UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stanowisko UKNF dotyczące prawidłowego wykorzystania w sektorze finansowym rozwiązań w zakresie nawiązywania stosunków gospodarczych bez fizycznej obecności klienta

wrzesień 2023

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stanowisko UKNF dotyczące prawidłowego wykorzystania w sektorze finansowym rozwiązań w zakresie nawiązywania stosunków gospodarczych bez fizycznej obecności klienta

Stanowisko[1] zawiera dobre praktyki dotyczące wypełniania obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[2] (dalej: ustawa), związanych m.in. z czynnościami jakie instytucje obowiązane, podlegające nadzorowi Komisji Nadzoru Finansowego (KNF), czyli podmioty nadzorowane, powinny podjąć:

- podczas wdrażania lub przeglądu stosowanych środków bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 pkt 1–3 ustawy, oraz w celu wypełnienia obowiązków wynikających z dyspozycji art. 37 ustawy w odniesieniu do nawiązywania stosunków gospodarczych z nowymi klientami bez ich fizycznej obecności;
- w przypadku korzystania z usług podmiotów trzecich zgodnie z przepisami prawa krajowego.

Praktyki te powinny znaleźć zastosowanie w bieżącej działalności podmiotów nadzorowanych, wykorzystujących metody nawiązywania stosunków gospodarczych lub przeprowadzania transakcji okazjonalnych (o których mowa w art. 35 ust. 1 pkt 2 i 3 ustawy) bez fizycznej obecności klienta, w celu zapewnienia zgodności z przepisami prawa w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (AML/CFT)[3].

Stanowisko[4] odnosi się również do polityk (strategii), systemu kontroli wewnętrznej i nadzoru wewnętrznego oraz procedur, jakie podmioty nadzorowane powinny wprowadzić

---

[1] Stanowisko uwzględnia Wytyczne EBA dotyczące wykorzystania rozwiązań w zakresie zdalnego nawiązywania relacji z klientami na podstawie art. 13 ust. 1 dyrektywy (UE) 2015/849 (EBA/GL/2022/15 z dnia 22 listopada 2022 r.), wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/20101, w odniesieniu do przepisów prawa polskiego i ram regulacyjnych dotyczących zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

[2] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124).

[3] Anti Money Laundering/Counter Financing of Terrorism

[4] Wydanie tego stanowiska nie uchyla oraz nie zmienia Stanowiska UKNF dotyczącego identyfikacji klienta i weryfikacji jego tożsamości w bankach oraz oddziałach instytucji kredytowych w oparciu o metodę wideoweryfikacji, opublikowanego 5 czerwca 2019 r. oraz Stanowiska Urzędu Komisji Nadzoru Finansowego dotyczącego identyfikacji klienta instytucjonalnego i weryfikacji jego tożsamości w sektorze finansowym podlegającym nadzorowi Komisji Nadzoru Finansowego w oparciu o metodę wideoweryfikacji, opublikowanego

w przypadku zdalnego stosowania środków bezpieczeństwa finansowego wobec klienta. Zgodnie z podejściem opartym na ryzyku, muszą być one proporcjonalne do specyfiki, wielkości i skali działalności podmiotów nadzorowanych.

W zakresie zarówno wdrożenia, jak i funkcjonowania modelu identyfikacji oraz weryfikacji tożsamości klientów w oparciu o rozwiązania technologiczne, mają zastosowanie standardy zawarte w odpowiednich rekomendacjach oraz wytycznych KNF dotyczących obszaru IT (odnoszących się do zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego), jak np.:

- Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach;
- Rekomendacja D-SKOK dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w spółdzielczych kasach oszczędnościowo-kredytowych;
- Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej publicznej lub hybrydowej.

Zgodnie z ustawą instytucje obowiązane (w tym przypadku podmioty nadzorowane) mają obowiązek stosowania środków bezpieczeństwa finansowego, w tym m.in. przeprowadzania identyfikacji klienta oraz weryfikacji jego tożsamości. Ich zastosowanie musi być poprzedzone rozpoznaniem ryzyka prania pieniędzy oraz finansowania terroryzmu związanego ze stosunkami gospodarczymi lub z transakcją okazjonalną oraz oceną poziomu tego ryzyka. Obowiązek ten dotyczy rozpoznania konkretnego profilu klienta oraz nadania mu kategorii ryzyka prania pieniędzy oraz finansowania terroryzmu związanego z danym stosunkiem gospodarczym lub transakcją okazjonalną oraz oceny jego poziomu. Ocena ta jest niezbędnym etapem poprzedzającym zastosowanie względem klienta środków bezpieczeństwa finansowego, proporcjonalnych do ryzyka prania pieniędzy, jakie dany klient generuje[5].

Oznacza to, że to na podmiotach nadzorowanych ciąży wymóg oszacowania poziomu ryzyka, w tym ustalenia profilu ryzyka klienta, wynikającego m.in. z rodzaju prowadzonej działalności gospodarczej, obszaru geograficznego, itd. Podmiot nadzorowany dokonuje identyfikacji poziomu ryzyka, profilu ryzyka klienta oraz oceny tego ryzyka, również wtedy, gdy nawiązywanie albo utrzymywanie stosunków gospodarczych następuje bez fizycznej obecności klienta. Dobór środków bezpieczeństwa finansowego oraz to z jaką intensywnością podmiot nadzorowany je zastosuje, zależy od zidentyfikowanego przez niego poziomu ryzyka.

---

3 marca 2022 r. (dalej: stanowiska UKNF dot. wideoweryfikacji), jak również pisma Zastępcy Przewodniczącego KNF z 17 lutego 2023 r. skierowanego do dostawców usług płatniczych w sprawie nieautoryzowanych transakcji.

[5] Art. 33 ust. 1, 2 i 4 oraz art. 34 ust. 1 pkt 1 ustawy.

Sytuacje, w których podmioty nadzorowane stosują środki bezpieczeństwa finansowego zostały wskazane w art. 35 ustawy i dotyczą m.in. nawiązywania stosunków gospodarczych oraz przeprowadzania transakcji okazjonalnej.

Jednym ze środków bezpieczeństwa finansowego, jakie podmiot nadzorowany ma obowiązek stosować, jest weryfikacja tożsamości (tj. dokonanie potwierdzenia ustalonych danych identyfikacyjnych):

- klienta;
- osoby upoważnionej/osób upoważnionych do działania w imieniu klienta oraz
- beneficjenta rzeczywistego/beneficjentów rzeczywistych, w przypadku których weryfikacja nie może polegać jedynie na sprawdzeniu informacji zawartych w Centralnym Rejestrze Beneficjentów Rzeczywistych lub rejestrze, o którym mowa w art. 30 lub art. 31 dyrektywy 2015/849, prowadzonym we właściwym państwie członkowskim (art. 37 ust. 3 ustawy).

Zgodnie z art. 37 ust. 1 ustawy do weryfikacji tożsamości niezbędne są:

- dokument stwierdzający tożsamość osoby fizycznej;
- dokument zawierający aktualne dane z wyciągu z właściwego rejestru;
- inne dokumenty, dane lub informacje pochodzące z wiarygodnego i niezależnego źródła, w tym, o ile są dostępne, ze środków identyfikacji elektronicznej lub z odpowiednich usług zaufania określonych w rozporządzeniu (UE) 910/2014[6].

W myśl art. 43 ust. 1 ustawy instytucje obowiązane (w tym przypadku podmioty nadzorowane) stosują wzmożone środki bezpieczeństwa finansowego m.in. w przypadkach wyższego ryzyka prania pieniędzy lub finansowania terroryzmu. Wskazany w art. 43 ust. 2 ustawy katalog okoliczności mogących świadczyć o wyższym ryzyku prania pieniędzy oraz finansowania terroryzmu (ML/FT) ma charakter otwarty. Oznacza to, że nie określono w nim w wyczerpujący sposób wszystkich przypadków, z którymi potencjalnie może wiązać się wyższe ryzyko. Ustawodawca nie określa przy tym katalogu wzmożonych środków bezpieczeństwa finansowego. Oznacza to, że zgodnie z wymogiem art. 33 ust. 4 ustawy to podmiot nadzorowany zobowiązany jest do utworzenia takiego katalogu. Do decyzji podmiotu nadzorowanego należy określenie, jakie wzmożone środki bezpieczeństwa finansowego zastosuje w konkretnym przypadku, na podstawie ustalonego dla danego rodzaju klienta poziomu ryzyka oraz na podstawie przyjętych procedur wewnętrznych.

W przypadku braku możliwości wykorzystania środków identyfikacji elektronicznej oraz usług zaufania (wg rozporządzenia (UE) 910/2014), podmiot nadzorowany powinien rozważyć zastosowanie – zgodnie z art. 43 ust. 1 w związku z ust. 2 pkt 7

[6] Rozporządzenie 910/2014 Parlamentu Europejskiego i Rady (UE) z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE (Dz. Urz. L 257 z 28.08.2014 r.).

ustawy – wzmożonych środków bezpieczeństwa finansowego. Należy przy tym uwzględnić dyspozycję art. 43 ust. 1 (w związku z ust. 2 pkt 9 ustawy) dotyczącą objęcia stosunkami gospodarczymi lub transakcjami nowych produktów lub usług albo oferowania produktów lub usług, przy wykorzystaniu nowych kanałów dystrybucji lub nowych rozwiązań technologicznych.

Tak określone normy wymagają ustalenia przez podmiot nadzorowany, jakimi dokumentami, danymi oraz informacjami (tj. materiałami weryfikacyjnymi) będzie się on posługiwać w celu weryfikacji (w rozumieniu ustawy) tożsamości klienta lub osoby upoważnionej do jego reprezentowania. Podmiot nadzorowany powinien także ustalić, jakie sposoby uzyskiwania dostępu do materiałów weryfikacyjnych będzie stosować. Oznacza to, że po dokonaniu oceny ryzyka, to podmiot nadzorowany ostatecznie decyduje o liczbie, rodzaju, zakresie i intensywności stosowania wzmożonych środków bezpieczeństwa finansowego (mitygantach ryzyka) w celu ograniczenia ryzyka błędnej weryfikacji klienta, stanowiących przy tym jeden z czynników dodatkowej oceny wiarygodności klienta.

Jednocześnie, zgodnie z dobrymi praktykami opisanymi w tym stanowisku UKNF, zakres stosowania tego rodzaju wzmożonych środków bezpieczeństwa powinien być odzwierciedlony w regulacjach wewnętrznych podmiotu nadzorowanego.

Procedury wewnętrzne dotyczące nawiązywania relacji z klientami bez ich fizycznej obecności

Podmioty nadzorowane, zgodnie z art. 50 ust. 1 ustawy, powinny wprowadzić oraz na bieżąco weryfikować i aktualizować polityki (strategie) oraz procedury, na podstawie których będą stosować środki bezpieczeństwa finansowego, o których mowa w art. 34 ust. 1 pkt 1–3 ustawy. Powinny także wypełniać obowiązki wskazane w art. 37 ustawy podczas nawiązywania relacji z klientami bez ich fizycznej obecności. Dokumenty te powinny uwzględniać ocenę poziomu ryzyka i zawierać co najmniej:

- opis rozwiązania przyjętego przez podmioty nadzorowane w celu gromadzenia, weryfikowania i rejestrowania informacji w całym procesie zdalnego nawiązywania relacji z klientami, ze szczególnym uwzględnieniem charakterystyki i sposobu działania tego rozwiązania;
- opis sytuacji, w których można zastosować rozwiązanie w zakresie zdalnego nawiązywania relacji z klientami, z uwzględnieniem zidentyfikowanych i ocenionych czynników ryzyka, obejmujących ryzyko dotyczące klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów dostaw, które kwalifikują się do zdalnego nawiązywania relacji z klientami;

- uwzględnienie w całościowej ocenie ryzyka instytucji możliwości zdalnego onboardingu, jako nieodłącznego czynnika ryzyka dotyczącego kanałów dystrybucji, mającego wpływ na końcową ocenę instytucji[7];
- określenie, które czynności mają być w pełni zautomatyzowane, a które wymagają ingerencji lub nadzoru pracownika podmiotu nadzorowanego;
- mechanizmy kontrolne wprowadzone w celu zapewnienia, aby pierwsza transakcja z nowym klientem została zrealizowana dopiero po zastosowaniu wszystkich koniecznych środków bezpieczeństwa finansowego wobec tego klienta;
- wymóg systematycznych szkoleń mających na celu podniesienie poziomu świadomości pracowników w zakresie omawianym w tym stanowisku oraz programy tych szkoleń, których celem jest przekazanie aktualnej wiedzy.

Polityki (strategie) i procedury wdrożone w tym zakresie, powinny umożliwić podmiotom nadzorowanym zapewnienie zgodności z zasadami określonymi w tym stanowisku[8].

Zarządzanie w ramach procesu nawiązywania relacji z klientami bez ich fizycznej obecności

Niezależnie od wymogów określonych w dziale „Rola i obowiązki AMLRO[9]" stanowiska UKNF dotyczącego AMLRO[10], powinien on – zapewnić skuteczne wdrażanie wskazanych w tym opracowaniu dokumentów dotyczących zdalnego nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnych, regularnie poddawać je przeglądowi i w razie potrzeby aktualizować. Powinno to odbywać się w ramach ogólnych zadań ALMRO w zakresie przygotowywania polityk (strategii) i procedur w celu spełnienia obowiązków wynikających z ustawy.

Organ zarządzający podmiotu nadzorowanego powinien zatwierdzać polityki (strategie) i procedury nawiązywania relacji z klientami oraz przeprowadzania transakcji okazjonalnych bez ich fizycznej obecności oraz nadzorować ich prawidłowe wdrażanie.

[7] Zgodnie ze Stanowiskiem UKNF dotyczącym oceny ryzyka instytucji obowiązanej, opublikowanym 15 kwietnia 2020 r.

[8] Wymogi odnośnie procedur dotyczących zdalnego nawiązania relacji oraz przeprowadzania transakcji okazjonalnych opisano szczegółowo w Stanowiskach UKNF dot. wideoweryfikacji.

[9] Według art. 8 ustawy jest to pracownik zajmujący kierownicze stanowisko, odpowiedzialny w podmiocie nadzorowanym za wykonanie obowiązków ustawowych.

[10] Stanowisko UKNF dotyczące AMLRO, opublikowane 1 grudnia 2022 r.

Analiza i ocena poprzedzająca wdrożenie omawianego rozwiązania

Przyjęcie nowego rozwiązania w zakresie nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnej bez ich fizycznej obecności powinno być poprzedzone analizą i oceną ryzyka. Należy wziąć pod uwagę m.in. model funkcjonowania podmiotu nadzorowanego, możliwe do zastosowania technologie i dostosowane do nich mechanizmy kontrolne zapewniające odpowiedni poziom bezpieczeństwa. Dotyczy to w szczególności mitygowania ryzyk związanych z nieprawidłową identyfikacją i weryfikacją tożsamości klienta lub osoby upoważnionej do działania w jego imieniu (np. ryzyka kradzieży tożsamości). Dotyczy to także ryzyk odnoszących się do wiarygodności materiałów weryfikacyjnych[11].

Podmioty nadzorowane powinny określić w swoich politykach (strategiach) i procedurach zakres, etapy i wymogi dotyczące udokumentowania analizy i oceny poprzedzającej wdrożenie, które powinny obejmować co najmniej:

a) ocenę adekwatności rozwiązania pod względem kompletności i rzetelności gromadzonych danych i dokumentów, a także wiarygodności i niezależności źródeł informacji wykorzystywanych w ramach danego rozwiązania;
b) ocenę wpływu stosowania omawianego rozwiązania na ogólne ryzyko działalności podmiotu nadzorowanego, w tym ryzyko: ML/FT, operacyjne, reputacyjne, prawne;
c) określenie możliwych środków ograniczających ryzyko, a także określenie działań naprawczych w odniesieniu do każdego rodzaju ryzyka zidentyfikowanego w toku analizy i oceny w przypadku jego materializacji;
d) mechanizmy kontrolne i sposoby testowania, służące ocenie ryzyka nadużyć finansowych, w tym ryzyka oszustw opartych na kradzieży tożsamości oraz innych rodzajów ryzyka związanego z technologią informacyjno-komunikacyjną (ICT)[12] i bezpieczeństwem informacji;
e) zasady kompleksowego badania sposobu funkcjonowania rozwiązania, tj. badania ukierunkowanego na klientów, produkty i usługi, o których mowa w polityce (strategii) i procedurach dotyczących zdalnego nawiązywania relacji z klientami.

Podmioty nadzorowane mogą uznać wymogi określone w pkt a), d) i e) za spełnione, jeżeli w ramach danego rozwiązania zastosowano jedno z poniższych kryteriów:

[11] Szczegółowe aspekty analizy ryzyka w odniesieniu do zdalnego nawiązania relacji z klientem oraz przeprowadzenia transakcji okazjonalnej opisano w stanowiskach UKNF dot. wideoweryfikacji.

[12] ICT (information and communication technologies), nazywane zamiennie technologiami informacyjno-telekomunikacyjnymi, teleinformatycznymi lub technikami informacyjnymi - oznacza zbiór technologii służących do przetwarzania, gromadzenia i przesyłania informacji w formie elektronicznej.

- systemy identyfikacji elektronicznej były notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniają wymogi „średniego" lub „wysokiego" poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;
- odpowiednie kwalifikowane usługi zaufania spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcji 3 tego rozporządzenia.

Podmioty nadzorowane powinny udokumentować:

- przeprowadzenie analizy i oceny przed wdrożeniem rozwiązania w zakresie zdalnego nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnej;
- rezultaty i wnioski ze swojej oceny;
- wyjaśnienia dotyczące tego w jaki sposób stosowanie danego rozwiązania jest odpowiednie w świetle ryzyka ML/FT, zidentyfikowanego w odniesieniu do rodzajów klientów, usług, obszaru geograficznego i produktów objętych zakresem rozwiązania.

Ponadto podmioty nadzorowane powinny być w stanie udokumentować na żądanie organu informacji finansowej oraz organu nadzoru przeprowadzenie analizy i oceny przed wdrożeniem rozwiązania w zakresie zdalnego nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnej, rezultaty i wnioski ze swojej oceny, jak również wyjaśnić, w jaki sposób stosowanie danego rozwiązania jest odpowiednie w świetle ryzyka ML/FT, zidentyfikowanego w odniesieniu do rodzajów klientów, usług, obszaru geograficznego i produktów objętych zakresem rozwiązania.

Rozpoczęcie korzystania z omawianego rozwiązania powinno nastąpić dopiero po upewnieniu się, że może ono zostać włączone do całego systemu kontroli wewnętrznej i systemu informacji zarządczej podmiotu nadzorowanego. Umożliwi to odpowiednie zarządzanie ryzykiem ML/FT, wynikającym z zastosowania rozwiązania w zakresie zdalnego nawiązywania relacji z klientami.

Bieżące monitorowanie omawianego rozwiązania

Podmioty nadzorowane powinny na bieżąco monitorować rozwiązanie w zakresie nawiązywania relacji z klientami oraz przeprowadzania transakcji okazjonalnej bez ich fizycznej obecności, aby zapewnić jego funkcjonowanie zgodnie z założonymi celami i oczekiwaniami. Powinny one wprowadzać i aktualizować swoje polityki (strategie) i procedury co najmniej w zakresie:

- czynności, jakie podejmą w celu bieżącego zapewnienia jakości, aktualności, kompletności, dokładności i adekwatności danych zgromadzonych w trakcie zdalnego nawiązywania relacji z klientami oraz przeprowadzania transakcji okazjonalnej. Czynności te powinny być proporcjonalne do poziomu ryzyka prania pieniędzy oraz finansowania terroryzmu, na jakie narażony jest podmiot nadzorowany;

- zakresu i częstotliwości okresowego przeglądu danych;
- okoliczności, które wymagają przeprowadzenia przeglądu doraźnego, w tym dotyczących co najmniej:
  - zmian w poziomie narażenia podmiotu nadzorowanego na ryzyko ML/FT,
  - słabości w funkcjonowaniu rozwiązań zidentyfikowanych w trakcie jego monitorowania, działań podejmowanych w ramach kontroli wewnętrznej lub czynności organu informacji finansowej oraz organu nadzoru,
  - znaczącego wzrostu liczby przypadków usiłowania popełnienia oszustwa lub innego przestępstwa,
  - zmian w zakresie przepisów prawa lub ram regulacyjnych.

Procedury i procesy powinny określać proces działań naprawczych na wypadek materializacji ryzyka lub na wypadek wykrycia błędów, które mają wpływ na wydajność i skuteczność rozwiązania w zakresie zdalnego nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnych. Działania te powinny obejmować co najmniej:

- przegląd wszystkich stosunków gospodarczych, których to dotyczy, w celu ustalenia, czy podmioty nadzorowane podjęły konieczne środki bezpieczeństwa finansowego wobec klienta. Dokonanie takiego przeglądu powinno następować po ustaleniu priorytetów w zależności od poziomu ryzyka prania pieniędzy lub finansowania terroryzmu;
- ocenę uwzględniającą informacje uzyskane w wyniku przeprowadzonego przeglądu, czy dany stosunek gospodarczy powinien:
  - podlegać wzmożonym środkom bezpieczeństwa finansowego (dodatkowym mitygantom ryzyka),
  - podlegać ograniczeniom[13], jak np. limit liczby i kwot transakcji, w przypadkach dopuszczalnych na mocy przepisów prawa,
  - zostać rozwiązany,
  - w zakresie transakcji – zgłoszony do Generalnego Inspektora Informacji Finansowej w trybie przewidzianym w ustawie,
  - zostać przeklasyfikowany do innej (np. wyższej) kategorii ryzyka.

Podmioty nadzorowane powinny dążyć do najskuteczniejszego sposobu monitorowania bieżącej adekwatności i niezawodności rozwiązań w zakresie zdalnego nawiązywania relacji z klientami. Należy rozważyć zastosowanie co najmniej jednego z następujących środków (proporcjonalnych do charakteru i skali działalności):

- testowania pionowego i poziomego;
- automatycznych alertów (ostrzeżeń) oraz powiadomień o krytycznym znaczeniu;

[13] Ograniczenia podmiotowe i przedmiotowe w zakresie stosunków gospodarczych i przeprowadzanych transakcji opisano w Stanowiskach UKNF dot. wideoweryfikacji.

- okresowej sprawozdawczości w tym zakresie;
- przeglądów manualnych.

Ma to również zastosowanie w przypadku, gdy wykorzystywane są w pełni zautomatyzowane rozwiązania w zakresie nawiązywania relacji z klientami, które są w dużym stopniu zależne od automatycznie funkcjonujących algorytmów i prowadzone bez udziału pracownika lub przy jego niewielkiej ingerencji.

Podmioty nadzorowane powinny być w stanie wykazać organowi informacji finansowej oraz organowi nadzoru, sposób i zakres przeprowadzonych przeglądów, a także podjęte działania naprawcze w celu wyeliminowania wszelkich nieprawidłowości i uchybień stwierdzonych w całym okresie funkcjonowania rozwiązania w omawianym zakresie.

Identyfikacja klienta, osoby upoważnionej i beneficjenta rzeczywistego[14]

Podmioty nadzorowane powinny określić rodzaje dokumentów niezbędnych do zidentyfikowania klienta, osoby upoważnionej i beneficjenta rzeczywistego.
Należy zapewnić, aby:

- informacje uzyskane za pośrednictwem rozwiązania w zakresie zdalnego nawiązywania relacji z klientami były aktualne i spełniały wymogi obowiązujących norm prawnych i regulacyjnych dotyczących zastosowania środków bezpieczeństwa finansowego wobec klienta;
- wszelkie zapisy elektroniczne (obrazy, nagrania audio i wideo, dane) były rejestrowane w formacie czytelnym i odpowiedniej jakości, tak aby klient był jednoznacznie rozpoznawalny;
- procesu identyfikacji nie kontynuowano w przypadku wykrycia usterek technicznych lub nieoczekiwanych przerw w połączeniu.

Podmioty nadzorowane mogą uznać wymienione wymogi jako spełnione, jeżeli w ramach danego rozwiązania zastosowano jedno z poniższych kryteriów:

- systemy identyfikacji elektronicznej były notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniają wymogi „średniego” lub „wysokiego” poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;
- odpowiednie kwalifikowane usługi zaufania spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcji 3 tego rozporządzenia.

Podmiot nadzorowany powinien, zgodnie z dyspozycją art. 49 ustawy, w bezpieczny sposób przechowywać, archiwizować i opatrzyć znacznikiem czasu dokumenty i informacje zgromadzone podczas procesu zdalnej identyfikacji w celu udokumentowania zastosowanych

[14] Identyfikację klienta, osoby upoważnionej i beneficjenta rzeczywistego opisano szczegółowo w Stanowiskach UKNF dot. wideoweryfikacji.

środków bezpieczeństwa finansowego (wg art. 34 ust. 3 ustawy). Treść przechowywanych zapisów elektronicznych, w tym obrazów, nagrań audio i wideo oraz danych, powinna być dostępna w czytelnym formacie i umożliwiać kontrolę ex post.

Podmioty nadzorowane powinny określić w swoich regulacjach[15] zakres informacji niezbędnych w procesie zdalnego nawiązania relacji, zgodnie z art. 34 ust. 1 pkt 1-3 i ust. 2 ustawy oraz art. 36 ustawy. Ponadto należy określić, jakie informacje:

- wprowadzane są manualnie przez klienta;
- pobierane są automatycznie z dokumentacji dostarczonej przez klienta;
- gromadzone są z wykorzystaniem innych źródeł wewnętrznych lub zewnętrznych.

Podmioty nadzorowane powinny wdrożyć odpowiednie mechanizmy kontrolne zapewniające wiarygodność pobieranych automatycznie informacji. W tym zakresie niezbędne jest stosowanie środków kontroli w celu przeciwdziałania zagrożeniom takim, jak ukrywanie lokalizacji urządzenia klienta poprzez podstawianie fałszywych adresów IP lub wykorzystywanie wirtualnych sieci prywatnych (VPN). Należy też zwrócić uwagę na ryzyka związane z automatycznym pobieraniem danych.

Jeśli podmioty nadzorowane nawiązują relacje z klientami instytucjonalnymi[16] zdalnie, to powinny one określić w polityce (strategii) i procedurach, z jakimi kategoriami tego rodzaju klientów będą w ten sposób nawiązywać relacje. Należy uwzględnić poziom ryzyka ML/FT oraz stopień ingerencji pracownika, wymagany do zatwierdzenia danych identyfikacyjnych.

Podmioty nadzorowane powinny zapewnić, aby rozwiązanie w zakresie zdalnego nawiązywania relacji lub zdalnego przeprowadzania transakcji okazjonalnej z klientami instytucjonalnymi posiadało funkcje umożliwiające zgromadzenie:

- wszelkich istotnych danych i dokumentów służących identyfikacji i weryfikacji takiego klienta;
- wszystkich istotnych danych i dokumentów służących zweryfikowaniu, czy osoba upoważniona do działania w imieniu klienta posiada prawidłowe umocowanie do tego działania;
- informacji w zakresie identyfikacji i weryfikacji beneficjentów rzeczywistych.

W odniesieniu do osoby upoważnionej do działania w imieniu klienta należy stosować proces identyfikacji obejmujący ustalenie danych, o których mowa w art. 36 ust. 1 pkt 1 lit. a-d ustawy. Natomiast wobec osoby reprezentującej osobę prawną lub jednostkę organizacyjną

[15] Zgodnie z Działem tego Stanowiska dotyczącym procedur wewnętrznych.
[16] Klient instytucjonalny rozumiany jest jako osoba fizyczna prowadząca działalność gospodarczą, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.

nieposiadającą osobowości prawnej – ustalenie danych, o których mowa w art. 36 ust. 1 pkt 1 lit. a i c ustawy.

Ocena stosunków gospodarczych

W zakresie oceny stosunków gospodarczych podmioty nadzorowane, stosownie do sytuacji, uzyskują informacje na temat celu i zamierzonego charakteru stosunku gospodarczego. Należy zrealizować określone w tym zakresie działania przed końcem procesu zdalnego nawiązania stosunków gospodarczych z klientem.

Autentyczność i integralność dokumentów[17]

W przypadku gdy podmioty nadzorowane akceptują kopię (skan) oryginalnego dokumentu (nie badając dokumentu oryginalnego), powinny podjąć odpowiednie czynności mające na celu upewnienie się, że kopia jest wiarygodna. Należy wówczas ustalić co najmniej:

- czy kopia zawiera zabezpieczenia zawarte w oryginalnym dokumencie i czy cechy dokumentu oryginalnego, którego kopię okazano, są ważne i dopuszczalne zgodnie z wymogami prawa krajowego; w szczególności dotyczy to rodzaju i wielkości znaków oraz struktury dokumentu, czego dokonuje się poprzez porównanie ich z oficjalnymi bazami danych, takimi jak m.in. PRADO[18];
- czy dane osobowe zostały zmienione lub w inny sposób naruszone, lub czy zdjęcie klienta zawarte w dokumencie nie zostało zamienione;
- czy zachowano integralność algorytmu wykorzystywanego do wygenerowania niepowtarzalnego numeru identyfikacyjnego oryginalnego dokumentu, w przypadku gdy dokument urzędowy posiada pole przeznaczone do odczytu maszynowego (strefa MRZ)[19];
- czy przekazana kopia jest odpowiedniej jakości i rozdzielczości, aby zapewnić jednoznaczność istotnych informacji;
- czy przekazana kopia nie została wyświetlona na ekranie na podstawie fotografii lub skanu oryginalnego dokumentu tożsamości.

W przypadku gdy podmioty nadzorowane korzystają z funkcji automatycznego odczytywania informacji z dokumentów, takich jak algorytmy optycznego rozpoznawania znaków (OCR) lub weryfikacji strefy przeznaczonej do odczytu maszynowego (strefa MRZ), powinny

[17] Dobre praktyki w tym zakresie opisane są szczegółowo w Stanowiskach UKNF dot. wideoweryfikacji.

[18] Publiczny rejestr *on-line* autentycznych dokumentów tożsamości i dokumentów podróży.

[19] Strefa MRZ - obszar na dokumencie, zawierający zapisane czcionką do odczytu maszynowego (najczęściej OCR-B) dane zawarte w danym dokumencie w sposób skrócony.

one podjąć czynności niezbędne do zapewnienia, aby narzędzia te rejestrowały informacje w sposób niezawodny i spójny.

Jeżeli urządzenie, z którego korzystają klienci w celu potwierdzenia swojej tożsamości, umożliwia gromadzenie odpowiednich danych (np. danych znajdujących się na chipie krajowego dowodu tożsamości), a dostęp do tych danych jest technicznie możliwy dla podmiotów nadzorowanych, powinny one 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.

Ponadto należy, w miarę możliwości, zweryfikować zawarte w dokumencie urzędowym zabezpieczenia stanowiące dowód ich autentyczności, takie jak hologramy, o ile dany dokument zawiera takie zabezpieczenia.

Podmioty nadzorowane powinny określić w swoich politykach (strategiach) i procedurach, w jaki sposób dostosują swoje wymogi dokumentacyjne do celów przeciwdziałania wykluczeniu społecznemu pod względem finansowym. Jeśli akceptowane są mniej wiarygodne lub niestandardowe formy dokumentacji, to podmioty nadzorowane powinny stosować wzmożone środki bezpieczeństwa finansowego (dodatkowe mityganty ryzyka) lub zwiększoną ingerencję pracownika. Jest to kluczowe dla zapewnienia kontroli ryzyka prania pieniędzy lub finansowania terroryzmu związanego z danym stosunkiem gospodarczym[20].

Weryfikacja tożsamości klienta w ramach procesu nawiązywania relacji z klientami bez ich fizycznej obecności[21]

Podmioty nadzorowane powinny określić rodzaje dokumentów, danych lub informacji, które będą wykorzystane do weryfikacji tożsamości klienta, osoby upoważnionej i beneficjenta rzeczywistego, a także sposób, w jaki informacje te będą weryfikowane.
Rozwiązania stosowane przez podmioty nadzorowane, w zakresie nawiązywania relacji z klientami bez ich fizycznej obecności, powinny umożliwiać w ramach procesu weryfikacji tożsamości co najmniej:

- stwierdzenie zgodności uzyskanych informacji dotyczących osoby fizycznej z przedstawioną dokumentacją;

[20] Według ust. 37 Wytycznych EBA EBA/GL/2022/15: „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”.
[21] Dobre praktyki w tym zakresie zostały opisane szczegółowo w Stanowiskach UKNF dot. wideoweryfikacji.

- w przypadku klienta instytucjonalnego – ustalenie, że jest on ujęty w rejestrach publicznych;
- ustalenie, że osoba upoważniona do działania w imieniu klienta jest do tego odpowiednio umocowana.

W przypadku wykorzystywania danych biometrycznych do weryfikacji tożsamości klienta, należy upewnić się, że są one wystarczająco unikalne, aby można je było jednoznacznie powiązać z jedną osobą fizyczną. Podmiot nadzorowany powinien stosować silne i wiarygodne algorytmy w celu weryfikacji zgodności danych biometrycznych podanych w przedstawionym dokumencie tożsamości z wyglądem klienta, z którym nawiązywana jest relacja. W sytuacjach, w których rozwiązanie to nie zapewnia wymaganego poziomu zgodności, należy zastosować dodatkowe środki kontroli (mityganty ryzyka).

W sytuacjach, w których jakość lub wiarygodność przedstawionych materiałów weryfikacyjnych jest niewystarczająca, należy przerwać proces zdalnego nawiązywania relacji z klientem i rozpocząć go ponownie lub przekierować klienta do weryfikacji bezpośredniej.

Standardowym środkiem kontroli stosowanym w praktyce działania podmiotów nadzorowanych w przypadku jakichkolwiek wątpliwości powstałych w toku zdalnej identyfikacji i weryfikacji tożsamości klienta, powinno być nawiązanie relacji w trakcie bezpośredniej wizyty klienta w placówce podmiotu nadzorowanego lub wykorzystanie innego bezpiecznego kanału dystrybucji.

W przypadku gdy podmioty nadzorowane stosują rozwiązanie zdalnego nawiązywania relacji z klientami bez udziału pracownika, tj. gdy klient w procesie weryfikacji nie wchodzi w interakcję z pracownikiem, należy:

- zapewnić, aby wszelkie fotografie lub nagrania wideo były wykonywane w odpowiednich warunkach oświetleniowych, z wykorzystaniem przez klienta sprzętu zgodnego z określonymi wymogami oraz aby wymagana jakość fotografii lub nagrań była wystarczająca, w celu umożliwienia właściwej weryfikacji tożsamości klienta;
- zapewnić, aby wszelkie fotografie lub nagrania wideo zostały wykonane w toku procesu zdalnej weryfikacji (sesji komunikacyjnej);
- przeprowadzić weryfikację wykrywania aktywności klienta, w przypadku której od klienta wymaga się podjęcia konkretnych czynności. Weryfikacja ta ma służyć sprawdzeniu, czy klient jest obecny na sesji komunikacyjnej. Można też przeprowadzić weryfikację opierającą się na analizie otrzymanych danych i niewymagającą konkretnego działania ze strony klienta;
- zastosować silne i wiarygodne algorytmy w celu sprawdzenia, czy wykonane fotografie lub nagrania wideo są zgodne z obrazem pobranym z dokumentu tożsamości należącego do klienta.

W przypadku gdy podmioty nadzorowane stosują rozwiązania w zakresie zdalnego nawiązywania relacji z klientami pod nadzorem pracownika, tj. gdy klient w procesie weryfikacji wchodzi w interakcję z pracownikiem, podmioty nadzorowane powinny:

- zapewnić wystarczającą jakość obrazu i dźwięku, aby umożliwić właściwą weryfikację tożsamości klienta oraz stosowanie wiarygodnych systemów technicznych;
- zapewnić w procesie udział pracownika, który posiada wystarczającą wiedzę na temat obowiązujących przepisów w obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Poza tym powinien on znać aspekty bezpieczeństwa zdalnej weryfikacji. Pracownik powinien być wystarczająco przeszkolony, aby przewidywać celowe stosowanie technik manipulacji związanych ze zdalną weryfikacją oraz zapobiegać takiemu działaniu - wykrywać je i właściwie reagować w przypadku jego wystąpienia;
- 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 cech, które mogą wskazywać na podejrzane zachowanie podczas zdalnej weryfikacji.

W miarę możliwości podmioty nadzorowane powinny korzystać z takich rozwiązań w tym obszarze, które obejmują losową sekwencję czynności wykonywanych przez klienta na potrzeby weryfikacji. Ma to stanowić ochronę przed takimi zagrożeniami, jak stosowanie fałszywych tożsamości lub przymusu. Pracownika odpowiedzialnego za proces zdalnej weryfikacji należy przydzielać, w miarę możliwości, w sposób losowy, aby uniknąć zmowy pomiędzy nim a klientem.

Podmioty nadzorowane mogą uznać wymienione wymogi jako spełnione, jeżeli w ramach danego rozwiązania zastosowano jedno z poniższych kryteriów:

- systemy identyfikacji elektronicznej były notyfikowane zgodnie z art. 9 rozporządzenia (UE) nr 910/2014 i spełniają wymogi „średniego" lub „wysokiego" poziomu bezpieczeństwa zgodnie z art. 8 tego rozporządzenia;
- odpowiednie kwalifikowane usługi zaufania spełniają wymogi rozporządzenia (UE) nr 910/2014, w szczególności rozdziału III sekcji 3 tego rozporządzenia.

Ponadto, jeżeli jest to współmierne do poziomu ryzyka ML/FT, związanego z danym stosunkiem gospodarczym, podmioty nadzorowane powinny stosować co najmniej jeden z dodatkowych mitygantów ryzyka w celu zwiększenia wiarygodności procesu weryfikacji. Takimi środkami bezpieczeństwa lub innymi środkami kontroli mogą być między innymi:

- dokonanie pierwszej płatności na rachunek płatniczy klienta w podmiocie nadzorowanym przeprowadzającym weryfikację tożsamości, z rachunku którego klient jest właścicielem lub współwłaścicielem. Przy czym rachunek ten powinien być 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. Nie należy jednak traktować ww. środka jako podstawowego lub jedynego sposobu weryfikowania tożsamości klienta. Należy pamiętać, że z uwagi na minimalny zakres danych dotyczących zleceniodawcy przelewu (zawartych w informacji przekazywanej wraz z przelewem), dane te mogą służyć jedynie pomocniczo do weryfikacji tożsamości klienta, przeprowadzonej na podstawie innych materiałów weryfikacyjnych;

- wysłanie klientowi wygenerowanego losowo hasła w celu potwierdzenia obecności podczas procesu zdalnej weryfikacji (sesji komunikacyjnej). Hasło powinno być kodem jednorazowego użytku, który należy zastosować w określonym czasie;
- pobranie danych biometrycznych i, jeśli to możliwe, porównanie ich z danymi zgromadzonymi w innych niezależnych i wiarygodnych źródłach;
- kontakt telefoniczny z klientem;
- wysłanie do klienta korespondencji bezpośredniej (zarówno elektronicznej – np. w toku sesji komunikacyjnej, jak i drogą pocztową).

Powierzenie podmiotowi trzeciemu działającemu w imieniu i na rzecz instytucji obowiązanej stosowania środków bezpieczeństwa finansowego dotyczących rozwiązań w zakresie nawiązywania relacji z klientami bez ich fizycznej obecności

W zakresie powierzenia przedmiotowych funkcji operacyjnych, zgodnego z przepisami prawa krajowego[22], podmioty nadzorowane powinny mieć na uwadze następujące kluczowe zasady:

- odpowiedzialność za przestrzeganie obowiązków ustawowych, zleconych na zewnątrz, spoczywa na podmiocie nadzorowanym;
- prawa i obowiązki podmiotu nadzorowanego oraz dostawcy usług powinny być w sposób jasny rozdzielone i określone w umowie sporządzonej na piśmie;
- podmiot nadzorowany jest odpowiedzialny za monitorowanie i kontrolowanie jakości świadczonych usług;
- w sytuacji outsourcingu realizowanego wewnątrz grupy, podmiot nadzorowany powinien zidentyfikować konflikty interesów, które mogłyby wyniknąć z umowy outsourcingu;
- outsourcing wewnątrz grupy powinien podlegać tym samym wymogom, co zlecanie zadań w ramach outsourcingu dostawcom usług spoza grupy;
- podmioty nadzorowane, przy zlecaniu dostawcy usług zadań operacyjnych, powinny m.in. zidentyfikować i ocenić rodzaje ryzyka związane z umową outsourcingu oraz uzasadnić decyzję o zleceniu zadania w ramach outsourcingu w świetle zamierzonych celów;
- AMLRO powinien:

[22] Zasady powierzenia stosowania środków bezpieczeństwa finansowego innemu podmiotowi działającemu w imieniu i na rzecz instytucji obowiązanej regulują art. 47 i art. 48 ustawy.

  - skutecznie monitorować działania dostawcy usług,
  - przeprowadzać regularną kontrolę przestrzegania przez dostawcę usług zobowiązań wynikających z umowy,
  - regularnie (w ramach potrzeb również doraźnie) składać organowi zarządzającemu sprawozdania z wykonania usług;
- zlecanie w ramach outsourcingu zadań związanych z AML/CFT dostawcom usług mającym siedzibę w państwach trzecich, powinno podlegać dodatkowym mechanizmom ograniczania ryzyka. Jest to wskazane w celu zapewnienia, aby outsourcing nie zwiększał ryzyka naruszenia przepisów prawa, nie powodował nieefektywnego wykonywania zleconych zadań, ani nie ograniczał zdolności właściwego organu do skutecznego wykonywania uprawnień nadzorczych wobec dostawcy usług. Nieakceptowane jest korzystanie przez podmioty nadzorowane z usług podmiotów trzecich mających siedzibę w państwach wysokiego ryzyka. Z tego zakazu mogą być wyłączone oddziały podmiotów obowiązanych mających siedzibę w UE i jednostki zależne z większościowym udziałem tych podmiotów, jeżeli w pełni stosują się do strategii i procedur obejmujących całą grupę.

Ponadto podmioty nadzorowane powinny:

- jednoznacznie określić w swoich regulacjach wewnętrznych, które funkcje i czynności związane ze zdalnym nawiązywaniem relacji z klientami będą realizowane przez same podmioty, a które przez podmioty trzecie (usługodawcę);
- zapewnić, aby wprowadzone przez podmioty trzecie wewnętrzne procesy i procedury zdalnego nawiązywania relacji z klientami i środki bezpieczeństwa finansowego stosowane wobec klienta oraz informacje i dane, które podmioty trzecie gromadzą w tym kontekście, były wystarczające i zgodne z wymogami określonymi w tym stanowisku;
- zapewnić wzmożone monitorowanie stosunków gospodarczych nawiązanych między klientem a podmiotem nadzorowanym, w celu minimalizacji ryzyka ML/FT wynikającego z procesu zdalnego nawiązywania relacji z klientami przeprowadzanego przez podmiot trzeci.

W przypadku gdy całość lub część procesu zdalnego nawiązywania relacji z klientami jest zlecana przez podmioty nadzorowane podmiotowi trzeciemu – powinny one stosować przed zawarciem umowy z usługodawcą i w trakcie jej trwania następujące środki:

- przeprowadzenie analizy i oceny w celu zapewnienia, aby usługodawca posiadał wystarczające wyposażenie, wiedzę i umiejętności do przeprowadzania procesu zdalnego nawiązywania relacji z klientami. Analizy mogą obejmować m.in. ocenę szkolenia pracowników, sprawności technologicznej i zarządzania danymi przez usługodawcę świadczącego usługi na zasadzie outsourcingu;
- zapewnienie, aby usługodawca skutecznie wdrażał politykę (strategię) i procedury podmiotu nadzorowanego dotyczące zdalnego nawiązywania relacji z klientami zgodnie

z umową outsourcingu oraz przestrzegał zapisów uwzględnionych w tych dokumentach. Można to osiągnąć dzięki regularnej sprawozdawczości, stałemu monitorowaniu, wizytom i kontroli na miejscu lub przeprowadzanym testom;

- zapewnienie, aby usługodawca informował podmioty nadzorowane o wszelkich proponowanych zmianach w procesie zdalnego nawiązywania relacji z klientami lub o wszelkich zmianach wprowadzonych w rozwiązaniu oferowanym przez takiego usługodawcę.

Zakres tych środków należy dostosować do poziomu ryzyka ML/FT.

W przypadku gdy zgodnie z zawartą umową usługodawca przechowuje dane klientów, w tym fotografie, filmy wideo i dokumenty, w trakcie procesu zdalnego nawiązywania relacji, podmioty nadzorowane powinny zapewnić, aby:

- gromadzono jedynie niezbędne dane klienta, przestrzegając ściśle określonego przepisami prawa okresu przechowywania (wg art. 49 ust. 1 pkt 1 ustawy);
- dostęp do danych był rejestrowany i ściśle ograniczony do uprawnionych osób;
- wdrożono odpowiednie mechanizmy kontrolne w celu zapewnienia ochrony przechowywanych danych.

Zarządzanie ryzykiem związanym z technologiami i bezpieczeństwem ICT

Podmioty nadzorowane powinny identyfikować ryzyko związane z technologiami i bezpieczeństwem ICT w odniesieniu do funkcjonowania procesu zdalnego nawiązywania relacji z klientami i przeprowadzania transakcji okazjonalnych. Powinny także zarządzać tym ryzykiem, również wówczas gdy korzystają z usług osób trzecich lub gdy usługa ta jest zlecana na zasadzie outsourcingu, w tym podmiotom należącym do grupy.

Biorąc pod uwagę poziom ryzyka, należy korzystać z bezpiecznych kanałów komunikacji z klientem podczas procesu zdalnego nawiązywania relacji i przeprowadzania transakcji okazjonalnych. Rozwiązania w tym zakresie powinny wykorzystywać bezpieczne protokoły i algorytmy kryptograficzne, zgodne z najlepszymi praktykami branżowymi, w celu zabezpieczenia poufności, autentyczności i integralności przekazywanych danych.

Podmioty nadzorowane 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 pkt 30 rozporządzenia (UE) nr 910/2014, lub certyfikatów uwierzytelniania witryn internetowych, o których mowa w art. 3 pkt 39 tego rozporządzenia. Należy również poinformować klienta o obowiązujących środkach bezpieczeństwa, które należy zastosować w celu zapewnienia bezpiecznego korzystania z systemu.

W przypadku gdy do realizacji procesu zdalnego nawiązywania relacji z klientami wykorzystywane jest urządzenie wielofunkcyjne, w stosownych przypadkach, do wykonania kodu oprogramowania po stronie klienta należy zastosować bezpieczne środowisko. W celu zapewnienia bezpieczeństwa i niezawodności kodu oprogramowania i zgromadzonych danych, należy wdrożyć dodatkowe środki bezpieczeństwa. Powinny one być odpowiednie do oceny ryzyka bezpieczeństwa określonej w wytycznych EUNB[23] w sprawie zarządzania ryzykiem związanym z technologiami i bezpieczeństwem ICT[24]. Ich wdrożenie powinno odbyć się bez uszczerbku dla innych standardów zawartych w przeznaczonych dla podmiotów nadzorowanych rekomendacjach i wytycznych KNF dotyczących obszaru IT (dotyczących zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego).

Korzystanie przez podmioty nadzorowane z usług zaufania i krajowych procesów identyfikacji, o których mowa w art. 13 ust. 1 lit. a) dyrektywy (UE) 2015/849

Podmioty nadzorowane mogą korzystać z odpowiednich usług zaufania i procesów identyfikacji elektronicznej regulowanych, uznanych, zatwierdzonych lub zaakceptowanych przez odpowiednie organy krajowe, o których mowa w art. 13 ust. 1 lit. a) dyrektywy (UE) 2015/849, w celu zapewnienia zgodności z tym stanowiskiem. Stosując takie rozwiązania należy ocenić w jakim stopniu dane rozwiązanie jest zgodne z tym stanowiskiem. Ponadto należy stosować środki niezbędne do ograniczenia wszelkich istotnych zagrożeń, które wynikają z zastosowania tych rozwiązań. Należy w szczególności wziąć pod uwagę, czy uwzględnione zostały następujące rodzaje ryzyka:

- ryzyko związane z uwierzytelnianiem – w tym przypadku podmioty nadzorowane powinny określić w politykach (strategiach) i procedurach szczególne środki ograniczania ryzyka, zwłaszcza w odniesieniu do ryzyka przestępstw połączonych z podszywaniem się pod inne osoby;
- ryzyko fałszywej tożsamości klienta;
- ryzyko utraty, kradzieży, zawieszenia, cofnięcia lub wygaśnięcia ważności dokumentu stwierdzającego tożsamość oraz czy w odpowiednich przypadkach korzystano z narzędzi służących do wykrywania i zapobiegania przestępstwom związanym z fałszywą tożsamością.

Mając na względzie istotny poziom ryzyka związanego ze zdalną identyfikacją i weryfikacją tożsamości klienta, w tym osób upoważnionych do jego reprezentowania, oczekuje się, że podmioty nadzorowane przez KNF, będą stosowały dobre praktyki związane z wykorzystaniem rozwiązań w zakresie zdalnego nawiązywania relacji z klientami.

[23] Europejski Urząd Nadzoru Bankowego.
[24] EBA/GL/2019/04.

Urząd Komisji Nadzoru Finansowego oczekuje, aby podmioty nadzorowane przeprowadziły analizę stopnia dostosowania do wymogów stanowiska oraz bez zbędnej zwłoki wprowadziły jego założenia do praktyki działania, odpowiednio zmieniając swoje regulacje wewnętrzne oraz funkcjonujące procesy, proporcjonalnie do skali, rodzaju i charakteru prowadzonej działalności.

Urząd Komisji Nadzoru Finansowego

ul. Piękna 20

00-549 Warszawa

www.knf.gov.pl