ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XL
2/2021

IDENTIFIKÁCIA A OVERENIE IDENTIFIKÁCIE KLIENTA NA DIAĽKU Z POHĽADU LEGALIZÁCIE PRÍJMOV Z TRESTNEJ ČINNOSTI A FINANCOVANIA TERORIZMU

JUDr. Yana Daudrikh, PhD.

Univerzita Komenského v Bratislave, Právnická fakulta
Katedra finančného práva
yana.daudrikh@flaw.uniba.sk

Identifikácia a overenie identifikácie klienta na diaľku z pohľadu legalizácie príjmov z trestnej činnosti a financovania terorizmu

Príspevok sa zameriava na analýzu spôsobu výkonu identifikácie a overenia identifikácie klienta použitím technologických prostriedkov umožňujúcich vykonávať identifikáciu klienta na diaľku. Súčasťou článku je bližšie rozpracovanie uplatnenia jednotlivých požiadaviek upravených v odporúčaniach FATF a V. AML smernici, s dôrazom na uplatnenie RBA prístupu a inštitútu plnenia tretích strán. Osobitne sa venujeme analýze výkonu identifikácie a overenia identifikácie klienta obsiahnutej v legislatíve Slovenskej republiky.

Identification and verification of remote client identification in terms of money laundering and terrorist financing

The paper focuses on the analysis of the method of identification and verification of client identification using technological means when performing client identification remotely. We also further elaborate on the application of individual requirements regulated in the recommendations of the FATF and the V. AML Directive, with emphasis on the application of the RBA approach and the institute of third-party reliance requirements. In particular, we analyze the performance of identification and verification of client identification contained in the legislation of the Slovak Republic.

Удаленная идентификация и аутентификация клиента с точки зрения легализации доходов, полученных преступным путем и финансированию терроризма

Статья посвящена анализу способа идентификации и аутентификации клиента с использованием технологических средств коммуникации, позволяющих осуществлять удаленную идентификацию клиента. В статье представлена подробная разработка применения индивидуальных требований, находящихся в рекомендациях ФАТФ и V. AML директивы, с акцентом на применение мер определения степени (уровня) риска клиента и облати передачи информации и документов. В частности, анализируется эффективность идентификации и проверки идентификации клиента, в соответствии с законодательством Словацкой Республики.

Kľúčové slová: identifikácia na diaľku, FATF, V. AML smernica, plnenie tretími stranami

Keywords: remote client identification, FATF, V. AML Directive, third-party reliance requirements

Ключевые слова: удаленная идентификация, ФАТФ, V. AML директива, передача информации и документов

Úvod

Identifikáciu klienta považujeme za jeden zo základných prvkov zameraných na zmiernenie rizika spojeného s legalizáciou príjmov z trestnej činnosti a financovaním terorizmu a s tým súvisiaceho vytvorenia rizikového profilu klienta. Ešte donedávna za jedinú najbezpečnejšiu formu identifikácie klienta bola považovaná výlučne forma tvárou v tvár.[1] Vo svete plurality finančných inštitúcií poskytujúcich viaceré produkty však bolo nevyhnutné zabezpečiť čo najmenej „rušivý“ prístup klientov k pre nich zaujímavým produktom. Práve pokročilý technologický vývoj a konkurenčný boj o klienta sa stali základom pre diskusiu na medzinárodnej úrovni o hľadaní nových možností vykonávania identifikácie klienta s použitím nových technológií.

V. AML smernica umožnila realizovať identifikáciu klienta na „online“ úrovni. Overenie identifikácie klienta sa realizuje pomocou použitia technických prostriedkov umožňujúcich bezpečnú identifikáciu na

[1] KYNCL, L.: Poznej svého klienta základní zásada finančního práva. Brno: Masarykova univerzita, Spisy Právnické fakulty Masarykovy univerzity. Řada teoretická sv. 433, 2012, s. 35 – 36.

diaľku.[2] Identifikácia na diaľku tak má za úlohu uľahčiť a zjednodušiť prístup klientom, respektíve potenciálnym klientom, k produktom ponúkaným finančnými inštitúciami.

Vo všeobecnosti predstavuje identifikácia zber údajov, ktoré zodpovedajú konkrétnej identite. V rámci identifikácie klient deklaruje svoju identitu. V tomto prípade môžeme hovoriť o realizácii vyhlásenia o identite klienta (*identity claim*).[3]

Identifikácia klienta sa realizuje v dvoch rovinách: prvotná identifikácia klienta a následné overovanie identifikácie. Identifikácia a overenie vzájomne súvisia, ale zároveň ide o samostatné procesy.[4]

Prvotnú identifikáciu klienta vykonáva povinná osoba ešte pred nadviazaním obchodného vzťahu s takýmito osobami.[5] V rámci prvotnej identifikácie sa realizuje zber a overenie získaných informácií pri prvom kontakte klienta s príslušnou inštitúciou. **Následná identifikácia klienta** prebieha počas uzatvárania obchodného vzťahu. Identifikácia klienta a overenie identifikácie sa uskutočňujú vždy v prípade, ak je hodnota obchodu najmenej 1000 eur.[6] V tomto prípade nepôjde o prvý kontakt s klientom, ale už o trvajúci obchodný vzťah, v rámci ktorého klient môže realizovať rôzne druhy finančných operácií (napríklad prevod finančných prostriedkov na bankový účet).

Overenie identifikácie predstavuje kontrolu údajov získaných od klienta. Overenie sa realizuje z dostupných zdrojov, napríklad z obchodného registra, webových stránok orgánov verejnej moci a pod.

1. Identifikácia klienta v súlade s odporúčaniami FATF

V súlade s FATF DI (Guidance on digital identity) (ďalej len „FATF DI“) sa za **úradnú totožnosť** (official identity) považuje špecifikácia konkrétnej fyzickej osoby, ktorá musí spĺňať nasledovné podmienky:[7]

---

[2] Bližšie k prostriedkom elektronickej identifikácie viď: Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

[3] ANDRAŠKO, J., HORVAT, M., MESARČÍK, M.: Vybrané kapitoly práva informačných technológií I. Bratislava : Právnická fakulta UK, 2019, s. 97.

[4] DE KOKER, L.: The FATF‘s customer identification framework: fit for purpose? In Journal of money laundering control, vol. 17, no. 3, 2014, p. 284.

[5] THE WOLFSBERG GROUP: WOLFSBERG ANTI-MONEY LAUNDERING PRINCIPLES FOR PRIVATE BANKING, 2012, P. 2.

[6] § 10 ods. 3 zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[7] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 18.

– identifikácia fyzickej osoby musí byť založená na presne definovaných vlastnostiach, teda konkrétnych atribútoch respektíve identifikátoroch, ktoré umožňujú zabezpečenie presnej identifikácie osoby z pomedzi ostatných subjektov;
– spôsob identifikácie fyzickej osoby musí byť uznaný a používaný v konkrétnom štáte na regulačné a iné účely.

Identifikácia fyzickej osoby sa realizuje na podklade **dokladu o totožnosti.**[8] Doklad o totožnosti predstavuje určitú formu dokumentu respektíve osvedčenia vydaného príslušnými orgánmi verejnej správy, obsahujúceho základné údaje fyzickej osoby, ktoré je možné použiť na účely identifikácie a overenie totožnosti subjektu.

Za základné **identifikačné údaje** je možné napríklad považovať meno, priezvisko, dátum a miesto narodenia, atď.

Forma predloženého dokladu sa môže líšiť v závislosti od činnosti orgánov verejnej správy v konkrétnom štáte; tak napríklad za doklad preukazujúci totožnosť sa môže považovať občiansky preukaz, zahraničný pas, vodičský preukaz, rodný list, atď. Vo viacerých krajinách doklad totožnosti obsahuje aj identifikačné číslo, ktoré sa používa ako univerzálne, respektíve na obmedzené účely (napr. identifikačné čísla daňových poplatníkov, vodičské preukazy, atď.).

Je zrejmé, že spoľahlivosť predloženého dokladu totožnosti sa bude líšiť v závislosti od krajiny.[9] V tomto prípade FATF, v súlade s metodikou vzájomného hodnotenia, výslovne nevyžaduje, aby hodnotitelia prešetrili spoľahlivosť konkrétnym štátom vydaných dokladov totožnosti.[10] Práve z tohto dôvodu je veľmi diskutabilné, či doklad totožnosti vydaný v tretích krajinách je možné považovať za spoľahlivý z hľadiska pravosti údajov v ňom uvedených.

Identifikácia sa považuje za **dokončenú**, keď sa získa dostatok informácií, aby inštitúcia mohla spoľahlivo zistiť, kto je jej klientom. Klient bude pravdepodobne klasifikovaný ako anonymný na účely FATF RN, ak povinná osoba získa nedostatočné množstvo informácií o klientovi.[11]

Vo všeobecnosti platí, že opakovanú identifikáciu klienta a následné overovanie identifikačných údajov nie je potrebné realizovať pri každej jednej transakcii. Pre povinnú osobu je preto smerodajná nepochyb-

[8] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 18.

[9] DE KOKER, L.: The FATF's customer identification framework: fit for purpose? In Journal of money laundering control, vol. 17, no. 3, 2014, p. 289.

[10] FATF: Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems. France; Paris, 2020.

[11] DE KOKER, L.: Anonymous clients, identified clients and the shades in between – Perspectives on the FATF AML/CFT standards and mobile banking, 2009, p. 1 – 17. Dostupné na: http://dx.doi.org/10.2139/ssrn.2634305 [cit. 21.08.2021].

nosť o pravdivosti získaných údajov o klientovi.[12] Je zrejmé, že v prípade podozrenia z prania špinavých peňazí vo vzťahu k danému klientovi alebo v prípade zmeny správania sa klienta vo vzťahu k vytvorenému rizikovému profilu klienta (napr. výber vysokých peňažných čiastok z účtu), môže dôjsť k prehodnoteniu a potrebnosti aktualizácie získaných údajov.

Okrem potrebnosti zabezpečenia identifikácie klienta, FATF CDD (Anti-money laundering and terrorist financing measures and financial inclusion – with a supplement on customer due diligence – ďalej len „FATF CDD“) požaduje aj zabezpečenie overenia získaných informácií o klientovi a konečnom užívateľovi výhod. V tomto kontexte hovoríme o povinnosti zabezpečenia **overenia identifikácie klienta** povinnými osobami.[13] Identifikácia predstavuje zistenie požadovaných údajov o totožnosti subjektu, zatiaľ čo overenie identifikácie klienta sa realizuje formou „porovnania respektíve kontroly“ získaných identifikačných údajov na podklade predložených dokladov totožnosti (napr. porovnanie podobizne osoby s podobou v občianskom preukaze).

1.1 Uplatnenie požiadaviek *customer due diligence*

Identifikácia a overenie identifikácie klienta sú jednými zo základných prvkov uplatnenia širšej požiadavky „poznať svojho klienta“ (know your customer – ďalej len „KYC“), ktorá je bezprostredne spojená s uplatnením požiadaviek starostlivosti vo vzťahu ku klientovi (customer due diligence – ďalej len „CDD“).

Kompletné uplatnenie požiadaviek CDD sa musí aplikovať v nasledovných prípadoch: nadväzovanie obchodného vzťahu; realizácie príležitostných transakcií nad stanovenú úroveň 15000 eur; existencia podozrenia z prania špinavých peňazí alebo financovania terorizmu; existencia pochybnosti o vierohodnosti alebo primeranosti predtým získaných identifikačných údajov klienta. FATF RN (FATF Recommendation – ďalej len „FATF RN“) výslovne zakazuje vedenie anonymných účtov alebo účtov otvorených na vymyslené mená.[14]

V rámci uplatnenia opatrení FATF RN priamo vyžaduje zabezpečenie identifikácie klienta a overenie identifikácie klienta pomocou **spo-**

[12] FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012, p. 67.

[13] FATF: Anti-money laundering and terrorist financing measures and financial inclusion -With a supplement on customer due diligence. Frace: Paris, 2011, p. 54.

[14] FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012, p. 64 – 72.

ľahlivých a nezávislých zdrojov.[15] Vyššie uvedené odporúčanie FATF je technologicky neutrálne. Odporúčanie 10 FATF RN neukladá žiadne obmedzenia z hľadiska formy predkladaných dokladov totožnosti. Doklady totožnosti predložené povinnej osobe vo fyzickej alebo digitálnej podobe sú tak postavené na rovnakú úroveň. Z toho vyplýva, že pri overení identifikácie klienta je možné použiť systémy digitálnej identifikácie, ak obsahujú požadované údaje. V tomto prípade FATF DI necháva „voľnú ruku" pristúpivším členským štátom v otázke vnútroštátnej úpravy spôsobu získavania identifikačných údajov.[16]

Pojem **spoľahlivé a nezávislé zdroje** nie je bližšie špecifikovaný v odporúčaní FATF RN. Jedinú zmienku nachádzame vo FATF DI, ktoré odkazuje na potrebnosť zabezpečenia „istoty" používaných systémov digitálnej identifikácie povinnými osobami. Používaný systém digitálnej identifikácie tak musí spĺňať podmienky nezávislosti a spoľahlivosti na účely boja proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu. Splnenie týchto podmienok predovšetkým závisí od typu používanej technológie, procesov a postupov aplikácie prístupu založeného na riziku (Risk based Approach – ďalej len „RBA") a s tým spojeného zavedenia zmierňujúcich opatrení povinnými osobami.[17]

1.2 Aplikácia prístupu RBA

Vo všeobecnosti pristúpivšie krajiny by mali identifikovať, posúdiť a pochopiť existujúce riziká legalizácie príjmov z trestnej činnosti a financovania terorizmu a prijať vhodné opatrenia na ich zmiernenie. Pri hodnotení rizika musia povinné osoby brať do úvahy celkovú úroveň rizika a tomu zodpovedajúcu úroveň opatrení, ktoré sa majú uplatniť vo vzťahu ku konkrétnemu klientovi. V prípade zistenia existencie zvýšeného rizika bude potrebné zavedenie prísnejších opatrení, zatiaľ čo v prípade nízkeho rizika bude postačovať aj uplatnenie zjednodušených opatrení.[18]

V súlade s odporúčaním 10 FATF RN sa overenie identifikácie klienta môže vykonať pred alebo aj **počas uzatvárania obchodného vzťahu**. Overenie identifikácie klienta počas uzatvárania obchodného vzťahu je možné realizovať za kumulatívneho splnenia dvoch požiadaviek: ak je to potrebné na neprerušenie zvyčajného vedenia podnikania

[15] FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012, p. 64 – 72.

[16] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 54.

[17] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 28 – 29.

[18] FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012, p. 31 – 36.

a súčasnej existencie nízkeho rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu.

Za prípad, pri ktorom je prípustné overenie identifikácie klienta počas uzatvorenia obchodného vzťahu, sa považuje okrem iného aj ***non-face-to-face business***. V tomto prípade sa predpokladá, že k interakcii medzi subjektami dochádza na diaľku, teda použitím alternatívnych prostriedkov komunikácie, ktoré sú alternatívou fyzickej prítomnosti subjektov (napr. telefón, pošta, video hovor, atď.).[19]

Non-face-to-face obchodné vzťahy a transakcie spadajú do kategórie rizikových faktorov a sú považované za **vysokorizikové**.[20] FATF DI zdôraznilo, že zoznam rizikových faktorov obsahuje výpočet viacerých príkladov respektíve potenciálnych situácií spojených so zvýšeným rizikom. V tomto kontexte *non-face-to-face* obchodné vzťahy a transakcie treba vnímať iba ako príklady, pri ktorých riziko legalizácie príjmov z trestnej činnosti a financovania terorizmu môže byť potenciálne vyššie.[21] Z poskytnutej interpretácie vyplýva, že *non-face-to-face* obchodné vzťahy a transakcie sa môžu, ale zároveň nemusia, považovať za vysokorizikové. Rizikovosť v tomto prípade bude predovšetkým závisieť od úrovne rizika, ktoré povinný subjekt určil na podklade uplatnenia prístupu RBA v spojení s vytvoreným rizikovým profilom klienta.

1.3 Plnenie tretími stranami

V prípade využitia systémov digitálnej identifikácie povinné osoby môžu, obdobne ako v prípade identifikácie klienta za jeho fyzickej prítomnosti, využiť inštitút plnenia tretími stranami. Plnenie tretími stranami spočíva v možnosti povinnej osoby „sa spoľahnúť“ na banku respektíve inú finančnú inštitúciu, od ktorej prevezme potrebné podklady a údaje na zabezpečenie identifikácie a overenia identifikačných údajov klienta.[22]

Využitie plnenia tretími stranami nezbavuje povinnú osobu povinnosti aj naďalej vykonávať primeranú starostlivosť vo vzťahu ku klientovi. Povinná osoba tak nesie konečnú zodpovednosť za správnu aplikáciu požiadaviek CDD a za celkové priebežné monitorovanie obchodného vzťahu. FATF DI rovnako zdôraznilo, že uplatnenie

[19] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 30.
[20] FATF: Guidance for a risk-based approach virtual asset service providers, 2019, p. 26.
[21] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 30.
[22] FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012, p. 18.

inštitútu plnenia tretími stranami je možné realizovať jedine za účelom zabezpečenia identifikácie a overenia identifikačných údajov klienta.[23]

Použitie inštitútu plnenia tretími stranami je podmienené splnením viacerých podmienok bližšie upravených v odporúčaní 17 FATF RN. V prípade vykonania identifikácie a overenia identifikácie klienta pomocou **systému digitálnej identifikácie** musia byť splnené nasledovné **podmienky**:[24]

- tretia strana (banka alebo iná finančná inštitúcia) musí byť regulovaným subjektom a podliehať dohľadu zo strany príslušných orgánov konkrétneho štátu. Do úvahy sa pritom berie celková úroveň rizikovosti krajiny tretej strany;
- systém digitálnej identifikácie tretej strany umožňuje povinnej osobe okamžite získať požadované identifikačné údaje klienta;
- povinná osoba by sa mala ubezpečiť, že tretia strana disponuje kópiami alebo inými vhodnými formami dokladov totožnosti klienta (napr. dokumenty v papierovej forme alebo na iných nosičoch informácií) a je schopná ich predložiť bezodkladne na požiadanie povinnej osobe. Ako príklad sa uvádza otvorenie účtu klientom, obsahujúce jeho základné identifikačné údaje, ktoré na podklade overenia vykonaného treťou stranou je možné poskytnúť bezodkladne povinnej osobe.

V prípade využitia **outsourcingu alebo agentúr** poskytujúcich obdobné služby plnenia tretími stranami sa odporúčanie 17 FATF RN neuplatňuje.

2. Identifikácia klienta prostredníctvom technických prostriedkov na území Slovenskej republiky

V. AML smernica zdôraznila potrebnosť zabezpečenia presnej identifikácie a overenia údajov fyzických a právnických osôb, ktorú považuje za kľúčový prvok pre boj proti legalizácii príjmov z trestnej činnosti a financovaniu terorizmu.[25]

Za najbezpečnejší spôsob identifikácie klienta v súčasnosti sa predovšetkým považuje identifikácia tvárou v tvár (*face-to-face*), avšak v dôsledku rozvoja nových technológii V. AML smernica umožnila

[23] FATF: Guidance on Digital Identity. France: Paris, 2020, p. 31.

[24] . FATF: Guidance on Digital Identity. France: Paris, 2020, p. 32.

[25] Recitál 22 smernice Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.

používanie nových technológií za účelom vykonania bezpečnej identifikácie na diaľku, respektíve elektronickej identifikácie klienta.[26]

Implementáciou V. AML smernice došlo k prevzatiu príslušných ustanovení do vnútroštátneho zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov (ďalej len „zákon o legalizácii"). V súlade s § 8 zákona o legalizácii, overenie identifikácie klienta je možné realizovať aj použitím technických prostriedkov a postupov, úroveň ktorých však musí z hľadiska dôveryhodnosti výsledku overenia byť obdobná overeniu za fyzickej prítomnosti klienta. V prípade fyzických osôb – podnikateľov sa vyžaduje zabezpečenie overenia ďalších údajov súvisiacich s podnikaním osoby.

Finančná spravodajská jednotka (Financial Intelligence Unit – ďalej len „FIU") poskytla bližšie vysvetlenie pojmov **technických prostriedkov a postupov**, pod ktorými sa rozumejú: *„softvérové riešenia vymedzené zabezpečeným digitálnym rozhraním umožňujúcim získavanie a prenos údajov, dokumentov a informácií prostredníctvom technických zariadení a ich následné spracovanie, a to účelným, ustáleným súhrnom na seba nadväzujúcich krokov pri identifikácii klienta."*[27] Obdobné definície vyššie uvedených pojmov nachádzame aj v stanovisku Národnej banky Slovenska (ďalej len „NBS"). Zároveň NBS upravuje zoznam funkcií (s dôrazom na biometrické údaje), ktoré zvolený technický prostriedok musí spĺňať.[28]

Povinná osoba je povinná zabezpečiť vykonanie **spoľahlivej a dôveryhodnej identifikácie a overenia identifikácie klienta**, a to jedným zo spôsobov upraveným v zákone o legalizácii.[29] V tomto prípade vyvstáva otázka, či je možné automaticky stotožňovať aplikáciu konkrétneho spôsobu identifikácie upraveného v zákone o legalizácii s vykonaním spoľahlivej a dôveryhodnej identifikácie? Nie je totiž

---

[26] Recitál 22 smernice Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.

[27] Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 2.

[28] Čl. 1 ods. 4 a Čl. 4 ods. 1 a 2 stanoviska Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 10. decembra 2018 č. 1/2018 k identifikácii a overeniu identifikácie klienta – fyzickej osoby, bez jej fyzickej prítomnosti prostredníctvom technických prostriedkov a postupov podľa zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.

[29] Spôsoby identifikácie klienta môžeme rozdeliť na: identifikácia klienta za jeho fyzickej prítomnosti; identifikácia prostredníctvom technických prostriedkov a postupov; použitie inštitútu plnenia tretími stranami. Bližšie k tomu viď: Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 1 – 2.

celkom zrejmé, čo sa myslí pod pojmom spoľahlivá a dôveryhodná identifikácia.

V tejto súvislosti NBS bližšie špecifikuje postup uskutočnenia identifikácie a overenia identifikácie klienta. **Overenie správnosti a úplnosti získaných údajov o fyzickej osobe** sa musia realizovať buď prostredníctvom použitia interných zdrojov povinnej osoby alebo externých zdrojov alebo ich kombinácie. Podmienkou použitia interných zdrojov povinnej osoby je existencia obchodného vzťahu s klientom. V rámci externých zdrojov je možné použiť napríklad overenie údajov uvedených v doklade totožnosti alebo nahliadnutie do zoznamu politicky exponovaných osôb, atď.

Komisia pre elektronickú identifikáciu a vzdialené procesy KYC[30] navrhuje uplatnenie kombinácie viacerých metód identifikácie klienta, a to za účelom zvýšenia bezpečnosti a lepšieho riadenia existujúcich rizík.[31]

Celkovo je možné konštatovať, že FIU a NBS v rámci svojich stanovísk poskytujú iba rámcový pohľad na problematiku zabezpečenia identifikácie klienta na diaľku. Bližší spôsob zabezpečenia identifikácie, vrátane zvolených technických prostriedkov a postupov, je ponechaný na zváženie povinným osobám. Teda povinné osoby musia, na základe aplikácie RBA prístupu (Risk-based approach – ďalej len „RBA"), zhodnotiť vhodnosť a dostatočnosť použitej technológie. Zároveň v prípade potreby sú povinné osoby povinné na požiadanie FIU a NBS preukázať ako identifikovali, vyhodnotili a zmiernili zistené rizikové faktory.

Vyššie uvedený postoj FIU a NBS v otázke dobrovoľnosti výberu technologických prostriedkov a postupov je potrebné chápať v širšom kontexte. V. AML smernica totiž upravuje povinnosť uplatnenia zásady **technologickej neutrality**.[32] Okrem uloženia spomínanej povinnosti, V. AML smernica neposkytuje žiadne vysvetlenie tohto pojmu. V tomto prípade je potrebné sa obrátiť na nariadenie eIDAS, ktoré pod technologickou neutralitou rozumie neznevýhodnenie žiadneho konkrétneho

[30] Komisia pre elektronickú identifikáciu a vzdialené procesy KYC bola zriadená Európskou komisiou v súlade s čl. 8 Commission Decision C (2017) 8405 final setting up the Commission expert group on electronic identification and remote Know-Your-Customer processes (eID/KYG EG).

[31] European Commission: Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, 2019, p. 2.

[32] Recitál 22 smernice Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.

vnútroštátneho technického riešenia elektronickej identifikácie v rámci členského štátu.[33]

2.1 Aplikácia prístupu RBA

Nadväzujúc na FATF RN a V. AML smernicu musia povinné osoby, v súvislosti s identifikáciou a overením identifikácie klienta na diaľku, zohľadniť okolnosti vykonávania obchodu a bezpečnostné riziká používania technického prostriedku. V tejto súvislosti by mala povinná osoba posúdiť rizikový profil klienta, správanie sa klienta počas používania technického prostriedku a ďalšie rizikové faktory, predovšetkým upravené v prílohe č. 2 zákona o legalizácii.[34]

Spôsob hodnotenia a riadenia rizík musí byť upravený v programe vlastnej činnosti povinnej osoby. Pri **hodnotení rizika** je potrebné zohľadniť vlastné rizikové faktory povinnej osoby, ktoré sa odvíjajú od jej povahy a veľkosti a zohľadniť aj národné hodnotenie rizík. Okrem vyššie uvedených náležitostí by malo hodnotenie rizík reflektovať aj nadnárodné hodnotenie rizík vykonané Európskou komisiou, či odporúčania EBA, ESMA, EIOPA.[35]

FIU zdôrazňuje, že identifikácia a overenie identifikácie klienta s využitím technických prostriedkov a postupov sa môže použiť jedine v prípade produktov a služieb, ktoré sú vhodné a primerané.[36] Ďalej sa však bližšie nešpecifikuje, o aké produkty a služby má ísť.

Vo všeobecnosti je identifikácia a overenie identifikácie klienta s využitím technických prostriedkov spojená so **zvýšeným rizikom**. V súlade s **národným hodnotení rizika** sa za osobitný rizikový faktor považuje zakladanie obchodného vzťahu bez fyzickej prítomnosti klienta, teda ide o vykonanie online identifikácie prostredníctvom rôznych mobilných aplikácií alebo iných digitálnych prostriedkov. Zároveň národné hodnotenie rizík upravuje aj zoznam determinantov zraniteľnosti, s ktorými sa spája najväčšie riziko zneužívania online

[33] Čl. 12 ods. 3 písm. a) nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

[34] Čl. 2 ods. 2 a 5 stanoviska Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 10. decembra 2018 č. 1/2018 k identifikácii a overeniu identifikácie klienta – fyzickej osoby, bez jej fyzickej prítomnosti prostredníctvom technických prostriedkov a postupov podľa zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.

[35] Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 2.

[36] Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 2.

identity (napr. možnosť digitálnej úpravy tváre klienta).[37] Ďalšie príklady zneužívania online identity podrobnejšie opisuje aj Komisia pre elektronickú identifikáciu a vzdialené procesy KYC.[38]

V tejto súvislosti je potrebné zdôrazniť, že **zákon o legalizácii** automaticky bez ďalšieho nestotožňuje identifikáciu a overenie identifikácie na diaľku s faktorom zvýšeného rizika. V súčasnosti stále platí, že v prípade uzatvorenia zmluvného vzťahu s použitím identifikačných systémov (non-face-to-face), identifikácia a overenie identifikácie klienta sa považuje za obdobnú uzatvoreniu zmluvného vzťahu za fyzickej prítomnosti klienta, ak zároveň spĺňa podmienky v zmysle príslušného stanoviska NBS.[39] Základnou zásadou pre určenie výkonu zvýšenej starostlivosti stále zostáva uplatnenie RBA prístupu. Z toho vyplýva, že povinná osoba je povinná uplatniť RBA prístup vo vzťahu ku konkrétnemu klientovi a následne sa sama rozhodnúť, či v prípade vykonania identifikácie a overenia identifikácie klienta na diaľku bude postačovať vykonať základnú alebo aj zvýšenú starostlivosť. V prípade, ak sa povinná osoba rozhodne vykonať zvýšenú starostlivosť vo vzťahu k takému klientovi, musí postupovať v súlade s § 12 ods. 2 písm. a) zákona o legalizácii.

V tomto prípade vyvstáva otázka vhodnosti úpravy RBA prístupu, ako rozhodujúceho faktora, pri určovaní stupňa rizikovosti klienta. Samozrejme uplatnenie RBA prístupu je v súlade s FATF RN a AML smernicou a odráža flexibilný prístup ku klientovi. Každý klient sa tak má posudzovať jednotlivo s ohľadom na možnú existenciu rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu. Avšak zastávame názor, že navrhovaná zmena zákona o legalizácii,[40] ktorá navrhuje vypustiť možnosť uplatnenia RBA prístupu v prípade uzatvorenia zmluvného vzťahu na diaľku s použitím identifikačných systémov, a tým začleniť identifikáciu a overenie identifikácie na diaľku do faktorov so zvýšeným rizikom, za správne riešenie.

V rámci všeobecnej úpravy overenia identifikácie klienta zákon o legalizácii obdobne umožňuje vykonať **dodatočné overenie identi-**

---

[37] Záverečná sprava z národného hodnotenia rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu v podmienkach Slovenskej republiky, s. 96.

[38] European Commission: Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, 2019, p. 97.

[39] Stanovisko Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 10. decembra 2018 č. 1/2018 k identifikácii a overeniu identifikácie klienta – fyzickej osoby, bez jej fyzickej prítomnosti prostredníctvom technických prostriedkov a postupov podľa zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.

[40] K bodu 10 a 11 Dôvodová sprava. Osobitná časť. LP/2021/200 Zákon o centrálnom registri účtov a o zmene a doplnení niektorých zákonov.

fikácie počas uzatvárania obchodného vzťahu, a to za predpokladu, že je to potrebné na neprerušenie zvyčajného vedenia podnikania a zároveň existuje nízke riziko legalizácie alebo financovania terorizmu. Dodatočné overenie identifikácie sa vykonáva neodkladne po tom, keď je klient prvýkrát fyzicky prítomný u povinnej osoby.[41] Je potrebné zdôrazniť, že dodatočne je možné iba overiť identifikáciu, zatiaľ čo prvotná identifikácia klienta musí byť vykonaná ešte pred alebo súčasne s uzatvorením obchodného vzťahu.

V tejto súvislosti **NBS** stanovuje voči povinným osobám dodatočnú požiadavku splnenia **notifikačnej povinnosti**.[42] Opierajúc sa o uvedené odkazy na právne predpisy je zrejmé, že vyššie uvedená požiadavka sa vzťahuje na banky, platobné inštitúcie a inštitúcie poskytujúce spotrebiteľské úvery. Vyššie uvedené inštitúcie sú povinné vopred písomne informovať NBS o zmenách podmienok, údajov a skutočností, ktoré boli podkladom na udelenie príslušného povolenia.[43] V tomto kontexte NBS vyžaduje od povinných osôb splnenie notifikačnej povinnosti pred zavedením identifikácie a overenia identifikácie klienta na diaľku. Notifikačná povinnosť je spojená s povinnosťou vypracovania a aktualizovania programu vlastnej činnosti povinnej osoby.

EBA, ESMA a EIOPA vo svojom spoločnom usmernení okrem iného spomínajú aj možnosť **zmiernenia zvýšeného rizika**, a to aplikáciou primeraných dodatočných ochranných opatrení. Ako príklad sa uvádza **zavedenie elektronických podpisov a certifikátov elektronickej identifikácie vydaných v súlade s nariadením eIDAS**.[44]

Nariadenie eIDAS predstavuje základný ochranný prostriedok na zmiernenie existujúcich rizík súvisiacich s možným podvodom s totož-

---

[41] § 8 ods. 3 zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[42] Čl. 2 ods. 11 stanoviska Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 10. decembra 2018 č. 1/2018 k identifikácii a overeniu identifikácie klienta – fyzickej osoby, bez jej fyzickej prítomnosti prostredníctvom technických prostriedkov a postupov podľa zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.

[43] § 9 ods. 4 zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 65 ods. 4 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 20 ods. 6 zákona č. 129/2010 Z. z. o spotrebiteľských úveroch a o iných úveroch a pôžičkách pre spotrebiteľov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[44] European banking authority: Usmernenia podľa článkov 17 a 18 ods. 4 smernice (EÚ) 2015/849 týkajúce sa povinnej starostlivosti vo vzťahu ku klientovi a faktorov, ktoré by úverové a finančné inštitúcie mali zvážiť pri hodnotení rizika prania špinavých peňazí a financovania terorizmu spojeného s jednotlivými obchodnými vzťahmi a príležitostnými transakciami („usmernenia týkajúce sa rizikových faktorov spojených s praním špinavých peňazí a financovaním terorizmu“), ktorými sa zrušujú a nahrádzajú usmernenia JC/2017/37, EBA/GL/2021/02, 2021, p. 39.

nosťou.[45] Napriek tomu **V. AML smernica** nevylučuje možnosť použitia aj iných bezpečných procesov identifikácie na diaľku alebo elektronickej identifikácie, ktoré musia spĺňať podmienku regulárnosti, uznania, schválenia alebo akceptovateľnosti príslušným vnútroštátnym orgánom. Aj v tomto prípade sa aplikuje zásada technologickej neutrality.[46]

Prostriedky elektronickej identifikácie obsiahnuté v nariadení eIDAS sa svojou spoľahlivosťou najviac približujú identifikácii za fyzickej prítomnosti klienta. **FIU** obdobne umožňuje povinnej osobe využiť dôveryhodné formy preukázania sa klienta **kvalifikovaným elektronickým podpisom**[47] **alebo s použitím úradného autentifikátora**. Vyššie uvedený spôsob sa považuje za overenie obdobné identifikácie klienta za jeho fyzickej prítomnosti.[48] Je dôležité poznamenať, že FIU nespája použitie vyššie uvedeného spôsobu preukázania sa klienta s faktorom zvýšeného rizika.

2.2 Plnenie tretími stranami

V súlade so IV. AML smernicou sa za **tretiu stranu** považujú úverové a finančné inštitúcie ako aj ďalšie fyzické alebo právnické osoby konajúce pri výkone svojej odbornej činnosti (napr. audítor, notár, atď.).[49] Pod pojem tretie strany sa rovnako zahrnujú členské organizácie

---

[45] European Commission: Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, 2019, p. 13.

[46] Recitál 22 smernice Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.

[47] Za kvalifikovaný elektronický podpis sa považuje: *„zdokonalený elektronický podpis vyhotovený s použitím kvalifikovaného zariadenia na vyhotovenie elektronického podpisu a založený na kvalifikovanom certifikáte pre elektronické podpisy.“* V súlade s nariadením eIDAS má kvalifikovaný elektronický podpis právny účinok, ktorý je rovnocenný s vlastnoručným podpisom. Zároveň sa uplatňuje zásada vzájomného uznávania kvalifikovaného elektronického podpisu členskými štátmi EÚ, a to za splnenia stanovených podmienok. Bližšie k tomu viď: oddiel 4 nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.

[48] Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 4.

[49] Čl. 2 ods. 1-3 smernice Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES.

alebo federácie povinných osôb, ako aj iné inštitúcie či osoby, nachádzajúce sa v členskom štáte alebo v tretej krajine.[50]

V porovnaní so IV. AML smernicou upravuje zákon o legalizácii užší okruh tretích strán. Za tretie strany považuje iba úverové a finančné inštitúcie (napr. burza cenných papierov, obchodník s cennými papiermi, atď.).[51] V tomto prípade sú z definície vyňaté ďalšie fyzické a právnické osoby a rovnako tak členské organizácie a federácie povinných osôb. Môžeme teda konštatovať, že zákon o legalizácii má prísnejšiu reguláciu v porovnaní so IV. AML smernicou.

Prevzatie údajov a podkladov povinnou osobou je vo všeobecnosti spojené s **miestom pôsobenia tretej strany**. V súlade so IV. AML smernicou môže povinná osoba prevziať údaje od tretích strán, ktoré sa nachádzajú v členskom štáte alebo v tretej krajine. Zákon o legalizácii priamo také ustanovenie neobsahuje, preto je potrebné sa obrátiť na metodické usmernenie NBS, ktoré upresňuje, že musí ísť o úverové a finančné inštitúcie pôsobiace na území Európskeho hospodárskeho priestoru (ďalej len „EHP"), respektíve na území Slovenskej republiky.[52] Výslovný zákaz prevzatia údajov a podkladov sa vzťahuje na tretie krajiny, ktoré Európska únia (ďalej len „EÚ") určila za vysokorizikové. V tomto prípade je dôležité zistiť, či sa konkrétna tretia krajina skutočne nachádza v zozname vysokorizikových tretích krajín vedenom EÚ a či nedošlo k jej vymazaniu zo zoznamu.[53]

Na to, aby tretia strana mohla poskytovať plnenie, sa nevyhnutne vyžaduje splnenie nasledovných **podmienok**:

- tretia strana vykonáva povinnú starostlivosť vo vzťahu ku klientovi (základná, zvýšená a zjednodušená starostlivosť) na úrovni zodpovedajúcej právu Európskej únie;
- tretia strana uplatňuje vedenie záznamov na úrovni zodpovedajúcej právu Európskej únie;

---

[50] Čl. 25 ods. 1 smernice Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES.

[51] § 5 ods. 1 písm. b) bod 1-10 zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[52] Čl. 8 ods. 10 metodického usmernenia Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 20. novembra 2012 č. 9/2012 k ochrane banky a pobočky zahraničnej banky pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu.

[53] Bližšie k tomu viď: DAUDRIKH, Y.: High-risk third countries in relation to EU legislation and financial action task force recommendations. In Concepts, strategies and mechanisms of economic systems management in the context of modern world challenges. Bulgarian: Sofia, 2021, s. 379 – 390.

– tretia strana podlieha dohľadu na úrovni zodpovedajúcej právu Európskej únie.[54]

Podľa názoru FIU by sa spolupráca medzi odovzdávajúcou a prijímajúcou povinnou osobou mala zakladať na **zmluvnom vzťahu**, obsahom ktorého by mal byť konkrétny spôsob poskytovania údajov, výška vecných nákladov alebo lehota na poskytnutie podkladov.[55] Prijímajúca povinná osoba musí mať prístup ku všetkým informáciám, ktoré nevyhnutne potrebuje na vykonanie starostlivosti.

Pri využití inštitútu plnenia tretími stranami vyvstáva otázka potrebnosti **získania predchádzajúceho súhlasu** klienta na prevzatie konkrétnych údajov od tretej strany. V tejto súvislosti NBS poukazuje na existujúcu prax v členských štátoch Európskeho hospodárskeho priestoru, v rámci ktorej vyžadovanie súhlasu nie je potrebné.[56] Zároveň však netreba zabúdať na existenciu uplatnenia všeobecných obmedzení pre poskytovanie informácií. Tak napríklad informácie a doklady o záležitostiach, ktoré sú chránené bankovým tajomstvom, je možné poskytnúť tretím osobám len na základe predchádzajúceho písomného súhlasu dotknutého klienta alebo na jeho písomný pokyn.[57] Je zrejmé, že aj v prípade prevzatia údajov povinnou osobou, bude nevyhnutné získať obdobný predchádzajúci súhlas klienta daný k takému účelu.[58]

Prijímajúca povinná osoba nesie **konečnú zodpovednosť** za prevzaté údaje. Takto prevzaté údaje musia spĺňať požiadavky na starostlivosť vo vzťahu ku klientovi vyplývajúce zo zákona o legalizácii.[59] Prijímajúca povinná osoba je povinná overiť aktuálnosť takto získaných údajov a dôveryhodnosť tretej strany. Zároveň musí overiť aj spô-

[54] Čl. 26 ods. 1 smernice Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES. § 13 ods. 1 zákona č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.

[55] Usmernenie Finančnej spravodajskej jednotky k plneniu zákonných povinnosti o zdieľaní informácií medzi poisťovňami a inými finančnými inštitúciami, najmä bankami podľa § 13 zákona č. 297/2008 Z. z., s. 2.

[56] Čl. 8 ods. 10 metodického usmernenia Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 20. novembra 2012 č. 9/2012 k ochrane banky a pobočky zahraničnej banky pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu.

[57] § 91 ods. 1 zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[58] Usmernenie Finančnej spravodajskej jednotky k plneniu zákonných povinnosti o zdieľaní informácií medzi poisťovňami a inými finančnými inštitúciami, najmä bankami podľa § 13 zákona č. 297/2008 Z. z., p. 2.

[59] Čl. 8 ods. 10 metodického usmernenia Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 20. novembra 2012 č. 9/2012 k ochrane banky a pobočky zahraničnej banky pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu.

sob získania údajov treťou stranou. Zároveň platí, že odovzdávajúca tretia strana sama nesmie použiť inštitút plnenia treťou stranou a musí osobne vykonať starostlivosť vo vzťahu ku klientovi.[60] Po prevzatí údajov je prijímajúca povinná osoba povinná vykonať základnú starostlivosť vo vzťahu ku klientovi, rozsah ktorej je upravený v § 10 ods. 1 písm. d) až g) zákona o legalizácii.[61]

Použitie inštitútu plnenia tretími stranami má **fakultatívny charakter** a je iba na povinnej osobe, či vôbec zvolí vyššie uvedený spôsob zisťovania informácií. V tomto prípade však netreba zabúdať na existenciu **rizika** spojeného s nedostatkom informácií získaných treťou stranou, ktoré môžu byť neúplné, nesprávne alebo neaktuálne. Zároveň EBA (European Banking Authority) poukazuje na existenciu ďalšieho rizika spojeného s dôveryhodnosťou tretej strany. Za faktor zvýšeného rizika sa považuje práve spoliehanie sa na opatrenia povinnej starostlivosti vo vzťahu ku klientovi vykonané treťou stranou, s ktorou preberajúca povinná osoba nemá dlhodobý vzťah.[62]

Je v záujme povinnej osoby zistiť na podklade prevzatých údajov, či klient alebo druh obchodu nepredstavuje zvýšené riziko. V prípade zistenia existencie zvýšeného rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu, povinná osoba nemôže aplikovať inštitút plnenia tretími stranami a musí pristúpiť k identifikácii klienta tvárou v tvár, respektíve použiť technologické prostriedky a postupy, úroveň ktorých musí z hľadiska dôveryhodnosti výsledku overenia byť obdobnou overeniu za fyzickej prítomnosti klienta.[63]

Záver

Identifikácia klienta sa vykonáva v dvoch rovinách: prvotná identifikácia a následné overenie identifikácie klienta, ktoré sa vykonáva

[60] Usmernenie Finančnej spravodajskej jednotky k plneniu zákonných povinnosti o zdieľaní informácií medzi poisťovňami a inými finančnými inštitúciami, najmä bankami podľa § 13 zákona č. 297/2008 Z. z., s. 2.

[61] Usmernenie Finančnej spravodajskej jednotky k plneniu zákonných povinnosti o zdieľaní informácií medzi poisťovňami a inými finančnými inštitúciami, najmä bankami podľa § 13 zákona č. 297/2008 Z. z., s. 2.

[62] European banking authority: Usmernenia podľa článkov 17 a 18 ods. 4 smernice (EÚ) 2015/849 týkajúce sa povinnej starostlivosti vo vzťahu ku klientovi a faktorov, ktoré by úverové a finančné inštitúcie mali zvážiť pri hodnotení rizika prania špinavých peňazí a financovania terorizmu spojeného s jednotlivými obchodnými vzťahmi a príležitostnými transakciami („usmernenia týkajúce sa rizikových faktorov spojených s praním špinavých peňazí a financovaním terorizmu“), ktorými sa zrušujú a nahrádzajú usmernenia JC/2017/37, EBA/GL/2021/02, 2021, s. 39.

[63] Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona, s. 2.

počas trvania obchodného vzťahu s klientom. Problematika identifikácie klienta je vo všeobecnosti priblížená vo FATF RN. FATF RN požaduje vykonanie identifikácie a overenie identifikácie klienta na základe spoľahlivých a nezávislých zdrojov. V tomto prípade sa apeluje na istotu povinných osôb v dostatočnosť používaných systémov digitálnej identifikácie klienta.

FATF RN spája *non-face-to-face* business s faktorom zvýšeného rizika. Zároveň však umožňuje vykonanie overenia identifikácie klienta aj počas trvania obchodného vzťahu s klientom.

Právna úprava identifikácie a overenia identifikácie klienta na území Slovenskej republiky je odvodená od implementácie V. AML smernice, ktorá umožnila okrem klasickej formy identifikácie klienta (tvárou v tvár), vykonávať identifikáciu a overenie identifikácie klienta na diaľku, teda bez fyzickej prítomnosti klienta a s použitím vhodných technických prostriedkov. Výber technických prostriedkov bol však ponechaný na samotnú povinnú osobu, ktorá musí sama zvážiť vhodnosť a dostatočnosť používaných systémov. Obdobne aj vnútroštátny zákon o legalizácii, s prihliadnutím na zásadu technologickej neutrality, nejakým spôsobom neobmedzuje možnosť výberu technických prostriedkov a postupov povinnými osobami.

Základný rozpor badáme v otázke určovania stupňa rizikovosti identifikácie a overenia identifikácie klienta na diaľku. Zatiaľ čo FATF RN, EBA, ESMA, EIOPA, FIU klasifikujú identifikáciu a overenie identifikácie ako faktor zvýšeného rizika, súčasný zákon o legalizácii uplatňuje menej prísny spôsob, ktorý sa výlučne opiera o RBA prístup. Napriek kritike odbornej verejnosti a odvolávaniu sa na vyššiu úroveň bezpečnosti, ktorú prinášajú nové technológie, je zrejmé, že súčasný stav je v rozpore so stanoviskom FIU, ktorá považuje identifikáciu a overenie identifikácie klienta na diaľku za zvýšené riziko. Zároveň však zdôrazňuje, že kvalifikovaný elektronický podpis, ako aj použitie úradného autentifikátora, sa považujú za dôveryhodnú identifikáciu klienta a preto sa nespájajú so zvýšeným rizikom.

FATF RN a zákon o legalizácii umožňujú uplatnenie inštitútu plnenia tretími stranami. Použitie vyššie uvedeného inštitútu je spojené s predchádzajúcim splnením výslovne stanovených podmienok. Zásadnou podmienkou je nemožnosť prevzatia údajov z tretích krajín, ktoré EÚ určila za vysokorizikové. Bližšie vysvetlenie aplikácie inštitútu plnenia tretími stranami nachádzame v metodickom usmernení NBS a v stanovisku FIU. V tomto kontexte sa zdôrazňujú potrebnosť zabezpečenia zmluvného vzťahu medzi povinnými osobami, na podklade ktorého má dôjsť k prevzatiu požadovaných informácií, prípadne získanie predchádzajúceho súhlasu klienta s poskytnutím takých údajov, ak ide

o oblasť všeobecných obmedzení pre poskytovanie dôverných informácií. Konečnú zodpovednosť za prevzatie údajov od tretej strany bude vždy znášať prijímajúca povinná osoba.

Použitá literatúra

1. Andraško, J., Horvat, M., Mesarčík, M.: *Vybrané kapitoly práva informačných technológií I.* Bratislava: Právnická fakulta UK, 2019. 104 s. ISBN 978-80-7160-523-2.
2. Daudrikh, Y.: High-risk third countries in relation to EU legislation and financial action task force recommendations. In *Concepts, strategies and mechanisms of economic systems management in the context of modern world challenges*. Bulgarian: Sofia, 2021, s. 379 – 390. ISBN 978-619-7622-11-9.
3. De Koker, L.: Anonymous clients, identified clients and the shades in between – Perspectives on the FATF AML/CFT standards and mobile banking, 2009, p. 1 – 17. Dostupné na: http://dx.doi.org/10.2139/ssrn.2634305
4. de Koker, L.: The FATF's customer identification framework: fit for purpose? In *Journal of money laundering control*, vol. 17, no. 3, 2014, p. 281 – 295.
5. Kyncl, L.: *Poznej svého klienta základní zásada finančního práva.* Brno: Masarykova univerzita, Spisy Právnické fakulty Masarykovy univerzity. Řada teoretická sv. 433, 2012. 165 s. ISBN 978-80-210-6085-2.
6. Commission Decision C (2017) 8405 final setting up the Commission expert group on electronic identification and remote Know-Your-Customer processes (eID/KYG EG).
7. European banking authority: Usmernenia podľa článkov 17 a 18 ods. 4 smernice (EÚ) 2015/849 týkajúce sa povinnej starostlivosti vo vzťahu ku klientovi a faktorov, ktoré by úverové a finančné inštitúcie mali zvážiť pri hodnotení rizika prania špinavých peňazí a financovania terorizmu spojeného s jednotlivými obchodnými vzťahmi a príležitostnými transakciami („usmernenia týkajúce sa rizikových faktorov spojených s praním špinavých peňazí a financovaním terorizmu"), ktorými sa zrušujú a nahrádzajú usmernenia JC/2017/37, EBA/GL/2021/02, 2021. 130 s.
8. European Commission: Report on existing remote on-boarding solutions in the banking sector: Assessment of risks and associated mitigating controls, including interoperability of the remote solutions, 2019. 188 p.
9. FATF: Anti-money laundering and terrorist financing measures and financial inclusion -With a supplement on customer due diligence. Frace: Paris, 2011. 75 p.

10. FATF: Guidance for a risk-based approach virtual asset service providers, 2019. 57 p.
11. FATF: Guidance on Digital Identity. France: Paris, 2020. 46 p.
12. FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. France: Paris, 2012. 136 p.
13. FATF: Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems. France; Paris, 2020. 192 p.
14. The Wolfsberg Group: Wolfsberg Anti-Money Laundering Principles for Private Banking, 2012.
15. Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.
16. Smernica Európskeho parlamentu a Rady (EÚ) 2015/849 z 20. mája 2015 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu, ktorou sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 648/2012 a zrušuje smernica Európskeho parlamentu a Rady 2005/60/ES a smernica Komisie 2006/70/ES.
17. Smernica Európskeho parlamentu a Rady (EÚ) 2018/843 z 30. mája 2018, ktorou sa mení smernica (EÚ) 2015/849 o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí alebo financovania terorizmu a smernice 2009/138/ES a 2013/36/EÚ.
18. Stanovisko Finančnej spravodajskej jednotky k identifikácii a overeniu identifikácie klienta podľa AML zákona.
19. Záverečná sprava z národného hodnotenia rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu v podmienkach Slovenskej republiky. 219 s.
20. Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
21. Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a o ochrane pred financovaním terorizmu a o zmene a doplnení niektorých zákonov.
22. Usmernenie Finančnej spravodajskej jednotky k plneniu zákonných ovinnosti o zdieľaní informácií medzi poisťovňami a inými finančnými inštitúciami, najmä bankami podľa § 13 zákona č. 297/2008 Z. z.
23. Zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
24. Zákon č. 129/2010 Z. z. o spotrebiteľských úveroch a o iných úveroch a pôžičkách pre spotrebiteľov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

25. Metodické usmernenie Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 20. novembra 2012 č. 9/2012 k ochrane banky a pobočky zahraničnej banky pred legalizáciou príjmov z trestnej činnosti a pred financovaním terorizmu.
26. Stanovisko Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 10. decembra 2018 č. 1/2018 k identifikácii a overeniu identifikácie klienta – fyzickej osoby, bez jej fyzickej prítomnosti prostredníctvom technických prostriedkov a postupov podľa zákona o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.
27. Dôvodová sprava. Osobitná časť. LP/2021/200 Zákon o centrálnom registri účtov a o zmene a doplnení niektorých zákonov.