# 4
# Metodické usmernenie Útvaru dohľadu nad finančným trhom Národnej banky Slovenska zo 17. decembra 2009 k ochrane banky a pobočky zahraničnej banky pred praním špinavých peňazí a financovaním terorizmu

Národná banka Slovenska, útvar dohľadu nad finančným trhom, na základe ustanovenia § 1 ods. 3 písm. a) bodu 3 zákona č. 747/2004 Z. z. o dohľade nad finančným trhom v znení neskorších predpisov, v spolupráci s Ministerstvom vnútra SR, Spravodajskou jednotkou finančnej polície, a s Ministerstvom financií SR vydáva toto metodické usmernenie.

## ÚČEL A OBSAH

Banky a pobočky zahraničných bánk (ďalej spolu „banka“) sú v priebehu svojej činnosti vystavené riziku, že klienti zneužijú ich služby v procese legalizácie príjmov získaných trestnou činnosťou (ďalej “pranie špinavých peňazí“) alebo na financovanie terorizmu. Bankám hrozia finančné straty, ak zanedbajú identifikáciu a posudzovanie ich klientov, nezistia neobvyklé finančné operácie klientov, alebo ak ich zamestnanci budú pomáhať klientom zneužiť banku na pranie špinavých peňazí, na financovanie terorizmu alebo na podvody. Ak sa banka dostane kvôli nedostatočnej obozretnosti pri výkone bankových činností do spojitosti s praním špinavých peňazí alebo financovaním terorizmu, utrpí v dôsledku negatívnej publicity stratu dobrého mena a tým aj stratu dôvery verejnosti a hospodársku stratu, čo môže spôsobiť stratu dôvery verejnosti v ďalšie bankové subjekty a narušenie stability bankového systému.

Bezúhonnosť a poctivosť manažmentu a jeho odhodlanie zabrániť tomu, aby banka bola použitá na pranie špinavých peňazí alebo financovanie terorizmu je prvoradou ochranou proti takýmto snahám. Manažéri bánk musia mať nielen koncepciu na ochranu pred praním špinavých peňazí a financovaním terorizmu, ale musia aj presadzovať účinné opatrenia, ktoré zabezpečia predovšetkým

- zisťovanie (ďalej aj „identifikácia“) a overovanie (ďalej aj „verifikácia“) skutočnej totožnosti klientov - osôb vstupujúcich s bankou do obchodných vzťahov,
- odhalenie a odmietnutie klientov a operácií, ktoré sú neobvyklé a
- potrebnú spoluprácu s policajnými orgánmi adohliadacími orgánmi, prokuratúrou a súdmi.

Banky sú povinné od 1. septembra 2008 dodržiavať povinnosti a uplatňovať oprávnenia zamerané na zabraňovanie praniu špinavých peňazí a financovaniu terorizmu v bankovom systéme, upravené zákonom 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 „zákon“) a zároveň postupovať aj v súlade s ustanoveniami zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej „ZOB“).

Povinnosti a oprávnenia upravené zákonom vyplývajú z implementácie smernice 2005/60/ES o predchádzaní využívaniu finančného systému na účely prania špinavých peňazí a financovania terorizmu (ďalej „tretia smernica“), prijatej v júni 2005, uverejnenej 26. októbra 2005 v Úradnom vestníku Európskej únie a účinnej od 15. decembra 2005. Podrobnosti a realizačné opatrenia ku tretej smernici upravuje smernica 2006/70/ES, ktorá stanovuje definíciu a technické aspekty definície politicky činných osôb a technické kritériá pre postupy pri zjednodušenej starostlivosti.

Účelom tohto metodického usmernenia je poskytnúť bankám vysvetľujúci materiál k plneniu ich úloh, vyplývajúcich z ustanovení zákona a ZOB a zameraných na prevenciu prania špinavých peňazí a financovania terorizmu vo finančnom systéme, ktorými bolo prevzatých štyridsať odporúčaní z júna 2003 a deväť špeciálnych odporúčaní Financial Action Task Force (okrem povinností vyplývajúcich z Nariadenia EÚ č. 1781/2006 o údajoch o príkazcovi, ktoré sprevádzajú prevody finančných prostriedkov a špeciálneho odporúčania VII).

Povinnosti určené uvedenými zákonmi sú minimálnymi požiadavkami kladenými na banky pri ich ochrane pred praním špinavých peňazí a ochrane pred financovaním terorizmu. Banky však v súlade s účelom sledovaným zákonom a týmto metodickým usmernením môžu využívať aj dokonalejšie a prísnejšie postupy, najmä také, ktoré sú už zaužívané a overené v ich praxi alebo v praxi ich materských spoločností z iných členských štátov Európskej únie. Môžu tak lepšie prispieť k realizácii globálnej politiky prevencie a ochrany pred praním špinavých peňazí a financovaním terorizmu v rámci finančnej skupiny, ktorej sú súčasťou.

**Metodické usmernenie sa člení na nasledujúce časti:**

A. Koncepcia a základné princípy ochrany pred praním špinavých peňazí a pred financovaním terorizmu
B. Zamestnanci zodpovední za realizáciu úloh ochrany pred praním špinavých peňazí a financovaním terorizmu
C. Program činnosti banky proti praniu špinavých peňazí a financovaniu terorizmu
D. Informovanosť a vzdelávanie zamestnancov, informačný systém
E. Identifikácia a akceptovanie klienta, rizikový profil klienta, základná, zjednodušená zvýšená starostlivosť, plnenie tretími stranami
F. Rozpoznávanie, zdržania a ohlasovanie neobvyklých obchodných operácií
G. Opatrenia proti financovaniu terorizmu
H. Uchovávanie údajov a dokumentácie
I. Zabezpečovanie, systém a výkon vnútornej kontroly

Text tohto metodického usmernenia, ktorý sa vzťahuje na banku, štatutárny orgán banky, člena štatutárneho orgánu banky alebo predsedu predstavenstva banky a zamestnancov banky, sa v primeranom rozsahu a zohľadnení súvislostí vzťahuje aj na pobočku zahraničnej banky, vedúceho pobočky zahraničnej banky, zástupcu vedúceho pobočky zahraničnej banky a zamestnancov pobočky zahraničnej banky.

## A. KONCEPCIA A ZÁKLADÉ PRINCÍPY OCHRANY BANKY PRED PRANÍM ŠPINAVÝCH PEŇAZÍ A PRED FINANCOVANÍM TERORIZMU

Základné povinnosti a oprávnenia banky zamerané na ochranu pred praním špinavých peňazí a financovaním terorizmu upravujú zákon a ZOB.

Banka pri tvorbe predpisov a konkrétnych postupov vychádza okrem zákona a ZOB aj z opatrení Národnej banky Slovenska, najmä Opatrenia NBS č. 12/2004 o rizikách a systéme riadenia rizík v znení Opatrenia NBS č. 15/2006 ako aj z vlastných stanov. Pritom zohľadňuje svoje obchodné zámery, existujúcu klientelu, rozsah bankových činností a produktov (druhov obchodov) a s tým súvisiacu potenciálnu hrozbu ich zneužitia na účely prania špinavých peňazí a financovania terorizmu.

Stanovy banky vymedzujú organizačnú štruktúru banky a systém riadenia banky, zodpovednosti osôb a útvarov a v rámci toho aj riadenie rizík, ktorým je banka vystavená pri svojej činnosti. Ochrana pred praním špinavých peňazí a financovaním terorizmu je súčasťou riadenia rizík v banke.

Banka musí mať vlastnú koncepciu ochrany pred jej zneužitím na pranie špinavých peňazí a financovanie terorizmu (ďalej aj „koncepcia ochrany banky“), a to ako vo vzťahu ku jej klientom, tak aj vo vzťahu k vlastným zamestnancom, ktorí by mohli pri výkone pracovných povinností zneužiť svoje pracovné zaradenie v banke na účel spojený s praním špinavých peňazí alebo financovaním terorizmu. Koncepciu ochrany banky prijíma štatutárny orgán, pričom koncepcia musí byť

a) premietnutá do organizačnej štruktúry banky a jej vnútorných predpisov v podobe primeraných postupov a činností a
b) trvale presadzovaná a realizovaná členmi štatutárneho orgánu, vedúcimi zamestnancami[1]) a zamestnancami, ktorí na jednotlivých pracoviskách banky vykonávajú finančné operácie klientov banky.

V rámci koncepcie ochrany banky by štatutárny orgán mal deklarovať a zverejniť svoj zámer a predstavu, ako zabrániť zneužitiu banky na pranie špinavých peňazí a financovanie terorizmu. Takýto postoj štatutárneho orgánu by mal byť jasne oznámený nielen zamestnancom, ale aj klientom banky a verejnosti, uverejnením napríklad v prevádzkových priestoroch banky, na internetovej stránke banky alebo aj vo výročnej správe banky.
Súčasťou koncepcie ochrany banky je stanovenie základných predpokladov a podmienok pre priebežnú realizáciu opatrení na ochranu pred praním špinavých peňazí a financovaním terorizmu pri výkone bankových činností a realizácii obchodov s klientmi v oblastiach upravených v zákone a v častiach B až I tohto metodického usmernenia.

## B. ZAMESTNANCI ZODPOVEDNÍ ZA REALIZÁCIU ÚLOH OCHRANY PRED PRANÍM ŠPINAVÝCH PEŇAZÍ A FINANCOVANÍM TERORIZMU

Za celkovú ochranu banky pred praním špinavých peňazí a financovaním terorizmu zodpovedá štatutárny orgán banky. Banka určí organizačným opatrením člena štatutárneho orgánu (predsedu predstavenstva alebo iného vedúceho zamestnanca) ako osobu zodpovednú

[1]) § 7 ods. 20 zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

za riadenie ochrany banky pred praním špinavých peňazí a pred financovaním terorizmu. Osoba poverená riadením uvedenej oblasti primerane zodpovedá spolu s určenou osobou za realizáciu politiky ochrany banky.

Za praktickú realizáciu hlavných úloh, dodržiavanie a priebežnú aktualizáciu postupov banky v tejto oblasti v súlade s právnymi predpismi, stanovami banky a medzinárodnými štandardmi zodpovedá určená osoba.
V bankovej terminológii, resp. v terminológii medzinárodných inštitúcií presadzujúcich princípy prevencie prania špinavých peňazí a financovania terorizmu je zaužívaný pojem „anti-money laundering compliance officer“, označujúci zamestnanca banky (prípadne finančnej alebo inej inštitúcie), ktorý zabezpečuje plnenie úloh ochrany pred praním špinavých peňazí a financovaním terorizmu. Vzhľadom na to, že slovenčina nemá priliehavý výraz pre tento post, resp. funkciu, v metodickom usmernení sa v súlade s § 20 ods. 2 písm. h) zákona používa pojem „určená osoba“ alebo skratka „UO“.

V rámci povinnosti banky rozdeliť a upraviť v stanovách banky právomoci a zodpovednosť za ochranu pred praním špinavých peňazí a ochranu pred financovaním terorizmu[2]) banka upraví postavenie UO tak, aby organizačne priamo podliehala najvyššej riadiacej úrovni v banke. UO pôsobí v rámci ústredia banky. Banka zabezpečí plnohodnotnú zastupiteľnosť UO určením zástupcu UO.
Ak banka zriadi aj útvar zodpovedný za výkon činností potrebných na zabezpečenie úloh preventívneho systému (ďalej „útvar prevencie“), UO je vedúcou uvedeného útvaru. Tento organizačný útvar má v náplni zodpovednosť za prípravu potrebných predpisov a postupov a plnenie riadiacich a kontrolných úloh v tejto oblasti.

Dostatočne nezávislé postavenie UO, jej zástupcu a útvaru prevencie v štruktúre vedúcich zamestnancov a organizačných útvarov je dôležitým prvkom systému ochrany pred praním špinavých peňazí a financovaním terorizmu. Začlenenie UO v organizačnej štruktúre banky obsahuje nasledujúce prvky zaručujúce relatívne nezávislé postavenie UO, jej zástupcu a útvaru prevencie:
- vymenovanie a odvolávanie UO a jej zástupcu štatutárnym orgánom, po predchádzajúcom prerokovaní s dozornou radou banky, resp. jej predsedom,
- upravenie právomocí a povinností UO a jej zástupcu v ich pracovných náplniach,
- oddelenie od útvarov zabezpečujúcich pre klientov banky výkon obchodov, resp. finančných operácií klientov,
- neobmedzený prístup UO a jej zástupcu ku všetkým dokumentom a databázam banky,
- samostatné rozhodovanie UO a jeho zástupcu pri posudzovaní neobvyklosti obchodných operácií (ďalej aj „NOO“) klientov banky, oznámených príslušnými zamestnancami banky v rámci interného systému oznamovania,
- rozhodovanie o zaslaní hlásenia o NOO finančnej spravodajskej jednotke (ďalej aj „FSJ“),
- kontrolná funkcia UO, jej zástupcu a útvaru prevencie vo vzťahu k útvarom a príslušným zamestnancom zabezpečujúcim výkon obchodov, resp. finančných operácií klientov,
- oddelenie UO, jej zástupcu a útvaru prevencie od útvaru vnútornej kontroly a vnútorného auditu v organizačnej štruktúre banky, ale pri súčasnom zachovaní ich činnosti

[2]) § 23, ods. 1, písm h) zákona č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

následnému výkonu kontroly uskutočňovanému útvarom vnútornej kontroly a vnútorného auditu.

Banka pri výberovom konaní na funkciu UO a jej zástupcu vyžaduje od kandidátov preukázanie občianskej bezúhonnosti, primerané vzdelanie a zodpovedajúcu odbornú prax. UO a jeho zástupca sú povinní vykonávať ich funkcie s riadnou starostlivosťou. Zodpovedajú za vypracovanie príslušných vnútorných predpisov, vzdelávanie príslušných zamestnancov, prijímanie interných oznámení o NOO a ich posudzovanie, rozhodovanie o ohlásení NOO a ich včasné ohlasovanie NOO finančnej spravodajskej jednotke.

Medzi povinnosti a oprávnenia určenej osoby patrí predovšetkým
- zabezpečovanie realizácie koncepcie ochrany banky,
- vypracovanie a priebežná aktualizácia vnútorného predpisu na ochranu pred praním špinavých peňazí a ochranu pred financovaním terorizmu, spolupráca na vypracovaní prípadných súvisiacich predpisov týkajúcich sa tejto problematiky pre jednotlivé útvary banky, druhy obchodov a finančné operácie klientov,
- spolupráca s útvarom vnútornej kontroly a vnútorného auditu pri postupe podľa § 41 ods. 2 ZOB ako aj právomoci zúčastniť sa na procese pripomienkovania, resp. hodnotenia pripravovaných nových druhov obchodov (produktov) banky z pohľadu rizika spojeného s praním špinavých peňazí a financovaním terorizmu a vyjadriť nesúhlasné stanovisko so zavádzaným novým druhom obchodu v prípade, že predstavuje pre banku neúmerné vystavenie sa tomuto riziku,
- organizácia vzdelávania príslušných zamestnancov banky a novoprijatých zamestnancov podieľajúcich sa na realizácii obchodov a finančných operácií klientov,
- prijímanie interných oznámení o NOO,
- ohlasovanie NOO finančnej spravodajskej jednotke a priebežné udržiavanie pracovných kontaktov s FSJ,
- monitorovanie dodržiavania vnútorných predpisov a postupov pre túto oblasť, vrátane výkonu kontroly vo vzťahu k posudzovaniu a oznamovaniu NOO príslušnými zamestnancami v súvislosti s realizáciou obchodov a finančných operácií klientov,
- pravidelné informovanie štatutárneho orgánu banky (najmenej však dvakrát ročne a v prípade potreby aj mimoriadne) o výsledkoch vlastnej činnosti a činnosti útvaru prevencie, osobitne o počte a obsahu zistených NOO, najčastejšie sa opakujúcich typoch NOO, počte a obsahu hlásení o NOO zaslaných FSJ, počte a obsahu nezaslaných hlásení a dôvodoch, ktoré viedli k rozhodnutiu o neohlásení,
- navrhovanie opatrení štatutárnemu orgánu v súvislosti s posudzovanými a zistenými NOO ako aj nedostatkami v oblasti ochrany banky.

V pobočkách banky, prípadne iných externých pracovných miestach, môže byť niektorý z príslušných zamestnancov poverený výkonom činností spojených s ochranou pred praním špinavých peňazí a ochranou pred financovaním terorizmu za pobočku. Tento zamestnanec je v priebežnom pracovnom kontakte s UO. Interné oznamovanie o zistených podozreniach o NOO zasielaných príslušnými zamestnancami z pobočiek banky určenej osobe v ústredí banky však nesmie byť podmienené súhlasom uvedeného povereného zamestnanca pobočky ani iného riadiaceho zamestnanca pobočky.

## C. PROGRAM ČINNOSTI BANKY PROTI PRANIU ŠPINAVÝCH PEŇAZÍ A FINANCOVANIU TERORIZMU

Stanovy banky v zmysle § 23 ZOB upravujú organizačnú štruktúru banky a jej vnútorný systém riadenia. Banka je povinná v stanovách rozdeliť a upraviť právomoci a zodpovednosť v banke za ochranu pred praním špinavých peňazí a financovaním terorizmu. Stanovy upravia aj oddelené riadenie rizík od riadenia bankových činností vrátane systému riadenia rizík, ktorým je banka vystavená pri výkone jej činností. Súčasťou úpravy riadenia rizík je aj ochrana banky pred praním špinavých peňazí a financovaním terorizmu.

Banka vypracuje Program činnosti banky proti legalizácii a financovaniu terorizmu (ďalej „Program“). Vnútorný predpis, ktorý obsahuje Program, schvaľuje štatutárny orgán banky. Program vychádza zo všeobecne záväzných právnych predpisov, najmä zo zákona, ZOB, opatrenia NBS o riadení rizík a z metodických usmernení FSJ, ako aj zo stanov banky. Program konkretizuje koncepciu na ochranu banky. Upravuje základné zásady a postupy banky na ochranu pred praním špinavých peňazí a pred financovaním terorizmu, najmä skutočnosti podľa § 20 ods. 2 zákona. Obsahuje aj konkrétne oprávnenia, povinnosti a postupy UO, preventívneho útvaru a príslušných zamestnancov banky, pri výkone bankových činností, druhov obchodov a finančných operácií klientov z hľadiska požiadaviek, ktoré vyžaduje ochrana pred praním špinavých peňazí a pred financovaním terorizmu, kontrolné oprávnenia týchto subjektov a kontrolné oprávnenia útvaru vnútornej kontroly a vnútorného auditu (časť I).

Banka zohľadňuje pri tvorbe Programu vlastné špecifiká, najmä jej veľkosť a podiel na trhu, organizačné členenie, druh a rozsah povolených a vykonávaných bankových činností, druhy obchodov a ich rozsah a špecifiká, druh a množstvo klientov a špecifiká a rozsah operácií týchto klientov. Program obsahuje nielen informácie o zákonných ustanoveniach, zodpovednostiach zamestnancov, ale najmä všetky operatívne postupy a povinnosti zamestnancov v podmienkach banky pri výkone relevantných druhov obchodov a finančných operácií klientov.

**Program činnosti banky proti legalizácii a financovaniu terorizmu upravuje najmä**

- určenie okruhu pozícií alebo funkcií zodpovedných za komplexnú ochranu banky pred zneužitím na pranie špinavých peňazí a financovanie terorizmu a za politiku a realizáciu postupov; vytvorenie organizačného systému tejto ochrany, zahrňujúceho člena štatutárneho orgánu, UO, prípadne útvar prevencie a príslušných zamestnancov vykonávajúcich finančné operácie pre klientov (ďalej „príslušní zamestnanci“),
- určenie osoby podľa § 20 ods. 2 písm. h) zákona, zodpovednej za zabezpečovanie ochrany pred praním špinavých peňazí a financovaním terorizmu, prijímanie oznámení o zistených NOO z organizačných útvarov banky, vyhodnocovanie týchto oznámení a ohlasovanie NOO finančnej spravodajskej jednotke a zabezpečujúcej priebežný pracovný styk banky s FSJ, prípadne orgánmi činnými v trestnom konaní,
- stanovenie základných úloh príslušných zamestnancov, ich postupu pri zisťovaní NOO a oznamovaní UO (prípadne aj vzorový formulár interných oznámení o NOO) a spôsob zabezpečenia ochrany príslušných zamestnancovv súvislosti s nimi zistenými NOO, oznámenými určenej osobe,
- povinnosť identifikovania klientov pri výkone obchodov a jednotlivých finančných operácií a povinnosť overovania (verifikácie) tejto identifikácie,

- povinnosť zaznamenania uskutočnenej identifikácie a overenia identifikácie klientov ako aj o všetkých finančných operácií vykonávaných pre klientov,
- povinnosť uchovávania záznamov o identifikácii a overení identifikácie klientov a o finančných operáciách uskutočnených klientmi,
- prehľad známych druhov NOO podľa činností a druhov obchodov vykonávaných bankou,
- hodnotenie a riadenie rizík - postupy pri posudzovaní klientov na základe rizikovo orientovaného prístupu a rizikových analýz, so zohľadnením výsledkov prvotnej a priebežnej identifikácie klientov a jej overenia podľa druhov obchodov a typov účtov,
- určenie spôsobu a rozsahu vykonávania starostlivosti vo vzťahu ku klientovi na základe výsledkov hodnotenia rizík, podľa § 10 ods. 4 zákona,
- postup pri posudzovaní, či je pripravovaný alebo vykonávaný obchod neobvyklý; podrobnejšie znaky neobvyklosti, podľa ktorých možno rozpoznať neobvyklú obchodnú operáciu klienta; tento postup by mal byť založený na predchádzajúcej analýze obchodných operácií uskutočňovaných konkrétnym klientom, s využitím elektronických informačných systémov, resp. programov,
- postup UO pri posudzovaní NOO oznámenej príslušnými zamestnancami, pri ohlasovaní NOO finančnej spravodajskej jednotke a spôsob a rozsah realizácie tzv. spätnej väzby v rámci banky o interných oznámeniach NOO,
- postup príslušných zamestnancov a UO pri zdržaní neobvyklej obchodnej operácie podľa § 16 zákona,
- obsah a harmonogram odbornej prípravy zamestnancov, ktorí môžu pri svojej práci prísť do styku s NOO, prípravu zamestnancov na zabezpečenie úloh ochrany banky pred praním špinavých peňazí a pred financovaním terorizmu pri výkone konkrétnych bankových činností, druhov obchodov a operácií klientov,
- povinnosť zachovávať mlčanlivosť o internom oznámení NOO a jej ohlásení FSJ a o vykonaných opatreniach FSJ (§ 18 zákona), a to predovšetkým vo vzťahu ku klientovi, ktorého sa to týka ako aj ku osobám, ktoré majú ku klientovi určitý vzťah (napr. iné osoby oprávnené disponovať s účtom klienta, alebo ak ide o viacerých vlastníkov finančných prostriedkov na jednom účte alebo vlastníkov právnickej osoby alebo iných konečných užívateľov výhod spojených s operáciou), ako aj k tretím osobám, okrem výnimiek určených zákonom,
- opatrenia, ktorými sa zamedzí zneužitiu postavenia alebo funkcie príslušných zamestnancov na vedomé zapojenie sa do prania špinavých peňazí alebo financovania terorizmu pri výkone ich funkcie,
- spôsob a lehoty uchovávania údajov a dokumentácie (bližšie v časti H),
- spôsob vykonávania kontroly dodržiavania povinností vyplývajúcich zo zákona a z Programu; určenie zodpovednosti za kontrolu a pravidelné správy v súvislosti so zistenými nedostatkami, obsahujúce hodnotenie dodržiavania povinností, zistené nedostatky a návrhy opatrení na odstránenie nedostatkov (interný audit) vrátane predkladania týchto správ štatutárnemu orgánu banky (vedúcemu pobočky zahraničnej banky).

Problematika ochrany pred praním špinavých peňazí a ochrany pred financovaním terorizmu si vyžaduje, aby Program bol vypracovaný ako ucelený predpis, ktorý je k dispozícii príslušnému členovi štatutárneho orgánu, UO a všetkým príslušným zamestnancom.
Banka je povinná Program primerane aktualizovať nielen pri zmene relevantných všeobecne záväzných právnych predpisov, ale aj pri zmenách týkajúcich sa jej vlastného výkonu činnosti a druhov obchodov ako aj pri zmenách jej organizačného usporiadania.

Pobočka zahraničnej banky sa taktiež riadi vnútornými predpismi v tejto oblasti[3]), ktoré musia zodpovedať obsahovou kvalitou požiadavkám vyplývajúcim zo zákona, ZOB, a regulačných opatrení Národnej banky Slovenska a FSJ.

## D. INFORMOVANOSŤ, VZDELÁVANIE ZAMESTNANCOV, INFORMAČNÝ SYSTÉM

### 1. Informovanosť zamestnancov

Manažéri aj zamestnanci banky si musia uvedomovať, že účasť klientov banky na praní špinavých peňazí alebo na financovaní terorizmu môže ohroziť banku. Banka môže utrpieť v konečnom dôsledku finančné straty, ak uskutoční operácie s výnosmi alebo prostriedkami pochádzajúcimi z akejkoľvek trestnej činnosti, pričom dôjde aj k ohrozeniu alebo strate jej dobrého mena. Sankciám za nesplnenie alebo porušenie povinností v tejto oblasti podliehajú nielen banky ako právnické osoby, ale môžu byť postihnutí osobne aj členovia štatutárneho orgánu, dozornej rady, vedúci zamestnanci uskutočňujúci kontrolu a príslušní zamestnanci, ktorí sú v priamom styku s klientmi a realizujú pokyny klientov na vykonanie obchodov a finančných operácií.

Banka vhodným spôsobom zverejnení informáciu pre zamestnancov o tom, kto vykonáva funkciu UO a kto zastupuje UO. Táto informácia obsahuje aj prehľad o základných prvkoch systému prevencie, ktorý je v banke uplatňovaný, o základných oprávneniach a povinnostiach UO a jej zástupcu ako aj o zabezpečovaní ochrany príslušných zamestnancov, ktorí zisťujú NOO.

Efektívnosť prípravy príslušných zamestnancov a ich náležité oboznámenie sa s ich povinnosťami a oprávneniami sú rozhodujúce pre úspešnosť nepretržitého procesu ochrany pred praním špinavých peňazí a pred financovaním terorizmu. Štatutárny orgán a UO musia zabezpečiť informovanosť zamestnancov o zodpovednosti banky ako aj osobnej zodpovednosti vedúcich zamestnancov a príslušných zamestnancov banky v tejto oblasti.

Banka stanoví optimálny režim a spôsob
- informovania jej príslušných zamestnancov o princípoch, postupoch, povinnostiach a oprávneniach pri ochrane pred praním špinavých peňazí a financovaním terorizmu
- sprístupnenia Programu a prípadne ďalších relevantných predpisov príslušným zamestnancom a
- organizácie odbornej prípravy a vzdelávacích akcií pre príslušných zamestnancov.

Banka pri informovaní a vzdelávaní zamestnancov zohľadňuje svoje podmienky, najmä veľkosť a organizačné členenie na pobočky a menšie pracoviská, bankové činnosti a druhy obchodov a finančné operácie vykonávané pre klientov, aby sa všetky potrebné informácie dostali ku všetkým zamestnancom, pre ktorých sú určené. Je dôležité, aby model poskytovania informácií zamestnancom zo strany štatutárneho orgánu, UO a vedúcich zamestnancov banky ako aj realizácie odbornej prípravy zamestnancov bol efektívny, flexibilný a plnil očakávaný cieľ.

[3]) § 5 ods. 2 v spojení s § 20 zákona

## 2. Informačný systém v banke

Systémový prístup k riadeniu rizika banky a zabezpečovaniu ochrany banky pred praním špinavých peňazí a financovaním terorizmu vyžaduje vybudovanie vhodného informačného systému v banke a zabezpečenie plynulého a včasného toku informácií medzi jednotlivými riadiacimi úrovnami banky, vrátane štatutárneho orgánu banky, UO, jej zástupcu a útvaru prevencie, útvaru vnútornej kontroly a vnútorného auditu a príslušných zamestnancov. Systémový prístup si okrem zabezpečenia plynulého a včasného toku týchto informácií vyžaduje aj vybudovanie a udržiavanie tokov interných informácií na jednotlivých riadiacich úrovniach banky.V širšom ponímaní ide o systém získavania, spracovania, vyhodnocovania, odovzdávania a aj používania informácií týkajúcich sa tejto oblasti. Jeho súčasťou sú toky informácií v procese jednotlivých činností banky a vykonávaných druhov obchodov pri ochrane pred praním špinavých peňazí a financovaním terorizmu.

Je dôležité, aby vedenie banky dostávalo pravidelne informácie o funkčnosti a účinnosti systému prevencie prania špinavých peňazí a financovania terorizmu v banke. Tieto informácie by mali štatutárnemu orgánu banky a vedúcim zamestnancom slúžiť ako podklad pre prijímanie zásadných a systémových opatrení pre odstraňovanie pripadných systémových nedostatkov a zachovanie potrebnej úrovne systému prevencie. Tvorcom týchto informácií by mal byť predovšetkým útvar vnútornej kontroly a vnútorného auditu banky a UO s útvarom prevencie.

Banka je povinná zabezpečiť a používať vlastný informačný systém na

- prenos informácií smerom k príslušným zamestnancom o princípoch ochrany pred praním špinavých peňazí a financovaním terorizmu, postupoch, povinnostiach a oprávneniach a s tým súvisiacim zabezpečovaním každodenných úloh,
- sprístupnenie Programu a ďalších relevantných vnútorných predpisov príslušným zamestnancom,
- prenos potrebných informácií medzi členom štatutárneho orgánu banky zodpovedným za oblasť ochrany pred praním špinavých peňazí a financovaním terorizmu (prípadne predsedom predstavenstva) a UO,
- prenos informácií medzi príslušnými zamestnancami a UO a naopak, vrátane interného oznamovania NOO,
- vedenie evidencie, t. j. zaznamenávanie, spracúvanie a aktualizovanie údajov o klientoch a zaznamenávanie a monitorovanie obchodných operácií klientov,
- oboznamovanie štatutárneho orgánu, resp. jeho zodpovedného člena (prípadne predsedu predstavenstva) s výsledkami kontroly uskutočňovanej UO a útvarom vnútornej kontroly a vnútorného auditu ako aj informovanie príslušných zamestnancov o týchto výsledkoch,
- prenos informácií medzi UO a FSJ, vrátane ohlasovania NOO a poskytovania ďalších potrebných informácií a podkladov FSJ ako aj poskytovania tzv. spätnej väzby od FSJ banke.

Pravidelné, sústavné získavanie a vyhodnocovanie informácií v procese identifikácie a verifikácie, monitorovania obchodného vzťahu a posudzovania obchodov, interného oznamovania obchodov so znakmi NOO a ohlasovania NOO finančnej spravodajskej jednotke sú nedeliteľnými súčasťami povinností zamestnancov zainteresovaných v tomto procese.

Formu, obsah a pravidlá tohto informačného toku by si mala stanoviť banka v závislosti od jej veľkosti, zamerania, rozsahu a zložitosti ňou vykonávaných činností a ponúkaných druhov obchodov a služieb ako aj charakteristických znakov klientov a ich obchodov.
Informačný systém má vyhovovať špecifickým podmienkam banky a z technického hľadiska má mať také parametre, aby banka bola spôsobilá plniť povinnosti, ktoré pre ňu ako povinnú osobu vyplývajú zo zákona.

Podstatnou súčasťou informačného systému banky je elektronický informačný systém (ďalej „EIS“), ktorý z hľadiska hardvérového a softvérového vybavenia zodpovedá požiadavkám zákona stanoveným pre banky, s cieľom zabezpečenia dostatocnej kvality ochrany pred praním špinavých peňazí a financovaním terorizmu.

EIS, zaznamenávajúci a spracúvajúci údaje o klientoch banky a ich finančných operáciách, musí zohľadňovať požiadavky upravené v § 9 písm. e) zákona. Ak ide o klienta - fyzickú osobu, EIS musí obsahovať záznamy najmenej s menom, priezviskom, dátumom narodenia alebo rodným číslom a čísla účtov klienta a pri fyzickej osobe - podnikateľovi aj identifikačné číslo, ak mu bolo pridelené. Ak ide o klienta - právnickú osobu, EIS musí obsahovať záznamy obsahujúce najmenej názov (obchodné meno) a identifikačné číslo takéhoto klienta.

EIS musí zároveň obsahovať informácie/záznamy o povahe obchodného vzťahu klienta. Povaha obchodného vzťahu je daná druhom obchodu v zmysle § 9 písm. i) zákona alebo len obchodom podľa § 9 písm. h) zákona. EIS a spôsob jeho využívania majú umožňovať rozpoznať NOO uskutočňované klientmi, prípadne sledovať aj ich priebeh alebo vývoj, ako aj spojitosti medzi finančnými operáciami určitého klienta a, pokiaľ je to možné, aj neobvyklými obchodnými operáciami rôznych klientov.

Osobitnou časťou informácií zaznamenaných a sledovaných prostredníctvom EIS sú údaje o politicky exponovaných osobách (§ 6 zákona) a o fiktívnych bankách [§ 9 písm. d) a § 24 ods. 1 zákona], ktoré príslušní zamestnanci získali pri výkone pracovných úloh.

EIS má slúžiť banke aj na sledovanie potrebných údajov na účel vedenia registra podozrivých klientov podľa § 92 ods. 6 písm. a) ZOB a výmenu informácií s inými bankami podľa § 92 ods. 6 písm. b) ZOB. Ďalšie situácie, v ktorých môže banka využiť EIS pri poskytovaní informácií, vyplývajú z ustanovenia § 18 ods. 8 zákona.

EIS má umožniť, aby banka bezodkladne poskytla FSJ na jej žiadosť informácie o tom, či má, alebo mala obchodný vzťah s konkrétnou osobou v predchádzajúcich piatich rokoch ako aj o povahe takého obchodného vzťahu (§ 24 ods. 4 zákona).

EIS má byť taktiež spôsobilý včasne a v dostatočnom rozsahu poskytovať údaje FSJ, Národnej banke Slovenska - útvaru dohľadu nad finančným trhom ako dohliadaciemu orgánu a orgánom činným v trestnom konaní v zákonom určených prípadoch. V neposlednom rade EIS má zodpovedať požiadavkám na účely kontroly pre vlastnú potrebu banky a pre potrebu FSJ (§ 30 zákona) a na štatistické účely.

### 3. Vzdelávanie zamestnancov

Efektívnosť ochrany banky pred praním špinavých peňazí a financovaním terorizmu závisí od prístupu jej manažmentu a zamestnancov k tejto problematike a osvojení si základných právnych predpisov, Programu a ďalších súvisiacich vnútorných predpisov banky.

Rôznorodosť vykonávaných bankových činností a druhov obchodov a najmä rôznorodosť štruktúry klientov zahrňujú aj rôzny stupeň rizika prania špinavých peňazí a/alebo financovania terorizmu. Príslušní zamestnanci musia mať všetky potrebné informácie o bankových činnostiach a druhoch obchodov vykonávaných bankou, ktoré budú realizovať pre klientov a musia si čo najskôr osvojiť kritériá (znaky neobvyklosti) na posudzovanie, resp. zisťovanie NOO. Títo zamestnanci musia dokázať posúdiť konanie klientov banky ako aj obsah klientmi vykonávaných finančných operácií z hľadiska stupňa ich rizikovosti, neobvyklosti alebo podozrivosti.

Príslušní zamestnanci sú dôležitým článkom pre zamedzenie zneužitiu banky na pranie špinavých peňazí a/alebo financovanie terorizmu. Rovnako však môžu byť aj jeho najslabším prvkom, ak neplnia určené povinnosti, alebo ak sa vedome ci nevedome zúčastnia na realizácii NOO klienta.

Skôr, než zamestnanec nastúpi do pracovného pomeru v banke na pracovné miesto alebo do funkcie, kde bude v priamom kontakte s klientmi zabezpečovať realizáciu finančných operácií, banka sa na základe výpisu z registra trestov budúceho zamestnanca presvedčí, že budúci zamestnanec nemá v registri trestov záznam o predchádzajúcej majetkovej, hospodárskej alebo inej závažnej trestnej činnosti. Banka môže budúceho zamestnanca požiadať o informáciu aj nad rámec výpisu z registra trestov, vtedy by však mala zohľadniť, že v zmysle trestného zákona ak bolo odsúdenie osoby zahladené, hľadí sa na túto osobu, ako keby nebola odsúdená. Banka by mala vyžiadať od budúceho zamestnanca aj dostatočne uspokojivú referenciu, resp. posudok o jeho predchádzajúcej pracovnej bezúhonnosti, vydaný jeho predchádzajúcim zamestnávateľom.

Aj v rámci vzdelávania banka zabezpečí, aby boli zamestnanci oboznámení s dôsledkami zanedbania alebo nedbalého plnenia svojich pracovných povinností a prípadnej vedomej či nevedomej účasti na praní špinavých peňazí alebo financovaní terorizmu, ako aj porušenia zákazu poskytnutia informácií klientovi, na ktoré sa vzťahuje povinnosť mlčanlivosti (§ 18 zákona).

Vzdelávanie zamestnancov má významne prispieť k tomu, aby príslušní zamestnanci získali predpoklady pre zvládnutie postupov na uplatňovanie zásady „poznaj svojho klienta“ („Know Your Customer“, ďalej „KYC“) a rozpoznávanie stupňa rizikovosti konania klientov banky, a to aj so zohľadnením zaradenia klientov do jednej z troch skupín pre výkon povinnej starostlivosti, t. j. základnej, zjednodušenej a zvýšenej starostlivosti.

Banka musí mať projekt, resp. plán vzdelávania zamestnancov, zohľadňujúci pracovné zaradenie zamestnancov a z toho vyplývajúce zodpovednosti a povinnosti. Plán vzdelávania, resp. jeho základné zásady, by mal byť súčasťou Programu a mal by určiť základnú osnovu, periodicitu a obsah odbornej prípravy zamestnancov, najmä ustanovenia príslušných zákonov, vnútorné predpisy a pravidlá banky, resp. skupiny do ktorej banka patrí, ako aj analýzu obsahu a súvislostí najčastejšie sa vyskytujúcich druhov interných oznámení o NOO v rámci banky, prípadne v rámci skupiny.

Banka je povinná v zmysle § 20 ods. 3 zákona zabezpečiť odbornú prípravu zamestnancov, zameranú na oboznámenie sa s Programom, a to najmenej raz za kalendárny rok a zároveň vždy pred zaradením zamestnanca na prácu, pri ktorej bude plniť úlohy stanovené zákonom a

Programom. Každý príslušný zamestnanec, ktorý plní úlohy podľa zákona, musí byť oboznámený s platným Programom upravujúcim postupy pri posudzovaní klientov a nimi vykonávaných finančných operácií a musí mať tento Program vždy k dispozícii.

Vzdelávanie zahŕňa odbornú prípravu novoprijatých zamestnancov a priebežné špecializované odborné vzdelávanie príslušných zamestnancov realizujúcich finančné operácie klientov. Frekvencia vzdelávacích podujatí má byť primeraná, aby umožnila poskytnutie informácií o nových všeobecne záväzných právnych predpisoch, Programe a aktuálnych vnútorných predpisoch a sprístupnila vlastné poznatky vyplývajúce z činnosti banky, z činnosti iných bankových subjektov ako aj dostupné poznatky vychádzajúce z činnosti FSJ, prípadne dohliadacieho orgánu.
Špecializované vzdelávanie, ktoré príslušní zamestnanci majú absolvovať skôr, než budú spracovávať pokyny klientov na vykonanie finančných operácií, by im malo dať potrebné znalosti pre zisťovanie a overovanie totožnosti klientov pri vzniku obchodného vzťahu a pri výkone obchodov a operácií. Účasťou na vzdelávacích podujatiach (semináre, stáže) príslušní zamestnanci získajú predpoklady pre spoznanie typu očakávaných obchodných aktivít klientov, s ktorými súvisia ich finančné operácie, a teda aj potrebné vedomosti a spôsobilosť identifikovať skutočnosti vymykajúce sa z očakávaného správania klientov a konkrétne prejavy ich neobvyklých obchodnych operácií.

Banka má vzdelávanie opakovať a doplňovať o nové poznatky v prípade potreby aj častejšie ako v 12-mesačnom cykle, aby sa zabezpečilo, že príslušní zamestnanci budú schopní priebežne vykonávať ich povinnosti a oprávnenia.

Banka zabezpečí vypracovanie záznamov o uskutočnenej odbornej príprave zamestnancov, ktoré obsahujú dátum účasti príslušných zamestnancov na vzdelávaní, obsah vzdelávania a aj podpisy zamestnancov, ktorí absolvovali odbornú prípravu. Okrem toho od príslušných zamestnancov je potrebné získať písomné potvrdenie aj o tom, že sa oboznámili s Programom a súvisiacimi predpismi upravujúcimi postupy pri ochrane banky pred praním špinavých peňazí a financovaním terorizmu.

## E. IDENTIFIKÁCIA A AKCEPTOVANIE KLIENTA, RIZIKOVÝ PROFIL KLIENTA; ZÁKLADNÁ, ZJEDNODUŠENÁ, ZVÝŠENÁ STAROSTLIVOSŤ, PLNENIE TRETÍMI STRANAMI

Základné povinnosti banky v týchto oblastiach určujú príslušné ustanovenia zákona, najmä ustanovenia § 7, 8 a 10 až 13, ako aj ZOB, najmä ustanovenia § 89 a § 93a.

V praxi to znamená, že banka uskutoční všetky prvky základnej starostlivosti o klienta (fyzickú osobu aj právnickú osobu) podľa § 10 ods. 1 zákona vždy v situáciách uvedených v odseku 2 tohto ustanovenia. Pri jednorazových obchodoch mimo obchodného vzťahu banka identifikuje a overuje identifikáciu vždy, ak obchod dosiahne hodnotu aspoň 2 000 EUR.
Nasleduje povinnosť zisťovať, či klient koná vo vlastnom mene. Pre účel tohto metodického usmernenia je potrebné chápať „vykonávanie obchodu na vlastný účet“, resp. s „vlastnými prostriedkami“ ako konanie vo vlastnom mene. Podľa ustanovenia § 10 ods. 10 zákona je potrebné túto skutočnosť zistiť vždy v situáciách uvedených v ustanovení § 10 ods. 2 a v súlade s ustanovením § 89 ods. 3 ZOB aj ak ide o obchod aspoň vo výške 15 000 EUR (teda nie iba „príležitostný“, ako to vyplýva zo zákona).

Zisťovanie a v primeranom rozsahu aj overovanie konečného užívateľa výhod sa riadi predovšetkým ustanoveniami § 9 a 10 zákona, pričom aj ZOB čiastočne rieši tento dôležitý prvok základnej aj zvýšenej starostlivosti o klienta v § 93a. Táto oblasť je jedným zo základných preventívnych opatrení, ktoré umožňujú FSJ a neskôr aj orgánom činným v trestnom konaní sledovať pohyb finančných prostriedkov a zisťovať aj možné prepojenia fyzických osôb a právnických osôb nielen na území SR, ale aj v zahraničí, a to prostredníctvom výmeny informácií medzi finančnými spravodajskými jednotkami rôznych štátov. (V ideálnom prípade po vynesení právoplatného rozsudku súdu alebo ešte aj počas súdneho procesu a v prípade „zmrazenia" finančných prostriedkov na základe medzinárodných sankcií sa realizáciou identifikácie a overenia identifikácie klientov a konečných užívateľov výhod umožňuje dočasne alebo trvale siahnuť na finančné prostriedky od uplatnenia prechodných opatrení, ako napr. zaistenia majetku, až po prepadnutie majetku.).
Ide zároveň asi aj o najprácnejšiu a najnákladnejšiu časť uskutočňovania základnej a zvýšenej starostlivosti, v ktorej je mimoriadne dôležité uplatniť rizikovo orientovaný prístup banky voči klientom a ich finančným operáciám. Znamená to, že konečného užívateľa výhod je potrebné zisťovať vždy; v prípade právnických osôb nesmie právna forma spoločnosti (napr. akciová spoločnosť s akciami na doručiteľa alebo združenie majetku) prekážať pri zisťovaní konečného užívateľa výhod. Overovanie získanej informácie o konečnom užívateľovi výhod v súlade so zákonom sa má uskutočňovať v primeranom rozsahu; napr. vyžiadanim písomného vyhlásenia o konečnom užívateľovi výhod a následným overením takejto informácie z dostupných zdrojov.

Význam ustanovení § 10 ods. 1 písm. a) až c) a ods. 10 zákona je zvýraznený v ustanoveniach § 15 a § 24 ods. 2 zákona, v ktorých je banke uložená povinnosť odmietnuť nového klienta, ukončiť existujúci obchodný vzťah s klientom, alebo odmietnuť uskutočnenie konkrétnej obchodnej operácie v prípade, ak nie je možné uskutočniť základnú starostlivosť. Porovnateľná povinnosť vyplýva z ustanovenia § 89 ods. 1 ZOB. Takéto prípady je banka povinná podľa § 17 ods. 1 ihneď ohlásiť FSJ.

Pri nových klientoch by malo byť súčasťou akceptovania klienta okrem uskutočnenia základnej starostlivosti aj jeho zaradenie do určitej rizikovej skupiny, pričom predpokladom by malo byť dôsledné uplatňovanie princípu, „KYC", čo vlastne znamená zabezpečenie získania dostatočných informácií o charaktere očakávaných obchodov klienta a akejkoľvek predvídateľnej schémy ním uskutočňovaných operácií. Na základe toho je možné vytvoriť rizikový profil klienta. Pri uplatnení základnej starostlivosti banka nesmie vstúpiť do obchodného vzťahu s klientom, kým spoľahlivo nezistí všetky relevantné okolnosti týkajúce sa klienta (vrátane zistenia konečného užívateľa výhod a primeraných opatrení na overenie tejto informácie), ako aj klientom realizovaný alebo predpokladaný charakter obchodovania, resp. podnikania alebo jeho inej činnosti.
Vedúci zamestnanci a príslušní zamestnanci banky musia poznať klientov banky a ich bežnú obchodnú, podnikatelskú alebo inú činnosť. Na základe získaných informácií sú potom príslušní zamestnanci banky a ich priami nadriadení schopní počas existencie obchodného vzťahu banky s klientom posúdiť každý pokyn klienta na nakladanie s finančnými prostriedkami vedenými na jeho účte, v porovnaní s očakávaným správaním tohto klienta. Zohľadňujú pritom okolnosti, ktoré môžu naznačovať zmenu charakteru podnikania klienta alebo zmenu jeho obvyklej činnosti a primerane tieto skutočnosti overujú.

Banka aktualizuje informácie o klientovi podľa rizikovej skupiny, do ktorej bol klient zaradený; s týmto cieľom požaduje od klienta aktualizovanie údajov, ktoré jej klient pôvodne poskytol, resp. už predtým aktualizoval, a to v rozumných časových intervaloch a v závislosti od zmien, ktoré sa týkajú osoby klienta či jeho obchodných alebo iných aktivít, s ktorými sú spojené jeho finančné operácie uskutočňované bankou. Banka môže túto aktualizáciu uskutočňovať aj prostredníctvom požiadania o vyplnenie príslušného formuláru, napríklad raz za rok, ak nie je nevyhnutná častejšia aktualizácia, alebo dohodnutím zmluvnej podmienky s klientom o povinnosti ohlásenia príslušných zmien banke vopred.

Banka vykoná v zmysle prechodného ustanovenia § 36 ods. 1 zákona postupy na zistenie všetkých prvkov základnej starostlivosti, vrátane identifikácie a verifikácie konečného užívateľa výhod podľa § 10 zákona a zvýšenú starostlivosť podľa § 12 zákona, aj vo vzťahu k existujúcim klientom, v závislosti od rizika legalizácie alebo financovania terorizmu, a to do 31. decembra 2009.
V praxi to znamená, že je nutné rozčleniť súčasnú klientelu banky podľa rizika prania špinavých peňazí a/alebo financovania terorizmu, pričom zákon v § 10 ods. 4 uvádza, že pri takomto členení sa dajú využiť informácie o klientovi, druhu obchodu, obchodného vzťahu, atď. Súčasťou základnej starostlivosti je podľa ustanovenia § 10 ods. 11 zákona aj zisťovanie, či je klient politicky exponovanou osobou; v kladnom prípade tu banka realizuje zvýšenú starostlivosť.

V tejto súvislosti je potrebné využiť doterajšie poznatky o klientoch a o uplatňovaní preventívneho systému v banke z predchádzajúcej právnej úpravy, základom ktorej bolo ohlasovanie NOO. Zákon ponechal definícii NOO rovnaký obsah; v ustanovení § 4 však pribudol odsek 2, príkladmo uvádzajúci obchody, ktoré je potrebné považovať za NOO a ktoré by mali byť ohlásené FSJ (v závislosti od konkrétnych okolností prípadu). Okrem toho je vhodné využívať aj materiály vypracované expertmi Financial Action Task Force (zverejnené na internete), napríklad:
- pravidelne publikované závery priebežného monitoringu krajín, ktoré majú výrazné nedostatky pri presadzovaní opatrení proti praniu špinavých peňazí a financovaní terorizmu („FATF statement“),
- podrobné hodnotiace správy o jednotlivých krajinách a ich systéme prevencie a represie v oblasti prania špinavých peňazí a financovania terorizmu (v podobe „Mutual Evaluation Report“),
- vysvetľujúcu prezentáciu „Guidance on the risk-based approach to combating money laundering and terrorist financing“ z júna 2007,
- tzv. zoznam tretích ekvivalentných krajín, ktorý vznikol na základe dohody členských štátov EÚ vo výbore Európskej komisie (CPMLTF - Committee on Prevention Money Laundering & Terrorist Financing) a je publikovaný na internetovej stránke FSJ.

V súvislosti s rozčlenením klientov podľa ich rizikovosti je potrebné, aby banka vzala do úvahy ustanovenia § 10 ods. 1 písm. d) a ods. 8 zákona, ktoré zakladajú povinnosť priebežne aktualizovať rizikový profil klienta. Vhodná periodicita akualizácie záleží na vnútornom rozhodnutí banky, v každom prípade je potrebné takúto povinnosť zahrnúť do vnútorného predpisu upravujúceho Program banky podľa § 20 zákona.

Prostredníctvom rozčlenenia klientov podľa ich rizikového profilu banka potom môže v praxi uplatňovať ustanovenie § 10 ods. 1 písm. d) zákona – priebežné monitorovanie obchodného vzťahu, ktoré vedie k rozpoznaniu a aj ohláseniu NOO.

Vyššia rizikovosť klienta si vyžaduje podrobnejšie posudzovanie klienta, jeho konania a ním zadávaných príkazov na realizáciu finančných operácií. Následne je nutné prijať opatrenia na elimináciu rizika na prijateľnú úroveň.
Banka uplatňuje zvýšenú starostlivosť voči klientovi v situáciách, ktoré vzhľadom na svoju povahu môžu predstavovať vyššie riziko prania špinavých peňazí alebo financovania terorizmu. Banka venuje osobitnú pozornosť vybraným skupinám subjektov, a to okrem už uvedených politicky exponovaných osôb (§ 6, § 10 a § 12 zákona), najmä združeniam majetku (§ 25 ods. 2) a fiktívnym bankám (§ 24 ods. 1).
Banka rovnako postupuje, ak sa pripravuje založenie

- nového obchodného vzťahu alebo účtu bez fyzickej prítomnosti klienta a
- nových korešpondenčných vzťahov so zahraničnými bankami, resp. úverovými inštitúciami.

Zákon v súlade s implementovanými smernicami EÚ vymedzuje iba základné situácie, ktoré predstavujú zvýšené riziká prania špinavých penazi a financovania terorizmu. Sprísnený postup identifikácie a verifikacie získaných faktov a následného monitorovania obchodného vzťahu s klientom však banka musí uplatňovať aj v ďalších situáciách, podľa rizikového profilu klienta alebo podľa miery rizika poskytovanej služby, resp. druhu obchodu pre klienta (právnické osoby nezapísané v obchodnom registri, napr. politické strany, právnické osoby vo forme akciových spoločností s akciami na doručiteľa, spoločné účty, účty spojené s držiteľskou správou, atď.).

Presadzovanie a dodržiavanie všetkých uvedených postupov a pravidiel (identifikácia, verifikácia, KYC) poskytuje okrem rozoznávania NOO a minimalizácie rizika prania špinavých peňazí a financovania terorizmu aj ochranu pred podvodmi. Súčasne umožňuje banke vybrať a ponúknuť zo škály druhov obchodov tie, ktoré konkrétnym klientom vyhovujú podľa obsahu a rozsahu ich aktivít. Tým napomáha banke udržať si klientov, ktorí nie sú spojení s praním špinavých peňazí a podvodmi a súčasne eliminovať riziko finančných strát a riziko straty dobrého mena banky.

Použitie už uskutočnenej základnej starostlivosti - okrem jednej súčasti základnej starostlivosti, ktorou je priebežné monitorovanie obchodného vzťahu v zmysle § 10 ods. 1 písm. d) zákona - inou úverovou alebo finančnou inštitúciou pri uplatňovaní postupov starostlivosti vo vzťahu ku klientovi umožňuje zákon v ustanovení § 13, tzv. plnením tretími stranami. Ide o to, že za splnenia predpokladov uvedených v tomto ustanovení je možné spoľahnúť sa na už vykonanú identifikáciu a verifikáciu klienta a konečného užívateľa výhod a prevziať údaje o tejto identifikácii a verifikácii od úverovej alebo finančnej inštitúcie (v rozsahu podľa ustanovenia § 5 ods. 1 písm. b) bodov 1 až 10 zákona), ktorá pôsobí na území EÚ (tzv tretia strana), vrátane tých, ktoré pôsobia na území SR. (Zmenárne a devízové miesta sú mimo okruhu povinných osôb, od ktorých je možné prevziať identifikáciu a verifikáciu klienta a konečného užívateľa výhod). Zodpovednosť za to, že takto nadobudnuté údaje spĺňajú požiadavky na výkon starostlivosti voči klientovi podľa ustanovení zákona, však ostáva na banke, ktorá sa rozhodla spoliehať sa na postup „plnenia tretími stranami“.
Zákon podľa ustanovenia § 13 ods. 4 považuje „outsourcing“ za činnosť vykonávanú pre banku na základe jej pravidiel a predpisov, a preto sa takéto situácie nepovažujú za plnenie tretími stranami.

Zákon definuje v ustanovení § 11 rozsah a podmienky využitia zjednodušenej starostlivosti vo vzťahu ku klientovi. Ide o také situácie a klientov, keď je možné získať a overiť základné informácie z verejne dostupných a spoľahlivých zdrojov – ako je to uvedené v ustanovení § 11 ods. 1 zákona. Odsek 2 toho istého ustanovenia upravuje druhy produktov, pri ktorých je možné použiť zjednodušené postupy starostlivosti vo vzťahu ku klientovi. Dôležitá je skutočnosť, že predtým, než banka rozhodne o použití zjednodušenej starostlivosti, je potrebné o klientovi alebo druhu obchodu (produkte) získať informácie, ktoré opodstatňujú uplatnenie zjednodušenej starostlivosti. Využitie zjednodušenej starostlivosti v žiadnom prípade neznamená výnimku z povinnosti priebežného monitorovania obchodného vzťahu [§ 10 ods. 1 písm. d) zákona], ani z ďalších povinností vymedzených zákonom, tak, aby bolo možné dodržiavať ustanovenia § 14 a 17 zákona ako aj ďalšie, vrátane povinností spracovávať a uchovávať údaje podľa ustanovení § 19 a § 21 zákona.

V súvislosti s využívaním zjednodušenej starostlivosti prichádza do úvahy aj možnosť využitia zoznamu tzv. tretích ekvivalentných krajín, ktorý vznikol dohodou členských štátov EÚ a je chápaný ako minimálny. Zoznam je uverejnený na internetovej stránke FSJ. Skutočnosť, že niektorá krajina je uvedená v tomto zozname však nevylučuje, že konkrétneho klienta z tejto krajiny nemožno zaradiť do vyššieho rizika. Vždy je totiž potrebné dôsledne uplatňovať povinnosti podla ustanovení § 10 ods. 1 písm. d), ods. 4 a ods. 8 zákona.

## F. ROZPOZNÁVANIE, ZDRŽANIE A OHLASOVANIE NOO

Pre rozpoznávanie neobvyklých obchodných operácií bankou je rozhodujúce uplatnovanie ustanovení § 2 až 4, § 10 až 12, § 14 a § 20 zákona.

Podľa § 14 ods. 1 zákona je banka povinná posudzovať, či pripravovaný alebo vykonávaný obchod je neobvyklý a podľa § 14 ods. 2 písm. a) zákona je povinná venovať osobitnú pozornosť všetkým zložitým, nezvyčajne veľkým obchodom a všetkým obchodom s nezvyčajnou povahou, ktoré nemajú zrejmý ekonomický účel alebo zrejmý zákonný účel. Banka je súčasne povinná preskúmať v čo najväčšej možnej miere účel týchto obchodov a podľa § 14 ods. 3 zákona musí urobiť o takýchto obchodoch písomný záznam na účely kontroly.

Podľa § 4 zákona NOO je právny úkon alebo iný úkon, ktorý nasvedčuje tomu, že jeho vykonaním môže dôjsť k praniu špinavých peňazí alebo financovaniu terorizmu. Ustanovenie § 4 ods. 2 zákona uvádza demonštratívny výpočet NOO. V každej NOO uvedenej v tomto ustanovení je však niekoľko znakov neobvyklosti (napr. nezvyčajne vysoký objem finančných prostriedkov vzhľadom na druh obchodu, nezvyčajne vysoký objem finančných prostriedkov bez zrejmého ekonomického alebo zákonného účelu, atď.), ktoré musí banka posudzovať a zároveň uplatňovať princíp KYC. Až na základe takéhoto postupu je možné kvalifikovane posúdiť, či pripravovaná alebo vykonávaná obchodná operácia klienta je alebo nie je neobvyklá. Zákon v ustanovení § 4 neupravuje žiadne kritériá, napr. v podobe hraničných súm finančných prostriedkov, ktoré by viedli k automatickému určeniu, že pri určitom type financnej operacie ide automaticky o NOO.
Rozhodujúcim prvkom pre posudzovanie obchodných operácií klienta je uplatnenie princípu KYC a kvalifikované rozpoznávanie tzv. znakov neobvyklosti, ktoré sú uvedené v jednotlivých ustanoveniach § 4 ods. 2 zákona, ako aj ďalších znakov alebo kriterii, ktoré si banka musí stanoviť v závislosti od predmetu a rozsahu svojej činnosti a druhu a rozsahu

vykonávaných obchodov a finančných operácií pre klientov, v rámci tvorby prehľadu foriem NOO [§ 20 ods. 2 písm. a) zákona].

Podmienky pre kvalifikované uplatnenie princípu KYC vyplývajú z povinností banky a klienta, určených v ustanoveniach § 10 až 12 zákona. Rozhodujúce sú ustanovenia § 10 ods. 1, 4, a 5 a prípadne aj § 11 ods. 3 zákona.
Postup podľa ustanovení § 10 ods. 1, prípadne § 11 ods. 3 zákona umožní banke primerane sa presvedčiť o skutočnej identite každého klienta a rozpoznať účel a plánovanú povahu obchodných aktivít, ktoré bude klient pravdepodobne vykonávať. Tento postup je zároveň východiskovým bodom banky pre vytvorenie rizikového profilu klienta, následné určenie rozsahu starostlivosti podľa ustanovenia § 10 ods. 4 zákona a pre akceptovanie klienta. Banka potom v závislosti od výsledku uplatní postupy v rámci základnej starostlivosti podľa § 10 zákona alebo zjednodušenej starostlivosti podľa § 11 zákona alebo zvýšenej starostlivosti § 12 zákona.
Bez ohľadu na to, či banka postupuje podľa ustanovení § 10, § 11 alebo § 12 zákona, je povinná okrem iného vždy postupovať podľa § 14 zákona. Banka musí teda v každom prípade posudzovať, či pripravovaný alebo vykonávaný obchod je neobvyklý (§ 14 ods. 1 zákona) a venovať osobitnú pozornosť všetkým zložitým, nezvyčajne veľkým obchodom a všetkým obchodom s nezvyčajnou povahou, ktoré nemajú zrejmý ekonomický účel alebo zrejmý zákonný účel a urobiť o nich príslušný záznam podľa § 14 ods. 3 zákona.

Banka vykonáva kvalifikované posudzovanie pripravovaných alebo vykonávaných obchodov podľa § 14 zákona na rôznych úrovniach. Proces posudzovania prebieha v „prvej línii“, kde sú zamestnanci banky v kontakte s existujúcim alebo potenciálnym klientom, ďalej v rámci priebežného monitorovania existujúceho obchodného vzťahu a v rámci následného/spätného posudzovania obchodov klienta.

**1. Posudzovanie obchodov v „prvej línii“**
Posudzovanie obchodov klienta uskutočňujú „v prvej línii“ zamestnanci banky, ktorí sú pri plnení svojich povinností v kontakte s klientom, najmä tí, čo spracúvajú prikazy klienta na realizáciu jeho obchodov, resp. finančných operácií. Ide predovšetkým o pokladníkov, zamestnancov zabezpečujúcich realizáciu peňažných prevodov, resp. platobného styku a ďalších zamestnancov zapojených do poskytovania služieb klientom a spracovania údajov ako aj o zamestnancov priamo nadriadených týmto zamestnancom. Posudzovanie obchodov v prvej línii je závislé od odbornosti a pripravenosti príslušných zamestnancov, ktoré nadobudli v rámci povinnej odbornej prípravy (§ 20 ods. 3 zákona).
Každý príslušný zamestnanec musí mať nepretržite k dispozícii Program banky proti legalizácii a financovaniu terorizmu, či už v papierovej alebo elektronickej podobe a musí si ho osvojiť a podľa neho postupovať. Zamestnanec banky sa riadi v tejto etape predovšetkým ustanoveniami § 10 ods. 1, prípadne § 11 ods. 3 zákona, čo mu umožní primerane sa presvedčiť o skutočnej identite klienta a poznať účel a plánovanú povahu obchodných aktivít, ktoré bude klient pravdepodobne vykonávať. Tento postup je zároveň východiskovým bodom pre akceptovanie klienta bankou, vytvorenie rizikového profilu klienta a určenie rozsahu starostlivosti voči klientovi podľa ustanovenia § 10 ods. 4 zákona.

Rozhodujúcim prvkom pre posudzovanie obchodných operácií klienta je aj tu príslušné uplatnenie princípu KYC a jeho postupov a kvalifikované rozpoznávanie znakov neobvyklosti. Tento postup umožní príslušnému zamestnancovi posudzovať pripravované alebo vykonávané obchody klienta v súlade s prehľadom foriem NOO [§ 20 ods. 2 písm. a)

zákona] a odhaliť tie, ktoré sú neobvyklé vo vzťahu ku klientovi a jeho inak obvyklým obchodom. Ak príslušný zamestnanec posúdi pripravovaný alebo vykonávaný obchod ako neobvyklý, urobí o tomto obchode písomný záznam podľa ustanovenia § 14 ods. 3 zákona a neodkladne oznámi toto zistenie určenej osobe (ďalej len „oznámenie o NOO“).

**2. Posudzovanie obchodov v rámci priebežného monitorovania obchodného vzťahu**

V závislosti od toho, či ide o uzatváranie obchodného vzťahu [§ 10 ods. 2 písm. a) zákona] alebo o príležitostný obchod [§ 10 ods. 2 písm. b), prípadne c) zákona] príslušní zamestnanci banky posudzujú obchody klienta aj v rámci priebežného monitorovania obchodného vzťahu. Posudzovanie pripravovaných a vykonávaných obchodov v rámci priebežného monitorovania obchodného vzťahuje je špecifické tým, že obchodný vzťah už vznikol a trvá [§ 10 ods. 2 písm. a) zákona]. Prípadne je klient banke známy vzhľadom na to, že už vykonal viaceré príležitostné obchody [§ 10 ods. 2 písm. b), príp. c) zákona]. Nejde teda o prvý kontakt s klientom a banka môže zohľadniť existujúci rizikový profil klienta a históriu ním vykonaných obchodov.

Postup podľa ustanovenia § 10 ods. 1 písm. d) zákona, vrátane overovania úplnosti a platnosti identifikačných údajov a informácií podľa ustanovenia § 10 ods. 8 zákona a povinnosť klienta podľa ustanovenia § 10 ods. 5 zákona, tvoria základ priebežného monitorovania obchodného vzťahu. Tento druh monitorovania si vyžaduje vytváranie rizikových profilov klientov a ich triedenie s ohľadom na možné riziko prania špinavých peňazí alebo financovania terorizmu podľa ustanovenia § 10 ods. 4 zákona. Priebežné monitorovanie obchodného vzťahu predpokladá využívanie vhodného elektronického informačného systému, čo banke umožní v súlade s rizikovo orientovanou prevenciou vytvoriť finančné, či iné kritériá, resp. limity ako jedny zo znakov neobvyklosti obchodných operácií klientov, ktoré by oddeľovali určité úrovne procesu monitorovania, zodpovedajúce stupňu rizikovosti operácií uskutočňovaných klientmi. Stanovené kritériá alebo limity, definované bankou na tento účel, musia byť pravidelne preverované, aby bolo možné určiť ich primeranosť voči zisteným úrovniam rizík. Banka musí taktiež pravidelne prehodnocovať primeranosť existujúceho systému a jednotlivych procesov ochrany a prevencie.

Pre posudzovanie obchodov budú v rámci priebežného monitorovania obchodného vzťahu dôležité tie pripravované alebo vykonávané obchody klienta, ktoré sa nezhodujú so známou alebo očakávanou aktivitou klienta. Takéto obchody klienta musia byť predmetom hodnotenia (§14 ods. 1 zákona) a musí byť urobený o nich písomný záznam (§14 ods. 3 zákona), pričom UO môže na základe výsledkov ďalšieho posudzovania jednotlivých okolností obchodu a s ohľadom na prehľad foriem NOO [§ 20 ods. 2 písm. a)] dospieť k záveru, že v danom prípade nejde o NOO. Ak to nie je možné len na základe informácií o klientovi, ktoré banka už má k dispozícii, môže podľa okolností žiadať od klienta ďalšie potrebné informácie a doklady v zmysle ustanovenia § 10 ods. 5 zákona.

V prípadoch, keď UO nedokáže ani týmto postupom zdôvodniť obchody klienta, ktoré sa nezhodujú s jeho rizikovým profilom a/alebo s jeho známymi alebo očakávanými aktivitami, postačí, že tieto operácie len nasvedčujú tomu, že ich vykonaním môže dôjsť k praniu špinavých peňazí alebo k financovaniu terorizmu a UO je povinná postupovať podľa § 17 zákona, t. j. ohlásiť NOO finančnej spravodajskej jednotke.

Posudzovanie obchodov v rámci priebežného monitorovania obchodného vzťahu vykonávajú v závislosti od obchodu príslušní zamestnanci, ako aj UO.

**3. Posudzovanie obchodov v rámci následného/spätného posudzovania obchodov klienta**
Prostriedkom následného monitorovania obchodov klientov je napríklad následný náhodný výber uskutočnených obchodov v rámci výkonu kontroly zo strany vedúceho zamestnanca, nadriadeného príslušnému zamestnancovi, ktorý realizoval pokyny a operácie klienta, ako aj v rámci výkonu kontroly uskutočňovanej UO a útvarom vnútornej kontroly (časť I).

**4. Interné oznámenia o NOO**
Všetky interné oznámenia o NOO zaslané príslušnými zamestnancami určenej osobe musia byť zdokumentované podľa ustanovenia § 14 ods. 3 zákona a musia byť k dispozícii pre účely kontroly podľa ustanovenia § 29 zákona. UO eviduje a uchováva oznámenia o interných oznámeniach o NOO vrátane funkcie, mena, priezviska, označenia pobočky alebo útvaru banky a všetkých údajov o predmetnom klientovi a obchode.

UO, ako aj príslušní zamestnanci banky vrátane vedúcich zamestnancov (a členov štatutárneho orgánu), ktorí sa podieľajú na posudzovaní obchodov podľa § 14 zákona, sú povinní zachovávať mlčanlivosť o ohlásenej NOO a o opatreniach, ktoré vykoná FSJ (§ 18 zákona), vrátane plnenia povinností podľa ustanovení § 17 ods. 5 a § 21 zákona. Banka musí mať preto určený postup od zistenia NOO po neodkladné ohlásenie NOO, vrátane postupu a zodpovednosti zamestnancov, ktorí obchod posudzujú.
Povinnosti mlčanlivosti sa však banka nemôže dovolávať voči Národnej banke Slovenska a Ministerstvu financií SR v súvislosti s výkonom dohľadu a kontroly podľa ustanovenia § 29 zákona (§ 18 ods. 5 zákona). Za predpokladu, že poskytnuté informácie sa použijú výhradne na účely predchádzania praniu špinavých peňazí alebo financovaniu terorizmu, sa povinnosť mlčanlivosti nevzťahuje na poskytovanie informácií medzi úverovými alebo finančnými inštitúciami za podmienok podľa ustanovení § 18 ods. 8 písm. a) a c) zákona.

Banka môže podľa ustanovenia § 92 ods. 6 písm. a) ZOB viesť register klientov, ktorí sa dopustili konania posúdeného ako NOO a na ktorých sa vzťahujú medzinárodné sankcie a podľa ustanovenia § 92 ods. 6 písm. b) ZOB môže poskytnúť aj bez súhlasu klienta informácie z tohto registra (za predpokladu ochrany poskytnutých údajov) iným bankám.

UO po prijatí interného oznámenia o NOO môže potvrdiť prijatie oznámenia o NOO príslušnému zamestnancovi, ktorý zaslal oznámenie. Potvrdenie by malo obsahovať poučenie o povinnosti zachovávať mlčanlivosť podľa ustanovenia § 18 zákona. V prípade, ak má banka elektronický systém zberu interných hlásení, ktorý umožňuje príslušnému zamestnancovi sledovať stav, resp. prijatie podaného interného hlásenia o NOO určenou osobou, resp. útvarom prevencie, nie je potrebné individuálne potvrdenie prijatia takéhoto oznámenia.

Interné oznámenie o NOO, resp. konanie klienta a obchod alebo finančná operácia, ktorej sa oznámenie týka, musia byť predmetom hodnotenia (posúdenia) určenou osobou, ktorá môže na základe výsledkov ďalšieho posudzovania jednotlivých okolností obchodu a s ohľadom na prehľad foriem NOO [§ 20 ods. 2 písm. a) zákon] rozhodnúť, či ide alebo nejde o NOO. Ak rozhodnutie nie je možné len na základe informácií o klientovi, ktoré banka už má k dispozícii, môže podľa okolností žiadať od klienta ďalšie potrebné informácie a doklady podľa ustanovenia § 10 ods. 5 zákona. Ak určená osoba dospeje k odôvodnenému záveru, že v prípade oznámenej NOO nejde o NOO, musí toto rozhodnutie písomne zadokumentovať a všetky súvisiace údaje, písomné podklady a elektronickú dokumentáciu naďalej uchovávať.

V prípadoch, keď UO nemôže ani týmto postupom dospieť k záveru, že nejde o NOO, postačí, že oznámený obchod, resp. finančná operácia nasvedčuje tomu, že ich vykonaním môže dôjsť k praniu špinavých peňazí alebo k financovaniu terorizmu a UO je povinná postupovať podľa ustanovenia § 17 zákona, t. j. ohlásiť NOO finančnej spravodajskej jednotke.

Podľa ustanovenia § 17 ods. 1 zákona NOO alebo pokus o jej vykonanie musia byť ohlásené FSJ bez zbytočného odkladu, t. j. pri najbližšej príležitosti. Zakaždým je treba brať do úvahy konkrétne okolnosti situácie, v ktorej sa realizuje zistenie a ohlásenie NOO a ohlásiť NOO čo najskôr. Rozhodnutie UO ohlásiť NOO nesmie byť podmienené súhlasom alebo schválením akoukoľvek inou osobou.
Hlásenie o NOO musí obsahovať údaje určené ustanoveniami § 17 ods. 3 a 4 zákona. Označenie hlásenia o každej NOO by malo mať podobu: poradové číslo/rok/znakový kód banky, napr. 1/2009/SUBA.
Ohlásiť NOO je možné písomne, elektronickou formou alebo telefonicky (v takomto prípade je potrebné do 3 dní ohlásiť NOO aj osobne, písomne alebo elektronickou poštou). Vzor tlačiva hlásenia o NOO vydáva FSJ.
Doplnenie hlásenia o NOO z vlastnej iniciatívy banky je možné urobiť najneskôr do 30 dní. Po tejto lehote je potrebné dodatočne získané informácie a podklady ohlásiť ako ďalšiu NOO. V tejto ďalšej NOO banka uvedie, s ktorou NOO dodatočne získané informácie a podklady súvisia.

### 5. Zdržiavanie NOO

Podľa ustanovenia § 16 zákona banka zdržiava NOO, teda určitý obchod (§ 9 písm. h), ktorý by bol inak vykonaný. Pokiaľ nedôjde k ukončeniu, resp. vykonaniu obchodu, napr. ak klient nepodá príslušný príkaz na úhradu, banka nemá aký obchod zdržiavať.

Banka je povinná podľa ustanovenia § 16 ods. 1 zákona zdržať NOO do jej ohlásenia FSJ, pričom vždy sa zohľadňujú prevádzkové a technické možnosti, ako aj okamih, kedy bola, resp. mala byť obchodná operácia posúdená ako neobvyklá. Napríklad obchod klienta posúdený v rámci následného/spätného posudzovania obchodov klienta už zdržať nemožno.

Banka je povinná zdržať NOO, ak hrozí nebezpečenstvo, že vykonaním NOO môže byť zmarené alebo podstatne sťažené zaistenie príjmu z trestnej činnosti alebo prostriedkov určených na financovanie terorizmu, alebo ak ju o to písomne požiada FSJ (§ 16 ods. 2 zákona). Lehota začína plynúť od okamihu, kedy mala byť určitá NOO vykonaná a trvá najviac 48 hodín. Táto lehota môže byť predĺžená na základe oznámenia FSJ o tom, že FSJ vec odovzdala orgánom činným v trestnom konaní, najviac však na ďalších 24 hodín. Celková doba zdržania NOO môže teda trvať najviac 72 hodín.

## G. OPATRENIA PROTI FINANCOVANIU TERORIZMU

### 1. Definície terorizmu a financovania terorizmu

Terorizmus predstavuje jeden z najzávažnejších spôsobov porušovania hodnôt, akými sú ľudská dôstojnosť, sloboda, rovnosť a solidarita a dodržiavanie ľudských práv a základných slobôd, na ktorých je založená Európska únia. Predstavuje aj jeden z najvážnejších útokov na zásadu demokracie a zásadu právneho štátu, ktoré sú spoločné členským štátom a na ktorých je založená Európska únia.

Financovanie terorizmu znamená podľa smernice č. 2005/60/ES poskytovanie alebo zhromažďovanie finančných prostriedkov akýmkoľvek spôsobom, s úmyslom použiť ich, alebo s vedomím, že sa majú použiť čo i len sčasti na spáchanie ktoréhokoľvek z trestných činov špecifikovaných v článkoch 1 až 4 rozhodnutia Rady č. 2002/475/SVV o boji proti terorizmu z 13. 06. 2002.

**2. Ohlasovacia povinnosť**
Banky používajú v rámci ochrany pred financovaním terorizmu vo vzťahu ku klientom obdobné postupy ako pri ochrane pred praním špinavých peňazí, vrátane ohlasovania NOO, spojených s financovaním terorizmu, FSJ.

Banka je povinná podľa ustanovenia § 91 odsek 8 ZOB poskytovať Ministerstvu financií SR v lehotách ním určených (štvrťročná lehota) zoznam klientov, na ktorých sa vzťahujú medzinárodné sankcie zavedené podľa zákona č. 460/2002 Z. z. o vykonávaní medzinárodných sankcií zabezpečujúcich mier a bezpečnosť v znení neskorších predpisov (ďalej „zákon 460/2002“). Poskytnutý zoznam musí obsahovať aj čísla účtov a výšku zostatku na účtoch týchto klientov, t. j. tzv. sankcionovaných osôb.

Banka je povinná ohlásiť NOO finančnej spravodajskej jednotke bez zbytočného odkladu (§ 17 ods. zákona). NOO zákon definuje okrem iného aj ako obchod, pri ktorom je odôvodnený predpoklad, že klientom alebo konečným užívateľom výhod je osoba, voči ktorej sú vykonávané medzinárodné sankcie, alebo obchod, pri ktorom je odôvodnený predpoklad, že jeho predmetom je, alebo má byť, vec alebo služba, ktoré môžu súvisieť s vecou alebo službou, voči ktorým sú vykonávané sankcie podľa zákona 460/2002.

**3. Konsolidovaný zoznam teroristov**
Zoznamy sankcionovaných osôb (fyzických osôb aj právnických osôb) sú súčasťou príloh jednotlivých nariadení a rozhodnutí Európskych spoločenstiev (ďalej „ES“), ktoré zaväzujú všetky finančné inštitúcie členských štátov okamžite zmraziť finančné a ekonomické zdroje sankcionovaných osôb zo štátov určených v prílohách jednotlivých nariadení a rozhodnutí ES. Predmetné nariadenia a rozhodnutia ES týkajúce sa výlučne sankcionovaných subjektov a komplexných reštriktívnych opatrení, vrátane konsolidovaného zoznamu, ktorý obsahuje mená a identifikačné údaje o všetkých osobách, skupinách, či subjektoch, na ktoré sa vzťahujú finančné obmedzenia Spoločnej zahraničnej a bezpečnostnej politiky EÚ (Common Foreign and Security Police) sú uverejnené na internetovej stránke.

**4. Sankcie**
Zákon 460/2002 definuje medzinárodné sankcie ako súhrn obmedzení, príkazov alebo zákazov zavedených na účel zachovania alebo obnovenia medzinárodného mieru a bezpečnosti, ktoré vyplývajú z konkrétnych medzinárodných záväzných dokumentov a opatrení. Súčasne konkrétne vymedzuje medzinárodné sankcie v oblasti obchodu a nefinančných služieb, v oblasti finančných služieb, v oblasti dopravy, v oblasti technickej infraštruktúry, v oblasti vedecko-technických stykov, v oblasti kultúrnych stykov a športových stykov.

Cieľom sankcií je udržať alebo obnoviť medzinárodný mier a bezpečnosť podľa princípov Charty OSN a Spoločnej zahraničnej a bezpečnostnej politiky. Ide predovšetkým o zmenu politiky vlády, štátu, jednotlivca alebo skupiny, ktoré nerešpektujú základné zásady právneho štátu, porušujú ľudské práva, medzinárodné právo alebo ohrozujú bezpečnosť.

Reštriktívne opatrenia sú prijímané buď transpozíciou sankčných rezolúcií Bezpečnostnej Rady Organizácie spojených národov (ďalej len „BR OSN“), alebo ide o autonómne sankcie prijímané iba Európskou úniou. Sankcie sú prijímané spoločnými pozíciami EÚ a implementované na úrovni ES. Ak ide o autonómne sankcie, EÚ môže prijať i tvrdšie a širšie sankcie v porovnaní so sankčnou rezolúciou.
Súčasné autonómne reštriktívne sankcie EÚ sú voči štátom: Bielorusko, Uzbekistan, Moldavsko.
Ostatné súčasné reštriktívne sankcie EÚ: Bosna a Hercegovina, Čierna Hora, Haiti, Irak, Irán, Kórejská ľudová demokratická republika, Libanon, Libéria, Macedónsko, Mjanmarsko/Barma, Moldavsko, Pobrežie Slonoviny, Sierra Leone, Somálsko, Srbsko, Sýria, Zimbabwe, USA, Juhoslávia, Bielorusko, Demokratická republika Kongo, Severná Kórea a Sudán.
Iné reštriktívne opatrenia: podpora implementácie mandátu ICTY (International Criminal Tribunal for the Former Yugoslavia), Líbya, USA, ostatné teroristické organizácie (Usama bin Ládin, Al Kaidá).
Reštriktívne opatrenia sú prijímané vo viacerých podobách. Ide napr. o diplomatické sankcie, prerušenie spolupráce s treťou krajinou, bojkot športových alebo kultúrnych podujatí, obchodné sankcie, zbrojné embargá, finančné sankcie, zákazy letov, obmedzenia vstupu na územie členského štátu. Sankčné opatrenia OSN týkajúce sa zbraňového embarga alebo reštrikcie vstupu (VISA-ban) sú implementované priamo členským štátom.

Sankčné opatrenia týkajúce sa ekonomických vzťahov s tretími štátmi, napr. zmrazovanie finančných aktív a ekonomických zdrojov, sú implementované nariadením ES (schváleným Radou) a sú priamo záväzné a aplikovateľné v ES. Nariadenia majú na základe článku 249 Zmluvy o založení Európskeho spoločenstva všeobecnú platnosť a sú priamo uplatniteľné vo všetkých členských štátoch. Ako právne záväzné akty spoločenstva majú prednosť pred zákonmi Slovenskej republiky a finančné inštitúcie v SR sú povinné uplatňovať sankcie vyhlásené nariadeniami EÚ priamo. Sú zároveň predmetom právneho posudzovania európskymi súdmi.

**5. Sankčné rezolúcie Bezpečnostnej rady OSN**
Rezolúcia BR OSN proti terorizmu je dokumentom, ktorý poskytuje základ pre kriminalizáciu podnecovania ku teroristickým činom a náboru osôb na tieto činy. Rezolúcie vyzývajú štáty, aby prijali potrebné a primerané opatrenia a v súlade so svojimi záväzkami vyplývajúcimi z medzinárodného práva zakázali zákonom podnecovanie k páchaniu teroristických činov a zabránili takejto činnosti.
Vzhľadom na vyššie uvedené, sankcie sú prijímané transpozíciou sankčných rezolúcií BR OSN. To znamená, že po vydaní rezolúcie BR OSN je potrebné predmetnú rezolúciu implementovať v čo najkratšom čase do nariadenia EÚ alebo do spoločnej pozície EÚ.

Najdôležitejšie rezolúcie BR OSN v boji proti terorizmu sú nasledovné: 1390/2002, 1333/2000, 1373/2001, 1378/2001, 1267/1999, 1363/2001, 1368/2001, 1269/1999, 1383/2001, 1386/2001 a týkajú sa opatrení proti Usama bin Ládinovi, Al Kaide, Talibanu, Afghanistanu, zbraňového embarga, zákazu určitých služieb, zmrazenia finančných aktív a ekonomických zdrojov, záväzku členského štátu na policajnú a justičnú spoluprácu. Prehľad o komplexných rezolúciách, sankčných výboroch a politike OSN proti terorizmu je zverejnený na internetovej stránke BR OSN http://www.un.org/Docs/sc/.

**6. Postup v prípade osôb, voči ktorým boli vyhlásené sankcie v zmysle nariadenia vlády Slovenskej republiky**

Európska únia spoločnou pozíciou 2001/931/CFSP v znení Spoločnej pozície 2008/586/CFSP uverejnila zoznam sankcionovaných osôb (fyzických osôb a právnických osôb), ktoré sú spájané s terorizmom a voči ktorým je potrebné uplatniť sankcie v rámci boja proti terorizmu. Osoby v zozname Spoločnej pozície EÚ 2001/931/CFSP sú rozdelené na „externých teroristov" a „interných teroristov" (v tomto prípade ide o osoby označené „*", ktoré sú občanmi EÚ respektíve majú sídlo v EÚ, napr. príslušníci baskickej organizácie E.T.A. a extrémistické skupiny najmä zo Španielska a Severného Írska).

Voči skupine tzv. externých teroristov sa uplatňujú finančné sankcie podľa čl. 3 Spoločnej pozície EÚ 2001/931/CFSP. Implementácia týchto sankcií je upravená rozhodnutím Rady EÚ 2005/428/CFSP a nariadením Rady č. 2580/2001, čo v praxi znamená, že na základe priamo aplikovateľnej legislatívy EÚ sú sankcie záväzné pre každého vo všetkých členských krajinách EÚ a priamo vykonateľné.

Voči interným teroristom sa neuplatňujú finančné sankcie, nakoľko to neumožňuje Zmluva o EÚ, ktorá dáva mandát na implementáciu reštriktívnych opatrení v rámci spoločného trhu a finančných služieb len voči tretím krajinám (čl. 60 a 301 Zmluvy o EÚ, t. j. zavedenie finančných sankcií z komunitárnej úrovne voči vlastným občanom EÚ nemá mandát). Voči interným teroristom sa uplatňuje na EÚ úrovni jedine tzv. posilnená justičná a policajná spolupráca na základe čl. 4 Spoločnej pozície EÚ 2001/931/CFSP, a súčasne v súlade s rozhodnutím Rady 2005/671/JHA z 20. septembra 2005 o výmene informácií a spolupráci vo veci trestného činu terorizmu.

Osoby uvedené na zozname Spoločnej pozície EÚ 2008/586/CFSP, označené „*" sú však teroristi a na základe rezolúcie BR OSN 1373/2001 o potlačovaní financovania terorizmu, ako aj na základe čl. 2 Spoločnej pozície EÚ 2001/930/CFSP majú všetky krajiny povinnosť zmraziť ekonomické a finančné aktíva všetkým osobám, ktoré boli označené ako teroristi, resp. Napomáhajú, alebo sú akýmkoľvek spôsobom v spojení s teroristickými štruktúrami.

Slovenská republika, vzhľadom na uvedené, nemohla vyhlásiť sankcie voči interným teroristom EÚ, preto zmrazovanie teroristických aktív voči uvedeným osobám bolo potrebné zakotviť na úrovni národnej legislatívy. K tomu došlo nariadením vlády SR č. 397/2005 Z. z., ktorým sa vyhlasujú medzinárodné sankcie zabezpečujúce medzinárodný mier a bezpečnosť novelizovaným nariadeniami vlády č. 209/2006 Z. z., č. 484/2006 Z. z., č. 488/2007 Z. z. a č. 239/2008 Z. z. (ďalej „nariadenie č. 397/2005 Z. z."). Nariadenie č. 397/2005 Z. z. obsahuje zoznam tých sankcionovaných osôb, ktorých činnosť sa viaže na územie členských krajín EÚ, alebo sú občanmi EÚ.

Banky sú povinné neodkladne zmraziť všetky finančné a ekonomické aktíva sankcionovaným osobám zaradeným na zoznam uverejnený v prílohe nariadenia vlády SR č. 397/2005 Z. z..

## H. UCHOVÁVANIE ÚDAJOV A DOKUMENTÁCIE

Banka je oprávnená na účely vykonania starostlivosti vo vzťahu ku klientovi (§ 10 až 12 zákona) aj bez súhlasu a informovania klienta, ktorého sa to týka, zisťovať, získavať, zaznamenávať, uchovávať, využívať a inak spracúvať osobné údaje klienta a iné údaje v rozsahu podľa ustanovení § 10 ods. 1 a § 12 zákona. Banka je oprávnená získavať nevyhnutné osobné údaje aj kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosičoch informácií ako aj spracúvať rodné čísla a ďalšie údaje a doklady bez súhlasu klienta a v rozsahu podľa uvedených ustanovení zákona.

Banka uchováva (archivuje) údaje o identifikácii klientov a o overovaní identifikácie, záznamy o obchodoch a finančných operáciách klientov a záznamy o zistení identifikácie konečných užívateľov výhod, vrátane fotokópií relevantných dokladov. Banka je v zmysle ustanovenia § 19 ods. 1 a 2 zákona povinná uchovávať počas piatich rokov

- od skončenia zmluvného vzťahu s klientom údaje a písomné doklady získané postupom podľa ustanovení § 10 až 12 zákona,
- od vykonania obchodu všetky údaje a písomné doklady o klientovi.

Banka je povinná uchovávať uvedené údaje a písomné doklady aj dlhšie ako päť rokov, ak ju o to požiada FSJ písomnou žiadosťou, obsahujúcou lehotu a rozsah uchovávania údajov a písomných dokladov.

Uvedené povinnosti má aj banka, ktorá ukončí činnosť, a to až do uplynutia doby, počas ktorej je povinná tieto údaje a písomné doklady uchovávať.

Postup banky pri uchovávaní údajov a dokumentácie - záznamov súvisiacich s ochranou pred praním špinavých peňazí a financovaním terorizmu upravuje Program banky, ktorý má v súlade so zákonom podrobnejšie stanoviť

- ktoré záznamy treba archivovať (aspoň údaje o identifikácii klienta a záznamy o jeho obchodných operáciách a údaje o identifikácii konečného užívateľa výhod),
- formu záznamov (papierová, elektronická),
- kde, ako a ako dlho sa záznamy uchovávajú, so zohľadnením
  1. skončenia zmluvného vzťahu s klientom,
  2. vykonania obchodu s klientom a
  3. písomnej žiadosti FSJ a určenej lehoty (§ 19 ods. 3 zákona).

Záznamy vypracované a uchovávané bankou majú spĺňať zákonné požiadavky na vedenie záznamov o údajoch o klientoch a súčasne majú umožniť

- vyhodnotenie efektívnosti dodržiavania základných princípov ako aj postupov banky na ochranu pred praním špinavých peňazí a financovaním terorizmu nezávislou osobou,
- zrekonštruovať priebeh finančných operácií uskutočnených bankou pre klienta,
- riadne identifikovať a lokalizovať ktoréhokoľvek klienta,
- identifikovať všetky interné oznámenia NOO a externé hlásenia o NOO,
- splniť v primeranom čase zákonné požiadavky FSJ, dohliadacieho orgánu a orgánov činných v trestnom konaní, týkajúce sa klienta a finančnej operácie.

Záznamy o rizikovosti klientov

Predmetom uchovávania sú špecifické dotazníky súvisiace so zaradením klientov do skupín podľa rizikovosti ich aktivít, resp. operácií. Akúkoľvek dôležitú informáciu, ktorá potvrdzuje okolnosti opodstatňujúce preradenie klienta do inej rizikovej skupiny (a teda zmenu jeho rizikového profilu), získanú komunikáciou s klientom alebo inak, banka zaznamená a uchováva spolu s ostatnými údajmi o klientovi.

Záznamy o finančných operáciách

Vnútorné predpisy banky majú stanoviť povinnosť zaznamenania všetkých finančných operácií uskutočnených pre klientov, do účtovníctva a výkazníctva banky. Záznamy o finančných operáciách, ktoré dokladujú účtovné položky, sa majú archivovať vo forme, ktorá umožní FSJ, orgánom dohľadu, orgánom kontroly a orgánom činným v trestnom konaní zostavenie uspokojivého záznamu a overenie rizikového profilu každého klienta. Podporné záznamy obsahujú pokyny klienta súvisiace s platbami klienta.

Banka archivuje záznamy o každej finančnej operácii realizovanej klientom, vrátane jednorazových a vykonaných pre klientov, ktorí nemajú otvorený účet v banke. Lehota na uchovávanie je v takomto prípade rovnaká ako pre uchovávanie identifikačných záznamov a dokumentácie.

Záznamy o interných oznámeniach NOO a hláseniach o NOO
Banka musí uchovávať všetky hlásenia o neobvyklých aktivitách klientov, a to interné oznámenia NOO určené pre UO aj hlásenia o NOO, ktoré UO zaslala FSJ.
Ak UO, po posúdení relevantných informácií a poznatkov týkajúcich sa neobvyklej aktivity klienta, rozhodol, že nešlo o NOO a nezaslal hlásenie FSJ, dôvody takéhoto rozhodnutie musia byť taktiež zaznamenané a uchovávané spolu so záznamami o príslušnej obchodnej operácii.

Záznamy o uskutočnenom vzdelávaní a odbornej príprave
Banka uchováva záznamy o uskutočnenej odbornej príprave príslušných zamestnancov, ktoré obsahujú dátum a obsah uskutočneného vzdelávania a podpis príslušného zamestnanca potvrdzujúci, že príslušný zamestnanec sa zúčastnil odbornej prípravy a oboznámil sa s Programom banky na ochranu pred praním špinavých peňazí a financovaním terorizmu a súvisiacimi vnútornými predpismi banky.

Forma uchovávaných záznamov, vyhľadávanie záznamov.
Predmetom uchovávania údajov sú originály, prípadne aj fotokópie papierových podkladov a dokumentácie ako aj dáta uložené v osobných počítačoch a mechanické nosiče elektronických údajov. Lehoty uchovávania sú rovnaké bez ohľadu na podobu, v akej sú tieto údaje archivované.
Vzhľadom na potrebu dodatočného poskytovania údajov o klientoch a finančných operáciách klientov, najmä pre FSJ a orgány činné v trestnom konaní, je dôležité, aby banka bola schopná vyhľadať potrebné podklady (dokumentáciu a nosiče) s údajmi, resp. záznamami bez zbytočného odkladu a v prípade začatého preverovania alebo vyšetrovania ich uchovávala aj po uplynutí zákonnej lehoty až dovtedy, kým príslušný orgán neoznámi, že ich ďalšie uchovávanie už nie je potrebné.

## I. ZABEZPEČOVANIE, SYSTÉM A VÝKON VNÚTORNEJ KONTROLY

V banke musí spoľahlivo fungovať systém kontroly, zameraný aj na plnenie opatrení ochrany pred praním špinavých peňazí a financovaním terorizmu. Systém kontroly tvorí určenie kontrolných zodpovedností na všetkých stupňoch riadenia a zabezpečovania výkonu bankových činností ako aj výkon kontrolnej činnosti

- dozornou radou banky,
- členmi štatutárneho orgánu,
- určenou osobou (jej zástupcom a útvarom prevencie),
- vedúcimi zamestnancami,
- príslušnými zamestnancami v rámci spracovávania pokynov (finančných operácií) klientov a
- útvarom vnútornej kontroly a vnútorného auditu, ktorému prináleží kontrolovať všetky útvary banky, vrátane UO a útvaru prevencie a príslušných zamestnancov.

Kontrola vykonávaná štatutárnym orgánom banky a dozornou radou banky
Vychádza zo všeobecne záväzných právnych predpisov a vnútorných predpisov banky a vyplýva z postavenia v hierarchii riadiaceho systému banky. Štatutárny orgán banky a vedúci pobočky zahraničnej banky pravidelne, najmenej raz ročne, vyhodnocuje účinnosť existujúceho systému – koncepcie na ochranu banky pred praním špinavých peňazí, Programu a konkrétnych opatrení, vrátane činnosti príslušných útvarov a zamestnancov.

Kontrolná činnosť UO a vedúcich zamestnancov
Vyplýva z kompetencií, povinností a zodpovedností UO a každého vedúceho zamestnanca a je vykonávaná ako pravidelná a priebežná činnosť kontroly plnenia pracovných povinností podriadených zamestnancov v oblasti ochrany pred praním špinavých peňazí a financovaním terorizmu.

Vnútorná kontrola a vnútorný audit
Útvar vnútornej kontroly a vnútorného auditu banky kontroluje plnenie dodržiavania Programu a vnútorných predpisov a postupov prijatých bankou na účely ochrany pred praním špinavých peňazí a financovaním terorizmu ako aj výkon povinností príslušnými zamestnancami banky, vedúcimi zamestnancami a určenou osobou (jej zástupcom a útvarom prevencie).
Výkon kontroly má byť zameraný najmä na kontrolovanie
- uskutočňovania príslušných stupňov (úrovní) starostlivosti vo vzťahu ku klientom,
- postupov na zabezpečenie aktuálnosti získaných informácií o klientoch (verifikácia),
- posudzovania konkrétnych finančných operácií, monitorovania klientov, ich finančných operácií a obchodných vzťahov,
- hodnotenia a riadenia rizík,
- interného oznamovania NOO a ohlasovania NOO finančnej spravodajskej jednotke,
- uskutočňovania odbornej prípravy zamestnancov a
- uchovávania záznamov.

Kontrolné postupy a druh a rozsah výsledných informácií sú podkladom na overenie, či opatrenia banky na ochranu pred praním špinavých peňazí a financovaním terorizmu sú dostatočné.
O výsledkoch vykonaných kontrol a auditov by mal byť štatutárny orgán pravidelne informovaný, napr. dvakrát ročne a v prípade zistenia závažných nedostatkov bezodkladne.

Okrem kontrolnej činnosti zameranej na dodržiavanie každodenných rutinných činností zamestnancami banky na jednotlivých pracoviskách v ústredí ako aj v pobočkovej sieti banky, má byť v dostatočnom časovom intervale podrobený vnútornému auditu aj celý systém a proces prevencie, resp. ochrany banky pred praním špinavých peňazí a financovaním terorizmu. V rámci toho má byť vyhodnotená funkčnosť, účinnosť a efektívnosť všetkých prvkov, nástrojov, postupov a riadiacich a kontrolných mechanizmov uplatňovaných bankou v tejto oblasti.
Vnútorný audit tohto druhu by mal byť vykonaný v súlade s plánom činnosti útvaru vnútornej kontroly a vnútorného auditu v periodicite, ktorá vyplynie z hodnotenia rizikovosti jednotlivých oblastí činnosti banky. Vzhľadom na riziko straty dobrého mena banky spojené s neželanou účasťou na praní špinavých peňazí a financovaní terorizmu je vhodné, aby tento tematický vnútorný audit bol vykonaný najmenej raz za kalendárny rok.

## ZÁVER

Zrušuje sa Metodické usmernenie Útvaru dohľadu nad finančným trhom Národnej banky Slovenska z 19. decembra 2008 č. 7/2008 k ochrane banky a pobočky zahraničnej banky pred praním špinavých peňazí a financovaním terorizmu.

**Ing. Martin Barto, CSc. v. r.**
**viceguvernér**

Príloha

## PRÍKLADY MOŽNÝCH NEOBVYKLÝCH OBCHODNÝCH OPERÁCIÍ

### 1. Pranie špinavých peňazí prostredníctvom hotovostných transakcií

(a) Nezvyčajne vysoké hotovostné vklady realizované fyzickou alebo právnickou osobou, pri obchodných aktivitách ktorých by za bežných okolností boli používané šeky a iné nástroje.

(b) Výrazný nárast hotovostných vkladov akejkoľvek fyzickej alebo právnickej osoby bez zjavného dôvodu, najmä ak takéto vklady sú následne v krátkej dobe prevedené z účtu a/alebo na miesto určenia, ktoré za bežných okolností nie je spájané s klientom.

(c) Klienti, ktorí vkladajú hotovosť pomocou mnohých formulárov pre uloženie peňazí na účet, takže celková suma každého vkladu je nevýznamná, ale celková suma všetkých vkladov je vysoká.

(d) Účty právnickej osoby, ktorej obchodné operácie, ako vklady, tak aj výbery, sú realizované skôr v hotovosti, a nie vo forme debetu a kreditu zvyčajne používanej v prípade obchodných spoločností (napr. šeky, akreditívy, zmenky, a pod.)

(e) Klienti, ktorí stále vkladajú alebo ukladajú hotovosť na krytie bankových zmeniek, peňažných prevodov alebo na iné obchodovateľné a rýchlo likvidné peňažné nástroje.

(f) Klienti, ktorí žiadajú o výmenu veľkého množstva bankoviek v nízkej nominálnej hodnote za bankovky vo vyššej nominálnej hodnote.

(g) Častá výmena hotovosti za iné meny.

(h) Pobočky, ktoré majú oveľa viac hotovostných transakcií ako zvyčajne.

(i) Klienti, ktorých vklady obsahujú falošné bankovky alebo sfalšované dokumenty.

(j) Klienti prevádzajúci vysoké sumy peňazí do zahraničia alebo zo zahraničia s využitím príkazov na platbu v hotovosti.

(k) Veľké hotovostné vklady prostredníctvom služieb nočnej bezpečnostnej schránky, čím je možné sa vyhnúť priamemu kontaktu so zamestnancami.

### 2. Pranie špinavých peňazí prostredníctvom bankových účtov

(a) Klienti, ktorí chcú mať mnoho držiteľských účtov alebo klientskych účtov, ktoré zrejme nesúvisia s druhom obchodnej činnosti, vrátane obchodných operácií, do ktorých sú zapojení správcovia držiteľských účtov.

(b) Klienti, ktorí majú mnoho účtov a vkladajú hotovosť na každý z nich za okolností, za akých celkový súčet vkladov predstavuje vysokú sumu.

(c) Akákoľvek fyzická alebo právnická osoba, ktorej účet nezobrazuje žiadne bežné aktivity súkromného účtu alebo firemného bankovníctva, ale je využívaný na prijímanie alebo vyplácanie vysokých súm, ktoré nemajú žiadny zrejmý účel alebo vzťah s majiteľom účtu a/alebo s jeho firmou (napr. značné zvýšenie obratu na účte).

(d) Klienti, ktorí majú účty v niekoľkých finančných inštitúciách v tej istej oblasti, najmä keď banka vie o procese pravidelného zlučovania finančných prostriedkov z takýchto účtov pred uplatnením príkazu o ďalšom prevode prostriedkov.

(e) Spárovanie prevodných príkazov z účtu s finančnými prostriedkami vloženými v hotovosti na účet v ten istý deň alebo v predošlý deň.

(f) Vkladanie šekov tretích osôb znejúcich na vysokú sumu indosovaných v prospech klienta.

(g) Výbery vysokých súm peňazí z účtu v minulosti spiaceho/neaktívneho alebo z účtu, na ktorý práve prišiel nečakaný vysoký vklad zo zahraničia.

(h) Klienti, ktorí spolu alebo naraz používajú rôzne bankové priehradky na zrealizovanie veľkých hotovostných obchodných operácií alebo devízových transakcií.

(i) Časté využívanie služieb bezpečnostných schránok. Zvýšená aktivita zo strany fyzických osôb. Používanie zapečatených vkladaných a vyberaných balíčkov.

(j) Zástupcovia právnických osôb sa vyhýbajú kontaktu s pobočkou.

(k) Výrazné zvýšenie vkladov hotovosti alebo obchodovateľných cenných papierov zo strany právnickej osoby s využitím účtov iného klienta alebo interných účtov spoločnosti alebo držiteľských účtov, najmä ak sú vklady okamžite prevedené medzi inou spoločnosťou klienta a držiteľskými účtami.

(l) Klienti, ktorí odmietnu poskytnúť informácie, na základe ktorých by za bežných okolností mohli získať úver alebo iné bankové služby.

(m) Nedostatočné využívanie bežných bankových služieb, napr. vyhýbanie sa službám s vysokými úrokovými sadzbami za vysoký zostatok.

(n) Veľký počet ľudí, ktorí realizujú platby na rovnaký účet bez primeraného vysvetlenia.

**3. Pranie špinavých peňazí prostredníctvom bankových aktivít**

(a) Používanie akreditívov a iných metód financovania obchodu na presun peňazí medzi krajinami, v ktorých takýto obchod nie je v súlade s bežnou obchodnou činnosťou klienta.

(b) Klienti, ktorí realizujú pravidelné a veľké platby vrátane bankových transakcií, ktoré nie je možné jasne identifikovať ako transakcie v dobrej viere do krajín, ktoré sú

bežne spájané s výrobou, spracovaním alebo predajom drog, s teroristickými organizáciami, alebo prijímajú pravidelné a veľké platby z takýchto krajín.

(c) Nárast vysokých zostatkov na účte, ktorý nie je v súlade so známym obratom spoločnosti klienta a následný prevod na účet (účty) v zahraničí.

(d) Nevysvetlené elektronické prevody prostriedkov zo strany klientov na účet alebo z účtu alebo bez prechodu cez účet.

(e) Časté žiadosti o vystavenie cestovných šekov, zmeniek v cudzej mene alebo iných obchodovateľných cenných papierov.

(f) Časté vklady cestovných šekov alebo zmeniek v cudzej mene, predovšetkým ak pochádzajú zo zahraničia.

**4. Pranie špinavých peňazí prostredníctvom obchodných operácií súvisiacich s investíciami**

(a) Nákup cenných papierov, ktoré majú byť držané v bezpečnostných schránkach finančnej inštitúcie v prípadoch, kedy sa to zdá byť neprimerané v súvislosti so zjavnou situáciou klienta.

(b) Na seba nadväzujúce vkladové/úverové transakcie s dcérskymi spoločnosťami alebo pobočkami zahraničných finančných inštitúcií v známych oblastiach nezákonného obchodovania s drogami.

(c) Požiadavka klientov na služby riadenia investícií (cenných papierov), kde je zdroj prostriedkov neznámy, alebo nie je v súlade so zjavnou situáciou klienta.

(d) Vyššie alebo nezvyčajné vyrovnanie cenných papierov v hotovosti.

(e) Nákup a predaj cenného papiera bez zistiteľného účelu alebo za okolností, ktoré sa zdajú byť nezvyčajné.

**5. Pranie špinavých peňazí so zainteresovaním zamestnancov a sprostredkovateľov**

(a) Zmeny základného spôsobu správania sa zamestnancov, napr. nákladný životný štýl alebo vyhýbanie sa dovolenke.

(b) Zmeny výkonu zamestnanca alebo sprostredkovateľa, napr. predajca predávajúci produkty za hotovosť nápadne alebo neočakávane zvýšil výkon.

(c) Akákoľvek transakcia so sprostredkovateľom, kedy identita konečného užívateľa výhod alebo protistrany je utajená, v rozpore s bežným postupom pre daný typ príslušného obchodu.

**6. Pranie špinavých peňazí prostredníctvom zabezpečených a nezabezpečených pôžičiek**

(a) Klienti, ktorí splatia problémové úvery neočakávane.

(b) Požiadavka na pôžičku oproti aktívam v držbe finančnej inštitúcie alebo tretej osoby, kde pôvod aktív nie je známy alebo aktíva nezodpovedajú situácii klienta.

(c) Požiadavka zo strany klienta pre finančnú inštitúciu, aby poskytla alebo zabezpečila finančné prostriedky, kde zdroj finančného príspevku klienta pre obchodnú operáciu je nejasný, najmä ak ide o využitie nehnuteľnosti.

Dôležité informácie a dokumenty týkajúce sa preventívnych opatrení proti praniu špinavých peňazí a financovaniu terorizmu sa nachádzajú na nasledujúcich internetových stránkach:

www.un.org
www.fatf-gafi.org
www.coe.int/moneyval
www.bis.org
www.amlcft.org
www.wolfsberg-principles.com
www.fsa.gov.uk
www.fdic.gov
www.c-ebs.org

Kontakty:
Národná banka Slovenska
- odbor povoľovací a konaní pred NBS: tel. č. 02 5787 2873, 02 5787 2883
- odbor dohliadací: tel. č. 02 5787 2834
Ministerstvo vnútra SR, Spravodajská jednotka finančnej polície: tel. č. 09610 514 05
09610 514 02
0905 962 815
Ministerstvo financií SR: tel. č. 02 5958 2520