

## Wytyczne zmieniające wytyczne EBA/GL/2021/02

---

na podstawie art. 17 i art. 18 ust. 4 dyrektywy (UE) 2015/849 dotyczących środków należytej staranności wobec klienta oraz czynników, które instytucje kredytowe i finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy i finansowania terroryzmu związanego z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznymi („wytyczne w sprawie czynników ryzyka prania pieniędzy i finansowania terroryzmu”)

# 1. Zgodność i obowiązki sprawozdawcze

---

## Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010<sup>1</sup>. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, by zastosować się do wytycznych.
2. W wytycznych określono stanowisko EUNB w sprawie odpowiednich praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego oraz w sprawie sposobu, w jaki należy stosować prawo Unii w danym obszarze. Właściwe organy określone w art. 4 pkt 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez odpowiednie włączenie ich do swoich praktyk (np. poprzez zmianę swoich ram prawnych lub procesów nadzorczych), również gdy wytyczne są skierowane przede wszystkim do instytucji.

## Wymogi sprawozdawcze

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą do dnia 28.08.2024 powiadomić EUNB, czy stosują się lub zamierzają zastosować się do niniejszych wytycznych, albo podać powody niestosowania się do nich. W razie braku powiadomienia w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Powiadomienia należy wysyłać poprzez złożenie formularza dostępnego na stronie internetowej EUNB z dopiskiem „EBA/GL/2024/01”. Powiadomienia powinny przekazywać osoby odpowiednio upoważnione do informowania o stosowaniu się do wytycznych w imieniu właściwych organów. Do EUNB należy także zgłaszać wszelkie zmiany dotyczące stosowania się do wytycznych.
4. Zgodnie z art. 16 ust. 3 powiadomienia publikuje się na stronie internetowej EUNB.

---

<sup>1</sup> 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).

## 2. Przedmiot, zakres stosowania i definicje

---

### Adresaci

5. Niniejsze wytyczne są skierowane do instytucji kredytowych i instytucji finansowych określonych w art. 3 pkt 1 i 2 dyrektywy (UE) 2015/849<sup>2</sup> oraz do właściwych organów określonych w art. 4 pkt 2 ppkt (iii) rozporządzenia (UE) nr 1093/2010.

---

<sup>2</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (Dz.U. L 141 z 5.6.2015, s. 73).

## 3. Wdrożenie

---

### Data rozpoczęcia stosowania

6. Niniejsze wytyczne mają zastosowanie od dnia 30 grudnia 2024 r.

## 4. Zmiany

---

### **(i) Zmiana tytułu wytycznych**

7. Tytuł wytycznych otrzymuje brzmienie:

„Wytyczne EBA/2021/02 na podstawie dyrektywy (UE) 2015/849 dotyczące środków należytej staranności wobec klienta oraz czynników, które instytucje kredytowe i finansowe powinny uwzględnić podczas oceny ryzyka prania pieniędzy i finansowania terroryzmu związanego z indywidualnymi stosunkami gospodarczymi i transakcjami sporadycznymi («wytyczne w sprawie czynników ryzyka prania pieniędzy i finansowania terroryzmu»).

### **(ii) Zmiany przedmiotu, zakresu stosowania i definicji**

8. W pkt 12 formuła wprowadzająca otrzymuje brzmienie:

„O ile nie określono inaczej, terminy stosowane i zdefiniowane w dyrektywie (UE) 2015/849 i rozporządzeniu (UE) 2023/1113 mają takie samo znaczenie w niniejszych wytycznych. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:”.

9. W pkt 12 skreśla się lit. f) i m).

### **(iii) Zmiany w wytycznej 1: Oceny ryzyka: kluczowe zasady dla wszystkich instytucji**

10. W wytycznej 1.7 dodaje się następującą literę:

„d) w przypadku gdy instytucja wprowadza nowe produkty, usługi lub praktyki gospodarcze lub znacząco je zmienia, w tym w przypadku gdy wprowadza nowy kanał dostawy, lub przyjmuje innowacyjną technologię w ramach swoich systemów i ram kontroli w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, przed wprowadzeniem tych produktów, usług lub praktyk gospodarczych powinna ona ocenić ekspozycję na ryzyko prania pieniędzy i finansowania terroryzmu. W przypadku gdy te produkty, usługi lub praktyki gospodarcze mają znaczący wpływ na ekspozycję instytucji na ryzyko prania pieniędzy i finansowania terroryzmu, instytucja powinna odzwierciedlić tę ocenę w swojej ogólnej ocenie ryzyka przeprowadzonej zgodnie z art. 8 ust. 2 dyrektywy (UE) 2015/849 oraz swoich politykach i procedurach.”.

### **(iv) Zmiany w wytycznej 2: Określenie czynników ryzyka prania pieniędzy i finansowania terroryzmu**

11. Wytyczna 2.4 lit. b) otrzymuje brzmienie:

„b) czy klient lub beneficjent rzeczywisty mają powiązania z sektorami, które są kojarzone z wyższym ryzykiem prania pieniędzy i finansowania terroryzmu, np. niektórymi przedsiębiorstwami świadczącymi usługi pieniężne, dostawcami usług w zakresie

kryptoaktywów opisanymi w wytycznych 9.20 i 9.21, kasynami lub sprzedawcami metali szlachetnych?”.

#### **(v) Zmiany w wytycznej 4: Środki należytej staranności wobec klienta, które mają być stosowane przez wszystkie instytucje**

12. W wytycznej 4.29 formuła wprowadzająca otrzymuje brzmienie:

„4.29 Aby wywiązać się ze swoich obowiązków wynikających z art. 13 ust. 1 dyrektywy (UE) 2015/849, w przypadku gdy stosunki gospodarcze są inicjowane, nawiązywane lub prowadzone w sytuacjach niebezpośrednich lub transakcja sporadyczna jest przeprowadzana w sytuacjach niebezpośrednich zgodnie z wytycznymi EUNB (EBA/GL/2022/15) dotyczącymi wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849, instytucje powinny:”.

13. Wytyczna 4.35 otrzymuje brzmienie:

„4.35 Jeżeli dostawca zewnętrzny jest instytucją mającą siedzibę w państwie niebędącym członkiem UE, instytucja powinna zagwarantować, że rozumie związane z tym ryzyko prawne i operacyjne oraz wymogi w zakresie ochrony danych, a także skutecznie ogranicza to ryzyko. Instytucja powinna również zapewnić sobie możliwość szybkiego dostępu do odpowiednich danych i informacji dotyczących klientów w razie potrzeby, w tym w przypadku rozwiązania umowy outsourcingu.”.

14. Wytyczna 4.60 lit. a) otrzymuje brzmienie:

„a) różnią się od transakcji, których instytucja mogłaby normalnie oczekiwać na podstawie swojej wiedzy o kliencie, stosunkach gospodarczych lub kategorii, do której klient należy, pod względem kwoty, częstotliwości, złożoności lub podobnych czynników, w tym w przypadku gdy transakcje opiewają na większe kwoty lub są częstsze niż zazwyczaj lub w przypadku transakcji opiewających na niewielkie kwoty, które są przeprowadzane nietypowo często, lub w przypadku kolejnych transakcji, które nie mają oczywistego ekonomicznego uzasadnienia, takich jak transakcje, które są dzielone w celu obejścia limitów związanych ze sprawozdawczością lub dostosowania transakcji nietypowych do normalnie oczekiwanego zachowania i schematów działania, jak wynika z informacji zgromadzonych w trakcie procedury nawiązywania relacji oraz w ramach bieżącego monitorowania stosunków gospodarczych.”.

15. Wytyczna 4.61 lit. a) otrzymuje brzmienie:

„a) podjęcie racjonalnych i odpowiednich środków w celu zrozumienia podstaw i celu tych transakcji, na przykład przez ustalenie źródła i przeznaczenia tych środków pieniężnych lub kryptoaktywów lub pozyskanie dodatkowych informacji na temat działalności klienta, aby uzyskać pewność co do prawdopodobieństwa przeprowadzenia takich transakcji przez klienta; oraz”.

16. Wytyczna 4.74 lit. b) otrzymuje brzmienie:

„b) czy będą monitorowały transakcje ręcznie, czy przy użyciu zautomatyzowanego systemu monitorowania transakcji. Instytucje, które przetwarzają dużą liczbę transakcji lub transakcje przeprowadzane z dużą częstotliwością, powinny rozważyć wprowadzenie zautomatyzowanego systemu monitorowania transakcji;”.

17. W wytycznej 4.74 dodaje się następującą literę:

„d) czy stosowanie zaawansowanych narzędzi analitycznych, takich jak rozproszony rejestr lub narzędzia do analizy łańcucha bloków, jest konieczne w świetle ryzyka prania pieniędzy lub finansowania terroryzmu, które jest związane z działalnością instytucji oraz z indywidualnymi transakcjami klientów instytucji.”.

### **(vi) Zmiany w wytycznej 6: Szkolenia**

18. Wytyczna 6.2 lit. c) otrzymuje brzmienie:

„c) jak rozpoznawać podejrzaną lub nietypową transakcję i działania, biorąc pod uwagę szczególny charakter ich produktów i usług, oraz jak postępować w takich sytuacjach;”.

19. W wytycznej 6.2 dodaje się następującą literę:

„d) jak korzystać z systemów zautomatyzowanych, w tym zaawansowanych narzędzi analitycznych, w celu monitorowania transakcji i stosunków gospodarczych oraz jak interpretować wyniki z tych systemów i narzędzi.”.

### **(vii) Zmiany w wytycznej 8: Wytyczna sektorowa dla relacji korespondenckich**

20. Wytyczna 8.6 lit. d) otrzymuje brzmienie:

„d) respondent prowadzi szeroko zakrojoną działalność z sektorami, które są powiązane z podwyższonymi poziomami ryzyka prania pieniędzy i finansowania terroryzmu. Na przykład respondent prowadzi:

- i. na szeroką skalę działalność z zakresu świadczenia usług przekazu pieniężnego;
- ii. działalność w imieniu niektórych podmiotów świadczących usługi przekazu pieniężnego lub kantorów wymiany walut;
- iii. działalność w imieniu dostawców usług w zakresie kryptoaktywów – innych niż dostawcy takich usług podlegający regulacji na podstawie rozporządzenia (UE) 2023/1114<sup>3</sup> – których obowiązuje system regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu mniej surowy niż system przewidziany w dyrektywie (UE) 2015/849 lub którzy nie podlegają żadnym

---

<sup>3</sup> Rozporządzenie (UE) 2023/1114 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.

obowiązkom w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, lub działalność z takimi dostawcami;

- iv. na szeroką skalę działalność w imieniu dostawców usług w zakresie kryptoaktywów, w przypadku których model biznesowy koncentruje się na dostarczaniu produktów i usług opisanych w wytycznej 21.3 lit. d);
- v. działalność z osobami niebędącymi rezydentami; lub
- vi. działalność w walucie innej niż waluta kraju, w którym ma siedzibę.”.

21. W wytycznej 8.6 dodaje się następującą literę:

„h) rachunek IBAN wskazany przez dostawcę usług w zakresie kryptoaktywów będącego respondentem, na który to rachunek wpływają środki od klientów w walucie urzędowej<sup>4</sup>, jest prowadzony w imieniu i na rzecz przedsiębiorstwa, które nie jest przedsiębiorstwem dostawcy usług w zakresie kryptoaktywów będącego respondentem ani nie jest w żaden sposób znane jako powiązane z tym dostawcą.”.

22. W wytycznej 8.8 dodaje się następującą literę:

„d) respondent nie jest w stanie zweryfikować z wystarczającym stopniem pewności, czy jego klienci nie mają siedziby w jurysdykcjach określonych w wytycznej 8.8 lit. a), w tym poprzez weryfikację adresów protokołu internetowego (IP) jego klientów lub w inny sposób, w okolicznościach, w których jest to wymagane przez politykę i procedury respondenta.”.

23. W wytycznej 8.17 lit. a) i c) otrzymują brzmienie:

„a) zgromadzenie dostatecznych informacji na temat instytucji będącej respondentem, aby w pełni zrozumieć charakter działalności respondenta w celu ustalenia zakresu, w jakim działalność respondenta naraża korespondenta na podwyższone ryzyko prania pieniędzy. Działania te powinny obejmować podjęcie kroków w celu zrozumienia charakteru bazy klientów respondenta – w razie potrzeby poprzez wypytanie respondenta o jego klientów – i rodzaju działalności, jaką respondent będzie prowadził za pośrednictwem rachunku korespondenta, lub, w stosownych przypadkach, rodzaju kryptoaktywów, które będą przedmiotem transakcji prowadzonych za pośrednictwem rachunku korespondenta przez dostawcę usług w zakresie kryptoaktywów będącego respondentem, a także w celu oceny tych elementów pod kątem ryzyka;”;

„c) dostęp do kontroli w zakresie przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu w instytucji będącej respondentem. Oznacza to, że korespondent powinien przeprowadzić ocenę jakościową ram kontroli respondenta w zakresie przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu, a nie tylko uzyskać egzemplarz strategii i procedur respondenta w zakresie przeciwdziałania praniu pieniędzy. Ocena ta powinna obejmować stosowane narzędzia monitorowania transakcji w celu zapewnienia, aby narzędzia te były odpowiednie dla rodzaju działalności prowadzonej przez respondenta. Ocenę taką należy

---

<sup>4</sup> W art. 3 pkt 8 rozporządzenia (UE) 2023/1114 walutę urzędową definiuje się jako walutę urzędową państwa, która jest wyemitowana przez bank centralny lub inny organ kształtujący politykę pieniężną.



odpowiednio udokumentować. Zgodnie z podejściem opartym na analizie ryzyka, jeżeli ryzyko jest szczególnie wysokie, a zwłaszcza jeżeli wielkość transakcji w ramach bankowości korespondenckiej jest znaczna, korespondent powinien rozważyć wizyty na miejscu lub badanie próby w celu zyskania pewności co do skutecznego wdrażania strategii i procedur respondenta w zakresie przeciwdziałania praniu pieniędzy;”.

## **(viii) Zmiany w wytycznej 9: Wytyczna sektorowa dla banków detalicznych**

24. Wytyczna 9.3 otrzymuje brzmienie:

„9.3. Banki powinny uwzględnić następujące środki i czynniki ryzyka wraz z tymi, o których mowa w tytule I niniejszych wytycznych. Banki, które świadczą usługi zarządzania majątkiem, powinny się także odnosić do wytycznej sektorowej 12, banki, które świadczą usługi inicjowania płatności lub usługi dostępu do informacji o rachunku, powinny się również odnosić do wytycznej sektorowej 18, a banki, które świadczą usługi w zakresie kryptoaktywów, powinny się także odnosić do wytycznej sektorowej 21.”.

25. Wytyczna 9.16 otrzymuje brzmienie:

„9.16 Jeżeli klient banku otwiera »rachunek depozytowy/zbiorczy« w celu zarządzania środkami pieniężnymi lub kryptoaktywami, które należą do klientów tego klienta, bank powinien stosować pełny zakres środków należytej staranności wobec klienta, w tym powinien traktować klientów swojego klienta jako beneficjentów rzeczywistych środków pieniężnych znajdujących się na rachunku depozytowym i sprawdzić ich tożsamość.”.

26. Wytyczna 9.17 otrzymuje brzmienie:

„9.17 Jeżeli na podstawie oceny ryzyka prania pieniędzy i finansowania terroryzmu przeprowadzonej zgodnie z niniejszymi wytycznymi bank ustalił, że poziom ryzyka prania pieniędzy lub finansowania terroryzmu związany ze stosunkami gospodarczymi jest wysoki, powinien w stosownych przypadkach stosować wzmożone środki należytej staranności określone w art. 18 dyrektywy (UE) 2015/849.”.

27. W wytycznej 9.18 formuła wprowadzająca otrzymuje brzmienie:

„9.18. W zakresie dopuszczanym w przepisach krajowych, jeżeli według indywidualnej oceny ryzyka prania pieniędzy i finansowania terroryzmu w odniesieniu do klienta ryzyko związane ze stosunkami gospodarczymi jest niskie, bank może jednak stosować uproszczone środki należytej staranności, o ile:”.

28. Nagłówek wytycznych 9.20–9.24 otrzymuje brzmienie:

„Klienci oferujący usługi związane z kryptoaktywami”.

29. Skreśla się wytyczne 9.20–9.23.

30. Dodaje się wytyczne 9.20 i 9.21 w brzmieniu:

„9.20 Przy nawiązywaniu stosunków gospodarczych z klientem będącym dostawcą usług w zakresie kryptoaktywów, innym niż dostawca usług w zakresie kryptoaktywów podlegający regulacji na podstawie rozporządzenia (UE) 2023/1114<sup>5</sup>, banki mogą być narażone na zwiększone ryzyko prania pieniędzy lub finansowania terroryzmu. Ryzyko to może być zmniejszone, jeżeli taki dostawca jest regulowany i nadzorowany zgodnie z ramami regulacyjnymi podobnymi do ram określonych w rozporządzeniu (UE) 2023/1114 lub dyrektywie (UE) 2015/849. Banki powinny przeprowadzać ocenę ryzyka prania pieniędzy i finansowania terroryzmu w odniesieniu do tych klientów przed nawiązaniem z nimi stosunków gospodarczych. W tym kontekście banki powinny również rozważyć ryzyko prania pieniędzy lub finansowania terroryzmu związane z konkretnym rodzajem kryptoaktywów, które są dostarczane lub obsługiwane przez tych dostawców.”

„9.21 W celu zapewnienia obniżenia poziomu ryzyka prania pieniędzy i finansowania terroryzmu związanego z klientami opisanymi w wytycznej 9.20 banki, w ramach swoich środków należytej staranności wobec klienta, powinny co najmniej:

- a) nawiązać dialog z klientem, aby zrozumieć charakter działalności i ryzyko prania pieniędzy i finansowania terroryzmu, na które jest narażony;
- b) oprócz weryfikacji tożsamości beneficjentów rzeczywistych klienta zachowywać należyłą staranność względem kadry kierowniczej wyższego szczebla w zakresie, w jakim są to inne osoby, m.in. rozważyć wszelkie niekorzystne informacje;
- c) zrozumieć zakres, w jakim ci klienci stosują swoje własne środki należytej staranności wobec swoich klientów ze względu na zobowiązanie prawne albo dobrowolnie;
- d) ustalić, czy klient uzyskał rejestrację lub zezwolenie w państwie członkowskim UE/EOG lub w państwie niebędącym członkiem UE, a w przypadku państwa spoza UE ocenić adekwatność istniejącego w tym państwie systemu regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu zgodnie z wytyczną 2.11;
- e) ustalić, czy usługi świadczone przez klienta wchodzą w zakres rejestracji lub zezwolenia klienta;
- f) ustalić, czy klient świadczy usługi inne niż te, w odniesieniu do których uzyskał rejestrację lub zezwolenie jako instytucja kredytowa lub finansowa;
- g) w przypadku gdy działalność klienta obejmuje emisję kryptoaktywów w celu pozyskiwania środków finansowych taką jak pierwsze oferty kryptowalutowe (ang. *Initial Coin Offerings*), banki powinny ustalić, czy taka działalność jest prowadzona zgodnie z obowiązującymi wymogami prawnymi oraz, w stosownych przypadkach, czy jest ona regulowana do celów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu zgodnie z normami uzgodnionymi na szczeblu międzynarodowym takimi jak normy opublikowane przez Grupę Specjalną ds. Przeciwdziałania Praniu

---

<sup>5</sup> Rozporządzenie (UE) 2023/1114 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.

Pieniądzy.”.

### **(ix) Zmiany w wytycznej 10: Wytyczna sektorowa dotycząca emitentów pieniądza elektronicznego**

31. Wytyczna 10.2 otrzymuje brzmienie:

„10.2. Instytucje emitujące pieniądz elektroniczny powinny uwzględnić następujące środki i czynniki ryzyka wraz z tymi, o których mowa w tytule I niniejszych wytycznych. Instytucje, których zezwolenie obejmuje prowadzenie działalności gospodarczej w postaci usług inicjowania płatności oraz usług dostępu do informacji o rachunku, powinny zapoznać się również z wytyczną sektorową 18. Wytyczna sektorowa 11 dla podmiotów świadczących usługi przekazu pieniężnego może być także odpowiednia w tym kontekście. Instytucje świadczące usługi w zakresie kryptoaktywów powinny zapoznać się również z wytyczną sektorową 21.”.

### **(x) Zmiany w wytycznej 15: Wytyczna sektorowa dla firm inwestycyjnych**

32. Wytyczna 15.1 otrzymuje brzmienie:

„15.1. Świadcząc usługi inwestycyjne lub wykonując działalność inwestycyjną w rozumieniu art. 4 ust. 1 pkt 2 dyrektywy (UE) 2014/65, firmy inwestycyjne w rozumieniu art. 4 ust. 1 pkt 1 dyrektywy (UE) 2014/65 powinny uwzględniać następujące środki i czynniki ryzyka wraz z tymi, o których mowa w tytule I niniejszych wytycznych. Wytyczne sektorowe 12 i 21 mogą być również odpowiednie w tym kontekście.”.

### **(xi) Zmiany w wytycznej 17: Wytyczna sektorowa dla regulowanych platform finansowania społecznościowego**

33. Wytyczna 17.4 lit. i) otrzymuje brzmienie:

„i) CSP zezwala na wykorzystywanie kryptoaktywów przez inwestorów i właścicieli projektu do rozrachunku ich transakcji płatniczych za pośrednictwem platformy finansowania społecznościowego, w przypadku gdy takie transfery mogą być narażone na zwiększone ryzyko prania pieniędzy lub finansowania terroryzmu ze względu na czynniki opisane w wytycznej 21.3 lit. d).”.

34. Wytyczna 17.6 lit. b) otrzymuje brzmienie:

„b) Inwestor lub właściciel projektu dokonuje transferu kryptoaktywów, w przypadku gdy taki transfer może być narażony na zwiększone ryzyko prania pieniędzy lub finansowania terroryzmu ze względu na czynniki opisane w wytycznej 21.3 lit. d).”.

35. Dodaje się wytyczną 21 w brzmieniu:

## (xii) „Wytyczna 21: Wytyczna sektorowa dla dostawców usług w zakresie kryptoaktywów

- 21.1. Dostawcy usług w zakresie kryptoaktywów powinni mieć na uwadze, że są narażeni na ryzyko prania pieniędzy lub finansowania terroryzmu ze względu na szczególne cechy ich modelu biznesowego i technologii wykorzystywanej w ramach ich działalności, która umożliwia im natychmiastowy transfer kryptoaktywów na całym świecie i nawiązywanie relacji z klientami w różnych jurysdykcjach. Ryzyko jest jeszcze większe, gdy przetwarzają lub ułatwiają transakcje lub oferują produkty lub usługi, które zapewniają wyższy stopień anonimowości.
- 21.2. Oferując usługi w zakresie kryptoaktywów, dostawcy takich usług powinni przestrzegać przepisów tytułu I, a także przepisów sektorowych określonych w tytule II, jeżeli są one istotne dla oferowanych przez nich produktów.

### Czynniki ryzyka

#### Czynniki ryzyka związane z produktami, usługami i transakcjami

- 21.3. Następujące czynniki mogą przyczyniać się do **zwiększenia ryzyka**:
- a) produkty lub usługi świadczone przez dostawcę usług w zakresie kryptoaktywów zapewniają wyższy stopień anonimowości;
  - b) produkt umożliwia płatności od osób trzecich, które nie są ani powiązane z produktem, ani zidentyfikowane i zweryfikowane z góry, w przypadku gdy takie płatności nie mają wyraźnego ekonomicznego uzasadnienia;
  - c) produkt nie nakłada z góry żadnych ograniczeń pod względem całkowitego wolumenu lub wartości transakcji;
  - d) produkt umożliwia transakcje między rachunkiem klienta a:
    - i. adresami niehostowanymi;
    - ii. rachunkami kryptoaktywów lub adresami rozproszonego rejestru zarządzanymi przez dostawcę usług w zakresie kryptoaktywów w rozumieniu wytycznej 9.20 lub dostawcę takich usług, który podlega systemowi regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu mniej surowemu niż system przewidziany w dyrektywie (UE) 2015/849;
    - iii. platformą wymiany kryptowalut na zasadzie *peer-to-peer* lub innego rodzaju zdecentralizowaną lub rozproszoną aplikacją w zakresie kryptoaktywów, która nie jest kontrolowana przez osobę prawną lub fizyczną ani na którą osoba prawna lub fizyczna nie ma wpływu (często nazywa się to „zdecentralizowanymi finansami” (DeFi));

- iv. platformami, które mają na celu zaciemnienie transakcji i zwiększenie anonimowości, takimi jak platformy usług miksowania;
- v. sprzętem wykorzystywanym do wymiany kryptoaktywów na waluty urzędowe lub odwrotnie (takim jak kryptobankomaty), który obejmuje korzystanie z gotówki lub pieniądza elektronicznego, który korzysta ze zwolnień przewidzianych w art. 12 dyrektywy (UE) 2015/849 lub który nie podlega systemowi regulacji i nadzoru w UE;
- e) produkty obejmujące nowe praktyki biznesowe, w tym nowe kanały dostaw, oraz wykorzystanie technologii, w przypadku których poziom ryzyka prania pieniędzy lub finansowania terroryzmu nie może być wiarygodnie oceniony przez dostawcę usług w zakresie kryptoaktywów zgodnie z wytyczną 1.7 lit. d) ze względu na brak informacji;
- f) gdy hurtowy dostawca usług w zakresie kryptoaktywów sprawuje słabą kontrolę nad usługą zagnieżdżoną świadczoną przez innego dostawcę usług w zakresie kryptoaktywów;
- g) wyniki analizy przeprowadzonej za pomocą zaawansowanych narzędzi analitycznych wskazują na zwiększony poziom ryzyka.

21.4. Następujące czynniki mogą przyczyniać się do **zmniejszenia ryzyka**:

- a) produkty o ograniczonej funkcjonalności takie jak niskie wolumeny lub wartości transakcji;
- b) produkt umożliwia transakcje między rachunkiem klienta a:
  - i. rachunkami kryptoaktywów lub adresami rozproszonego rejestru prowadzonymi w imieniu klienta, będącymi w posiadaniu dostawcy usług w zakresie kryptoaktywów;
  - ii. rachunkiem kryptoaktywów lub adresem rozproszonego rejestru prowadzonym w imieniu klienta, który to rachunek lub adres jest w posiadaniu dostawcy usług w zakresie kryptoaktywów innego niż dostawca usług w zakresie kryptoaktywów regulowany rozporządzeniem (UE) 2023/1114<sup>6</sup>, regulowanego poza UE ramami regulacyjnymi również surowymi co ramy przewidziane w rozporządzeniu (UE) 2023/1114 i podlegającego ramom regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu również surowym co ramy przewidziane w dyrektywie (UE) 2015/849;
  - iii. rachunkiem bankowym prowadzonym w imieniu klienta w instytucji kredytowej, która podlega ramom regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu określonym

---

<sup>6</sup> Rozporządzenie (UE) 2023/1114 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.

w dyrektywie (UE) 2015/849 lub innym ramom prawnym poza UE również surowym co ramy przewidziane w dyrektywie (UE) 2015/849; lub

- c) charakter i zakres kanałów lub systemów płatności wykorzystywanych przez dostawcę usług w zakresie kryptoaktywów jest ograniczony do systemów o obiegu zamkniętym lub systemów mających na celu ułatwienie mikropłatności lub płatności między instytucjami rządowymi a osobami;
- d) produkt jest dostępny tylko dla ograniczonej i zdefiniowanej grupy klientów takiej jak pracownicy przedsiębiorstwa, które wyemitowało kryptoaktywo.

### Czynniki ryzyka związane z klientami

21.5. Następujące czynniki mogą przyczyniać się do **zwiększenia ryzyka**:

- a) w odniesieniu do **charakteru klienta** w szczególności:
  - i. organizacja nienastawiona na zysk, która w oparciu o wiarygodne i niezależne źródła została powiązana z ekstremizmem, propagandą ekstremistyczną lub sympatiami i działaniami terrorystycznymi, lub była zaangażowana w wykroczenia lub działalność przestępczą, w tym w sprawy związane z praniem pieniędzy lub finansowaniem terroryzmu, lub korupcją;
  - ii. przedsiębiorstwo, które jest bankiem fikcyjnym w rozumieniu art. 3 pkt 17 dyrektywy (UE) 2015/849 lub innym rodzajem przedsiębiorstwa fasadowego;
  - iii. przedsiębiorstwo, które zostało niedawno utworzone i przetwarza duże wolumeny transakcji;
  - iv. zarejestrowane zgodnie z prawem przedsiębiorstwo, które przetwarza duże wolumeny transakcji po okresie braku aktywności od czasu jego utworzenia;
  - v. przedsiębiorstwo pozostające w stosunkach gospodarczych z innym przedsiębiorstwem lub innymi przedsiębiorstwami w ramach grupy w rozumieniu art. 3 pkt 15 dyrektywy (UE) 2015/849, które dostarcza produkty i usługi związane z kryptoaktywami;
  - vi. przedsiębiorstwo lub osoba używająca adresu IP związanego z ciemną siecią (ang. *darknet*) lub oprogramowaniem, które umożliwia anonimową komunikację, w tym zaszyfrowane wiadomości e-mail, anonimowe lub tymczasowe usługi poczty elektronicznej i VPN;
  - vii. osoba podatna na zagrożenia, co oznacza osobę, która prawdopodobnie nie będzie typowym klientem dostawcy usług w zakresie kryptoaktywów, lub osobę, która wykazuje bardzo niewielką wiedzę i zrozumienie w zakresie kryptoaktywów lub związanej z nimi technologii, co może być potwierdzone wynikami testu adekwatności/wiedzy lub w drodze innych kontaktów z klientem, a która mimo to decyduje się na częste transakcje lub transakcje o wysokiej wartości, co może zwiększać ryzyko wykorzystania klienta w charakterze słupa;

- b) w odniesieniu do **zachowania klienta** sytuacje, w których klient:
- i. próbuje otworzyć wiele rachunków kryptoaktywów u dostawcy usług w zakresie kryptoaktywów bez wyraźnego ekonomicznego uzasadnienia ani celu biznesowego;
  - ii. lub beneficjent rzeczywisty klienta nie jest w stanie lub nie chce dostarczyć niezbędnych informacji dotyczących należytej staranności wobec klienta na żądanie dostawcy usług w zakresie kryptoaktywów, bez żadnego uzasadnionego powodu, poprzez:
    - a) celowe unikanie bezpośredniego kontaktu z dostawcą usług w zakresie kryptoaktywów, zarówno osobiście, jak i zdalnie;
    - b) próby ukrycia beneficjenta rzeczywistego środków finansowych poprzez zaangażowanie agentów lub współpracowników, takich jak dostawcy usług zaufania lub usług korporacyjnych, w stosunki gospodarcze lub transakcje;
    - c) milczenie lub próby wprowadzenia dostawcy usług w zakresie kryptoaktywów w błąd co do źródła finansowania lub źródła kryptoaktywów wykorzystywanego do pozyskania kryptoaktywów lub co do celu transakcji;
  - iii. korzysta z adresu IP lub urządzenia mobilnego, które są powiązane z wieloma klientami, bez ekonomicznego wyraźnego uzasadnienia, lub o których wiadomo, że są powiązane z potencjalnie nielegalną lub przestępczą działalnością; lub dostęp do rachunku kryptoaktywów klienta jest uzyskiwany z wielu adresów IP bez wyraźnego powiązania z klientem;
  - iv. dostarcza informacji, które są niespójne, w tym w przypadku gdy adres IP klienta jest niezgodny z innymi informacjami na temat klienta, takimi jak informacje, które muszą towarzyszyć transferowi zgodnie z art. 14 ust. 1 i 2 rozporządzenia (UE) 2023/1113, lub miejsce zwykłego pobytu, rejestracji lub działalności gospodarczej klienta (zarówno w chwili nawiązania stosunków gospodarczych, jak i w chwili transakcji), informacje o źródłach środków finansowych lub źródle kryptoaktywów są niespójne z innymi informacjami dotyczącymi należytej staranności wobec klienta lub z ogólnym profilem klienta;
  - v. korzysta z adresu, lokalizacji lub adresu IP powiązanych z rachunkami kryptoaktywów zarejestrowanymi dla różnych użytkowników w ramach jednego dostawcy usług w zakresie kryptoaktywów lub u wielu dostawców takich usług;
  - vi. często zmienia swoje dane osobowe lub instrumenty płatnicze bez oczywistego powodu;
  - vii. często otrzymuje lub przekazuje z adresów niehostowanych kwoty kryptoaktywów tuż poniżej progu 1 000 EUR – określonego w art. 14 ust. 5 i art. 16 ust. 2 rozporządzenia (UE) 2023/1113 – którego przekroczenie

- wymaga weryfikacji beneficjenta lub inicjatora;
- viii. wskazuje, że celem jest inwestycja w pierwszą ofertę publiczną tokenów lub w kryptoaktywo lub produkt, które oferują nieproporcjonalnie wysoki zwrot i znajdują się w jurysdykcji wysokiego ryzyka lub są powiązane z wysokimi wskaźnikami oszustwa lub które nie są poparte dokumentem informacyjnym wymaganym zgodnie z rozporządzeniem (UE) 2023/1114<sup>7</sup>;
  - ix. przejawia zachowania lub stosuje schematy transakcji, które nie są zgodne z tym, czego można oczekiwać po danym rodzaju klienta lub kategorii ryzyka, do której on należy, lub są nieoczekiwane w świetle informacji, które klient przekazał dostawcy usług w zakresie kryptoaktywów w chwili nawiązania lub w trakcie trwania stosunków gospodarczych. Takie okoliczności obejmują sytuacje, w których klient:
    - a) nieoczekiwanie i bez oczywistego powodu znacznie zwiększa wolumen lub wartość transferu kryptoaktywów lub połączonych transferów po okresie uśpienia;
    - b) zawiera transakcje z nietypowo wysoką częstotliwością i nietypowo wysokim wolumenem kryptoaktywów, co jest niezgodne z celem i charakterem stosunków gospodarczych i nie ma wyraźnego celu gospodarczego;
    - c) zwiększa limit transakcji w stopniu, który nie jest współmierny do dochodu deklarowanego przez klienta lub w inny sposób przekracza oczekiwany wolumen działalności;
  - x. przejawia zachowania i stosuje schematy, które są nietypowe, ponieważ wiążą się z niewyjaśnionymi transferami do/z adresów rozproszonego rejestru lub rachunków kryptoaktywów w wielu jurysdykcjach bez wyraźnego celu biznesowego lub celu zgodnego z prawem;
  - xi. podczas wymiany kryptoaktywów na waluty urzędowe i odwrotnie klient:
    - a) korzysta z wielu rachunków bankowych lub płatniczych, kart kredytowych lub kart przedpłaconych w celu finansowania rachunku kryptoaktywów;
    - b) korzysta z konta bankowego lub płatniczego, karty kredytowej w imieniu osoby innej niż klient bez oczywistych powiązań z tą osobą;
    - c) korzysta z rachunku bankowego lub płatniczego znajdującego się w jurysdykcji, która jest niezgodna z podanym adresem lub lokalizacją klienta;
    - d) korzysta z usług wielu dostawców usług płatniczych;

---

<sup>7</sup> Rozporządzenie (UE) 2023/1114 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.



- e) wielokrotnie wnioskuje o wymianę kryptoaktywów na gotówkę lub anonimowy pieniądz elektroniczny lub wymianę gotówki lub anonimowego pieniądza elektronicznego na kryptoaktywa;
  - f) wykorzystuje protokoły, które łączą dwa łańcuchy bloków, w celu wymiany kryptoaktywów na inne kryptoaktywa w innej sieci, takie jak Monero, Zcash itp.;
  - g) wykorzystuje kryptobankomaty w różnych lokalizacjach do wielokrotnego przekazywania środków na rachunek bankowy;
  - h) wycofuje kryptoaktywa od dostawcy usług w zakresie kryptoaktywów na adres niehostowany natychmiast po zdeponowaniu kryptoaktywów lub wymianie na inne kryptoaktywa u dostawcy usług w zakresie kryptoaktywów;
- xii. inwestuje lub wymienia kryptoaktywa, które pożyczył za pośrednictwem platformy pożyczek społecznościowych lub innej platformy pożyczkowej, która nie jest objęta zakresem stosowania rozporządzenia (UE) 2023/1114 lub innych odpowiednich ram regulacyjnych w UE lub poza nią i która jest w szczególności zdecentralizowaną lub rozproszoną aplikacją bez żadnej osoby prawnej lub fizycznej sprawującej nad nią kontrolę lub wpływającej na nią;
  - xiii. otrzymuje lub wysyła bezpośrednio lub pośrednio kryptoaktywa, które są związane z ciemną siecią (ang. *darknet*) lub które są wynikiem nielegalnej działalności;
  - xiv. inwestuje lub wymienia kryptoaktywa, które same w sobie oferują wyższy stopień anonimowości, lub klient otrzymuje kryptoaktywa, które poddano działaniom zwiększającym anonimowość, w szczególności procesom zaciemniającym transakcję w technologii rejestru lub wykazującym inne cechy podobne do tych wymienionych w lit. a) wytycznej 21.5;
  - xv. wielokrotnie otrzymuje kryptoaktywa z poniższych instrumentów lub wysyła kryptoaktywa na nie:
    - a) rachunek kryptoaktywów przy pomocy pośredniczącego dostawcy usług w zakresie kryptoaktywów, który nie jest objęty zakresem stosowania rozporządzenia (UE) 2023/1114 ani żadnymi innymi odpowiednimi ramami regulacyjnymi w UE lub poza nią lub który podlega ramom regulacji i nadzoru w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu mniej surowym niż ramy przewidziane w dyrektywie (UE) 2015/849;
    - b) wiele adresów niehostowanych lub wiele rachunków kryptoaktywów prowadzonych przez tego samego dostawcę usług w zakresie kryptoaktywów lub różnych dostawców takich usług bez wyraźnego ekonomicznego uzasadnienia;

- c) nowo utworzony lub wcześniej nieaktywny rachunek kryptoaktywów lub adres rozproszonego rejestru należący do osoby trzeciej;
- d) adresy niehostowane na platformach zdecentralizowanych wykorzystujących usługi miksowania i inne technologie zwiększające prywatność, które mogą zaciemniać historię finansową związaną z adresem rozproszonego rejestru i źródłem finansowania na potrzeby transakcji, podważając tym samym zdolność dostawcy usług w zakresie kryptoaktywów do poznania swoich klientów oraz wdrażania skutecznych systemów i kontroli w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;
- e) rachunek kryptoaktywów wkrótce po nawiązaniu relacji przez dostawcę usług w zakresie kryptoaktywów, po czym w krótkim czasie następuje wycofanie lub transfer z takiego rachunku bez wyraźnego ekonomicznego uzasadnienia;
- f) rachunek kryptoaktywów często poniżej określonego progu lub, w przypadku transferów na adres niehostowany, poniżej progu 1 000 EUR określonego w art. 14 ust. 5 i art. 16 ust. 2 rozporządzenia (UE) 2023/1113;
- g) rachunek kryptoaktywów poprzez podział transakcji na wiele transakcji, które są wysyłane do wielu adresów rozproszonego rejestru przy użyciu technik *smurfingu*;
- xvi. klient wydaje się wykorzystywać usterki lub awarie technologiczne na swoją korzyść;
- xvii. klient wyjaśnia, że kryptoaktywa przekazane dostawcy usług w zakresie kryptoaktywów uzyskano jako nagrody za wydobywanie kryptowalut lub *staking*, ale nagrody te nie wydają się proporcjonalne do kryptoaktywów wygenerowanych w wyniku takich działań.

#### 21.6. Następujące czynniki mogą przyczyniać się do **zmniejszenia ryzyka**:

- a) podczas poprzednich transakcji na kryptoaktywach klient spełnił wymogi dotyczące informacji przewidziane w rozporządzeniu (UE) 2023/1113 i szczegółowo określone w sekcji 4 wytycznych EUNB dotyczących reguły *travel rule*<sup>8</sup> oraz przedstawił informacje umożliwiające identyfikację klienta lub możliwość sprawdzenia go w przypadku wątpliwości lub podejrzeń;
- b) poprzednie transakcje klienta na kryptoaktywach nie budziły podejrzeń ani obaw, a wybrany produkt lub wybrana usługa są zgodne z profilem ryzyka klienta;

---

<sup>8</sup> Wytyczne na podstawie rozporządzenia (UE) 2023/1113 dotyczące zapobiegania nadużyciom środków finansowych i niektórym transferom kryptoaktywów do celów prania pieniędzy i finansowania terroryzmu [... proszę wstawić w tym miejscu numer tych wytycznych po ich przyjęciu, obecnie będące przedmiotem konsultacji (EBA/CP/2023/35)] („wytyczne dotyczące reguły *travel rule*”).

- c) klient wnioskuje o wymianę na walutę urzędową/z waluty urzędowej, a źródłem albo miejscem przeznaczenia środków finansowych jest własny rachunek bankowy klienta w instytucji kredytowej w jurysdykcji uznanej przez dostawcę usług w zakresie kryptoaktywów za jurysdykcję niskiego ryzyka;
- d) klient wnioskuje o wymianę, a źródłem albo miejscem przeznaczenia kryptoaktywów jest własny rachunek kryptoaktywów klienta lub adres rozproszonego rejestru, który jest prowadzony przez dostawcę usług w zakresie kryptoaktywów regulowanego rozporządzeniem (UE) 2023/1114 albo przez dostawcę takich usług, innego niż dostawca usług w zakresie kryptoaktywów regulowanego i nadzorowanego poza UE na podstawie ram regulacyjnych również surowych co ramy przewidziane w rozporządzeniu (UE) 2023/1114 oraz podlegającego wymogom w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu również surowym co wymogi przewidziane w dyrektywie (UE) 2015/849, który to dostawca został umieszczony na białej liście lub w inny sposób uznany przez dostawcę usług w zakresie kryptoaktywów za dostawcę obciążonego niskim ryzykiem;
- e) klient wnioskuje o wymianę, a źródło albo miejsce przeznaczenia kryptoaktywów odnosi się do płatności o niskiej wartości za towary i usługi dokonywanych na rachunek kryptoaktywów lub adres rozproszonego rejestru lub z takiego rachunku lub adresu, na temat których to rachunków lub adresów nie są dostępne żadne niekorzystne informacje;
- f) transfery dokonywane przez klienta między dwoma dostawcami usług w zakresie kryptoaktywów lub między dostawcą usług w zakresie kryptoaktywów a dostawcą takich usług, innym niż dostawca usług w zakresie kryptoaktywów, który podlega regulacji i nadzorowi w UE albo w inny sposób podlega ramom regulacyjnym również surowym co ramy przewidziane w rozporządzeniu (UE) 2023/1114 i który podlega wymogom w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu również surowym co wymogi przewidziane w dyrektywie (UE) 2015/849.

### **Krajowe lub geograficzne czynniki ryzyka**

21.7. Następujące czynniki mogą przyczyniać się do **zwiększenia ryzyka**:

- a) środki finansowe klienta, które są wymieniane na kryptoaktywa, pochodzą ze stosunków osobistych lub gospodarczych z jurysdykcjami powiązаныmi z wyższym ryzykiem prania pieniędzy i finansowania terroryzmu;
- b) rachunek kryptoaktywów lub adres rozproszonego rejestru pochodzenia lub beneficjenta są skojarzone z jurysdykcją powiązaną z wyższym ryzykiem prania pieniędzy lub finansowania terroryzmu lub z jurysdykcjami/regionami znanymi z finansowania lub wspierania działalności terrorystycznej lub znanymi z działalności grup popełniających przestępstwa terrorystyczne oraz jurysdykcjami podlegającymi sankcjom finansowym, embargom lub środkom, które są związane

z terroryzmem, finansowaniem terroryzmu lub proliferacją;

- c) klient lub beneficjent rzeczywisty klienta jest rezydentem jurysdykcji powiązanej z wyższym ryzykiem prania pieniędzy lub finansowania terroryzmu lub ma siedzibę, prowadzi działalność lub utrzymuje stosunki osobiste lub gospodarcze w takiej jurysdykcji;
- d) stosunki gospodarcze są nawiązane za pośrednictwem dostawcy usług w zakresie kryptoaktywów lub kryptobankomatu, który to dostawca lub kryptobankomat znajduje się w regionie lub jurysdykcji powiązanych z wysokim poziomem ryzyka prania pieniędzy lub finansowania terroryzmu;
- e) klient uczestniczy w operacjach wydobywania kryptoaktywów, bezpośrednio lub pośrednio poprzez stosunki z osobami trzecimi, które to operacje mają miejsce w jurysdykcji wysokiego ryzyka określonej przez Komisję Europejską zgodnie z art. 9 dyrektywy (UE) 2015/849 lub w jurysdykcji podlegającej środkom ograniczającym lub ukierunkowanym sankcjom finansowym.

21.8. Czynniki, który może przyczyniać się do **zmniejszenia ryzyka**:

- a) transfer pochodzi z rachunku kryptoaktywów lub adresu rozproszonego rejestru prowadzonego przez dostawcę usług w zakresie kryptoaktywów lub innego dostawcę takich usług w jurysdykcji powiązanej z niskimi poziomami ryzyka prania pieniędzy lub finansowania terroryzmu lub jest wysyłany na taki rachunek lub taki adres.

### Czynniki ryzyka związane z siecią dystrybucji

21.9. Następujące czynniki mogą przyczyniać się do **zwiększenia ryzyka**:

- a) stosunki gospodarcze są nawiązywane przy użyciu rozwiązań w zakresie zdalnego nawiązywania relacji z klientami, które to rozwiązania nie są zgodne z wytycznymi EUNB dotyczącymi zdalnego nawiązywania relacji z klientami<sup>9</sup>;
- b) instrument finansowania nie podlega ograniczeniom, na przykład w przypadku gotówki, czeków lub produktów pieniądza elektronicznego, które są objęte zwolnieniem zgodnie z art. 12 dyrektywy (UE) 2015/849;
- c) stosunki gospodarcze między dostawcą usług w zakresie kryptoaktywów a klientem są nawiązywane przy pomocy pośredniczącego dostawcy usług w zakresie kryptoaktywów określonego w wytycznej 9.20 powyżej;
- d) identyfikację i weryfikację klienta przeprowadza dostawca usług w zakresie kryptoaktywów znajdujący się w jurysdykcji wysokiego ryzyka na podstawie umowy outsourcingu zgodnie z art. 29 dyrektywy (UE) 2015/849;

---

<sup>9</sup> Wytyczne EUNB dotyczące wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849 (EBA/GL/2022/15).

- e) nowe sieci dystrybucji lub nowe technologie wykorzystywane do dystrybucji kryptoaktywów, które to sieci lub technologie nie zostały jeszcze w pełni przetestowane lub wiążą się z wyższym poziomem ryzyka prania pieniędzy i finansowania terroryzmu;
- f) stosunki gospodarcze są nawiązywane za pomocą kryptobankomatów, co zwiększa ryzyko ze względu na wykorzystanie gotówki.

21.10. Czynniki, które mogą przyczynić się do **zmniejszenia ryzyka**:

- a) dostawca usług w zakresie kryptoaktywów polega na środkach należytej staranności wobec klienta stosowanych przez osobę trzecią zgodnie z art. 26 dyrektywy (UE) 2015/849, a ta osoba trzecia znajduje się w UE.

## Środki

21.11. Dostawcy usług w zakresie kryptoaktywów powinni zapewnić, aby systemy stosowane przez nich do identyfikowania i zwalczania ryzyka prania pieniędzy i finansowania terroryzmu spełniały kryteria określone w tytule I niniejszych wytycznych. Ze względu na swoje modele biznesowe dostawcy usług w zakresie kryptoaktywów powinni w szczególności dopilnować, aby dysponowali odpowiednimi i skutecznymi narzędziami monitorowania, w tym narzędziami monitorowania transakcji i zaawansowanymi narzędziami analitycznymi. Zakres takich narzędzi zależy od charakteru i wolumenu działalności dostawcy usług w zakresie kryptoaktywów, w tym rodzaju kryptoaktywów udostępnianych do obrotu lub wymiany. Dostawcy usług w zakresie kryptoaktywów powinni również zapewnić, aby odpowiedni pracownicy przeszli specjalistyczne szkolenie pozwalające dobrze zrozumieć ryzyko związane z kryptoaktywami oraz ryzyko prania pieniędzy i finansowania terroryzmu, na które mogą narazić takiego dostawcę.

## Wzmoczone środki należytej staranności wobec klienta

21.12. W przypadku zwiększonego ryzyka związanego ze stosunkami gospodarczymi lub transakcją sporadyczną dostawcy usług w zakresie kryptoaktywów muszą stosować wzmoczone środki należytej staranności wobec klienta zgodnie z art. 18 dyrektywy (UE) 2015/849 i zgodnie z tytułem I niniejszych wytycznych. Ponadto dostawcy usług w zakresie kryptoaktywów powinni w razie potrzeby stosować odpowiednie wzmoczone środki należytej staranności wobec klienta wymienione w poniższym wykazie, w zależności od ekspozycji na ryzyko stosunków gospodarczych:

- a) weryfikację tożsamości klienta i beneficjenta rzeczywistego klienta na podstawie więcej niż jednego wiarygodnego i niezależnego źródła;
- b) ustalenie i weryfikację tożsamości akcjonariuszy większościowych, którzy nie odpowiadają definicji beneficjentów rzeczywistych zgodnie z art. 3 dyrektywy (UE) 2015/849, lub wszelkich osób fizycznych, które są upoważnione do operacji na rachunku kryptoaktywów lub adresie rozproszonego rejestru w imieniu klienta lub

wydają polecenia dotyczące transferu lub wymiany kryptoaktywów lub innych usług związanych z tymi kryptoaktywami;

- c) uzyskanie dodatkowych informacji na temat klienta oraz charakteru i celu stosunków gospodarczych w celu nakreślenia bardziej kompletnego profilu klienta, na przykład przez przeszukanie ogólnodostępnych mediów lub niekorzystnych doniesień medialnych lub zamówienie sprawozdania z informacjami od osoby trzeciej. Przykłady rodzaju informacji, których dostawcy usług w zakresie kryptoaktywów mogą potrzebować, obejmują:
  - i. charakter działalności lub zatrudnienia klienta;
  - ii. źródło majątku klienta i źródło finansowania klienta, które to środki są wymieniane na kryptoaktywa, co służy uzyskaniu uzasadnionej pewności, że źródła te są zgodne z prawem;
  - iii. źródło kryptoaktywów klienta wymienianych na waluty urzędowe, w tym czas i miejsce ich zakupu;
  - iv. cel transakcji, w tym, w stosownych przypadkach, przeznaczenie transferu kryptoaktywów;
  - v. informacje o wszelkich powiązaniach klienta z innymi jurysdykcjami (siedziby główne, placówki, oddziały itp.) lub osobami, o których wiadomo, że wywierają znaczący wpływ na działalność klienta;
  - vi. żądanie lub uzyskanie danych na temat transakcji klienta na kryptoaktywach oraz, w przypadku gdy klient jest dostawcą usług w zakresie kryptoaktywów, jego historii transakcji w systemie dostawcy usług w zakresie kryptoaktywów;
- d) uzyskanie dowodów dotyczących źródła finansowania, źródła majątku lub źródła kryptoaktywów w odniesieniu do transakcji, które wiążą się z wyższym ryzykiem;
- e) zwiększenie częstotliwości monitorowania transakcji na kryptoaktywach. Wszystkie transakcje powinny być monitorowane pod kątem nieoczekiwanych zachowań, schematów i oznak podejrzanego zachowania, a także należy przy tym wziąć pod uwagę strony, z którymi klient przeprowadza transakcje;
- f) przegląd i w razie potrzeby aktualizację przechowywanych informacji, danych i dokumentacji przeprowadza się częściej, w szczególności w przypadku wystąpienia zdarzenia inicjującego;
- g) jeżeli ryzyko związane ze stosunkami jest szczególnie wysokie, dostawcy usług w zakresie kryptoaktywów powinni bardziej regularnie dokonywać przeglądu stosunków gospodarczych;
- h) częstsza lub dogłębniejsza ocena działań wykonywanych za pośrednictwem rachunków kryptoaktywów klienta przeprowadzana z użyciem narzędzi do badania kryptoaktywów;

- i) w przypadku gdy klient ma wiele adresów rozproszonego rejestru lub sieci łańcuchów bloków, dostawca usług w zakresie kryptoaktywów powinien powiązać te adresy z klientem;
- j) zwiększenie częstotliwości monitorowania adresów IP klienta i porównywania ich z adresami IP używanymi przez innych klientów;
- k) uzyskanie potwierdzenia poziomu wiedzy i zrozumienia klienta w zakresie kryptoaktywów w celu osiągnięcia pewności, że klient nie jest wykorzystywany w charakterze słupa;
- l) w przypadku gdy schemat wycofywania lub wykupu nie jest zgodny z profilem klienta lub charakterem i celem stosunków gospodarczych, dostawca usług w zakresie kryptoaktywów powinien wprowadzić dodatkowe środki w celu upewnienia się, że o takie operacje wnioskuje klient, a nie osoba trzecia. Ma to szczególne znaczenie w przypadku klientów wysokiego ryzyka, osób starszych lub bardziej podatnych na zagrożenia;
- m) uzyskanie potwierdzenia, że adres niehostowany, od którego otrzymano transfer, znajduje się pod kontrolą klienta dostawcy usług w zakresie kryptoaktywów lub należy do niego.

21.13. Dostawcy usług w zakresie kryptoaktywów powinni stosować zaawansowane narzędzia analityczne w odniesieniu do transakcji z uwzględnieniem ryzyka jako uzupełnienie standardowych narzędzi monitorowania transakcji. Dostawcy usług w zakresie kryptoaktywów powinni stosować zaawansowane narzędzia analityczne w celu oceny ryzyka związanego z transakcjami, w szczególności transakcjami z wykorzystaniem adresów niehostowanych, ponieważ umożliwia to dostawcy usług w zakresie kryptoaktywów śledzenie historii transakcji i identyfikację potencjalnych powiązań z działalnością przestępczą, przestępcami lub podmiotami przestępczymi.

21.14. Jeżeli chodzi o stosunki gospodarcze lub transakcje obejmujące państwa wysokiego ryzyka niebędące członkami UE, dostawcy usług w zakresie kryptoaktywów powinni postępować zgodnie z wytycznymi opisanymi w tytule I niniejszych wytycznych.

### **Uprozczone środki należytej staranności wobec klienta**

21.15. W sytuacjach charakteryzujących się niskim ryzykiem, sklasyfikowanych jako takie w wyniku oceny ryzyka prania pieniędzy i finansowania terroryzmu przeprowadzonej przez dostawcę usług w zakresie kryptoaktywów zgodnie z niniejszymi wytycznymi, oraz w zakresie dopuszczonym przez przepisy krajowe dostawcy usług w zakresie kryptoaktywów mogą stosować uproszczone środki należytej staranności, które mogą obejmować:

- a) w przypadku klientów, którzy podlegają ustawowemu systemowi licencjonowania i regulacji w UE lub w państwie niebędącym członkiem UE, weryfikację tożsamości na podstawie dowodów, że klient podlega takiemu systemowi, na przykład

w drodze wyszukiwania w rejestrze publicznym organu regulacyjnego;

- b) aktualizację informacji, danych lub dokumentacji dotyczących należytej staranności wobec klienta tylko w przypadku wystąpienia szczególnych zdarzeń inicjujących, takich jak wnioski klienta o nowy produkt lub produkt o wyższym ryzyku, lub zmian w zachowaniu klienta lub profilu transakcji, które wskazują na to, że ryzyko powiązane ze stosunkami gospodarczymi nie jest już niskie, przy jednoczesnym przestrzeganiu wszelkich okresów aktualizacji określonych w przepisach krajowych;
- c) obniżenie częstotliwości monitorowania transakcji w przypadku produktów obejmujących powtarzające się transakcje.

### **Przechowywanie dokumentacji**

21.16. W przypadku gdy informacje na temat klientów i transakcji są dostępne w rozproszonym rejestrze, dostawcy usług w zakresie kryptoaktywów nie powinni polegać na rozproszonym rejestrze do celów przechowywania dokumentacji, lecz powinni podjąć kroki w celu wypełnienia swoich obowiązków w tym zakresie zgodnie z dyrektywą (UE) 2015/849 oraz wytycznymi 5.1 i 5.2 powyżej. Dostawcy usług w zakresie kryptoaktywów powinni wprowadzić procedury umożliwiające im powiązanie adresu rozproszonego rejestru z kluczem prywatnym kontrolowanym przez osobę fizyczną lub prawną.