Rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA). Komentarz

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.Urz. UE L Nr 333, s. 1)

(sprost. Dz.Urz. UE L 2024/90177)

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 najważ-

[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.

niejszych 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 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 zwią-

zanych 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 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

[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).

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 jakościowym 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

[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).

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.

(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, mechanizmów kontrolnych 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

[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).

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.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

[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).

[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).

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

[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).

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.

(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 związa-

nymi 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