art. 79 ust. 1, jeżeli nie identyfikuje źródeł ryzyka operacyjnego lub nie minimalizuje tego ryzyka poprzez opracowywanie odpowiednich systemów, mechanizmów kontroli i procedur, w tym systemów ICT zarządzanych zgodnie z rozporządzeniem (UE) 2022/2554;

b) repozytorium transakcji narusza art. 79 ust. 2, jeżeli nie ustanawia, nie wprowadza ani nie utrzymuje odpowiedniej strategii na rzecz ciągłości działania i planu przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej ustanowionych zgodnie z rozporządzeniem (UE) 2022/2554, które służą zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenia działalności i wywiązywania się z obowiązków repozytorium transakcji.";

b) uchyla się lit. c);

7) w załączniku III wprowadza się następujące zmiany:

a) w sekcji II wprowadza się następujące zmiany:

(i) lit. c) otrzymuje brzmienie:

„c) CCP Tier II narusza art. 26 ust. 3, jeżeli nie utrzymuje ani nie stosuje struktury organizacyjnej zapewniającej ciągłość działania oraz prawidłowe funkcjonowanie w zakresie świadczenia usług i prowadzenia działalności lub jeżeli nie stosuje odpowiednich i proporcjonalnych systemów, zasobów lub procedur, w tym systemów ICT zarządzanych zgodnie z rozporządzeniem (UE) 22022/2554";

(ii) uchyla się lit. f);

b) sekcja III lit. a) otrzymuje brzmienie:

„a) CCP Tier II narusza art. 34 ust. 1, jeżeli nie ustanawia, nie wprowadza ani nie utrzymuje odpowiedniej strategii na rzecz ciągłości działania lub planu reagowania i przywracania sprawności utworzonych zgodnie z rozprowadzeniem (UE) 2022/2554, które służą zapewnieniu zachowania pełnionych funkcji, szybkiego przywrócenia działalności i wywiązywania się z obowiązków CCP, przy czym taki plan musi pozwalać co najmniej na odzyskanie wszystkich transakcji realizowanych w chwili wystąpienia zakłócenia, tak aby umożliwić CCP dalsze niezawodne prowadzenie działalności oraz ukończenie rozrachunku w wyznaczonym terminie;".

Artykuł 61

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 minimalizuje 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) 2022/2554 (*), a także poprzez stosowanie wszelkich innych stosownych narzędzi, mechanizmów kontroli i procedur w odniesieniu do innych rodzajów ryzyka operacyjnego, w tym dla wszystkich systemów rozrachunku papierów wartościowych, które prowadzi.

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

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 na rzecz ciągłości działania oraz plan przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej, które obejmują strategię na rzecz ciągłości działania w zakresie ICT oraz plany reagowania i przywracania sprawności ICT ustanowione zgodnie z rozporządzeniem (UE) 2022/2554, 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. 12 ust. 5 i 7 rozporządzenia (UE) 2022/2554";

4) ust. 6 otrzymuje brzmienie:

„6. 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 incydentach operacyjnych, innych niż w odniesieniu do ryzyka związanego z ICT, wynikających z takich ryzyk.";

5) ust. 7 akapit pierwszy otrzymuje brzmienie:

„7. 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, eliminowania lub minimalizacji tych ryzyk, w tym strategii na rzecz ciągłości działania i planów przywracania sprawności po wystąpieniu sytuacji nadzwyczajnej, o których mowa w ust. 3 i 4, oraz metod ich oceny.".

Artykuł 62

Zmiany w rozporządzeniu (UE) nr 600/2014

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

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

   a) ust. 4 otrzymuje brzmienie:

   „4. Zatwierdzony podmiot publikujący spełnia wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/2554 (*).

   _____

   (*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1).";

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

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

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

   a) ust. 5 otrzymuje brzmienie:

   „5. Dostawca informacji skonsolidowanych spełnia wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych określone w rozporządzeniu (UE) 2022/2554.";

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

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

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

   a) ust. 3 otrzymuje brzmienie:

   „3. Zatwierdzony mechanizm sprawozdawczy spełnia wymogi dotyczące bezpieczeństwa sieci i systemów informatycznych określone w rozporządzeniu (UE) 2022/2554.";

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

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

Artykuł 63

Zmiany w rozporządzeniu (UE) 2016/1011

W art. 6 rozporządzenia (UE) 2016/1011 dodaje się ustęp w brzmieniu:

„6. „W przypadku kluczowych wskaźników referencyjnych administrator stosuje solidne 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) 2022/2554 (*)

_____

(*) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 1 z 27.12.2022, s. 333).".

Artykuł 64

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 17 stycznia 2025 r.

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

Sporządzono w Strasburgu dnia 14 grudnia 2022 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	M. BEK