ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2025/295

z dnia 24 października 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych dotyczących harmonizacji warunków umożliwiających prowadzenie działań nadzorczych

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 ([1]), w szczególności jego art. 41 ust. 2 akapit drugi,

a także mając na uwadze, co następuje:

(1) Ustanowione rozporządzeniem (UE) 2022/2554 ramy dotyczące operacyjnej odporności cyfrowej sektora finansowego obejmują unijne ramy nadzoru nad zewnętrznymi dostawcami usług z zakresu technologii informacyjno-komunikacyjnych (ICT) dla sektora finansowego wyznaczonymi jako kluczowi zgodnie z art. 31 tego rozporządzenia.

(2) Zewnętrzny dostawca usług ICT, który postanawia złożyć dobrowolny wniosek o wyznaczenie go jako kluczowego, powinien przekazać Europejskiemu Urzędowi Nadzoru (EUN) otrzymującemu wniosek wszystkie informacje niezbędne do wykazania jego krytyczności zgodnie z zasadami i kryteriami określonymi w rozporządzeniu (UE) 2022/2554. Z tego powodu informacje, które należy zawrzeć w dobrowolnym wniosku, powinny być dostatecznie szczegółowe i wyczerpujące, aby umożliwić jasną i pełną ocenę krytyczności zgodnie z art. 31 ust. 11 tego rozporządzenia. Odpowiedni EUN powinien odrzucić każdy niekompletny wniosek i zażądać brakujących informacji.

(3) Identyfikacja prawna zewnętrznych dostawców usług ICT objętych zakresem niniejszych regulacyjnych standardów technicznych powinna być dostosowana do kodu identyfikacyjnego określonego w rozporządzeniu wykonawczym Komisji przyjętym zgodnie z art. 28 ust. 9 rozporządzenia (UE) 2022/2554.

(4) W ramach działań następczych w związku z zaleceniami wydanymi przez wiodący organ nadzorczy dla kluczowych zewnętrznych dostawców usług ICT wiodący organ nadzorczy powinien monitorować przestrzeganie zaleceń przez kluczowych zewnętrznych dostawców usług ICT. Aby zapewnić sprawne i skuteczne monitorowanie działań podjętych przez kluczowych zewnętrznych dostawców usług ICT lub środków zaradczych wdrożonych przez nich w związku z tymi zaleceniami, wiodący organ nadzorczy powinien móc zażądać przedłożenia sprawozdań przewidzianych w art. 35 ust. 1 lit. c) rozporządzenia (UE) 2022/2554, które powinny mieć formę sprawozdań śródokresowych i sprawozdań końcowych.

(5) Do celów oceny określonej w art. 42 ust. 1 rozporządzenia (UE) 2022/2554, zgodnie z którą wiodący organ nadzorczy ma obowiązek ocenić, czy wyjaśnienie przedstawione przez kluczowego zewnętrznego dostawcę usług ICT jest wystarczające, powiadomienie wiodącego organu nadzorczego przez kluczowego zewnętrznego dostawcę usług ICT o zamiarze zastosowania się do otrzymanych zaleceń należy uzupełnić o opis działań i środków, które wprowadzono w celu ograniczenia ryzyka określonego w zaleceniach, wraz z odpowiednimi terminami ich realizacji. Takie wyjaśnienie powinno mieć formę planu naprawczego.

(6) Ponieważ oczekuje się, że wiodący organ nadzorczy będzie oceniać umowy dalszego podwykonawstwa kluczowego zewnętrznego dostawcy usług ICT, należy opracować wzór do celów przekazywania informacji na temat tych umów. W tym wzorze należy uwzględnić fakt, że kluczowi zewnętrzni dostawcy usług ICT mają inne struktury niż podmioty finansowe.

([1]) Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) Po wydaniu zaleceń dla kluczowego zewnętrznego dostawcy usług ICT przez wiodący organ nadzorczy oraz po tym, jak właściwe organy poinformują odpowiednie podmioty finansowe o ryzyku zidentyfikowanym w tych zaleceniach, wiodący organ nadzorczy powinien monitorować i oceniać wdrażanie przez kluczowego zewnętrznego dostawcę usług ICT działań i środków zaradczych mających na celu zastosowanie się do zaleceń. Właściwe organy powinny monitorować i oceniać zakres, w jakim podmioty finansowe są narażone na ryzyko zidentyfikowane w tych zaleceniach. Aby utrzymać równe warunki działania, podczas wykonywania odpowiednich zadań, w szczególności gdy ryzyko zidentyfikowane w zaleceniach jest poważne i dotyczy dużej liczby podmiotów finansowych w wielu państwach członkowskich, zarówno właściwe organy, jak i wiodący organ nadzorczy powinny wymieniać między sobą wszelkie istotne ustalenia, które są niezbędne do wykonywania odpowiednich zadań tych organów. Celem wymiany informacji jest zapewnienie, aby w informacjach zwrotnych przekazywanych kluczowemu zewnętrznemu dostawcy usług ICT przez wiodący organ nadzorczy w odniesieniu do działań i środków zaradczych, które wdraża ten kluczowy zewnętrzny dostawca usług ICT, uwzględniono wpływ na ryzyko podmiotów finansowych oraz aby działania nadzorcze prowadzone przez właściwe organy były oparte na ocenie przeprowadzonej przez wiodący organ nadzorczy.

(8) Aby umożliwić sprawną i skuteczną wymianę informacji, właściwe organy powinny w ramach swoich działań nadzorczych oceniać, w jakim stopniu nadzorowane przez nie podmioty finansowe są narażone na ryzyko zidentyfikowane w zaleceniach. Ocenę tę należy przeprowadzić w sposób proporcjonalny i oparty na analizie ryzyka. Wiodący organ nadzorczy powinien zwrócić się do właściwych organów o udostępnienie wyników tej oceny w szczególnych przypadkach, gdy ryzyko związane z zaleceniami jest poważne i dotyczy dużej liczby podmiotów finansowych w wielu państwach członkowskich. Aby jak najlepiej wykorzystać zasoby właściwych organów, wiodący organ nadzorczy, który zwraca się o udostępnienie wyników tej oceny, powinien zawsze brać pod uwagę, że celem tych wniosków jest ocena realizacji działań i środków zaradczych wdrażanych przez kluczowych zewnętrznych dostawców usług ICT.

(9) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([2]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 22 lipca 2024 r.

(10) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przedłożony Komisji przez EUN.

(11) Wspólny Komitet EUN przeprowadził otwarte konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonał analizy potencjalnych powiązanych kosztów i korzyści oraz zwrócił się o opinię do Bankowej Grupy Interesariuszy powołanej zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([3]), do Grupy Interesariuszy z Sektora Ubezpieczeń i Reasekuracji i Grupy Interesariuszy z Sektora Pracowniczych Programów Emerytalnych powołanych zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1094/2010 ([4]) oraz do Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej zgodnie z art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([5]),

([2]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Informacje, które zewnętrzny dostawca usług ICT ma zawrzeć we wniosku o wyznaczenie go jako kluczowego

1. Zewnętrzny dostawca usług z zakresu technologii informacyjno-komunikacyjnych (ICT) przedkłada w uzasadnionym dobrowolnym wniosku na podstawie art. 31 ust. 11 rozporządzenia (UE) 2022/2554 o wyznaczenie go jako kluczowego zgodnie z art. 31 ust. 1 lit. a) rozporządzenia (UE) 2022/2554 następujące informacje:

a) nazwę podmiotu prawnego;

b) kod identyfikacyjny podmiotu prawnego;

c) imię i nazwisko osoby wyznaczonej do kontaktów oraz dane kontaktowe kluczowego zewnętrznego dostawcy usług ICT;

d) państwo, w którym podmiot prawny ma siedzibę statutową;

e) opis struktury korporacyjnej, w tym co najmniej informacje na temat jednostki dominującej i innych jednostek powiązanych świadczących usługi ICT na rzecz unijnych podmiotów finansowych. Informacje te obejmują, w stosownych przypadkach:

   (i) nazwę podmiotu prawnego;

   (ii) kod identyfikacyjny podmiotu prawnego;

   (iii) państwo, w którym podmiot prawny ma siedzibę statutową;

f) oszacowanie udziału w rynku zewnętrznego dostawcy usług ICT w unijnym sektorze finansowym oraz oszacowanie udziału w rynku w podziale na rodzaje podmiotów finansowych, o których mowa w art. 2 ust. 1 rozporządzenia (UE) 2022/2554, za rok złożenia wniosku o wyznaczenie go jako kluczowego i rok poprzedzający złożenie tego wniosku;

g) opis każdej usługi ICT świadczonej na rzecz unijnych podmiotów finansowych, w tym:

   (i) opis charakteru działalności gospodarczej i rodzaju usług ICT świadczonych na rzecz podmiotów finansowych;

   (ii) wykaz funkcji podmiotów finansowych wspieranych przez świadczone usługi ICT, jeżeli jest dostępny;

   (iii) informację, czy usługi ICT świadczone na rzecz podmiotów finansowych wspierają krytyczne lub istotne funkcje, jeżeli jest dostępna;

h) wykaz podmiotów finansowych, które korzystają z usług ICT świadczonych przez zewnętrznego dostawcę usług ICT, w tym następujące informacje dotyczące każdego podmiotu finansowego, który korzysta z usług, jeżeli są dostępne:

   (i) nazwa podmiotu prawnego;

   (ii) kod identyfikacyjny podmiotu prawnego, jeżeli jest znany zewnętrznemu dostawcy usług ICT;

   (iii) rodzaj podmiotu finansowego określony w art. 2 ust. 1 rozporządzenia (UE) 2022/2554;

   (iv) lokalizacja geograficzna, z której świadczone są usługi ICT na rzecz tego konkretnego podmiotu prawnego;

i) wykaz kluczowych zewnętrznych dostawców usług ICT wymienionych w najnowszym dostępnym wykazie takich dostawców opublikowanym przez EUN zgodnie z art. 31 ust. 9 rozporządzenia (UE) 2022/2554, którzy korzystają z usług świadczonych przez wnioskodawcę, jeżeli taki wykaz jest dostępny;

j) samoocenę w odniesieniu do:

   (i) stopnia substytucyjności każdej usługi ICT świadczonej przez wnioskodawcę z uwzględnieniem następujących elementów:

      — udziału w rynku zewnętrznego dostawcy usług ICT w unijnym sektorze finansowym,

— liczby znanych istotnych konkurentów w podziale na rodzaj usług ICT lub grupę usług ICT,

— opisu specyfiki oferowanych usług ICT, w tym w odniesieniu do wszelkich zastrzeżonych technologii, lub szczególnych cech organizacji lub działalności zewnętrznego dostawcy usług ICT;

(ii) wiedzy na temat dostępności alternatywnych zewnętrznych dostawców usług ICT, jeśli chodzi o świadczenie takich samych usług ICT jak zewnętrzny dostawca usług ICT składający wniosek;

k) informacje na temat przyszłej strategii biznesowej w odniesieniu do świadczenia usług ICT i udostępniania infrastruktury na rzecz podmiotów finansowych w Unii, w tym na temat wszelkich planowanych zmian w strukturze grupy lub zarządzania, wchodzenia na nowe rynki lub podejmowania nowych rodzajów działalności;

l) wskazanie podwykonawców zewnętrznego dostawcy usług ICT, którzy zostali wyznaczeni jako kluczowi zewnętrzni dostawcy usług ICT;

m) wszelkie inne powody istotne dla wniosku zewnętrznego dostawcy usług ICT o wyznaczenie go jako kluczowego.

2. W przypadku gdy zewnętrzny dostawca usług ICT należy do grupy, informacje, o których mowa w ust. 1, przekazuje się w odniesieniu do usług ICT świadczonych przez grupę jako całość.

Artykuł 2

Zakres, struktura i format informacji, które zewnętrzni dostawcy usług ICT mają przedłożyć, ujawnić lub zgłosić

1. Kluczowi zewnętrzni dostawcy usług ICT przekazują wiodącemu organowi nadzorczemu, na jego żądanie, wszelkie informacje niezbędne wiodącemu organowi nadzorczemu do wykonywania jego obowiązków nadzorczych zgodnie z wymogami rozporządzenia (UE) 2022/2554.

2. Informacje, o których mowa w ust. 1, obejmują między innymi następujące elementy:

a) informacje o umowach i kopie dokumentów umownych między:

(i) kluczowym zewnętrznym dostawcą usług ICT i podmiotami finansowymi, o których mowa w art. 2 ust. 1 rozporządzenia (UE) 2022/2554;

(ii) kluczowym zewnętrznym dostawcą usług ICT i jego podwykonawcami w celu uwzględnienia technologicznego łańcucha wartości usług ICT świadczonych na rzecz podmiotów finansowych w Unii;

b) informacje na temat struktury organizacyjnej i grupowej kluczowego zewnętrznego dostawcy usług ICT, w tym wskazanie wszystkich podmiotów należących do tej samej grupy, które bezpośrednio lub pośrednio świadczą usługi ICT na rzecz podmiotów finansowych w Unii;

c) informacje na temat głównych akcjonariuszy lub udziałowców, w tym ich struktury i rozkładu geograficznego, każdego z następujących podmiotów:

(i) podmiotów, które posiadają, samodzielnie lub wspólnie z podmiotami powiązanymi, co najmniej 25 % kapitału lub praw głosu kluczowego zewnętrznego dostawcy usług ICT;

(ii) podmiotów, które mają prawo wyznaczyć lub odwołać większość członków organu administracyjnego, zarządzającego lub nadzorczego kluczowego zewnętrznego dostawcy usług ICT;

(iii) podmiotów, które zgodnie z umową kontrolują większość praw głosu akcjonariuszy lub udziałowców lub członków kluczowego zewnętrznego dostawcy usług ICT;

d) informacje na temat udziału kluczowego zewnętrznego dostawcy usług ICT w rynku w podziale na rodzaj usług w odniesieniu do odpowiednich rynków, na których dostawca prowadzi działalność;

e) informacje na temat wewnętrznych zasad zarządzania kluczowego zewnętrznego dostawcy usług ICT, w tym na temat struktury z uwzględnieniem zakresów odpowiedzialności za zarządzanie i zasad rozliczalności;

f) protokoły posiedzeń organu zarządzającego kluczowego zewnętrznego dostawcy usług ICT i wszelkich innych odpowiednich komitetów wewnętrznych, które to protokoły w jakikolwiek sposób odnoszą się do działań i ryzyka związanych z zewnętrznymi usługami ICT wspierającymi funkcje podmiotów finansowych w Unii;

g) informacje na temat bezpieczeństwa ICT kluczowego zewnętrznego dostawcy usług ICT, w tym na temat odpowiednich strategii, celów, polityk, procedur, protokołów, procesów, środków kontroli mających na celu ochronę danych wrażliwych, kontroli dostępu, praktyk szyfrowania, planów reagowania na incydenty, oraz, w stosownych przypadkach, informacje na temat zgodności ze wszystkimi odpowiednimi przepisami oraz normami krajowymi i międzynarodowymi;

h) informacje na temat środków technicznych i organizacyjnych służących zapewnieniu ochrony danych i poufności danych, w tym danych osobowych i nieosobowych, wdrożonych środków kontroli mających na celu ochronę danych wrażliwych, kontroli dostępu, praktyk szyfrowania, planu reagowania na naruszenia ochrony danych; jeżeli w odniesieniu do przetwarzania danych osobowych zewnętrzny dostawca usług ICT podlega przepisom państw trzecich, w tym wymogowi złożenia do rządu państwa trzeciego wniosku o udzielenie dostępu – wykaz państw i mających zastosowanie przepisów;

i) informacje na temat mechanizmów, jakie kluczowy zewnętrzny dostawca usług ICT oferuje unijnym podmiotom finansowym w zakresie przenoszenia danych, możliwości przenoszenia aplikacji i interoperacyjności;

j) informacje na temat lokalizacji ośrodków przetwarzania danych i ośrodków produkcji ICT wykorzystywanych do celów świadczenia usług na rzecz podmiotów finansowych, w tym wykaz wszystkich odpowiednich obiektów i pomieszczeń kluczowego zewnętrznego dostawcy usług ICT, w tym poza Unią;

k) informacje na temat świadczenia usług przez kluczowego zewnętrznego dostawcę usług ICT z państwa trzeciego, w tym informacje na temat odpowiednich przepisów mających zastosowanie do danych osobowych i nieosobowych przetwarzanych przez zewnętrznego dostawcę usług ICT;

l) informacje na temat środków zastosowanych w celu przeciwdziałania ryzyku wynikającemu ze świadczenia usług ICT przez kluczowego zewnętrznego dostawcę usług ICT i jego podwykonawców z państw trzecich;

m) informacje na temat ram zarządzania ryzykiem i ram zarządzania incydentami, w tym na temat polityk, procedur, narzędzi, mechanizmów i zasad zarządzania kluczowego zewnętrznego dostawcy usług ICT i jego podwykonawców, w tym wykaz i opis poważnych incydentów mających bezpośredni lub pośredni wpływ na podmioty finansowe w Unii, wraz z istotnymi szczegółami umożliwiającymi określenie znaczenia incydentu dla podmiotów finansowych i ocenę ewentualnych skutków transgranicznych;

n) informacje na temat ram zarządzania zmianami, w tym na temat polityk, procedur i kontroli kluczowego zewnętrznego dostawcy usług ICT i jego podwykonawców;

o) informacje na temat ogólnych ram reagowania i przywracania sprawności kluczowego zewnętrznego dostawcy usług ICT, w tym na temat planów ciągłości działania oraz powiązanych ustaleń i procedur, polityki cyklu życia oprogramowania, planów reagowania i przywracania sprawności oraz powiązanych ustaleń i procedur, ustaleń i procedur dotyczących polityki tworzenia kopii zapasowych;

p) informacje na temat monitorowania skuteczności działania, monitorowania bezpieczeństwa i śledzenia incydentów, a także informacje na temat mechanizmów zgłaszania związanych z wykonywaniem usług, incydentami i zgodnością z uzgodnionymi umowami o gwarantowanym poziomie usług i celami dotyczącymi gwarantowanego poziomu usług lub podobnymi uzgodnieniami między kluczowymi zewnętrznymi dostawcami usług ICT i podmiotami finansowymi w Unii;

q) informacje na temat ram zarządzania zewnętrznymi dostawcami usług ICT kluczowego zewnętrznego dostawcy usług ICT, w tym na temat strategii, polityk, procedur, procesów i kontroli, wraz ze szczegółowymi informacjami na temat należytej staranności i oceny ryzyka przeprowadzanej przez kluczowego zewnętrznego dostawcę usług ICT wobec jego podwykonawców przed zawarciem z nimi umowy oraz w celu monitorowania relacji obejmującego wszelkie istotne ryzyko związane z ICT i ryzyko kontrahenta;

r) wyciągi z systemów monitorowania i skanowania kluczowego zewnętrznego dostawcy usług ICT i jego podwykonawców, obejmujące m.in. monitorowanie sieci, monitorowanie serwerów, monitorowanie aplikacji, monitorowanie bezpieczeństwa, skanowanie pod kątem podatności, zarządzanie rejestrami zdarzeń, monitorowanie skuteczności działania, zarządzanie incydentami i pomiary pod kątem realizacji celów w zakresie niezawodności, takich jak cele dotyczące gwarantowanego poziomu usług;

s) wyciągi z wszelkich systemów lub aplikacji produkcyjnych, przedprodukcyjnych i testowych wykorzystywanych przez kluczowego zewnętrznego dostawcę usług ICT i jego podwykonawców do świadczenia, bezpośrednio lub pośrednio, usług na rzecz podmiotów finansowych w Unii;

t) sprawozdania dotyczące zgodności i dostępne sprawozdania z audytów oraz wszelkie istotne ustalenia z audytów, w tym audytów przeprowadzonych przez organy krajowe w Unii i poza Unią, w przypadku gdy umowy o współpracy z odpowiednimi organami przewidują taką wymianę informacji, lub certyfikaty uzyskane przez kluczowego zewnętrznego dostawcę usług ICT lub jego podwykonawców, w tym sprawozdania audytorów wewnętrznych i zewnętrznych, certyfikaty lub oceny zgodności z normami branżowymi. Obejmuje to informacje na temat wszelkiego rodzaju dostępnych niezależnych testów odporności systemów ICT kluczowego zewnętrznego dostawcy usług ICT, w tym na temat wszelkiego rodzaju testów penetracyjnych pod kątem wyszukiwania zagrożeń przeprowadzanych przez zewnętrznego dostawcę usług ICT;

u) informacje na temat wszelkich ocen przeprowadzonych przez kluczowego zewnętrznego dostawcę usług ICT na jego żądanie lub w jego imieniu, dotyczących odpowiedniości i uczciwości osób zajmujących kluczowe stanowiska u kluczowego zewnętrznego dostawcy usług ICT;

v) informacje na temat wszelkich planów naprawczych służących realizacji zaleceń zgodnie z art. 3 oraz odpowiednie informacje powiązane umożliwiające potwierdzenie wdrożenia działań naprawczych;

w) informacje na temat dostępnych programów szkolenia pracowników i programów zwiększania świadomości w zakresie bezpieczeństwa, w tym, w stosownych przypadkach, informacje na temat inwestycji, zasobów i metod kluczowego zewnętrznego dostawcy usług ICT w zakresie szkolenia pracowników w dziedzinie przetwarzania wrażliwych danych finansowych i utrzymania wysokiego poziomu bezpieczeństwa;

x) informacje na temat działalności kluczowego zewnętrznego dostawcy usług ICT oraz sprawozdania finansowe, w tym informacje na temat budżetu i zasobów związanych z ICT i bezpieczeństwem.

Artykuł 3

Informacje przekazywane przez kluczowych zewnętrznych dostawców usług ICT po wydaniu zaleceń

1. Kluczowy zewnętrzny dostawca usług ICT przekazuje wiodącemu organowi nadzorczemu sprawozdanie zawierające plan naprawczy w odniesieniu do zaleceń oraz środki zaradcze, które kluczowy zewnętrzny dostawca usług ICT planuje wdrożyć w celu ograniczenia ryzyka zidentyfikowanego w zaleceniach, o których mowa w art. 35 ust. 1 lit. d) rozporządzenia (UE) 2022/2254. Sprawozdanie to musi być zgodne z harmonogramem określonym przez wiodący organ nadzorczy dla każdego zalecenia.

2. Aby umożliwić monitorowanie realizacji działań podjętych przez kluczowego zewnętrznego dostawcę usług ICT lub środków zaradczych wdrożonych przez niego w związku z otrzymanymi zaleceniami, kluczowy zewnętrzny dostawca usług ICT przedstawia wiodącemu organowi nadzorczemu na jego żądanie:

a) sprawozdania śródokresowe i powiązane dokumenty uzupełniające określające postępy we wdrażaniu działań i środków określonych w sprawozdaniu przekazanym wiodącemu organowi nadzorczemu przez kluczowego zewnętrznego dostawcę usług ICT w terminie określonym przez wiodący organ nadzorczy;

b) sprawozdania końcowe i powiązane dokumenty uzupełniające określające działania podjęte przez kluczowego zewnętrznego dostawcę usług ICT lub środki zaradcze wdrożone przez niego w celu ograniczenia ryzyka zidentyfikowanego w otrzymanych zaleceniach.

Artykuł 4

Struktura i format informacji przekazywanych przez kluczowych zewnętrznych dostawców usług ICT

1. Kluczowy zewnętrzny dostawca usług ICT przekazuje żądane informacje wiodącemu organowi nadzorczemu za pośrednictwem specjalnych bezpiecznych kanałów elektronicznych wskazanych przez wiodący organ nadzorczy w jego wniosku oraz w formie określonej przez wiodący organ nadzorczy.

2. Przekazując informacje wiodącemu organowi nadzorczemu, kluczowi zewnętrzni dostawcy usług ICT:

a) zachowują strukturę wskazaną przez wiodący organ nadzorczy w jego wniosku o udzielenie informacji;

b) wyraźnie wskazują odpowiednią informację w przedłożonej dokumentacji.

3. Informacje przedkładane, ujawniane lub zgłaszane wiodącemu organowi nadzorczemu przez kluczowego zewnętrznego dostawcę usług ICT muszą być sporządzone w języku zwyczajowo używanym w sferze finansów międzynarodowych.

Artykuł 5

Wzór do celów przekazywania informacji na temat umów dalszego podwykonawstwa

Kluczowy zewnętrzny dostawca usług ICT, który jest zobowiązany do przekazywania informacji na temat umów dalszego podwykonawstwa, przekazuje te informacje wiodącemu organowi nadzorczemu zgodnie ze wzorem określonym w załączniku.

Artykuł 6

Przeprowadzana przez właściwe organy ocena ryzyka zidentyfikowanego w zaleceniach wiodącego organu nadzorczego

1. W ramach nadzoru nad podmiotami finansowymi właściwy organ ocenia wpływ na podmioty finansowe środków zastosowanych przez kluczowego zewnętrznego dostawcę usług ICT na podstawie zaleceń wiodącego organu nadzorczego zgodnie z zasadą proporcjonalności.

2. Przeprowadzając ocenę, o której mowa w ust. 1, właściwy organ bierze pod uwagę wszystkie następujące elementy:

a) adekwatność i spójność środków naprawczych i zaradczych wdrożonych przez podmioty finansowe w celu ograniczenia ryzyka zidentyfikowanego w zaleceniach;

b) przeprowadzoną przez wiodący organ nadzorczy ocenę zastosowania przez kluczowego zewnętrznego dostawcę usług ICT środków i działań zawartych w sprawozdaniu, jeżeli wpływa to na narażenie podmiotów finansowych podlegających jego kompetencjom na ryzyko zidentyfikowane w zaleceniach;

c) opinię wszelkich innych właściwych organów, z którymi skonsultowano się zgodnie z art. 42 ust. 5 rozporządzenia (UE) 2022/2554;

d) czy wiodący organ nadzorczy uznał działania i środki zaradcze wdrożone przez kluczowego zewnętrznego dostawcę usług ICT za odpowiednie do ograniczenia narażenia podmiotów finansowych podlegających jego kompetencjom na ryzyko zidentyfikowane w zaleceniach.

3. Na wniosek wiodącego organu nadzorczego właściwy organ przedstawia w rozsądnym terminie wyniki oceny, o której mowa w ust. 1. Zwracając się o wyniki tej oceny, wiodący organ nadzorczy bierze pod uwagę zasadę proporcjonalności i skalę ryzyka związanego z zaleceniami, w tym transgraniczne skutki tego ryzyka, w przypadku gdy dotyczą one podmiotów finansowych działających w więcej niż jednym państwie członkowskim.

4. W stosownych przypadkach właściwy organ zwraca się do podmiotów finansowych o przekazanie wszelkich informacji niezbędnych do przeprowadzenia oceny, o której mowa w ust. 1.

Artykuł 7

Wejście w życie

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

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

Sporządzono w Brukseli dnia 24 października 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Wzór do celów przekazywania informacji na temat umów dalszego podwykonawstwa

Rodzaj informacji	Główne elementy informacji
Informacje ogólne	— Nazwa kluczowego zewnętrznego dostawcy usług ICT. — Kod identyfikacyjny kluczowego zewnętrznego dostawcy usług ICT. — Imię i nazwisko osoby wyznaczonej do kontaktów oraz dane kontaktowe kluczowego zewnętrznego dostawcy usług ICT. — Data przedłożenia wzoru.
Przegląd umów dalszego podwykonawstwa	— Wskazanie umów dalszego podwykonawstwa, w tym krótki opis celu i zakresu stosunków podwykonawstwa (w tym wskazanie poziomu krytyczności lub istotności umów dalszego podwykonawstwa dla kluczowego zewnętrznego dostawcy usług ICT). — Określenie i opis rodzajów usług ICT zleconych podwykonawcom oraz ich znaczenie dla usług ICT świadczonych na rzecz podmiotów finansowych, zgodnie z wykonawczymi standardami technicznymi przyjętymi na podstawie art. 28 ust. 9 rozporządzenia (UE) 2022/2554. — Przy określaniu rodzajów usług ICT należy odnieść się do wykazu w załączniku IV do wykonawczych standardów technicznych przyjętych na podstawie art. 28 ust. 9 rozporządzenia (UE) 2022/2554.
Informacje o podwykonawcach	— Nazwa i dane podmiotu prawnego (w tym kod identyfikacyjny) każdego podwykonawcy. — Dane kontaktowe pracowników odpowiedzialnych za poszczególne stosunki podwykonawstwa w ramach struktury zarządzania kluczowego zewnętrznego dostawcy usług ICT. — Przegląd wiedzy fachowej, doświadczenia i kwalifikacji związanych ze zleconymi usługami ICT w odniesieniu do każdego podwykonawcy.
Opis usług świadczonych przez podwykonawców	— Szczegółowy opis konkretnych usług ICT świadczonych przez poszczególnych podwykonawców. — Podział obowiązków i zadań przydzielonych podwykonawcom przez wyszczególnienie różnych ról na poszczególnych etapach procesów ICT. — Informacje na temat poziomu dostępu podwykonawców do danych osobowych lub innych danych wrażliwych lub systemów związanych z usługami ICT świadczonymi na rzecz podmiotów finansowych. — Informacje na temat obiektów, z których świadczone są usługi podwykonawców, oraz na temat środków zastosowanych w celu przeciwdziałania ryzyku wynikającemu z usług świadczonych poza Unią.
Zarządzanie podwykonawstwem i nadzór nad podwykonawstwem	— Opis istniejących ram umownych i ram zarządzania wykorzystywanych do zarządzania stosunkami podwykonawstwa, w tym klauzule ograniczające wykorzystanie danych wrażliwych. — Wyjaśnienie procesów wyboru, zatrudniania i monitorowania podwykonawców. — Przegląd mierników skuteczności działania, celów i umów dotyczących gwarantowanego poziomu usług oraz kluczowych wskaźników skuteczności działania wykorzystywanych do oceny monitorowania wyników i niezawodności podwykonawcy.
Zarządzanie ryzykiem i zgodność z przepisami	— Ocena profili ryzyka podwykonawcy i potencjalnego wpływu na usługi ICT świadczone na rzecz podmiotów finansowych. — Objaśnienie środków ograniczających ryzyko wdrożonych w celu przeciwdziałania ryzyku związanemu z podwykonawstwem. — Szczegółowe informacje na temat przestrzegania przez podwykonawcę odpowiednich przepisów, w tym przepisów dotyczących ochrony danych i norm branżowych.

Rodzaj informacji	Główne elementy informacji
Ciągłość działania i planowanie awaryjne	— Przegląd planów ciągłości działania oraz planów reagowania i przywracania sprawności posiadanych przez podwykonawcę. — Opis rozwiązań wprowadzonych w celu zapewnienia ciągłości usług w przypadku zakłóceń lub rozwiązania umowy przez podwykonawcę. — Częstotliwość testów planów ciągłości działania oraz planów reagowania i przywracania sprawności przeprowadzanych przez podwykonawców, daty ostatnich testów w ciągu ostatnich trzech lat oraz wskazanie, czy kluczowy zewnętrzny dostawca usług ICT uczestniczył w tych testach.
Sprawozdawczość	— Opis mechanizmów sprawozdawczych i częstotliwości przekazywania informacji między kluczowym zewnętrznym dostawcą usług ICT a jego podwykonawcami.
Środki zaradcze i zarządzanie incydentami	— Zarys procedur reagowania na incydenty, naruszenia lub nieprzestrzeganie przepisów ze strony podwykonawców.
Certyfikaty i audyty	— Informacje na temat wszelkich certyfikatów oraz niezależnych audytów lub ocen przeprowadzonych w odniesieniu do podwykonawców w celu zatwierdzenia ich kontroli bezpieczeństwa, standardów jakości lub zgodności regulacyjnej. — Data i częstotliwość audytów podwykonawców przeprowadzanych przez kluczowego zewnętrznego dostawcę usług ICT.