Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/299

13.2.2025

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) 2025/299

z dnia 31 października 2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 w sprawie rynków kryptoaktywów w odniesieniu do regulacyjnych standardów technicznych dotyczących ciągłości i regularności świadczenia usług w zakresie kryptoaktywów

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 ([1]), w szczególności jego art. 68 ust. 10 akapit trzeci,

a także mając na uwadze, co następuje:

(1) W art. 11 i 12 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 ([2]) przewidziano wymogi dotyczące reagowania i przywracania sprawności, polityki i procedur tworzenia kopii zapasowych oraz metod i procedur przywracania i odzyskiwania danych dotyczących systemów ICT podmiotów finansowych, w tym dostawców usług w zakresie kryptoaktywów. W rozporządzeniu delegowanym Komisji (UE) 2024/1774 ([3]) doprecyzowano elementy polityki ciągłości działania w zakresie ICT, testowanie planów ciągłości działania w zakresie ICT oraz elementy planów reagowania i przywracania sprawności ICT podmiotów finansowych, w tym dostawców usług w zakresie kryptoaktywów. Niniejsze rozporządzenie uzupełnia wspomniane przepisy rozporządzenia (UE) 2022/2554 i rozporządzenia delegowanego (UE) 2024/1774 w odniesieniu do ciągłości i regularności świadczenia usług w zakresie kryptoaktywów.

(2) Dostawcy usług w zakresie kryptoaktywów mogą wykorzystywać do świadczenia usług rozproszony rejestr, nad którym nie sprawują kontroli, w tym otwarty rozproszony rejestr. W takim przypadku mogą oni nie być w stanie zapewnić regularności i ciągłości świadczenia usług, gdy zakłócenia są powodowane problemami wynikającymi z działania takich rozproszonych rejestrów. Aby ograniczyć zmienność rynku, która może mieć niekorzystny wpływ na klientów dotkniętych takimi zakłóceniami, dostawcy usług w zakresie kryptoaktywów powinni uwzględnić w swojej polityce ciągłości działania środki zapewniające terminowe przekazywanie informacji klientom i innym zewnętrznym zainteresowanym stronom. Tego rodzaju działania komunikacyjne powinny obejmować istotne i aktualne informacje dla klientów na temat takich zakłóceń, w tym bieżące aktualizacje statusu, aż do momentu usunięcia zakłócenia i wznowienia świadczenia usług. W przypadku gdy informacje na temat statusu otwartego rozproszonego rejestru odpowiedzialnego za zakłócenie świadczenia usług nie są łatwo dostępne dla dostawcy usług w zakresie kryptoaktywów, dostawca ten powinien przekazywać aktualizacje klientom i innym zainteresowanym stronom, w tym właściwym organom, przy dołożeniu wszelkich starań, aby zapewnić klientom i zainteresowanym stronom jak najbardziej wyczerpujące informacje na temat takich zakłóceń.

([1]) Dz.U. L 150 z 9.6.2023, s. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

([3]) Rozporządzenie delegowane Komisji (UE) 2024/1774 z dnia 13 marca 2024 r. uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT (Dz.U. L, 2024/1774, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1774/oj).

(3) Aby uniknąć nieproporcjonalnych obciążeń administracyjnych dla małych i średnich przedsiębiorstw oraz przedsiębiorstw typu start-up, dostawcy usług w zakresie kryptoaktywów powinni uwzględnić w swojej polityce ciągłości działania skalę, charakter i zakres świadczonych przez siebie usług. Oznacza to, że dostawcy usług w zakresie kryptoaktywów powinni określić specyficzne dla siebie wymagania w zakresie ciągłości działania na podstawie rzetelnej samooceny, opartej na szeregu kryteriów, które umożliwią im realizację polityki ciągłości działania współmiernej do wpływu ich usług na rynek. W samoocenie należy również uwzględnić inne okoliczności, które nie zostały wymienione w załączniku, a które mogą mieć wpływ na dostawcę usług w zakresie kryptoaktywów.

(4) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przedłożony Komisji przez Europejski Urząd Nadzoru Giełd i Papierów Wartościowych.

(5) Europejski Urząd Nadzoru Giełd i Papierów Wartościowych przeprowadził otwarte konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonał analizy potencjalnych powiązanych z nim kosztów i korzyści oraz zasięgnął opinii Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej na podstawie art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010 ([4]),

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

a) „krytyczna lub istotna funkcja” oznacza krytyczną lub istotną funkcję zdefiniowaną w art. 3 pkt 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554;

b) „otwarty rozproszony rejestr” oznacza szczególny rodzaj rozproszonego rejestru, w którym żaden podmiot nie sprawuje kontroli nad rozproszonym rejestrem, a węzły sieci DLT mogą zostać utworzone przez dowolną osobę spełniającą wymogi techniczne i protokoły tego rozproszonego rejestru.

Artykuł 2

Rozwiązania organizacyjne dotyczące ciągłości działania

1. Polityka ciągłości działania, o której mowa w art. 68 ust. 7 rozporządzenia (UE) 2023/1114, obejmuje plany, procedury i środki.

2. Wykonując funkcje, o których mowa w art. 68 ust. 6 rozporządzenia (UE) 2023/1114, organ zarządzający dostawców usług w zakresie kryptoaktywów ustanawia i zatwierdza plany, procedury i środki, które wchodzą w skład polityki ciągłości działania. Organ zarządzający dostawcy usług w zakresie kryptoaktywów jest odpowiedzialny za wdrażanie polityki ciągłości działania oraz za dokonywanie co najmniej raz w roku przeglądu jej skuteczności.

3. Dostawcy usług w zakresie kryptoaktywów zapewniają, aby o wszelkich zmianach w polityce ciągłości działania informowano wszystkich odpowiednich pracowników wewnętrznych za pośrednictwem skutecznych kanałów komunikacji.

([4]) 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).

Artykuł 3

Polityka ciągłości działania

1. Polityka ciągłości działania, o której mowa w art. 68 ust. 7 rozporządzenia (UE) 2023/1114, musi zapewniać, aby dostawcy usług w zakresie kryptoaktywów odpowiednio reagowali na incydenty zakłócające działanie lub problemy z wydajnością związane z systemami o krytycznym znaczeniu dla funkcjonowania ich funkcji biznesowych, oraz musi być zapisana na trwałym nośniku.

2. Dostawcy usług w zakresie kryptoaktywów uwzględniają w polityce ciągłości działania wszystkie następujące elementy:

a) określenie zakresu polityki ciągłości działania, który ma być objęty planami, procedurami i środkami ciągłości działania, w tym jej ograniczeń i wyłączeń;

b) opis kryteriów uruchomienia planów ciągłości działania, w tym procedur eskalacji do szczebla organu zarządzającego;

c) przepisy dotyczące struktury organizacyjnej dostawcy usług w zakresie kryptoaktywów i zasad zarządzania tym dostawcą, z uwzględnieniem ról i obowiązków personelu, zapewniające dostępność wystarczających zasobów do skutecznego wdrożenia polityki;

d) przepisy zapewniające spójność między planami ciągłości działania a planami ciągłości działania w zakresie ICT oraz planami reagowania i przywracania sprawności ICT, o których mowa w art. 24 i 26 rozporządzenia delegowanego (UE) 2024/1774.

Artykuł 4

Plany ciągłości działania

1. Wdrażając politykę ciągłości działania, o której mowa w art. 68 ust. 7 rozporządzenia (UE) 2023/1114, dostawcy usług w zakresie kryptoaktywów ustanawiają plany ciągłości działania. W planach ciągłości działania określa się procedury niezbędne do ochrony i, w razie potrzeby, przywrócenia:

a) poufności, integralności i dostępności danych klientów,

b) dostępności funkcji biznesowych, procesów wspierających i zasobów informacyjnych dostawców usług w zakresie kryptoaktywów.

2. Plany ciągłości działania zawierają następujące elementy:

a) szereg możliwych niekorzystnych scenariuszy dotyczących funkcjonowania krytycznych lub istotnych funkcji, w tym brak dostępności funkcji biznesowych, personelu, miejsca do pracy, dostawców zewnętrznych lub centrów danych bądź utratę lub zmianę krytycznych danych i dokumentów;

b) procedury i zasady postępowania w przypadku incydentu zakłócającego działanie, w tym:

   (i) środki niezbędne do przywrócenia krytycznych lub istotnych funkcji;

   (ii) terminy, w których te krytyczne lub istotne funkcje mają zostać przywrócone;

   (iii) akceptowalny poziom utraty danych;

   (iv) maksymalny czas na wznowienie świadczenia usług;

c) procedury i zasady regulujące przenoszenie funkcji biznesowych wykorzystywanych do świadczenia usług w zakresie kryptoaktywów do zapasowej lokalizacji;

d) tworzenie kopii zapasowych krytycznych danych biznesowych, w tym aktualne informacje o niezbędnych osobach wyznaczonych do kontaktu w celu zapewnienia komunikacji w ramach dostawcy usług w zakresie kryptoaktywów oraz między dostawcą usług w zakresie kryptoaktywów a jego klientami;

e) procedury terminowego przekazywania informacji klientom i innym zewnętrznym zainteresowanym stronom, w tym właściwym organom.

3. W przypadku zakłócenia związanego z otwartym rozproszonym rejestrem wykorzystywanym przez dostawcę usług w zakresie kryptoaktywów do świadczenia usług działania komunikacyjne, o których mowa w ust. 2 lit. e), obejmują następujące informacje:

a) kiedy spodziewane jest wznowienie świadczenia usług;

b) przyczyny i skutki incydentu zakłócającego działanie;

c) wszelkie ryzyko dotyczące środków pieniężnych klientów i kryptoaktywów przechowywanych w ich imieniu;

d) środki, które dostawca usług w zakresie kryptoaktywów zamierza wprowadzić w odpowiedzi na zakłócenie otwartego rozproszonego rejestru.

Jeżeli informacje te nie są łatwo dostępne dla dostawcy usług w zakresie kryptoaktywów, dostawca ten, dokładając wszelkich starań, przekazuje klientom i zainteresowanym stronom, w tym właściwym organom, aktualizacje dotyczące informacji, o których mowa w akapicie pierwszym.

4. Plan ciągłości działania zawiera procedury mające na celu wyeliminowanie wszelkie zakłócenia krytycznych lub istotnych funkcji zlecanych w drodze outsourcingu, również w przypadku, gdy te krytyczne lub istotne funkcje stały się niedostępne.

Artykuł 5

Okresowe testowanie planów ciągłości działania

1. Dostawcy usług w zakresie kryptoaktywów testują funkcjonowanie planów ciągłości działania, o których mowa w art. 4, w oparciu o realistyczne scenariusze. W ramach takich testów weryfikuje się zdolność dostawcy usług w zakresie kryptoaktywów do przywrócenia sprawności po incydentach zakłócających działanie oraz do wznowienia świadczenia usług zgodnie z art. 4 ust. 2 lit. b).

2. Dostawcy usług w zakresie kryptoaktywów testują plany ciągłości działania co roku, biorąc pod uwagę:

a) wyniki testów, o których mowa w ust. 1;

b) najnowsze analizy zagrożeń;

c) wnioski wyciągnięte z poprzednich incydentów;

d) w stosownych przypadkach – wszelkie zmiany celów związanych z przywracaniem sprawności, w tym zakładanego czasu przywrócenia systemów i akceptowalnego poziomu utraty danych, o których mowa w art. 4 ust. 2 lit. b);

e) zmiany w funkcjach biznesowych.

3. Dostawcy usług w zakresie kryptoaktywów dokumentują na piśmie wyniki testów i przedkładają je swojemu organowi zarządzającemu oraz jednostkom operacyjnym zaangażowanym w opracowanie planów ciągłości działania.

4. Dostawcy usług w zakresie kryptoaktywów zapewniają, aby testowanie planów ciągłości działania nie kolidowało z normalnym świadczeniem usług.

Artykuł 6

Kwestie złożoności i ryzyka

1. Ustanawiając politykę ciągłości działania, w tym plany, procedury i środki, dostawcy usług w zakresie kryptoaktywów uwzględniają elementy zwiększonej złożoności lub zwiększonego ryzyka, w tym:

a) rodzaj i zakres oferowanych usług w zakresie kryptoaktywów;

b) stopień, w jakim usługi świadczone przez dostawcę usług w zakresie kryptoaktywów opierają się na otwartym rozproszonym rejestrze;

c) potencjalny wpływ wszelkich zakłóceń na ciągłość działania dostawcy usług w zakresie kryptoaktywów i dostępność jego usług.

2. Do celów ust. 1 dostawcy usług w zakresie kryptoaktywów przeprowadzają co roku samoocenę w odniesieniu do skali, charakteru i zakresu świadczonych przez siebie usług. Dostawcy usług w zakresie kryptoaktywów opierają tę samoocenę na kryteriach określonych w załączniku i wszelkich innych kryteriach, które dostawca usług w zakresie kryptoaktywów uznaje za istotne.

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 31 października 2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

KRYTERIA SAMOOCENY DOSTAWCÓW USŁUG W ZAKRESIE KRYPTOAKTYWÓW

a) Charakter dostawcy usług w zakresie kryptoaktywów w oparciu o następujące elementy:

   (i) oznaczenie klasy, o którym mowa w załączniku IV do rozporządzenia (UE) 2023/1114;

   (ii) w stosownych przypadkach średnie poziomy płynności lub głębokość rynku kryptoaktywów dostępnych do obrotu na platformie obrotu kryptoaktywami;

   (iii) rola dostawcy usług w zakresie kryptoaktywów w systemie finansowym, w tym czy dostawca usług w zakresie kryptoaktywów prowadzi platformę obrotu kryptoaktywami oraz czy kryptoaktywa będące przedmiotem obrotu na jego platformie są przedmiotem obrotu na innych platformach obrotu kryptoaktywami.

b) Skala, ustalana poprzez ocenę wpływu dostawcy usług w zakresie kryptoaktywów na prawidłowe funkcjonowanie rynków na podstawie – w stosownych przypadkach – następujących elementów:

   (i) czy dostawca usług w zakresie kryptoaktywów kwalifikuje się jako znaczący w rozumieniu art. 85 rozporządzenia (UE) 2023/1114;

   (ii) liczba państw, w których dostawca usług w zakresie kryptoaktywów prowadzi działalność gospodarczą;

   (iii) liczba klientów;

   (iv) liczba aktywnych użytkowników;

   (v) wartość przechowywanych kryptoaktywów;

   (vi) wolumen transakcji na platformie obrotu kryptoaktywami;

   (vii) liczba transferów kryptoaktywów dokonanych w imieniu klientów;

   (viii) liczba zleceń wykonanych w imieniu klientów.

c) Złożoność, ustalana w stosownych przypadkach poprzez ocenę następujących elementów:

   (i) struktura dostawcy usług w zakresie kryptoaktywów pod względem własności i zarządzania oraz jego obecność organizacyjna, operacyjna, techniczna, fizyczna i geograficzna;

   (ii) poziom outsourcingu stosowanego przez dostawcę usług w zakresie kryptoaktywów, a w szczególności to, czy którekolwiek krytyczne lub istotne funkcje operacyjne zostały zlecone na zasadzie outsourcingu;

   (iii) liczba i rodzaj rozproszonych rejestrów wykorzystywanych do świadczenia usług;

   (iv) liczba węzłów sieci DLT, które dostawca usług w zakresie kryptoaktywów obsługuje w jednym rozproszonym rejestrze lub wielu rozproszonych rejestrach;

   (v) liczba i rodzaj inteligentnych umów wdrożonych i utrzymywanych przez dostawcę usług w zakresie kryptoaktywów;

   (vi) sposób, w jaki zabezpieczone są prywatne klucze kryptograficzne klientów lub inne sposoby dostępu do kryptoaktywów;

   (vii) korzystanie z programowych i sprzętowych portfeli powierniczych lub portfeli, które zabezpieczają klucze kryptograficzne przy użyciu wielu powierników.

Do celów lit. b) pkt (iii)–(viii) dostawca usług w zakresie kryptoaktywów wykorzystuje do samooceny średnią dzienną z rocznego okresu odniesienia.