

Stanovisko
Útvary 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

Národná banka Slovenska (ďalej len „NBS“), útvary dohľadu nad finančným trhom na základe ustanovenia § 1 ods. 3 písm. a) bodu 3 zákona č. 747/2007 o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení neskorších predpisov po prerokovaní s Finančnou spravodajskou jednotkou národnej kriminálnej agentúry prezídia Policajného zboru Slovenskej republiky vydáva toto stanovisko:

Článok 1
Základné ustanovenia

1. S účinnosťou zákona od 15. marca 2018 môžu povinné osoby identifikovať a overovať identifikáciu klienta – fyzickej osoby, bez jej fyzickej prítomnosti s použitím technických prostriedkov a postupov¹⁾ (ďalej len „technológia“).
2. Pred začatím používania technológie je osoba, ktorou je dohliadaný subjekt alebo subjekt žiadajúci o povolenie na výkon činnosti podliehajúcej dohľadu NBS alebo o registráciu podľa osobitného zákona²⁾ (ďalej spoločne len „dohliadaný subjekt“), povinná vyhodnotiť, či takouto technológiou je možné vykonať identifikáciu a overenie identifikácie klienta - fyzickej osoby bez jej fyzickej prítomnosti na úrovni, ktorá je z hľadiska dôveryhodnosti výsledku overenia obdobná overeniu za jej fyzickej prítomnosti. Dohliadaný subjekt musí pri identifikácii a overovaní identifikácie zohľadniť okolnosti vykonávania obchodu a bezpečnostné riziká používaného technického prostriedku.
3. Cieľom tohto stanoviska je priblížiť dohliadaným subjektom rámcový pohľad NBS na technológie využívané na identifikáciu a overenie identifikácie fyzickej osoby bez jej fyzickej prítomnosti pri vykonaní starostlivosti vo vzťahu ku klientom dohliadaných subjektov podľa osobitného zákona.³⁾ Toto stanovisko sa nevzťahuje na identifikáciu a overenie identifikácie pri poskytovaní platobných služieb podľa osobitného predpisu.⁴⁾

¹⁾ § 8 ods. 1 písm. a) 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.

²⁾ Zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a 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.

³⁾ Zákon č. 297/2008 Z. z. o ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu v znení neskorších predpisov.

⁴⁾ § 2 ods. 1 písm. g) a h) zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

4. Na účely tohto stanoviska sa rozumie:
- technickým prostriedkom** prostriedok na identifikovanie a overenie identifikácie klienta - fyzickej osoby, ktorým je najmä softvérové riešenie dohliadaného subjektu vymedzené zabezpečeným digitálnym rozhraním umožňujúcim získavanie a prenos údajov, dokumentov a informácií prostredníctvom technických zariadení a ich následné spracovanie, na základe čoho dohliadaný subjekt vykoná identifikáciu a overenie identifikácie klienta - fyzickej osoby bez jej fyzickej prítomnosti na takej úrovni, ktorá je z hľadiska dôveryhodnosti výsledku overenia obdobná overeniu za jej fyzickej prítomnosti,
 - postupom** účelný, ustálený súhrn na seba naväzujúcich krokov pri identifikácii a overení identifikácie - klienta fyzickej osoby,
 - citlivým údajom** najmä osobný údaj podľa osobitného zákona,⁵⁾ ktorý je predmetom identifikácie a overenia identifikácie klienta - fyzickej osoby.

Článok 2

Povinnosti pri zavedení nového spôsobu identifikácie a overenia identifikácie klienta - fyzickej osoby bez jej fyzickej prítomnosti

- Pri zohľadňovaní rizikového faktora z hľadiska produktu, služby, obchodu, distribučného kanála a z geografického hľadiska, dohliadaný subjekt by mal zabezpečiť, aby identifikácia a overenie identifikácie klienta - fyzickej osoby bez jej fyzickej prítomnosti boli použité len pre také produkty a služby, ktoré sú svojou povahou a rozsahom vhodné a primerané pre tento spôsob overenia identifikácie klienta.
- Pri zohľadňovaní rizík dohliadaný subjekt by mal posúdiť rizikovú kategóriu klienta, správanie klienta počas používania technického prostriedku a všetky relevantné rizikové faktory, najmä faktory uvedené v prílohe č. 2 zákona.³⁾ Na požiadanie NBS by mal dohliadaný subjekt vedieť preukázať, ako identifikoval, vyhodnotil a zmiernil jednotlivé rizikové faktory. Dohliadaný subjekt by mal prijať také opatrenia, aby do procesu pri zavedení nového spôsobu identifikácie a overenia identifikácie klienta bez jej fyzickej prítomnosti bola zapojená aj osoba, ktorá zabezpečuje plnenie úloh pri ochrane pred legalizáciou príjmov z trestnej činnosti a financovaním terorizmu.
- Dohliadaný subjekt pred rozhodnutím o používaní technológie od externého dodávateľa by mal posúdiť a vyhodnotiť okrem rizík spojených s technickým prostriedkom aj iné riziká, napríklad vhodnosť dodávateľa technického prostriedku, dĺžku jeho pôsobenia na trhu, referencie od zákazníkov a celkovú reputáciu dodávateľa na trhu, ako aj výsledky testovania technického prostriedku.
- Za zavedenie technológie pri identifikácii a overení identifikácie klienta – fyzickej osoby bez jej fyzickej prítomnosti by mal byť zodpovedný príslušný riadiaci orgán dohliadaného subjektu, ktorý ju schvaľuje.
- Spôsob hodnotenia a riadenia rizík v súvislosti s identifikáciou a overením identifikácie klienta – fyzickej osoby bez fyzickej prítomnosti by mal byť obsahom Programu vlastnej činnosti podľa § 20 ods. 2 písm. c) zákona³⁾.

⁵⁾ § 2 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

6. Dohliadaný subjekt by mal zaradiť do obsahu a harmonogramu odbornej prípravy zamestnancov, ktorí môžu pri svojej práci prísť do styku s neobvyklou obchodnou operáciou, aj praktické používanie technického prostriedku, ako aj školenie na identifikovanie potenciálnych podozrivých situácií súvisiacich s používaním technického prostriedku. Školenie by malo byť súčasťou pravidelného vzdelávania v oblasti ochrany pred legalizáciou príjmov z trestnej činnosti a financovania terorizmu.
7. Kontrolný mechanizmus zavedenia a riadneho fungovania technológie by mal byť v súlade so všeobecne záväznými právnymi predpismi⁶⁾ a zohľadňovať záväzné postupy riadenia rizík.
8. Správnosť, kvalita a bezpečnosť prevádzky technického prostriedku by mala byť pravidelne testovaná. Dohliadaný subjekt by okrem toho mal priebežne monitorovať hodnotenie efektívnosti, bezpečnosti a správneho fungovania technického prostriedku. Všetky zistené chyby, nedostatky alebo zraniteľné miesta technológie je dohliadaný subjekt by mal odstrániť bez zbytočného odkladu po ich identifikácii a v prípade závažných zistení nepokračovať v používaní technického prostriedku až do ich odstránenia.
9. Dohliadaný subjekt by mal zaviesť postup aktualizácie technického prostriedku vrátane postupu pre opravy technického prostriedku v prípade bezpečnostných problémov, iných chýb a incidentov. Na tento účel by dohliadaný subjekt mal prijať také opatrenia, ktoré umožňujú potrebnú zmenu alebo zavedenie novej technológie.
10. Dohliadaný subjekt by mal mať vypracovaný plán na zabezpečenie kontinuity poskytovaných služieb a s nimi súvisiacich činností, ak technický prostriedok zlyhá a nebude schopný plnohodnotne zabezpečiť požadovanú kvalitu identifikácie a overenia identifikácie klienta - fyzickej osoby bez fyzickej prítomnosti. Dohliadaný subjekt by mal testovať plán na zabezpečenie kontinuity v pravidelných intervaloch.
11. Pred zavedením identifikácie a overenia identifikácie klienta - fyzickej osoby bez jeho fyzickej prítomnosti prostredníctvom technológie dohliadaný subjekt by si mal splniť voči NBS notifikačnú povinnosť v súlade s príslušnými zákonmi.⁷⁾

⁶⁾ Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES, zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

⁷⁾ § 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 zákon č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, § 20 ods. 6 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 v spojení s § 20 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.

Článok 3 Bezpečnosť technológie

1. Technológia by mala obsahovať postupnosť jednotlivých krokov a logické väzby medzi jednotlivými komponentmi systému na získanie údajov, informácií a dokumentov potrebných na identifikáciu a overenie identifikácie klienta - fyzickej osoby, na ich prenos, spracovanie a vyhodnotenie.
2. Technické prostriedky by mali spĺňať technické normy na bezpečnosť systému, na systém prístupov k citlivým údajom (napríklad šifrovanie, overovanie platnosti kľúčov a certifikátov, podpisovanie správ, technické a organizačné zabezpečenie citlivých údajov a pod.), musia byť v súlade najmä s nariadením GDPR⁸⁾ a zákonom o ochrane osobných údajov,⁹⁾ musia byť schopné zabezpečiť integritu a ochranu pred neoprávneným zásahom, zmenou, stratou a únikom citlivých údajov.

Článok 4 Funkcie technológie

1. Technický prostriedok, by mal porovnateľným spôsobom overiť pravosť, správnosť a úplnosť údajov, dokumentov a informácií o identifikovanej fyzickej osobe ako za jej fyzickej prítomnosti. Súčasťou postupov by malo byť overenie identifikácie z interných zdrojov dohliadaného subjektu (napríklad pri existujúcich klientoch) alebo z nezávislých externých zdrojov (napríklad evidencia dokladov totožnosti a údajov uvedených v dokladoch totožnosti, zoznamy politicky exponovaných osôb a sankcionovaných osôb v dôveryhodných databázach tretích osôb) alebo kombináciu vyššie uvedených zdrojov.
2. Pri identifikácii a overovaní identifikácie klienta - fyzickej osoby, bez jej fyzickej prítomnosti dohliadaný subjekt zabezpečí, aby mal technický prostriedok najmä tieto funkcie:
 - a) získanie autentických biometrických údajov¹⁰⁾ alebo iných porovnateľných údajov identifikovaním klienta - fyzickej osoby a ich dôveryhodné overenie,
 - b) detekcia nezrovnalostí biometrických údajov alebo iných porovnateľných údajov identifikovaním klienta - fyzickej osoby počas prenosu a nastavenie parametrov zhody,
 - c) overenie získaných biometrických údajov alebo iných porovnateľných údajov s údajmi z interných alebo externých zdrojov alebo ich kombináciou,
 - d) autentické biometrické údaje alebo iné porovnateľné údaje získane na účely identifikácie a overenie identifikácie klienta - fyzickej osoby, predstavujú porovnateľný /obdobný spôsob ako pri identifikácii a overení identifikácie klienta - fyzickej osoby za jej fyzickej prítomnosti,
 - e) získanie ďalších osobných údajov identifikovaného klienta - fyzickej osoby ako sú uvedené v písmene a) (napríklad doklad totožnosti),

⁸⁾ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES.

⁹⁾ Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

¹⁰⁾ § 5 písm. c) zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

- f) overenie pravosti a aktuálnosti získaných ďalších osobných údajov ako sú uvedené v písmene a) (napríklad na porovnanie dokladu totožnosti s údajmi z interných alebo externých zdrojov alebo ich kombináciou, vrátane overenia bezpečnostných prvkov dokladu totožnosti),
- g) identifikácia neštandardnej alebo rizikovej situácie a správania identifikovaného klienta - fyzickej osoby pri neverbálnej alebo verbálnej komunikácii alebo pri monitorovaní dohliadaného subjektu s identifikovaným klientom.

Článok 5 **Záverečné ustanovenie**

Toto stanovisko sa uplatňuje odo dňa jeho schválenia výkonným riaditeľom útvaru dohľadu nad finančným trhom NBS.

V Bratislave, dňa 13. decembra 2018.

Ing. Vladimír Dvořáček v. r.
člen bankovej rady, výkonný riaditeľ
útvaru dohľadu nad finančným trhom