EBA/GL/2022/15

22 listopada 2022 r.

Wytyczne

dotyczące wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do niniejszych wytycznych.

2. W wytycznych przedstawiono stanowisko EUNB w sprawie odpowiednich praktyk nadzorczych w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo unijne w konkretnym obszarze. Właściwe organy w rozumieniu art. 4 ust. 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 w zakresie sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 w terminie do dnia 30.05.2023 właściwe organy mają obowiązek poinformować EUNB, że stosują się lub zamierzają zastosować się do niniejszych wytycznych albo podać uzasadnienie niestosowania się do nich. W razie nieprzekazania tej informacji w wyznaczonym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Informację należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB z oznaczeniem „EBA/GL/2022/15”. Informacja powinna zostać przekazana przez osoby posiadające odpowiednie uprawnienia do przekazywania informacji o stosowaniu się do wytycznych w imieniu właściwych organów. Do EUNB należy również zgłaszać wszelkie zmiany związane ze stosowaniem się do wytycznych.

4. Powiadomienia zostaną opublikowane na stronie internetowej EUNB zgodnie z art. 16 ust. 3.

[1] 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

Przedmiot i zakres stosowania

5. W niniejszych wytycznych określono czynności, jakie instytucje kredytowe i finansowe powinny podjąć podczas przyjmowania lub przeglądu rozwiązań w celu wypełnienia swoich obowiązków wynikających z art. 13 ust. 1 lit. a), b) i c) dyrektywy (UE) 2015/849[2] w odniesieniu do zdalnego nawiązywania relacji z nowymi klientami. Określono w nich również czynności, jakie instytucje kredytowe i finansowe powinny podjąć w przypadku korzystania z usług osób trzecich zgodnie z rozdziałem I sekcją 4 dyrektywy (UE) 2015/849, jak również strategie, środki kontroli i procedury, jakie instytucje kredytowe i finansowe powinny wprowadzić w związku z procedurą należytej staranności wobec klienta, o której mowa w art. 8 ust. 3 i art. 8 ust. 4 lit. a) dyrektywy (UE) 2015/849, jeżeli środki należytej staranności wobec klienta realizuje się zdalnie.

6. Właściwe organy powinny uwzględniać niniejsze wytyczne przy ocenie, czy czynności podjęte przez instytucje kredytowe i finansowe w celu wypełnienia ich obowiązków wynikających z dyrektywy (UE) 2015/849 w kontekście zdalnego nawiązywania relacji z klientami są odpowiednie i skuteczne.

Adresaci

7. Niniejsze wytyczne są skierowane do właściwych organów, o których mowa w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010. Niniejsze wytyczne skierowane są również do podmiotów sektora finansowego zdefiniowanych w art. 4 ust. 1a tego rozporządzenia, które są instytucjami kredytowymi i finansowymi zdefiniowanymi w art. 3 ust. 1 i 2 dyrektywy (UE) 2015/849.

[2] 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.

Definicje

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

Dane biometryczne	Dane osobowe dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej, które umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby fizycznej, takie jak wizerunek twarzy lub dane daktyloskopijne, pozyskiwane i przetwarzane za pomocą środków technicznych.

3. Wdrożenie

Data rozpoczęcia stosowania

Niniejsze wytyczne będą miały zastosowanie od dnia 02.10.2023.

4. Wytyczne dotyczące wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849

4.1 Polityka i procedury wewnętrzne

4.1.1 Polityka i procedury dotyczące zdalnego nawiązywania relacji z klientami

9. Instytucje kredytowe i finansowe powinny wprowadzić i utrzymywać dokumenty polityki i procedury pozwalające im wypełnić obowiązki wynikające z art. 13 ust. 1 lit. a) i c) dyrektywy (UE) 2015/849 w sytuacjach zdalnego nawiązywania relacji z klientami. Takie dokumenty polityki i procedury powinny uwzględniać ryzyko i przedstawiać co najmniej:

    a) ogólny opis rozwiązania przyjętego przez instytucje kredytowe i finansowe w celu gromadzenia, weryfikowania i rejestrowania informacji w całym procesie zdalnego nawiązywania relacji z klientami. Powinny one obejmować wyjaśnienie cech i sposobu działania tego rozwiązania;

    b) sytuacje, w których można zastosować rozwiązanie w zakresie zdalnego nawiązywania relacji z klientami, z uwzględnieniem czynników ryzyka zidentyfikowanych i ocenionych zgodnie z art. 8 ust. 1 dyrektywy (UE) 2015/849 oraz w ramach oceny ryzyka dla ogółu działalności, w tym opis kategorii klientów, produktów i usług, które kwalifikują się do zdalnego nawiązania relacji z klientami;

    c) które czynności są w pełni zautomatyzowane, a które wymagają interwencji człowieka;

    d) środki kontroli wprowadzone w celu zapewnienia, aby pierwsza transakcja z nowym klientem została zrealizowana dopiero po zastosowaniu wszystkich wstępnych środków należytej staranności wobec tego klienta;

    e) opis programów wprowadzających i regularnych szkoleń mających na celu podniesienie poziomu świadomości pracowników i przekazanie im aktualnej wiedzy na temat funkcjonowania rozwiązania w zakresie zdalnego nawiązywania relacji z klientami, ryzyka związanego z tym rozwiązaniem oraz dokumentów polityki i procedur dotyczących zdalnego nawiązywania relacji z klientami i mających na celu ograniczenie tego ryzyka.

10. Dokumenty polityki i procedury, o ile zostaną wdrożone, powinny umożliwić instytucjom kredytowym i finansowym zapewnienie zgodności z przepisami sekcji 4.2–4.7 niniejszych wytycznych.

4.1.2 Zarządzanie

11. Oprócz przepisów określonych w sekcji 4.2.4 wytycznych EUNB dotyczących pracowników ds. zgodności z przepisami[3] pracownik ds. zgodności z przepisami AML/CFT[4] powinien – w ramach swojego ogólnego obowiązku przygotowywania strategii i procedur w celu spełnienia wymogów należytej staranności wobec klienta – zapewnić skuteczne wdrażanie dokumentów polityki i procedur dotyczących zdalnego nawiązywania relacji z klientami, regularnie poddawać je przeglądowi i w razie potrzeby zmieniać.

12. Organ zarządzający instytucji kredytowej i finansowej powinien zatwierdzać dokumenty polityki i procedury zdalnego nawiązywania relacji z klientami oraz nadzorować ich prawidłowe wdrażanie.

4.1.3 Ocena rozwiązania w zakresie zdalnego nawiązywania relacji z klientami poprzedzająca jego wdrożenie

13. Rozważając przyjęcie nowego rozwiązania w zakresie zdalnego nawiązywania relacji z klientami, instytucje kredytowe i finansowe powinny przeprowadzić ocenę takiego rozwiązania przed jego wdrożeniem.

14. Instytucje kredytowe i finansowe powinny określić w swoich dokumentach polityki i procedurach zakres, etapy i wymogi dotyczące prowadzenia dokumentacji na potrzeby oceny poprzedzającej wdrożenie, które powinny obejmować co najmniej:

    a) ocenę adekwatności rozwiązania pod względem kompletności i dokładności gromadzonych danych i dokumentów, a także wiarygodności i niezależności źródeł informacji wykorzystywanych w ramach danego rozwiązania;

    b) ocenę wpływu stosowania rozwiązania w zakresie zdalnego nawiązywania relacji z klientami na ryzyko dla ogółu działalności, w tym ryzyko prania pieniędzy i finansowania terroryzmu, ryzyko operacyjne, ryzyko utraty reputacji i ryzyko prawne;

    c) określenie możliwych środków ograniczania ryzyka i działań naprawczych w odniesieniu do każdego rodzaju ryzyka zidentyfikowanego w ocenie dokonanej na podstawie lit. b);

[3] Projekt wytycznych w sprawie strategii i procedur zarządzania zgodnością z przepisami oraz roli i obowiązków pracownika ds. zgodności z przepisami AML/CFT wydane na podstawie art. 8 i rozdziału VI dyrektywy.

[4] Zgodnie z kryteriami proporcjonalności określonymi w sekcji 4.2.2 wytycznych dotyczących pracowników ds. zgodności z przepisami.

d) testy służące ocenie ryzyka nadużyć finansowych, w tym ryzyka oszustw opartych na podszywaniu się pod inną osobę, oraz innego rodzaju ryzyka związanego z technologią informacyjno-komunikacyjną („ICT") i bezpieczeństwem, zgodnie z ust. 43 wytycznych EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT[5];

e) kompleksowe badanie funkcjonowania rozwiązania ukierunkowanego na klientów, produkty i usługi, o których mowa w polityce i procedurach dotyczących zdalnego nawiązywania relacji z klientami.

15. Instytucje kredytowe i finansowe powinny uznać kryteria określone w ust. 14 lit. a), d) i e) za spełnione, jeżeli w ramach danego rozwiązania stosuje się jedno z poniższych:

a) systemy identyfikacji elektronicznej notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniające wymogi „średniego" lub „wysokiego" poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;

b) odpowiednie kwalifikowane usługi zaufania, które spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcji 3 i art. 24 ust. 1 akapitu drugiego lit. b) tego rozporządzenia.

16. Instytucje kredytowe i finansowe powinny być w stanie wykazać właściwemu organowi, jakie oceny przeprowadziły przed wdrożeniem rozwiązania w zakresie zdalnego nawiązywania relacji z klientami, rezultaty swojej oceny, jak również wyjaśnić, w jaki sposób stosowanie danego rozwiązania jest odpowiednie w świetle ryzyka prania pieniędzy lub finansowania terroryzmu, które to ryzyko zidentyfikowano w odniesieniu do rodzajów klientów, usług, terytorium i produktów objętych zakresem rozwiązania.

17. Instytucje kredytowe i finansowe powinny zacząć korzystać z rozwiązania w zakresie zdalnego nawiązywania relacji z klientami dopiero po upewnieniu się, czy może ono zostać włączone do szerszego systemu kontroli wewnętrznej instytucji, co umożliwi instytucji odpowiednie zarządzanie ryzykiem prania pieniędzy lub finansowania terroryzmu, które to ryzyko może wynikać z zastosowania rozwiązania w zakresie zdalnego nawiązywania relacji z klientami.

4.1.4 Bieżące monitorowanie rozwiązania w zakresie zdalnego nawiązywania relacji z klientami

18. Instytucje kredytowe i finansowe powinny na bieżąco monitorować rozwiązanie w zakresie zdalnego nawiązywania relacji z klientami, aby zapewnić jego funkcjonowanie zgodne z

[5] EBA/GL/2019/04.

oczekiwaniami instytucji kredytowych i finansowych. Powinny one uzupełniać swoją politykę i procedury opisane w ust. 9 o opis co najmniej:

a) czynności, jakie podejmą w celu upewnienia się co do bieżącej jakości, kompletności, dokładności i adekwatności danych zgromadzonych w trakcie zdalnego nawiązywania relacji z klientami, przy czym czynności te powinny być współmierne do ryzyka prania pieniędzy lub finansowania terroryzmu, na jakie narażona jest instytucja kredytowa i finansowa;

b) zakresu i częstotliwości takiego regularnego przeglądu danych; oraz

c) okoliczności, które wymagają przeprowadzenia przeglądu *ad hoc*, wśród których powinny znaleźć się co najmniej:

   a. zmiany w ekspozycji instytucji kredytowej i finansowej na ryzyko prania pieniędzy lub finansowania terroryzmu;

   b. niedociągnięcia w funkcjonowaniu rozwiązania wykryte w trakcie jego monitorowania, działań audytowych lub nadzorczych;

   c. zauważalny wzrost liczby prób popełnienia oszustwa;

   d. zmiany ram prawnych lub regulacyjnych.

19. Instytucje kredytowe i finansowe powinny określić w swoich procedurach i procesach działania naprawcze na wypadek urzeczywistnienia się ryzyka lub na wypadek wykrycia błędów, które mają wpływ na wydajność i skuteczność ogólnego rozwiązania w zakresie nawiązywania relacji z klientami. Działania te powinny obejmować co najmniej:

a) przegląd wszystkich stosunków gospodarczych, których to dotyczy, w celu ustalenia, czy instytucje kredytowe i finansowe podjęły wystarczające wstępne środki należytej staranności wobec klienta w celu spełnienia wymogów wynikających z art. 13 ust. 1 lit. a), b) i c) dyrektywy w sprawie przeciwdziałania praniu pieniędzy. Instytucje kredytowe i finansowe powinny priorytetowo traktować te stosunki gospodarcze, które wiążą się z najwyższym poziomem ryzyka prania pieniędzy lub finansowania terroryzmu;

b) uwzględniając informacje uzyskane w ramach wyżej wspomnianego przeglądu – ocenę, czy dany stosunek gospodarczy, którego dotyczy, powinien:

   a. podlegać dodatkowym środkom należytej staranności;

   b. podlegać ograniczeniom, takim jak ograniczenia wielkości transakcji, w przypadkach dopuszczalnych na mocy prawa krajowego, do czasu przeprowadzenia przeglądu,;

c. zostać zakończony;

d. zostać zgłoszony jednostce analityki finansowej;

e. zostać uwzględniony w innej kategorii ryzyka.

20. Instytucje kredytowe i finansowe powinny rozważyć najskuteczniejszy sposób monitorowania bieżącej adekwatności i niezawodności rozwiązań w zakresie zdalnego nawiązywania relacji z klientami. Powinny one rozważyć między innymi co najmniej jeden z następujących środków:

    i. test zapewnienia jakości;

    ii. zautomatyzowane ostrzeżenia (alerty) i powiadomienia o krytycznym znaczeniu;

    iii. regularne zautomatyzowane sprawozdania dotyczące jakości;

    iv. testowanie wyrywkowe;

    v. przeglądy manualne.

21. Niniejsza sekcja ma również zastosowanie w przypadku, gdy wykorzystuje się w pełni zautomatyzowane rozwiązania w zakresie nawiązywania relacji z klientami, które są w dużym stopniu zależne od zautomatyzowanych algorytmów i prowadzone bez udziału człowieka lub przy niewielkim udziale człowieka.

22. Instytucje kredytowe i finansowe powinny być w stanie wykazać właściwym organom, jakie przeglądy przeprowadziły, a także jakie działania naprawcze podjęły, aby wyeliminować wszelkie niedociągnięcia stwierdzone w całym okresie funkcjonowania rozwiązania w zakresie zdalnego nawiązywania relacji z klientami.

4.2 Pozyskiwanie informacji

4.2.1 Identyfikacja klienta

23. Oprócz punktów określonych w ust. 9 instytucje kredytowe i finansowe powinny określić w swoich dokumentach polityki i procedurach informacje niezbędne do zidentyfikowania klienta, rodzaje dokumentów, danych lub informacji, które instytucja wykorzysta do weryfikacji tożsamości klienta, a także sposób, w jaki informacje te będą weryfikowane.

24. Instytucje kredytowe i finansowe powinny zapewnić, aby:

    a) informacje uzyskane za pośrednictwem rozwiązania w zakresie zdalnego nawiązywania relacji z klientami były aktualne i odpowiednie do spełnienia

obowiązujących norm prawnych i regulacyjnych dotyczących wstępnej procedury należytej staranności wobec klienta;

b) wszelkie obrazy, nagrania wideo, dźwięk i dane były rejestrowane w formacie czytelnym i odpowiedniej jakości, tak aby klient był jednoznacznie rozpoznawalny;

c) procesu identyfikacji nie kontynuowano w przypadku wykrycia usterek technicznych lub nieoczekiwanych przerw w połączeniu.

25. Instytucje kredytowe i finansowe powinny uznać kryteria określone w ust. 24 za spełnione, jeżeli w ramach danego rozwiązania stosuje się jedno z poniższych kryteriów:

a) systemy identyfikacji elektronicznej notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniające wymogi „średniego" lub „wysokiego" poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;

b) odpowiednie kwalifikowane usługi zaufania, które spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcji 3 i art. 24 ust. 1 akapitu drugiego lit. b) tego rozporządzenia.

26. Dokumenty i informacje zgromadzone podczas procesu zdalnej identyfikacji, które muszą być przechowywane zgodnie z art. 40 ust. 1 lit. a) dyrektywy (UE) 2015/849, powinny być opatrzone znacznikiem czasu i przechowywane przez instytucję kredytową i finansową w bezpieczny sposób. Treść przechowywanych zapisów, w tym obrazów, nagrań wideo, dźwięku i danych, powinna być dostępna w czytelnym formacie i umożliwiać kontrolę *ex post*.

4.2.2 Identyfikacja osób fizycznych

27. Instytucje kredytowe i finansowe powinny określić w swoich dokumentach polityki, jak podano w sekcji 4.1.1 ust. 9, informacje niezbędne do zdalnej identyfikacji klientów zgodnie z art. 13 ust. 1 lit. a) i c) dyrektywy (UE) 2015/849. Ponadto instytucje kredytowe i finansowe powinny określić, jakie informacje:

a) są wprowadzane manualnie przez klienta;

b) są pobierane automatycznie z dokumentacji dostarczonej przez klienta;

c) są gromadzone z wykorzystaniem innych źródeł wewnętrznych lub zewnętrznych.

28. Instytucje kredytowe i finansowe powinny wprowadzić i utrzymywać odpowiednie mechanizmy zapewniające wiarygodność informacji, które automatycznie pobierają zgodnie z ust. 27. Powinny one stosować środki kontroli w celu przeciwdziałania powiązanym zagrożeniom, w tym zagrożeniom związanym z automatycznym pobieraniem danych, takim jak ukrywanie lokalizacji urządzenia klienta poprzez podstawianie fałszywych adresów IP sfałszowanego (w wyniku spoofingu) lub poprzez wykorzystywanie usług takich jak wirtualne sieci prywatne (VPN).

4.2.3 Identyfikacja podmiotów prawnych

29. W przypadku gdy instytucje kredytowe i finansowe zdalnie nawiązują relacje z klientami będącymi podmiotami prawnymi, powinny one określić w swoich dokumentach polityki i procedurach, zgodnie z sekcją 4.1.1 ust. 9, z jaką kategorią podmiotów prawnych będą zdalnie nawiązywać relacje, biorąc pod uwagę poziom ryzyka prania pieniędzy lub finansowania terroryzmu związany z każdą z kategorii oraz poziom interwencji człowieka wymagany do zatwierdzenia informacji umożliwiających identyfikację.

30. Instytucje kredytowe i finansowe powinny zapewnić, aby rozwiązanie w zakresie zdalnego nawiązywania relacji z klientami posiadało funkcje umożliwiające gromadzenie:

    a) wszystkich istotnych danych i dokumentów służących identyfikacji i weryfikacji osoby prawnej;

    b) wszystkich istotnych danych i dokumentów służących zweryfikowaniu, czy dana osoba fizyczna działająca w imieniu osoby prawnej jest uprawniona do działania w takim charakterze;

    c) informacji dotyczących beneficjentów rzeczywistych zgodnie z ust. 4.12 wytycznych EUNB w sprawie czynników ryzyka[6].

31. W odniesieniu do osoby fizycznej działającej w imieniu osoby prawnej instytucje kredytowe i finansowe powinny stosować proces identyfikacji opisany w sekcji 4.2.2.

4.2.4 Charakter i cel stosunku gospodarczego

32. W przypadku gdy instytucje kredytowe i finansowe oceniają i – w stosownych przypadkach – uzyskują informacje na temat celu i zamierzonego charakteru stosunku gospodarczego zgodnie z art. 13 ust. 1 lit. c) dyrektywy (UE) 2015/849, jak określono szczegółowo w sekcji 4.38 wytycznych EUNB w sprawie czynników ryzyka, instytucje te powinny, do celów niniejszych wytycznych, zakończyć odpowiednie działania przed końcem procesu zdalnego nawiązywania relacji z klientem.

4.3 Autentyczność i integralność dokumentów

33. W przypadku gdy instytucje kredytowe i finansowe akceptują kopię oryginalnego dokumentu i nie badają dokumentu oryginalnego, powinny podjąć czynności w celu upewnienia się, że kopia jest wiarygodna. Instytucje kredytowe i finansowe powinny ustalić co najmniej:

    a) czy kopia zawiera zabezpieczenia zawarte w oryginalnym dokumencie i czy cechy dokumentu oryginalnego, którego kopię okazano, są ważne i dopuszczalne, w szczególności jeżeli chodzi o rodzaj, wielkość znaków i strukturę dokumentu, czego

[6] EBA/GL/2021/02

dokonuje się poprzez porównanie ich z oficjalnymi bazami danych, takimi jak PRADO[7];

b) czy dane osobowe zostały zmienione lub w inny sposób naruszone, lub, w stosownych przypadkach, czy zdjęcie klienta zawarte w dokumencie nie zostało zastąpione;

c) czy zachowano integralność algorytmu wykorzystywanego do wygenerowania niepowtarzalnego numeru identyfikacyjnego oryginalnego dokumentu, w przypadku gdy dokument urzędowy wydano z polem przeznaczonym do odczytu maszynowego (MRZ);

d) czy przekazana kopia jest odpowiedniej jakości i rozdzielczości, aby zapewnić jednoznaczność istotnych informacji;

e) czy przekazana kopia nie została wyświetlona na ekranie na podstawie fotografii lub skanu oryginalnego dokumentu tożsamości.

34. W przypadku gdy instytucje kredytowe i finansowe korzystają z funkcji automatycznego odczytywania informacji z dokumentów, takich jak algorytmy optycznego rozpoznawania znaków (OCR) lub weryfikacje pola przeznaczonego do odczytu maszynowego (MRZ), powinny one podjąć czynności niezbędne do zapewnienia, aby narzędzia te rejestrowały informacje w sposób dokładny i spójny.

35. Jeżeli urządzenie, z którego korzystają klienci w celu potwierdzenia swojej tożsamości, umożliwia gromadzenie odpowiednich danych, na przykład dlatego, że dane te znajdują się na chipie krajowego dowodu tożsamości, a dostęp do tych danych jest technicznie możliwy dla instytucji kredytowych i finansowych, instytucje kredytowe i finansowe powinny rozważyć wykorzystanie tych informacji w celu weryfikacji ich zgodności z informacjami uzyskanymi z innych źródeł, takich jak przesłane dane lub inne dokumenty przedłożone przez klienta.

36. W trakcie procesu weryfikacji instytucje kredytowe i finansowe powinny w miarę możliwości weryfikować zawarte w dokumencie urzędowym zabezpieczenia stanowiące dowód ich autentyczności, takie jak hologramy, o ile dokument zawiera takie zabezpieczenia.

37. Instytucje kredytowe i finansowe powinny określić w swoich dokumentach polityki i procedurach, w jaki sposób dostosują swoje wnioski o dokumentację do celów włączenia społecznego pod względem finansowym. Jeżeli w rezultacie akceptowane są słabsze lub nietradycyjne formy dokumentacji, instytucje kredytowe i finansowe powinny oprócz środków określonych w ust. 4.10 wytycznych EUNB w sprawie czynników ryzyka stosować środki kontroli lub zwiększoną interwencję człowieka, aby mieć pewność, że rozumieją ryzyko prania pieniędzy lub finansowania terroryzmu związane z danym stosunkiem gospodarczym.

[7] https://www.consilium.europa.eu/prado/en/prado-start-page.html

4.4 Dopasowywanie tożsamości klienta w ramach procesu weryfikacji

38. Rozwiązania w zakresie zdalnego nawiązywania relacji z klientami stosowane przez instytucje kredytowe i finansowe powinny umożliwiać w ramach procesu weryfikacji co najmniej:

    a) stwierdzenie zgodności widocznych informacji dotyczących osoby fizycznej z przedstawioną dokumentacją;

    b) w przypadku gdy klient jest osobą prawną, osobą fizyczną prowadzącą działalność gospodarczą lub jednostką organizacyjną nieposiadającą osobowości prawnej: stwierdzenie, że – w stosownych przypadkach – jest on ujęty w rejestrach publicznych;

    c) w przypadku gdy klient jest osobą prawną, osobą fizyczną prowadzącą działalność gospodarczą lub jednostką organizacyjną nieposiadającą osobowości prawnej: stwierdzenie, że osoba fizyczna, która go reprezentuje, jest uprawniona do działania w jego imieniu.

39. W przypadku gdy rozwiązanie w zakresie zdalnego nawiązywania relacji z klientami wiąże się z wykorzystaniem danych biometrycznych do weryfikacji tożsamości klienta, instytucje kredytowe i finansowe powinny upewnić się, że dane biometryczne są wystarczająco unikalne, aby można je było jednoznacznie powiązać z jedną osobą fizyczną. Instytucje kredytowe i finansowe powinny stosować silne i wiarygodne algorytmy w celu weryfikacji zgodności danych biometrycznych podanych w przedstawionym dokumencie tożsamości z klientem, z którym nawiązywana jest relacja. W sytuacjach, w których rozwiązanie nie zapewnia wymaganego poziomu ufności, należy zastosować dodatkowe środki kontroli.

40. W sytuacjach, w których jakość przedstawionych dowodów jest niewystarczająca, co prowadzi do niejasności lub niepewności, wpływając na przeprowadzanie kontroli zdalnej, należy przerwać proces zdalnego nawiązywania relacji z klientem i rozpocząć go ponownie lub przekierować klienta do weryfikacji bezpośredniej.

41. W przypadku gdy instytucje kredytowe i finansowe stosują rozwiązania zdalnego nawiązywania relacji z klientami bez nadzoru, tj. gdy przy stosowaniu takich rozwiązań klient w procesie weryfikacji nie wchodzi w interakcje z pracownikiem, instytucje te powinny:

    a) zapewnić, aby wszelkie fotografie lub nagrania wideo były wykonywane w odpowiednich warunkach oświetleniowych oraz aby wymagane cechy zostały uchwycone w sposób wystarczająco jasny, co ma umożliwić właściwą weryfikację tożsamości klienta;

    b) zapewnić, aby wszelkie fotografie lub nagrania wideo zostały wykonane w momencie, gdy klient przechodzi przez proces weryfikacji;

c) przeprowadzać weryfikację wykrywania aktywności klienta, mogącą obejmować procedury, w przypadku których od klienta wymaga się podjęcia konkretnego działania, co służy sprawdzeniu, czy klient jest obecny na sesji komunikacyjnej, lub mogącą opierać się na analizie otrzymanych danych i niewymagającą konkretnego działania ze strony klienta;

d) stosować silne i wiarygodne algorytmy w celu sprawdzenia, czy wykonane fotografie lub nagrania wideo są zgodne z obrazem(-ami) pobranym(-i) z oficjalnego(-ych) dokumentu(-ów) należącego(-ych) do klienta.

42. W przypadku gdy instytucje kredytowe i finansowe stosują rozwiązania w zakresie zdalnego nawiązywania relacji z klientami pod nadzorem, tj. gdy przy stosowaniu takich rozwiązań klient w procesie weryfikacji wchodzi w interakcje z pracownikiem, instytucje te powinny:

a) zapewnić wystarczającą jakość obrazu i dźwięku, aby umożliwić właściwą weryfikację tożsamości klienta oraz stosowanie wiarygodnych systemów technicznych;

b) przewidywać udział w procedurze pracownika, który posiada wystarczającą wiedzę na temat obowiązujących przepisów w obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz aspektów bezpieczeństwa zdalnej weryfikacji i który jest wystarczająco przeszkolony, aby przewidywać umyślne lub celowe stosowanie technik wprowadzania w błąd związanych ze zdalną weryfikacją oraz zapobiegać takiemu działaniu, wykrywać je i reagować w przypadku jego wystąpienia;

c) opracować scenariusz rozmowy, w którym określone zostaną kolejne etapy procesu zdalnej weryfikacji, a także działania wymagane od pracownika. Scenariusz rozmowy powinien zawierać wytyczne dotyczące obserwacji i identyfikacji czynników psychologicznych lub innych cech, które mogą wskazywać na podejrzane zachowanie podczas zdalnej weryfikacji.

43. W miarę możliwości instytucje kredytowe i finansowe powinny korzystać z takich rozwiązań w zakresie zdalnego nawiązywania relacji z klientami, które obejmują losową sekwencję czynności wykonywanych przez klienta na potrzeby weryfikacji, co ma stanowić ochronę przed takimi zagrożeniami jak stosowanie fałszywych tożsamości lub przymusu. W miarę możliwości instytucje kredytowe i finansowe powinny również w sposób losowy przydzielać pracownika odpowiedzialnego za proces zdalnej weryfikacji, aby uniknąć zmowy między klientem a pracownikiem odpowiedzialnym za weryfikację.

44. Ponadto, jeżeli jest to współmierne do ryzyka prania pieniędzy lub finansowania terroryzmu, które to ryzyko jest związane z danym stosunkiem gospodarczym, instytucje kredytowe i finansowe powinny stosować co najmniej jeden z następujących środków kontroli lub podobny środek w celu zwiększenia wiarygodności procesu weryfikacji. Takimi środkami kontroli lub innymi środkami mogą być między innymi:

a) dokonanie pierwszej płatności na rachunek płatniczy, którego klient jest jedynym właścicielem lub współwłaścicielem, prowadzony w instytucji kredytowej lub finansowej regulowanej w EOG lub w państwie trzecim, których wymogi w zakresie przeciwdziałania praniu pieniędzy lub finansowaniu terroryzmu są nie mniej rzetelne niż wymogi określone w dyrektywie (UE) 2015/849;

b) wysłanie klientowi wygenerowanego losowo hasła w celu potwierdzenia obecności podczas procesu zdalnej weryfikacji. Hasło powinno być kodem jednorazowego użytku, który należy zastosować w określonym czasie;

c) pobranie danych biometrycznych i porównanie ich z danymi zgromadzonymi w innych niezależnych i wiarygodnych źródłach;

d) kontakt telefoniczny z klientem;

e) wysłanie korespondencji bezpośredniej (zarówno elektronicznej, jak i pocztowej) do klienta.

45. Instytucje kredytowe i finansowe powinny uznać kryteria określone w ust. 38–43 za spełnione, jeżeli w ramach danego rozwiązania stosuje się jedno z poniższych kryteriów:

a) systemy identyfikacji elektronicznej notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniające wymogi „średniego” lub „wysokiego” poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;

b) odpowiednie kwalifikowane usługi zaufania, które spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcja 3 i art. 24 ust. 1 akapit drugi lit. b) tego rozporządzenia.

4.5 Korzystanie z usług osób trzecich i outsourcingu

46. Oprócz punktów określonych w ust. 9 instytucje kredytowe i finansowe powinny uwzględnić w swoich dokumentach polityki i procedurach specyfikacje określające, które funkcje i działania związane ze zdalnym nawiązywaniem relacji z klientami będą wykonywane lub przeprowadzane przez instytucję kredytową i finansową, a które przez osoby trzecie lub przez innego usługodawcę działającego w ramach outsourcingu.

4.5.1 Korzystanie z usług osób trzecich zgodnie z rozdziałem II sekcja 4 dyrektywy (UE) 2015/849

47. Oprócz wytycznych EUNB w sprawie czynników ryzyka[8], w szczególności wytycznych 2.20–2.21 oraz 4.32–4.37, państwa członkowskie powinny stosować następujące kryteria:

[8] EBA/GL/2021/02.

a) podjąć działania niezbędne do upewnienia się, że wprowadzone przez osoby trzecie wewnętrzne procesy i procedury zdalnego nawiązywania relacji z klientami i należytej staranności wobec klienta oraz informacje i dane, które osoby trzecie gromadzą w tym kontekście, są wystarczające i zgodne z wymogami określonymi w niniejszych wytycznych;

b) zapewnić ciągłość stosunków gospodarczych nawiązanych między klientem a instytucją kredytową i finansową w celu ochrony przed zdarzeniami, które mogą ujawnić niedociągnięcia w procesie zdalnego nawiązywania relacji z klientami przeprowadzanym przez osobę trzecią.

4.5.2 Outsourcing procedury należytej staranności wobec klienta

48. W przypadku gdy całość lub część procesu zdalnego nawiązywania relacji z klientami jest zlecana przez instytucje kredytowe i finansowe na zasadzie outsourcingu usługodawcy świadczącemu usługi na zasadzie outsourcingu, o którym mowa w art. 29 dyrektywy (UE) 2015/849, instytucje kredytowe i finansowe – oprócz wytycznych 2.20–2.21 oraz 4.32–4.37 wytycznych EUNB w sprawie czynników ryzyka oraz, w stosownych przypadkach, wytycznych EUNB w sprawie outsourcingu[9] – powinny stosować przed nawiązaniem stosunku gospodarczego z usługodawcą świadczącym usługi na zasadzie outsourcingu i w jego trakcie następujące środki, których zakres należy dostosować z uwzględnieniem ryzyka:

    a) zapewnienie, aby usługodawca świadczący usługi na zasadzie outsourcingu skutecznie wdrażał politykę i procedury instytucji kredytowej i finansowej dotyczące zdalnego nawiązywania relacji z klientami zgodnie z umową outsourcingu oraz przestrzegał tej polityki i tych procedur. Należy to osiągnąć dzięki regularnej sprawozdawczości, stałemu monitorowaniu, wizytom na miejscu lub testom wyrywkowym;

    b) przeprowadzenie oceny w celu zapewnienia, aby usługodawca świadczący usługi na zasadzie outsourcingu był wystarczająco wyposażony i zdolny do przeprowadzania procesu zdalnego nawiązywania relacji z klientami. Oceny mogą obejmować między innymi ocenę szkolenia pracowników, sprawności technologicznej i zarządzania danymi u usługodawcy świadczącego usługi na zasadzie outsourcingu;

    c) zapewnia, aby usługodawca świadczący usługi na zasadzie outsourcingu informował instytucje kredytowe i finansowe o wszelkich proponowanych zmianach w procesie zdalnego nawiązywania relacji z klientami lub o wszelkich zmianach wprowadzonych w rozwiązaniu oferowanym przez takiego usługodawcę.

49. W przypadku gdy usługodawca świadczący usługi na zasadzie outsourcingu przechowuje dane klientów, w tym fotografie, filmy wideo i dokumenty, w trakcie procesu zdalnego nawiązywania relacji, instytucje kredytowe i finansowe powinny zapewnić, aby:

[9] Wytyczne EUNB w sprawie outsourcingu (europa.eu)

a) gromadzono jedynie niezbędne dane klienta, przestrzegając ściśle określonego okresu przechowywania;

b) dostęp do danych był ściśle ograniczony i zarejestrowany;

c) wdrożono odpowiednie środki bezpieczeństwa w celu zapewnienia ochrony przechowywanych danych.

4.6 Zarządzanie ryzykiem związanym z technologiami i bezpieczeństwem ICT

50. Instytucje kredytowe i finansowe powinny identyfikować ryzyko związane z technologiami i bezpieczeństwem ICT w odniesieniu do korzystania z procesu zdalnego nawiązywania relacji z klientami i zarządzać tym ryzykiem, również wówczas gdy instytucje kredytowe i finansowe korzystają z usług osób trzecich lub gdy usługa ta jest zlecana na zasadzie outsourcingu, w tym podmiotom należącym do grupy.

51. Oprócz spełnienia wymogów określonych w wytycznych EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT [10] instytucje kredytowe i finansowe powinny, w stosownych przypadkach, korzystać z bezpiecznych kanałów komunikacji w celu interakcji z klientem podczas procesu zdalnego nawiązywania relacji z klientami. Aby zagwarantować poufność, autentyczność i integralność wymienianych danych, w stosownych przypadkach należy na potrzeby rozwiązania w zakresie zdalnego nawiązywania relacji z klientami stosować bezpieczne protokoły i algorytmy kryptograficzne zgodnie z najlepszymi praktykami branżowymi.

52. Instytucje kredytowe i finansowe powinny zapewnić bezpieczny punkt dostępu umożliwiający rozpoczęcie zdalnego procesu nawiązywania relacji z klientami z wykorzystaniem kwalifikowanych certyfikatów pieczęci elektronicznych, o których mowa w art. 3 ust. 30 rozporządzenia (UE) nr 910/2014, lub certyfikatów uwierzytelniania witryn internetowych, o których mowa w art. 3 pkt 39 tego rozporządzenia. Klienta należy również poinformować o obowiązujących środkach bezpieczeństwa, które należy zastosować w celu zapewnienia bezpiecznego korzystania z systemu.

53. Jeśli w celu przeprowadzania zdalnego procesu nawiązywania relacji z klientami używa się urządzenia wielofunkcyjnego, należy w stosownych przypadkach korzystać z bezpiecznego środowiska do wykonywania kodu oprogramowania po stronie klienta. Aby zapewnić bezpieczeństwo i wiarygodność kodu oprogramowania i zgromadzonych danych, należy wdrożyć dodatkowe środki bezpieczeństwa odpowiednie do oceny ryzyka bezpieczeństwa określonej w wytycznych EUNB w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT.

[10] EBA/GL/2019/04.

4.7 Przestrzeganie niniejszych wytycznych w przypadku korzystania przez instytucje kredytowe i finansowe z usług zaufania i krajowych procesów identyfikacji, o których mowa w art. 13 ust. 1 lit. a) dyrektywy (UE) 2015/849

54. W celu zapewnienia zgodności z niniejszymi wytycznymi instytucje kredytowe i finansowe mogą korzystać z odpowiednich usług zaufania i elektronicznych procesów identyfikacji regulowanych, uznanych, zatwierdzonych lub przyjętych przez właściwe organy krajowe, o których mowa w art. 13 ust. 1 lit. a) dyrektywy (UE) 2015/849. Stosując takie rozwiązania, instytucje kredytowe i finansowe powinny ocenić, w jakim stopniu dane rozwiązanie jest zgodne z przepisami niniejszych wytycznych, a także zastosować środki niezbędne do ograniczenia wszelkich istotnych zagrożeń wynikających ze stosowania tych rozwiązań. Powinny one w szczególności wziąć pod uwagę, czy uwzględniono następujące rodzaje ryzyka:

    a) ryzyko związane z uwierzytelnianiem – i określić w dokumentach polityki i procedurach szczególne środki ograniczania ryzyka, zwłaszcza w odniesieniu do ryzyka oszustwa polegającego na podszywaniu się pod inną osobę;

    b) ryzyko, że tożsamość klienta nie jest tożsamością deklarowaną;

    c) ryzyko utraty, kradzieży, zawieszenia, cofnięcia lub wygaśnięcia dowodu tożsamości, w tym, w stosownych przypadkach, narzędzia wykrywania oszustw dotyczących tożsamości i zapobiegania im.