ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2024/1773

z dnia 13 marca 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych doprecyzowujących szczegółową treść polityki w zakresie ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT

(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. 28 ust. 10 akapit trzeci,

a także mając na uwadze, co następuje:

(1) Ramy dotyczące operacyjnej odporności cyfrowej sektora finansowego ustanowione rozporządzeniem (UE) 2022/2554 zawierają wymóg, aby podmioty finansowe określiły pewne najważniejsze zasady zarządzania ryzykiem ze strony zewnętrznych dostawców usług ICT, które mają szczególne znaczenie, gdy podmioty finansowe współpracują z zewnętrznymi dostawcami usług ICT w celu wspierania swoich krytycznych lub istotnych funkcji.

(2) W kontekście swoich ram zarządzania ryzykiem związanym z ICT podmioty finansowe muszą przyjąć strategię dotyczącą ryzyka ze strony zewnętrznych dostawców usług ICT oraz regularnie dokonywać jej przeglądu. Zgodnie z art. 28 ust. 2 rozporządzenia (UE) 2022/2554 strategia ta ma obejmować politykę korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT. Ma ona być stosowana na zasadzie indywidualnej oraz, w stosownych przypadkach, na zasadzie subskonsolidowanej i skonsolidowanej.

(3) Podmioty finansowe różnią się znacznie pod względem wielkości, struktury i organizacji wewnętrznej oraz charakteru i stopnia złożoności realizowanych przez nie działań i operacji. Należy uwzględnić tę różnorodność przy nakładaniu pewnych podstawowych wymogów regulacyjnych, które byłyby odpowiednie dla wszystkich podmiotów finansowych przy opracowywaniu polityki w zakresie ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT („polityka”) oraz zapewnić, aby wymogi te były stosowane w sposób proporcjonalny.

(4) W przypadku gdy podmioty finansowe należą do grupy, jednostka dominująca odpowiedzialna za sporządzanie skonsolidowanego lub subskonsolidowanego sprawozdania finansowego grupy powinna zatem zapewnić konsekwentne i spójne stosowanie tej polityki w ramach grupy.

(5) Stosując tę politykę, dostawców usług ICT wewnątrz grupy, w tym dostawców będących w całości lub zbiorowo własnością podmiotów finansowych w ramach tego samego systemu ochrony instytucjonalnej, należy uznać za zewnętrznych dostawców usług ICT. Ryzyko stwarzane przez dostawców usług ICT wewnątrz grupy może być różne, ale wymogi mające do nich zastosowanie są takie same na podstawie rozporządzenia (UE) 2022/2554. Podobnie polityka ta powinna mieć zastosowanie do podwykonawców, którzy świadczą usługi ICT wspierające krytyczne lub istotne funkcje lub ich istotne części na rzecz zewnętrznych dostawców usług ICT, w przypadku gdy istnieje łańcuch zewnętrznych dostawców usług ICT.

(6) Ostateczna odpowiedzialność organu zarządzającego za zarządzanie w zakresie ryzyka związanego z ICT podmiotu finansowego stanowi nadrzędną zasadę, którą stosuje się również w odniesieniu do korzystania z usług zewnętrznych dostawców usług ICT. Odpowiedzialność ta powinna dodatkowo przekładać się na ciągłe zaangażowanie organu zarządzającego w kontrolę i monitorowanie zarządzania w zakresie ryzyka związanego z ICT, jak również w przyjęcie polityki i dokonywanie jej przeglądu co najmniej raz do roku.

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

(7) Aby zapewnić odpowiednie przekazywanie informacji organowi zarządzającemu, w polityce należy jasno wskazać i określić wewnętrzne obowiązki w zakresie zatwierdzania ustaleń umownych dotyczących korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT („ustalenia umowne"), w tym usług ICT świadczonych na podstawie ustaleń umownych, o których mowa w art. 28 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, a także w zakresie zarządzania tymi ustaleniami, ich kontroli i prowadzenia dokumentacji w tym zakresie.

(8) Aby uwzględnić wszystkie możliwe rodzaje ryzyka, które mogą pojawić się przy zawieraniu umów o świadczenie usług ICT wspierających krytyczną lub istotną funkcję, struktura polityki powinna być zgodna ze wszystkimi etapami każdego głównego etapu cyklu życia ustaleń umownych z dostawcami zewnętrznymi.

(9) Aby ograniczyć zidentyfikowane ryzyko, w polityce należy określić planowanie ustaleń umownych, w tym ocenę ryzyka, należytą staranność oraz proces zatwierdzania nowych lub istotnych zmian w tych ustaleniach umownych. W celu zarządzania ryzykiem, które może pojawić się przed zawarciem ustaleń umownych z zewnętrznym dostawcą usług ICT, w polityce należy określić odpowiedni i proporcjonalny proces wyboru i oceny odpowiedniości potencjalnych zewnętrznych dostawców usług ICT oraz zawrzeć wymóg, aby podmiot finansowy uwzględniał niewyczerpujący wykaz elementów, które powinni posiadać zewnętrzni dostawcy usług ICT. Wykaz powinien zawierać elementy związane z reputacją biznesową usługodawców, ich zasobami finansowymi, ludzkimi i technicznymi, bezpieczeństwem informacji, ich strukturą organizacyjną, w tym zarządzaniem ryzykiem, oraz ich kontrolami wewnętrznymi.

(10) Aby zapewnić należyte zarządzanie ryzykiem przy świadczeniu usług ICT wspierających krytyczne lub istotne funkcje przez zewnętrznych dostawców usług ICT, polityka powinna zawierać informacje na temat wdrażania i monitorowania ustaleń umownych oraz zarządzania nimi, w tym, w stosownych przypadkach, na poziomie skonsolidowanym i subskonsolidowanym. Obejmuje to wymogi w zakresie klauzul umownych dotyczących wzajemnych zobowiązań podmiotów finansowych i zewnętrznych dostawców usług ICT, które należy określić na piśmie. Aby zapewnić skuteczny nadzór i zwiększyć odporność w przypadku zmian w modelu biznesowym lub otoczeniu działalności gospodarczej, polityka powinna zapewniać prawa podmiotów finansowych lub wyznaczonych osób trzecich i właściwych organów do kontroli i dostępu do informacji, a także powinna dokładniej określać strategie wyjścia i procesy wypowiedzenia.

(11) W zakresie, w jakim dane osobowe są przetwarzane przez zewnętrznych dostawców usług ICT, polityka ta i wszelkie ustalenia umowne pozostają bez uszczerbku dla obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]), takich jak zawarcie pisemnej umowy opisującej przetwarzanie danych osobowych, wymogu zapewnienia bezpieczeństwa przetwarzania danych osobowych oraz określenia wszystkich innych elementów wymaganych na mocy tego rozporządzenia, a także powinny je uzupełniać.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) Wspólny Komitet Europejskich Urzędów Nadzoru, o którym mowa w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 ([3]), w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1094/2010 ([4]) i w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([5]), 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 (UE) nr 1093/2010, do Grupy Interesariuszy z Sektora Ubezpieczeń i Reasekuracji i Grupy Interesariuszy z Sektora Pracowniczych Programów Emerytalnych powołanych zgodnie z art. 37 rozporządzenia (UE) nr 1094/2010 oraz do Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej zgodnie z art. 37 rozporządzenia (UE) nr 1095/2010.

(13) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który swoją opinię wydał 24 stycznia 2024 r.,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Ogólny profil ryzyka i stopień złożoności

Polityka w zakresie korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT („polityka") uwzględnia wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i elementy zwiększonego lub zmniejszonego stopnia złożoności realizowanych usług, działań i operacji, w tym elementy związane z:

a) rodzajem usług ICT objętych ustaleniem umownym dotyczącym korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczonych przez zewnętrznych dostawców usług ICT („ustalenie umowne") zawartym między podmiotem finansowym a zewnętrznym dostawcą usług ICT;

b) siedzibą zewnętrznego dostawcy usług ICT lub siedzibą jego spółki dominującej;

c) faktem, czy usługi ICT wspierające krytyczne lub istotne funkcje są świadczone przez zewnętrznego dostawcę usług ICT mającego siedzibę w państwie członkowskim czy w państwie trzecim, biorąc również pod uwagę miejsce, z którego świadczone są usługi ICT, oraz miejsce, w którym dane są przetwarzane i przechowywane;

d) charakterem danych udostępnianych zewnętrznemu dostawcy usług ICT;

e) informacją, czy zewnętrzny dostawca usług ICT należy do tej samej grupy co podmiot finansowy, na rzecz którego świadczone są usługi;

([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).

([6]) 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).

f) korzystaniem z zewnętrznych dostawców usług ICT, którzy uzyskali zezwolenie od właściwego organu w państwie członkowskim, zostali zarejestrowani przez ten organ lub podlegają nadzorowi lub kontroli tego organu, lub podlegają ramom nadzoru na podstawie rozdziału V sekcja II rozporządzenia (UE) 2022/2554, oraz korzystaniem z zewnętrznych dostawców usług ICT, których wymienione elementy nie dotyczą;

g) korzystaniem z zewnętrznych dostawców usług ICT, którzy uzyskali zezwolenie od organu nadzorczego w państwie trzecim, zostali zarejestrowani przez ten organ lub podlegają nadzorowi lub kontroli tego organu, oraz korzystaniem z zewnętrznych dostawców usług ICT, których wymienione elementy nie dotyczą;

h) informacją o tym, czy świadczenie usług ICT wspierających krytyczne lub istotne funkcje koncentruje się na pojedynczym zewnętrznym dostawcy usług ICT lub niewielkiej liczbie takich dostawców usług;

i) możliwością przeniesienia usług ICT wspierających krytyczne lub istotne funkcje do innego zewnętrznego dostawcy usług ICT, w tym ze względu na specyfikę technologii;

j) potencjalnym wpływem zakłóceń w świadczeniu usług ICT wspierających krytyczne lub istotne funkcje na ciągłość działań podmiotu finansowego oraz na dostępność jego usług.

Artykuł 2

Zastosowanie na poziomie grupy

W przypadku gdy niniejsze rozporządzenie ma zastosowanie na zasadzie subskonsolidowanej lub skonsolidowanej, jednostka dominująca odpowiedzialna za sporządzanie skonsolidowanych lub subskonsolidowanych sprawozdań finansowych grupy zapewnia spójne wdrażanie polityki we wszystkich podmiotach finansowych wchodzących w skład grupy i jest odpowiednia do skutecznego stosowania niniejszego rozporządzenia na wszystkich odpowiednich szczeblach grupy.

Artykuł 3

Rozwiązania w zakresie zarządzania

1. Organ zarządzający dokonuje przeglądu polityki co najmniej raz w roku i w razie potrzeby aktualizuje ją. Zmiany w polityce wprowadza się w odpowiednim czasie i tak szybko, jak jest to możliwe w ramach odpowiednich ustaleń umownych. Podmiot finansowy dokumentuje planowany harmonogram wdrażania.

2. W polityce ustanawia się metodykę określania, które usługi ICT wspierają krytyczne lub istotne funkcje, lub odnosi się do niej. W polityce określa się również, kiedy ocena ta ma zostać przeprowadzona i poddana przeglądowi.

3. W polityce wyraźnie określa się wewnętrzne obowiązki w zakresie zatwierdzania odpowiednich ustaleń umownych, a także zarządzania tymi ustaleniami, ich kontroli i prowadzenia dokumentacji w tym zakresie, oraz zapewnia się utrzymanie odpowiednich umiejętności, doświadczenia i wiedzy w ramach podmiotu finansowego w celu skutecznej kontroli przestrzegania odpowiednich ustaleń umownych, w tym usług ICT świadczonych na podstawie tych ustaleń.

4. Bez uszczerbku dla ostatecznej odpowiedzialności podmiotu finansowego za skuteczną kontrolę nad przestrzeganiem odpowiednich ustaleń umownych polityka musi zawierać wymóg, aby zewnętrzny dostawca usług ICT został poddany ocenie pozwalającej stwierdzić, że posiada on wystarczające zasoby w celu zapewnienia, aby podmiot finansowy spełniał wszystkie wymogi prawne i regulacyjne dotyczące świadczonych usług ICT wspierających krytyczne lub istotne funkcje.

5. W polityce wyraźnie określa się stanowisko lub członka kadry kierowniczej wyższego szczebla odpowiedzialnego za monitorowanie odpowiednich ustaleń umownych. W polityce określa się sposób, w jaki to stanowisko lub członek kadry kierowniczej wyższego szczebla współpracują z funkcjami kontroli, jeżeli nie są ich częścią, oraz określa się strukturę raportowania wobec organu zarządzającego, w tym charakter informacji, które należy przekazać, oraz dokumenty, które należy przedstawić. Określa się w niej również częstotliwość takiego raportowania.

6. Polityka zapewnia zgodność ustaleń umownych z:

a) ramami zarządzania ryzykiem związanym z ICT, o których mowa w art. 6 rozporządzenia (UE) 2022/2554;

b) polityką bezpieczeństwa informacji, o której mowa w art. 9 ust. 4 rozporządzenia (UE) 2022/2554;

c) strategią na rzecz ciągłości działania w zakresie ICT, o której mowa w art. 11 rozporządzenia (UE) 2022/2554;

d) wymogami dotyczącymi zgłaszania incydentów określonymi w art. 19 rozporządzenia (UE) 2022/2554.

7. Polityka zawiera wymóg, aby usługi ICT wspierające krytyczne lub istotne funkcje świadczone przez zewnętrznych dostawców usług ICT podlegały niezależnemu przeglądowi i były uwzględnione w planie audytu.

8. W polityce wyraźnie wskazuje się, że ustalenia umowne:

a) nie zwalniają podmiotu finansowego i jego organu zarządzającego z obowiązków regulacyjnych i obowiązków wobec klientów;

b) nie uniemożliwiają skutecznego nadzoru nad podmiotem finansowym i nie naruszają żadnych ograniczeń nadzorczych dotyczących usług i działań;

c) zobowiązują zewnętrznych dostawców usług ICT do współpracy z właściwymi organami;

d) zapewniają, aby podmiot finansowy, jego audytorzy i właściwe organy mieli skuteczny dostęp do danych i pomieszczeń związanych z korzystaniem z usług ICT wspierających krytyczne lub istotne funkcje.

Artykuł 4

Główne etapy cyklu życia w odniesieniu do przyjmowania i stosowania ustaleń umownych

W polityce określa się wymogi, w tym zasady, obowiązki i procesy, dla każdego głównego etapu cyklu życia ustaleń umownych, obejmujące co najmniej następujące elementy:

a) obowiązki organu zarządzającego, w tym, w stosownych przypadkach, jego udział w procesie decyzyjnym dotyczącym korzystania z usług ICT wspierających krytyczne lub istotne funkcje świadczone przez zewnętrznych dostawców usług ICT;

b) planowanie ustaleń umownych, w tym oceny ryzyka, należytej staranności określonej w art. 5 i 6 oraz procesu zatwierdzania nowych lub istotnych zmian w ustaleniach umownych określonych w art. 8 ust. 4;

c) zaangażowanie jednostek gospodarczych, kontroli wewnętrznej i innych odpowiednich jednostek w odniesieniu do ustaleń umownych;

d) wdrażanie i monitorowanie ustaleń umownych, o których mowa w art. 7, 8 i 9, w tym, w stosownych przypadkach, na poziomie skonsolidowanym i subskonsolidowanym, oraz zarządzanie tymi ustaleniami umownymi;

e) dokumentację i prowadzenie rejestrów, z uwzględnieniem wymogów dotyczących rejestru informacji określonych w art. 28 ust. 3 rozporządzenia (UE) 2022/2554;

f) strategie wyjścia i procesy wypowiedzenia określone w art. 10.

Artykuł 5

Ocena ryzyka *ex ante*

1. Polityka zawiera wymóg określenia potrzeb biznesowych podmiotu finansowego przed zawarciem ustalenia umownego.

2. Polityka zawiera wymóg, aby zawarcie ustalenia umownego było poprzedzone oceną ryzyka na poziomie podmiotu finansowego oraz, w stosownych przypadkach, na poziomie skonsolidowanym i subskonsolidowanym.

W ocenie ryzyka uwzględnia się wszystkie odpowiednie wymogi określone w rozporządzeniu (UE) 2022/2554 i mające zastosowanie sektorowe przepisy Unii. Uwzględnia ona w szczególności wpływ świadczenia usług ICT wspierających krytyczne lub istotne funkcje przez zewnętrznych dostawców usług ICT na podmiot finansowy oraz wszystkie rodzaje ryzyka stwarzane przez świadczenie tych usług ICT wspierających krytyczne lub istotne funkcje przez zewnętrznych dostawców usług ICT, w tym:

a) ryzyka operacyjne;

b) ryzyka prawne;

c) ryzyka związane z ICT;

d) ryzyka utraty reputacji;

e) ryzyka związane z ochroną danych poufnych lub osobowych;

f) ryzyka związane z dostępnością danych;

g) ryzyka związane z miejscem, w którym dane są przetwarzane i przechowywane;

h) ryzyka związane z siedzibą zewnętrznego dostawcy usług ICT;

i) ryzyka koncentracji w obszarze ICT na poziomie podmiotu.

Artykuł 6

Należyta staranność

1. W polityce określa się odpowiedni i proporcjonalny proces wyboru i oceny potencjalnych zewnętrznych dostawców usług ICT, biorąc pod uwagę, czy dany zewnętrzny dostawca usług ICT jest dostawcą usług ICT wewnątrz grupy, oraz zawiera się wymóg, aby podmiot finansowy przed zawarciem ustalenia umownego ocenił, czy zewnętrzny dostawca usług ICT:

a) cieszy się odpowiednią reputacją biznesową, posiada wystarczające umiejętności, wiedzę fachową i odpowiednie zasoby finansowe, ludzkie i techniczne, stosuje standardy bezpieczeństwa informacji, ma odpowiednią strukturą organizacyjną, mechanizmy zarządzania ryzykiem i kontroli wewnętrznych oraz, w stosownych przypadkach, posiada zezwolenia lub rejestracje wymagane do świadczenia usług ICT wspierających krytyczne lub istotne funkcje w sposób wiarygodny i profesjonalny;

b) jest w stanie monitorować istotne zmiany technologiczne i określić wiodące praktyki w zakresie bezpieczeństwa ICT oraz wdrażać je, w stosownych przypadkach, aby dysponować skutecznymi i solidnymi ramami operacyjnej odporności cyfrowej;

c) korzysta lub zamierza korzystać z podwykonawców usług ICT do świadczenia usług ICT wspierających krytyczne lub istotne funkcje lub ich istotne części;

d) ma siedzibę lub przetwarza lub przechowuje dane w państwie trzecim, a jeżeli tak, to czy praktyka ta wpływa na poziom ryzyka operacyjnego lub ryzyka utraty reputacji lub na ryzyko objęcia środkami ograniczającymi, w tym embargiem i sankcjami, które mogą mieć wpływ na zdolność zewnętrznego dostawcy usług ICT do świadczenia usług ICT lub podmiotu finansowego do korzystania z tych usług ICT;

e) wyraża zgodę na ustalenia umowne, które zapewniają realną możliwość przeprowadzania audytów u zewnętrznego dostawcy usług ICT, w tym na miejscu, przez sam podmiot finansowy, wyznaczone osoby trzecie i właściwe organy;

f) działa w sposób etyczny i społecznie odpowiedzialny, przestrzega praw człowieka i praw dziecka, w tym zakazu pracy dzieci, przestrzega obowiązujących zasad ochrony środowiska oraz zapewnia odpowiednie warunki pracy.

2. W polityce określa się wymagany poziom pewności w odniesieniu do skuteczności ram zarządzania ryzykiem zewnętrznych dostawców usług ICT w odniesieniu do usług ICT wspierających krytyczne lub istotne funkcje, które mają być świadczone przez zewnętrznego dostawcę usług ICT. W polityce tej wymaga się, aby proces należytej staranności obejmował ocenę istnienia środków ograniczania ryzyka i środków zapewniających ciągłość działania oraz sposobu zapewnienia ich funkcjonowania u zewnętrznego dostawcy usług ICT.

3. W polityce określa się procedurę należytej staranności przy wyborze i ocenie potencjalnych zewnętrznych dostawców usług ICT oraz wskazuje się, które z poniższych elementów mają być wykorzystane do osiągnięcia wymaganego poziomu pewności w odniesieniu do wyników osiąganych przez zewnętrznego dostawcę usług ICT:

a) audyty lub niezależne oceny przeprowadzane przez sam podmiot finansowy lub w jego imieniu;

b) korzystanie z niezależnych sprawozdań z audytu sporządzanych na wniosek zewnętrznego dostawcy usług ICT;

c) korzystanie ze sprawozdań z audytu sporządzanych przez funkcję audytu wewnętrznego zewnętrznego dostawcy usług ICT;

d) stosowanie odpowiednich certyfikatów wydanych przez osoby trzecie;

e) wykorzystanie innych istotnych informacji, do których ma dostęp podmiot finansowy, lub innych informacji dostarczonych przez zewnętrznego dostawcę usług ICT.

4. Podmioty finansowe gwarantują odpowiedni poziom pewności w odniesieniu do wyników osiąganych przez zewnętrznego dostawcę usług ICT, z uwzględnieniem elementów wymienionych w ust. 3 lit. a)–e). W stosownych przypadkach wykorzystuje się więcej niż jeden element wymieniony w tych punktach.

Artykuł 7

Konflikty interesów

1. W polityce określa się odpowiednie środki służące identyfikacji faktycznych lub potencjalnych konfliktów interesów wynikających z korzystania z usług zewnętrznych dostawców usług ICT, zapobieganiu tym konfliktom i zarządzaniu nimi, które należy wprowadzić przed zawarciem odpowiednich ustaleń umownych, oraz przewiduje się bieżące monitorowanie takich konfliktów interesów.

2. W przypadku gdy usługi ICT wspierające krytyczne lub istotne funkcje są świadczone przez dostawców usług ICT wewnątrz grupy, w polityce określa się, że decyzje dotyczące warunków, w tym warunków finansowych, świadczenia usług ICT mają być podejmowane obiektywnie.

Artykuł 8

Klauzule umowne

1. W polityce określa się, że odpowiednie ustalenie umowne ma mieć formę pisemną i obejmować wszystkie elementy, o których mowa w art. 30 ust. 2 i 3 rozporządzenia (UE) 2022/2554. Polityka obejmuje również elementy dotyczące wymogów, o których mowa w art. 1 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, a także, w stosownych przypadkach, w innych odpowiednich przepisach unijnych i krajowych.

2. W polityce określa się, że odpowiednie ustalenia umowne mają obejmować prawo podmiotu finansowego do dostępu do informacji, przeprowadzania inspekcji i audytów oraz do przeprowadzania testów w odniesieniu do ICT. W tym celu w polityce zobowiązuje się podmiot finansowy do stosowania następujących metod, bez uszczerbku dla ostatecznej odpowiedzialności podmiotu finansowego:

a) własnego audytu wewnętrznego lub audytu przeprowadzanego przez wyznaczoną osobę trzecią;

b) w stosownych przypadkach – audytów zbiorczych i zbiorczych testów ICT, w tym testów penetracyjnych pod kątem wyszukiwania zagrożeń, które są organizowane wspólnie z innymi zamawiającymi podmiotami finansowymi lub firmami korzystającymi z usług ICT tego samego zewnętrznego dostawcy usług ICT i które są przeprowadzane przez te zamawiające podmioty finansowe lub firmy lub przez wyznaczoną przez nie osobę trzecią;

c) w stosownych przypadkach – certyfikatów wydanych przez osoby trzecie;

d) w stosownych przypadkach – sprawozdań z audytu wewnętrznego lub sprawozdania z audytu prowadzonego przez osobę trzecią udostępnionych przez zewnętrznego dostawcę usług ICT.

3. Podmiot finansowy nie może po pewnym czasie opierać się wyłącznie na certyfikatach, o których mowa w ust. 2 lit. c), ani na sprawozdaniach z audytu, o których mowa w lit. d) tego ustępu. W ramach polityki dopuszcza się stosowanie metod, o których mowa w ust. 2 lit. c) i d), wyłącznie w przypadku, gdy podmiot finansowy:

a) jest zadowolony z planu audytu zewnętrznego dostawcy usług ICT w odniesieniu do odpowiednich ustaleń umownych;

b) zapewnia, aby zakres certyfikatów lub sprawozdań z audytu obejmował zidentyfikowane przez siebie systemy i kluczowe mechanizmy kontroli oraz zapewniał zgodność z odpowiednimi wymogami regulacyjnymi;

c) na bieżąco dokładnie ocenia treść certyfikatów lub sprawozdań z audytu i sprawdza, czy sprawozdania lub certyfikaty są aktualne;

d) zapewnia uwzględnienie kluczowych systemów i mechanizmów kontroli w przyszłych wersjach sprawozdania z certyfikacji lub audytu;

e) jest usatysfakcjonowany umiejętnościami podmiotu certyfikującego lub przeprowadzającego audyt;

f) stwierdza, że certyfikaty są wydawane, a audyty są przeprowadzane zgodnie z powszechnie uznanymi odpowiednimi normami zawodowymi i obejmują test skuteczności operacyjnej stosowanych kluczowych mechanizmów kontroli;

g) ma wynikające z umowy prawo do żądania – z częstotliwością rozsądną i uzasadnioną z punktu widzenia zarządzania ryzykiem, zmian zakresu certyfikatów lub sprawozdań z audytu – do innych odpowiednich systemów i mechanizmów kontroli;

h) ma wynikające z umowy prawo do przeprowadzania audytów indywidualnych i zbiorczych wedle własnego uznania w odniesieniu do ustaleń umownych oraz wykonywania tych praw zgodnie z uzgodnioną częstotliwością.

4. W ramach polityki zapewnia się, aby istotne zmiany w ustaleniu umownym były formalizowane w sporządzonym na piśmie dokumencie opatrzonym datą i podpisami przez wszystkie strony; określa się w niej również proces przedłużenia obowiązywania ustaleń umownych.

Artykuł 9

Monitorowanie ustaleń umownych

1. Polityka zawiera wymóg, aby w ustaleniach umownych określano środki i kluczowe wskaźniki służące bieżącemu monitorowaniu wyników zewnętrznych dostawców usług ICT, w tym środki monitorowania przestrzegania wymogów dotyczących poufności, dostępności, integralności i autentyczności danych i informacji oraz przestrzegania przez zewnętrznych dostawców usług ICT odpowiednich polityk i procedur podmiotu finansowego. W polityce określa się również środki mające zastosowanie w przypadku niewywiązania się z postanowień umów o gwarantowanym poziomie usług, w tym, w stosownych przypadkach, kary umowne.

2. W polityce wskazuje się, jak podmiot finansowy ma ocenić, czy zewnętrzni dostawcy usług ICT zaangażowani na potrzeby usług ICT wspierających krytyczne lub istotne funkcje spełniają odpowiednie standardy pod względem wyników i jakości zgodnie z ustaleniem umownym i własnymi politykami podmiotu finansowego. W ramach polityki w szczególności zapewnia się, aby:

a) zewnętrzni dostawcy usług ICT przekazywali podmiotowi finansowemu odpowiednie sprawozdania ze swoich działań i usług, w tym sprawozdania okresowe, zgłoszenia incydentów, sprawozdania dotyczące świadczenia usług, sprawozdania dotyczące bezpieczeństwa ICT oraz sprawozdania dotyczące środków na rzecz zapewnienia ciągłości działania i testów ciągłości działania;

b) ocenę wyników zewnętrznych dostawców usług ICT przeprowadzano za pomocą kluczowych wskaźników efektywności, kluczowych wskaźników kontroli, audytów, samocertyfikacji i niezależnych przeglądów zgodnie z ramami zarządzania ryzykiem związanym z ICT podmiotu finansowego;

c) podmiot finansowy otrzymywał inne istotne informacje od zewnętrznych dostawców usług ICT;

d) podmiot finansowy był powiadamiany, w stosownych przypadkach, o incydentach związanych z ICT oraz incydentach operacyjnych lub incydentach w zakresie bezpieczeństwa związanych z płatnościami;

e) przeprowadzano niezależne przeglądy i audyty sprawdzające zgodność z wymogami i strategiami prawnymi i regulacyjnymi.

3. W polityce wskazuje się, że ocenę, o której mowa w ust. 2, należy udokumentować, a jej wyniki należy wykorzystać do aktualizacji oceny ryzyka podmiotu finansowego, o której mowa w art. 6.

4. W polityce ustanawia się odpowiednie środki, które podmiot finansowy ma przyjąć w przypadku stwierdzenia niedociągnięć ze strony zewnętrznych dostawców usług ICT, w tym incydentów związanych z ICT oraz incydentów operacyjnych lub incydentów w zakresie bezpieczeństwa związanych z płatnościami, w świadczeniu usług ICT wspierających krytyczne lub istotne funkcje lub w zakresie zgodności z ustaleniami umownymi lub wymogami prawnymi. Określa się w niej również, w jaki sposób należy monitorować wdrażanie takich środków w celu zapewnienia ich skutecznego przestrzegania w określonych ramach czasowych, z uwzględnieniem istotności niedociągnięć.

Artykuł 10

Wycofanie się z ustaleń umownych i ich wypowiedzenie

Polityka musi zawierać wymogi dotyczące udokumentowanego planu wyjścia w odniesieniu do każdego ustalenia umownego oraz okresowego przeglądu i testowania udokumentowanego planu wyjścia. W procesie opracowywania planu wyjścia uwzględnia się następujące elementy:

a) nieprzewidziane i trwałe przerwy w świadczeniu usług;

b) świadczenie usług w sposób nieodpowiedni lub brak świadczenia usług;

c) niespodziewane wypowiedzenie ustalenia umownego.

Plan wyjścia musi być realistyczny, wykonalny, oparty na prawdopodobnych scenariuszach i rozsądnych założeniach oraz zawierać harmonogram wdrożenia zgodny z warunkami wycofania się i wypowiedzenia określonych w ustaleniach umownych.

Artykuł 11

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 13 marca 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN