POKYNY PRO BOJ PROTI PRANÍ PENĚZ, FINANCOVÁNÍ TERORISMU A SANKČNÍ OPATŘENÍ.

ÚVOD

Účelem těchto pokynů pro opatření proti praní špinavých peněz (AML), financování terorismu (CFT) a sankcím je zajistit, aby společnost **Blockchain Finance s.r.o.** (Společnost) měla vnitřní směrnice pro předcházení zneužívání svého podnikání k praní špinavých peněz a financování terorismu a vnitřní směrnice pro provádění mezinárodních sankcí.

Tyto pokyny byly přijaty s cílem zajistit, aby společnost dodržovala pravidla a předpisy stanovené v:

- Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (zákon č. 253/2008) (AML zákon);
- Zákon o provádění mezinárodních sankcí (zákon č. 69/2006) (zákon o sankcích);
- obecné pokyny Finančního analytického úřadu ČR týkající se opatření proti praní špinavých peněz, financování terorismu a provádění mezinárodních sankcí;
- SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení zneužití finančního systému k praní peněz nebo financování terorismu a o změně směrnic (AMLD5).

Tyto pokyny přezkoumává generální ředitel nejméně jednou ročně. Návrh na přezkoumání a přezkum těchto Pokynů může být naplánován častěji na základě rozhodnutí pověřence Společnosti pro ohlašování praní špinavých peněz (MLRO) nebo pověřence pro vnitřní kontrolu.

Tyto pokyny se přijímají a schvalují usnesením generálního ředitele.

Společnost oznámí FAÚ znění systému vnitřních zásad, tj. těchto pokynů, do 60 dnů ode dne, kdy se stala povinnou osobou. Po provedení změn v těchto Směrnicích a nové znění těchto Směrnic s uvedením provedených změn oznámí FAÚ do 30 dnů ode dne jejich přijetí.

DEFINICE

Společnost je právnická osoba s následujícími údaji:

- název společnosti: Blockchain Finance s.r.o.;
- identifikační číslo: 22337016;
- adresa: Revoluční 1082/8, Nové Město, 110 00 Praha 1.

Pokyny - tento dokument včetně všech výše uvedených příloh. Pokyny obsahují mimo jiné pravidla vnitřní kontroly Společnosti týkající se Pokynů a politiku Společnosti v oblasti hodnocení rizik týkající se přístupu založeného na riziku praní peněz a financování terorismu.

Praním špinavých pen**ěz** se rozumí jednání, jehož cílem je zakrýt nezákonný původ jakéhokoli hospodářského prospěchu pocházejícího z trestné činnosti s cílem vytvořit zdání, že se jedná o majetkový prospěch získaný v souladu se zákonem; toto jednání spočívá zejména v tom, že

- při přeměně nebo převodu majetku s vědomím, že pochází z trestné činnosti, za účelem jeho zatajení nebo zastření jeho původu nebo za účelem pomoci osobě, která se podílí na páchání takové činnosti, aby unikla právním důsledkům svého jednání,
- zatajování nebo zastírání skutečné povahy, zdroje, umístění, pohybu nebo nakládání s majetkem nebo změny práv k majetku s vědomím, že tento majetek pochází z trestné činnosti,
- při nabývání, držení, používání nebo nakládání s majetkem s vědomím, že pochází z trestné činnosti, nebo
- ve zločinném spolčení osob nebo jiné formě spolupráce za účelem výše uvedeného jednání.

V procesu praní špinavých peněz existují tři uznávané fáze:

- umístění, které zahrnuje umístění výnosů z trestné činnosti do finančního systému;
- vrstvení, které zahrnuje přeměnu výnosů z trestné činnosti na jinou formu a vytváření složitých vrstev finančních transakcí s cílem zamaskovat auditní stopu a zdroj a vlastnictví finančních prostředků;
- integrace, která spočívá v tom, že se vyprané peníze vrátí zpět do ekonomiky, aby se vytvořil dojem legitimity.

Financování terorismu (TF) znamená:

- shromažďování nebo poskytování peněz nebo jiného majetku s vědomím, že budou použity, byť i jen částečně, ke spáchání teroristického trestného činu, teroristického útoku, účasti v teroristické skupině, podpoře a propagaci terorismu nebo trestného činu vyhrožování teroristickým trestným činem nebo trestného činu, který má umožnit spáchání takového trestného činu nebo k němu napomáhat, nebo k podpoře osoby nebo skupiny osob připravujících se na spáchání takového trestného činu, nebo

- jednání vedoucí k poskytnutí odměny nebo náhrady pachateli trestného činu teroru, teroristického útoku, účasti v teroristické skupině, podpory a propagace terorismu nebo trestného činu vyhrožování teroristickým trestným činem nebo trestného činu směřujícího k umožnění nebo napomáhání spáchání takového trestného činu, nebo osobě blízké pachateli podle trestního zákoníku, nebo shromažďování prostředků na takovou odměnu nebo náhradu,
- financování šíření zbraní hromadného ničení podle jeho definice uvedené v tomto dokumentu.

Financováním šíření zbraní hromadného ničení se rozumí shromažďování nebo poskytování finančních prostředků nebo jiného majetku s vědomím, že budou použity, a to i částečně, šiřitelem zbraní hromadného ničení nebo budou použity k podpoře šíření takových zbraní v rozporu s požadavky mezinárodního práva.

Sankce jsou základním nástrojem zahraniční politiky zaměřeným na podporu udržení nebo obnovení míru, mezinárodní bezpečnosti, demokracie a právního státu, dodržování lidských práv a mezinárodního práva nebo dosažení dalších cílů Charty Organizace spojených národů nebo společné zahraniční a bezpečnostní politiky Evropské unie. Sankce zahrnují:

- mezinárodní sankce, které jsou vůči státu, území, územní jednotce, režimu, organizaci, sdružení, skupině nebo osobě uloženy rezolucí Rady bezpečnosti OSN, rozhodnutím Rady Evropské unie nebo jiným právním předpisem ukládajícím České republice povinnosti;
- sankce vlády České republiky, které jsou nástrojem zahraniční politiky a které mohou být uloženy nad rámec cílů uvedených v předchozím odstavci za účelem ochrany bezpečnosti nebo zájmů České republiky.

Mezinárodní sankce mohou zakázat vstup subjektu mezinárodní sankce do státu, omezit mezinárodní obchod a mezinárodní transakce a uložit další zákazy nebo povinnosti.

Subjektem sankcí je jakákoli fyzická nebo právnická osoba, subjekt nebo orgán, který je uveden v právním aktu ukládajícím nebo provádějícím sankce a na který se sankce vztahují.

Země původu znamená:

- v případě fyzických osob každý stát:
    - jehož je státním příslušníkem,
    - ve kterém je přihlášen k trvalému nebo jinému pobytu, nebo
    - ve kterém pobývá déle než 1 rok,
- jednotliví podnikatelé, každý stát, který je podle výše uvedeného bodu jejich zemí původu nebo ve kterém mají sídlo,
- právnické osoby, stát, ve kterém má sídlo, a každý stát, ve kterém má pobočku nebo provozovnu,
- svěřenského fondu, stát, podle jehož práva je zřízen, a každý stát, který je zemí původu jeho správce podle výše uvedených bodů.

Zákazníkem se rozumí fyzická nebo právnická osoba, která je v obchodním vztahu se Společností, nebo fyzická či právnická osoba, se kterou Společnost uzavírá příležitostné transakce.

Skutečným vlastníkem se rozumí fyzická osoba, která s využitím svého vlivu provádí transakci, úkon, akci, operaci nebo krok nebo jiným způsobem vykonává kontrolu nad transakcí, úkonem, akcí, operací nebo krokem nebo nad jinou osobou a v jejímž zájmu nebo v jejíž prospěch nebo na jejíž účet je transakce nebo úkon, akce, operace nebo krok proveden. V případě právnické osoby je skutečným majitelem fyzická osoba, jejíž přímý nebo nepřímý podíl nebo součet všech přímých a nepřímých podílů v právnické osobě přesahuje 25 %, včetně podílů ve formě akcií nebo jiných forem na doručitele.

MLRO znamená pracovníka pro hlášení praní špinavých peněz, který je ve Společnosti jmenován jako kontaktní osoba ve smyslu § 22 odst. 2 AML zákona.

Zaměstnancem se rozumí zaměstnanec společnosti, včetně osob, které se podílejí na uplatňování těchto pokynů ve společnosti.

Generálním ředitelem se rozumí výkonný ředitel společnosti.

Obchodním vztahem se rozumí vztah, který vzniká uzavřením dlouhodobé smlouvy Společností v rámci hospodářské nebo profesní činnosti za účelem poskytování služby nebo její distribuce jiným způsobem nebo který není založen na dlouhodobé smlouvě, ale u něhož lze v době navázání kontaktu důvodně očekávat určitou dobu trvání a během něhož Společnost opakovaně uskutečňuje samostatné transakce v rámci hospodářské nebo profesní činnosti při poskytování služby.

Příležitostnou transakcí se rozumí transakce prováděná Společností v rámci hospodářské nebo profesní činnosti za účelem poskytnutí služby nebo prodeje zboží či jeho distribuce jiným způsobem Zákazníkovi mimo rámec navázaného obchodního vztahu.

Virtuální měnou se rozumí elektronicky uložitelná nebo převoditelná jednotka, která je:
(a) schopné plnit platební, směnnou nebo investiční funkci bez ohledu na to, zda mají nebo nemají emitenta, pokud nejsou:

1. cenný papír, investiční nástroj nebo hotovost podle zákona o platebním styku (zákon č. 370/2017),
2. jednotka podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku (zákon č. 370/2017 Sb.), nebo
3. jednotku, kterou se provádí platba podle § 3 odst. 3 písm. e) zákona o platebním styku (zákon č. 370/2017 Sb.), nebo

(b) jednotka uvedená v písmenu a) bodě 2, kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky skladovatelnou nebo převoditelnou jednotku uvedenou v písmenu a).

PEP je fyzická osoba, která vykonává nebo vykonávala významné veřejné funkce a u níž přetrvávají související rizika.

ZÁSADY STRUKTURY A ŘÍZENÍ SPOLEČNOSTI.

Organizační struktura společnosti musí odpovídat její velikosti a povaze, rozsahu a úrovni složitosti jejích činností a poskytovaných služeb, včetně rizikového apetitu a souvisejících rizik, a musí být strukturována v souladu se zásadou **tří linií obrany.** Organizační struktura Společnosti musí odpovídat úplnému pochopení potenciálních rizik a jejich řízení. Řetězce podřízenosti a podřízenosti Společnosti musí být zajištěny tak, aby všichni zaměstnanci znali své místo v organizační struktuře a znali své pracovní povinnosti.

Generální ředitel

Generální ředitel je nositelem kultury dodržování požadavků na prevenci praní špinavých peněz a financování terorismu a zaručuje, že generální ředitel a zaměstnanci Společnosti působí v prostředí, kde jsou si plně vědomi požadavků na prevenci praní špinavých peněz a financování terorismu a povinností s těmito požadavky spojených a v rozhodovacích procesech Společnosti jsou v přiměřené míře zohledněna příslušná rizika.

Generální ředitel nese konečnou odpovědnost za opatření přijatá s cílem zabránit využívání služeb společnosti k praní špinavých peněz nebo financování terorismu. Zajišťuje dohled a odpovídá za:

- zavádění a udržování procesů, postupů, rizik a kontrolních procesů v oblasti praní peněz[1] ;
- přijetí těchto pokynů a dalších interních směrnic a pokynů;
- stanovení pokynů společnosti pro opatření proti praní špinavých peněz;
- jmenování MLRO a zajištění toho, aby měl MLRO pravomoci, zdroje a odborné znalosti potřebné k plnění svého úkolu;
- přidělení dostatečných zdrojů k zajištění účinného provádění pokynů a dalších souvisejících dokumentů a k udržení organizace;
- zajistit, aby všichni příslušní zaměstnanci absolvovali každoroční školení o boji proti praní špinavých peněz.

První linie obrany - zaměstnanci

První linie obrany má za úkol uplatňovat opatření náležité péče při navazování obchodních vztahů a příležitostných transakcí a uplatňovat opatření náležité péče v průběhu obchodního vztahu. První linii obrany tvoří strukturální útvary a zaměstnanci Společnosti, s jejichž činností jsou spojena rizika, kteří musí tato rizika, jejich specifika a rozsah identifikovat a vyhodnocovat a kteří tato rizika řídí prostřednictvím svých běžných činností, především uplatňováním opatření náležité péče. Rizika vyplývající z činnosti a poskytování služeb Společností patří do první linie obrany. Jsou správci (vlastníky) těchto rizik a nesou za ně odpovědnost.

Zaměstnanci Společnosti musí jednat prozíravě a kompetentně, jak se od nich očekává, a v souladu s požadavky kladenými na jejich pozice, vycházet ze zájmů a cílů Společnosti a zajistit,

[1] Pro účely zjednodušení těchto pokynů zahrnuje pojem "AML" také prevenci financování terorismu a provádění sankcí.

aby finanční systém a ekonomický prostor země nebyly využívány k praní špinavých peněz a financování terorismu. Společnost přijímá opatření k posouzení vhodnosti zaměstnanců před jejich nástupem do práce s příslušným školením.

Z výše uvedených důvodů jsou zaměstnanci povinni:

- dodržovat všechny požadavky uvedené v pokynech a dalších souvisejících dokumentech;
- shromažďovat požadované informace o zákaznících v souladu s jejich funkcí a odpovědností;
- neprodleně hlásit MLRO informace, situace, činnosti, transakce nebo pokusy o transakce, které jsou neobvyklé pro jakýkoli typ služby nebo vztahu se zákazníkem, bez ohledu na výši částky, bez ohledu na to, zda transakce byla či nebyla dokončena;
- neinformovat ani jinak neseznamovat zákazníky s tím, zda zákazník nebo jiní zákazníci jsou nebo mohou být předmětem hlášení nebo zda bylo nebo může být podáno hlášení;
- absolvovat příslušné školení v oblasti boje proti praní špinavých peněz, které je pro danou pozici zaměstnance vyžadováno.

Druhá linie obrany - řízení rizik a dodržování předpisů, MLRO .

Druhou linii obrany tvoří funkce řízení rizik a dodržování předpisů. Tyto funkce mohou být vykonávány i stejnou osobou nebo strukturálním útvarem v závislosti na velikosti Společnosti a povaze, rozsahu a úrovni složitosti jejich činností a poskytovaných služeb, vč. rizikového apetitu a rizik vyplývajících z činností Společnosti.

Cílem **funkce compliance je zajistit,** aby společnost dodržovala platné právní předpisy, pokyny a další dokumenty, a posoudit možný dopad případných změn v právním nebo regulačním prostředí na činnost společnosti a na rámec compliance. Úkolem compliance je pomáhat první linii obrany jako vlastníkům rizik definovat místa, kde se rizika projevují (např. analýza podezřelých a neobvyklých transakcí, pro které mají zaměstnanci compliance potřebné odborné dovednosti, osobnostní kvality apod. a pomáhat první linii obrany tato rizika účinně řídit. Druhá linie obrany se nepodílí na podstupování rizik.

Politika řízení rizik je prováděna a rámec řízení rizik je kontrolován **funkcí řízení rizik**. Výkonný pracovník funkce řízení rizik zajišťuje, aby všechna rizika byla identifikována, hodnocena, měřena, monitorována a řízena, a informuje o nich příslušné útvary Společnosti. Vykonavatel funkce řízení rizik pro účely AML provádí především dohled nad dodržováním ochoty podstupovat rizika, dohled nad tolerancí k rizikům, dohled nad identifikací změn rizik, provádí přehled souvisejících rizik a plní další povinnosti související s řízením rizik.

Generální ředitel jmenoval **MLRO pro** výkon funkcí druhé linie obrany. Tato osoba není provozně zapojena do oblastí, které bude MLRO sledovat a ověřovat, a je tedy ve vztahu k nim nezávislá. MLRO odpovídá za následující činnosti:

- vypracovávat a v případě potřeby aktualizovat pokyny společnosti;
- průběžné sledování a ověřování, zda společnost plní požadavky stanovené těmito pokyny a souvisejícími dokumenty a v souladu s vnějšími právními předpisy.

- poskytovat zaměstnancům a generálnímu řediteli společnosti poradenství a podporu v souvislosti s pravidly týkajícími se praní špinavých peněz a financování terorismu.
- informovat a školit generálního ředitele a příslušné osoby o pravidlech týkajících se praní špinavých peněz a financování terorismu.
- prošetří a zaeviduje dostatek údajů o přijatých interních oznámeních a rozhodne, zda lze činnost odůvodnit, nebo zda je podezřelá;
- podávat příslušná hlášení příslušným regulačním orgánům v souladu s požadavky místní jurisdikce;
- kontrolovat a pravidelně vyhodnocovat, zda jsou postupy a pokyny společnosti pro prevenci zneužití podniku k praní špinavých peněz nebo financování terorismu vhodné a účinné;
- identifikovat incidenty v souladu s pokyny společnosti a přijmout opatření týkající se těchto incidentů.

MLRO podává čtvrtletní zprávy generálnímu řediteli. Tato zpráva musí být písemná a musí obsahovat alespoň následující body:

- počet zákazníků ve všech klasifikacích rizik
- počet pozitivních nálezů osob v souvislosti se sankčními seznamy a uplatňovanými opatřeními;
- počet zákazníků nebo zástupců zákazníků, kteří byli identifikováni jako osoby se sníženou důvěryhodností nebo osoby s vazbou na osobu se sníženou důvěryhodností;
- počet interních oznámení o podezřelé činnosti nebo transakcích;
- počet příslušných zpráv vykázaných Finančnímu analytickému úřadu (FAÚ);
- číslo a obsah žádosti o informace od FAÚ v rámci šetření;
- potvrzení, že hodnocení rizik praní špinavých peněz a financování terorismu je aktuální;
- potvrzení, že tyto pokyny a další související dokumenty jsou aktuální;
- potvrzení, že personální zajištění opatření proti praní peněz je dostatečné;
- byly odstraněny všechny nedostatky (pokud existují) zjištěné kontrolní funkcí;
- seznam povinných školení, která se konala pro zaměstnance v souvislosti s opatřeními proti praní špinavých peněz.

Třetí linie obrany - interní audit

Třetí linii obrany tvoří nezávislý a účinný interní audit. Funkci interního auditu může vykonávat jeden nebo několik zaměstnanců, strukturální útvar Společnosti s příslušnými funkcemi nebo třetí strana, která Společnosti poskytuje příslušné služby.

Zaměstnanci, strukturální jednotka Společnosti nebo třetí strana, která vykonává funkci interního auditu, musí mít požadované kompetence, nástroje a přístup k příslušným informacím ve všech

strukturálních jednotkách Společnosti. Metody interního auditu musí odpovídat velikosti Společnosti, povaze, rozsahu a úrovni složitosti činností a poskytovaných služeb, vč. rizikového apetitu a rizik vyplývajících z činností Společnosti.

O provedení interního auditu rozhoduje svým usnesením generální ředitel. Generální ředitel musí posoudit potřebu provedení interního auditu nejméně jednou ročně.

Poskytované služby

Hlavní hospodářskou činností společnosti jsou služby spojené s virtuální měnou.

IDENTIFIKACE ZÁKAZNÍKA

Společnost identifikuje zákazníka v souladu s postupem stanoveným v Pokynech a shromažďuje údaje o zákaznících v následujících případech:

- pokud je zřejmé, že hodnota příležitostných transakcí přesahuje částku 1 000 EUR;
- při navázání obchodního vztahu;
- při podezření na praní peněz nebo financování terorismu, bez ohledu na odchylky, výjimky nebo omezení stanovené v těchto pokynech a platných právních předpisech.

Provedení identifikace zákazníka

Identifikaci zákazníka, který je fyzickou osobou, provádí zaměstnanec za fyzické přítomnosti zákazníka. Zákazník, který je fyzickou osobou, nesmí při identifikaci použít zástupce.

Identifikaci Zákazníka, který je právnickou osobou, nebo svěřenského fondu provádí Zaměstnanec za fyzické přítomnosti fyzické osoby jednající jménem Zákazníka (např. generálního ředitele Zákazníka, člena představenstva apod.).

Po provedení identifikace Zákazníka bude Společnost v průběhu obchodního vztahu se Zákazníkem nebo při dalších transakcích kontrolovat platnost a úplnost identifikačních údajů Zákazníka, informací shromážděných v rámci procesu hloubkové kontroly nebo důvodů pro vynětí Zákazníka z procesu hloubkové kontroly a bude zaznamenávat případné změny a úpravy.

Identifikace zákazníka může být provedena na dálku, pokud jsou v průběhu procesu identifikace splněny následující požadavky:

1. Zákazník, který je fyzickou osobou, zašle Společnosti kopii dokladu totožnosti a alespoň jeden další podpůrný doklad, z něhož mohou být údaje o Zákazníkovi získány (např. další doklad totožnosti nebo doklad o adrese s uvedenými údaji o Zákazníkovi);
2. zástupce zákazníka, který je fyzickou osobou, zašle společnosti kopie dokumentů dle bodu 1. zástupce a oprávnění tohoto zástupce jednat jménem zákazníka;
3. zákazník, který je právnickou osobou, zašle povinnému subjektu doklad o své existenci a své identifikační údaje, nebo povinný subjekt zjistí existenci a identifikační údaje zákazníka z veřejného rejstříku nebo registru svěřenských fondů;
4. Společnost eviduje a ověřuje údaje a oprávnění zaslané podle bodů 1.-3. a nemá pochybnosti o skutečné totožnosti Zákazníka nebo jeho zástupce;
5. společnost uzavře se zákazníkem dohodu o této transakci nebo obchodním vztahu, jejíž obsah bude zaznamenán v textové podobě;
6. zákazník věrohodným způsobem prokáže existenci platebního účtu vedeného na jeho jméno u úvěrové instituce nebo zahraniční úvěrové instituce, který není veden ve vysoce rizikové třetí zemi;
7. první platba zákazníka bude provedena prostřednictvím účtu podle bodu 6.

Výše uvedenému požadavku (bod 1.) na zaslání dalšího podkladového dokumentu se lze vyhnout v případě, kdy jsou k první platbě zákazníka připojeny údaje zákazníka.

Identifikace zákazníka - fyzická osoba

Společnost identifikuje zákazníka, který je fyzickou osobou, na základě dokladu totožnosti[2] a uchovává o něm následující údaje:

- jméno a příjmení;
- osobní číslo, a pokud nebylo přiděleno, datum narození a pohlaví.
- místo narození;
- místo bydliště;
- občanství;
- kontaktní údaje (případně e-mail a telefonní číslo);
- údaje o zaměstnanosti (je-li to relevantní) a

následující údaje o použitém dokladu totožnosti:

- číslo dokladu totožnosti;
- typ dokladu totožnosti;
- státu nebo orgánu, který jej vydal;
- doba platnosti dokladu totožnosti.

Společnost ověří shodu podoby zákazníka s podobou v dokladu totožnosti.

Dokladem totožnosti se rozumí doklad vydaný orgánem veřejné správy, v němž je uvedeno jméno a příjmení, datum narození, z něhož je patrná podoba, nebo jiné údaje umožňující identifikaci osoby, která doklad předkládá, jako jeho oprávněného držitele.

Identifikace zákazníka - právnické osoby

Společnost identifikuje zákazníka, který je právnickou osobou, a uchovává o něm následující údaje:

- obchodní jméno nebo název (s právní formou);
- registrační kód nebo registrační číslo a datum registrace;
- adresa registrace;
- místo podnikání;
- jméno ředitele (ředitelů) nebo jména člena (členů) správní rady nebo člena (členů) jiného rovnocenného orgánu a jejich pravomoci při zastupování zákazníka;

[2] dokladem totožnosti se rozumí doklad vydaný orgánem veřejné správy, v němž je uvedeno jméno a příjmení, datum narození a z něhož je patrná podoba Zákazníka a další údaje umožňující identifikaci osoby, která doklad předkládá, jako jeho oprávněného držitele.

- kontaktní údaje (případně e-mail a telefonní číslo).

Pro identifikaci zákazníka lze použít následující doklady vydané příslušným orgánem nebo subjektem ne dříve než šest měsíců před jejich použitím:

- evidenční kartu příslušného rejstříku nebo
- osvědčení o zápisu do příslušného rejstříku nebo
- doklad rovnocenný s výše uvedenými doklady nebo příslušnými doklady o založení zákazníka.

Společnost ověřuje správnost výše uvedených údajů zákazníka, přičemž k tomuto účelu využívá informace pocházející z důvěryhodného a nezávislého zdroje. Pokud má Společnost přístup do příslušného registru cizího státu, není třeba od Zákazníka požadovat předložení výše uvedených dokumentů.

Zástupce právnické osoby se označuje jako zákazník, který je fyzickou osobou. Každý zástupce právnické osoby, který hodlá jménem právnické osoby provádět transakce se Společností, musí být identifikován odpovídajícím způsobem.

Identifikace politicky exponované osoby

V průběhu identifikace Zákazníka Společnost přijme opatření ke zjištění, zda Zákazník, Skutečný vlastník Zákazníka nebo zástupce tohoto Zákazníka není PEP, jeho rodinný příslušník[3] nebo blízká osoba[4] , nebo zda se Zákazník takovou osobou nestal.

Společnost si od zákazníka vyžádá informace, které umožní zjistit, zda je zákazník PEP, jeho rodinný příslušník nebo blízký spolupracovník (např. poskytne zákazníkovi možnost uvést příslušné informace v dotazníku KYC).

Společnost ověří údaje obdržené od zákazníka dotazem v příslušných databázích nebo veřejných databázích nebo dotazem či ověřením údajů na internetových stránkách příslušných dozorových orgánů nebo institucí země, ve které má zákazník bydliště nebo sídlo. V případě podezření musí být PEP dodatečně ověřen pomocí vyhledávače Google a místního vyhledávače země původu Zákazníka, pokud existuje, a to zadáním jména Zákazníka v latince i místní abecedě s datem narození Zákazníka.

Za PEP se považují přinejmenším tyto osoby:

- hlava státu nebo hlava vlády (předseda vlády nebo obdobný orgán);
- ministra, náměstka ministra nebo asistenta ministra;
- člen zákonodárného orgánu;

[3] **rodinným příslušníkem** se rozumí manžel/manželka nebo osoba považovaná za rovnocennou manželovi/manželce PEP; dítě a jeho/její manžel/manželka nebo osoba považovaná za rovnocennou manželovi/manželce PEP; rodič PEP.

[4] **blízkou osobou** fyzická osoba, o níž je známo, že je skutečným vlastníkem nebo spoluvlastníkem právnické osoby nebo právního uspořádání nebo má jiné úzké obchodní vztahy s politicky exponovanou osobou, a fyzická osoba, která je výlučným skutečným vlastníkem právnické osoby nebo právního uspořádání, o nichž je známo, že byly zřízeny ve faktický prospěch politicky exponované osoby.

- člen řídícího orgánu politické strany;
- předseda místní samosprávy
- soudce nejvyššího soudu země;
- generální auditor nebo člen dozorčí rady či výkonné rady centrální banky;
- velvyslanec, vyslanec nebo chargé d'affaires;
- vysoký důstojník ozbrojených sil;
- člen správního, řídícího nebo dozorčího orgánu státního podniku;
- ředitel, zástupce ředitele a člen řídícího orgánu mezinárodní organizace;
- za politicky exponovanou osobu se považuje osoba, která je podle seznamu zveřejněného Evropskou komisí považována za osobu vykonávající významnou veřejnou funkci členským státem Evropské unie, Evropskou komisí nebo mezinárodní organizací akreditovanou na území Evropské unie.

Středně postavení nebo nižší úředníci nejsou považováni za osoby se sníženou důvěryhodností.

Společnost identifikuje blízké spolupracovníky a rodinné příslušníky PEP pouze tehdy, pokud je jejich spojení s PEP veřejně známo nebo pokud má společnost důvod se domnívat, že takové spojení existuje.

Pokud zákazník, který je PEP, již nevykonává důležité veřejné funkce, které mu byly svěřeny, společnost alespoň do 12 měsíců zohlední rizika, která se zákazníkem nadále souvisejí, a uplatní příslušná opatření založená na citlivosti na rizika, pokud je jisté, že rizika charakteristická pro PEP v případě zákazníka již neexistují.

HLOUBKOVÁ KONTROLA ZÁKAZNÍKA

Hlavní zásady

Opatření hloubkové kontroly klienta (CDD) jsou vyžadována pro ověření totožnosti nového nebo stávajícího klienta jako dobře fungující průběžné sledování obchodního vztahu s klientem založené na riziku.

Opatření CDD uplatňuje Společnost prostřednictvím odpovědného zaměstnance v následujících případech:

- pokud je zřejmé, že hodnota příležitostných transakcí přesahuje částku 15 000 EUR;
- při příležitostných transakcích s PEP;
- při příležitostných transakcích se zákazníkem, jehož země původu se nachází ve vysoce rizikové třetí zemi[5] ;
- v průběhu obchodního vztahu;

[5] Nařízení Komise v přenesené pravomoci (EU) 2016/1675 ze dne 14. července 2016, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/849 určením vysoce rizikových třetích zemí se strategickými nedostatky

- když byl zákazník identifikován na dálku, jak je uvedeno výše;
- při podezření na praní peněz nebo financování terorismu, bez ohledu na odchylky, výjimky nebo omezení stanovené v těchto pokynech a platných právních předpisech.

Ve výše uvedených případech společnost uplatní opatření CDD uvedená v této kapitole.

V případě obdržení informací v cizích jazycích v rámci provádění opatření CDD může Společnost požádat o překlad dokumentů do jiného jazyka, který je pro ni použitelný. Překladů je třeba se vyvarovat v situacích, kdy jsou originální dokumenty vyhotoveny v jazyce použitelném pro Společnost.

Dosažení CDD je proces, který začíná zavedením opatření CDD. Po dokončení tohoto procesu zákazník přiřadí zdokumentovanou individuální úroveň rizika, která je základem pro následná opatření a která je v případě potřeby sledována a aktualizována.

Společnost uplatňuje opatření CDD přiměřeně, pokud je vnitřně přesvědčena, že splnila povinnost uplatňovat opatření náležité péče. Při posuzování vnitřního přesvědčení se dodržuje zásada přiměřenosti. To znamená, že Společnost musí při aplikaci opatření CDD získat vědomosti, porozumění a tvrzení, že shromáždila dostatek informací o Zákazníkovi, jeho aktivitách, účelu obchodního vztahu a transakcí prováděných v rámci obchodního vztahu, původu finančních prostředků apod. tak, aby porozuměla Zákazníkovi a jeho (obchodním) aktivitám, a tím zohlednila míru rizika Zákazníka, riziko spojené s obchodním vztahem a povahu tohoto vztahu. Taková úroveň tvrzení musí umožnit identifikovat komplikované, vysoce hodnotné a neobvyklé transakce a transakční vzorce, které nemají rozumný nebo zřejmý ekonomický nebo legitimní účel nebo nejsou charakteristické pro specifické rysy daného obchodu.

identifikace skutečného vlastníka zákazníka

Společnost musí identifikovat skutečného majitele zákazníka a přijmout opatření k ověření totožnosti skutečného majitele v rozsahu, který jí umožní ujistit se, že ví, kdo je skutečným majitelem.

Společnost si od zákazníka vyžádá informace o skutečném majiteli zákazníka (např. poskytne zákazníkovi možnost uvést skutečného majitele v dotazníku KYC).

Společnost nenaváže obchodní vztah, pokud má zákazník, který je fyzickou osobou, skutečného majitele, který není stejnou osobou jako zákazník.

Skutečný vlastník právnické osoby se zjišťuje postupně, přičemž povinný subjekt postupuje do každé následující fáze, pokud nelze skutečného vlastníka právnické osoby určit v případě předchozí fáze. Jednotlivé fáze jsou následující:

- je možné u zákazníka, který je právnickou osobou nebo osobou účastnící se transakce, identifikovat fyzickou osobu nebo osoby, které tuto právnickou osobu skutečně v konečném důsledku ovládají nebo na ni mají jakýkoli jiný vliv či nad ní vykonávají kontrolu, a to bez ohledu na velikost podílů, hlasovacích nebo vlastnických práv nebo jejich přímou či nepřímou povahu;
- zda má zákazník, který je právnickou osobou, nebo osoba účastnící se transakce fyzickou osobu nebo osoby, které vlastní nebo ovládají právnickou osobu prostřednictvím

přímého[6] nebo nepřímého[7] podílu. Zde je třeba vzít v úvahu i rodinné vazby a smluvní vazby;

- kdo je fyzickou osobou ve vrcholovém vedení[8] , která musí být definována jako skutečný majitel, neboť v důsledku provedení předchozích dvou fází nebylo povinnému subjektu umožněno skutečného majitele identifikovat.

Pokud z dokladů použitých k identifikaci právnické osoby nebo z jiných předložených dokladů přímo nevyplývá, kdo je skutečným majitelem právnické osoby, zapíší se příslušné údaje (včetně údajů o členství ve skupině a vlastnické a řídící struktuře skupiny) na základě prohlášení zástupce právnické osoby nebo na základě dokumentu vlastnoručně sepsaného zástupcem právnické osoby.

Společnost uplatní přiměřená opatření k ověření správnosti údajů zjištěných na základě výkazů nebo vlastnoručně podepsaného dokumentu (např. dotazem do příslušných rejstříků) a vyžádá si předložení výroční zprávy právnické osoby nebo jiného příslušného dokumentu. Pokud má Společnost pochybnosti o správnosti nebo úplnosti příslušných informací, ověří poskytnuté informace z veřejně dostupných zdrojů a v případě potřeby si od zákazníka vyžádá doplňující informace.

V případě, že Společnost naváže obchodní vztah se Zákazníkem, jehož údaje o Skutečných majitelích musí být v souladu se zákony členského státu Evropské unie předloženy státu nebo v něm registrovány, pořídí Společnost po identifikaci Skutečného majitele Zákazníka příslušné osvědčení o registraci nebo výpis z registru.

Skutečný vlastník nemusí být identifikován v případě zákazníka kótovaného na regulovaném trhu, který podléhá požadavkům na zveřejňování informací v souladu s právem Evropské unie nebo podléhá rovnocenným mezinárodním standardům, které zajišťují přiměřenou transparentnost informací o vlastnictví.

Postup pro zjištění nesrovnalosti

Po zjištění nesouladu mezi údaji o skutečných majitelích Zákazníka, který je právnickou osobou, dostupnými v příslušném rejstříku a údaji o skutečných majitelích téhož Zákazníka, které má k dispozici, Společnost na tuto skutečnost Zákazníka upozorní a navrhne mu, aby do příslušného rejstříku poskytl přesné údaje o svých skutečných majitelích.

Společnost v rámci oznámení uvede, v čem spatřuje nesrovnalost. Je-li to za daných okolností účelné, umožní Společnost zákazníkovi, aby se k této nesrovnalosti vyjádřil.

---

[6] **přímé vlastnictví** je způsob výkonu kontroly, kdy fyzická osoba vlastní 25 % podíl plus jednu akcii nebo vlastnické právo k více než 25 % akcií společnosti.

[7] **nepřímé vlastnictví** je způsob výkonu kontroly, kdy 25 procent akcií plus jednu akcii nebo vlastnické právo nad 25 procent ve společnosti vlastní společnost, která je ovládána fyzickou osobou, nebo několik společností, které jsou ovládány stejnou fyzickou osobou.

[8] **člen vrcholového** vedení je osoba, která činí strategická rozhodnutí, která zásadně ovlivňují obchodní činnosti a/nebo postupy a/nebo obecné (obchodní) trendy společnosti, nebo v případě její nepřítomnosti vykonává každodenní nebo běžné řídící funkce společnosti v rámci výkonné moci (např. výkonný ředitel (CEO), finanční ředitel (CFO), ředitel nebo prezident atd.).

Neodstraní-li Zákazník nesrovnalost nebo nevyvrátí-li ji bez zbytečného odkladu od oznámení, oznámí povinná osoba nesrovnalost soudu, který je příslušný k řízení o nesrovnalosti podle zákona upravujícího evidenci skutečných majitelů.

Pokud by výše uvedený postup mohl zmařit nebo ohrozit vyšetřování podezřelého obchodu nebo probíhající trestní řízení, může FAÚ dát Společnosti pokyn, aby jej nepoužila.

identifikace účelu a povahy obchodního vztahu nebo transakce

Společnost musí rozumět účelu a povaze navazování obchodního vztahu nebo provádění transakce. Společnost použije dodatečná opatření a shromáždí dodatečné informace, aby zjistila účel a povahu obchodního vztahu nebo příležitostné transakce v případech, kdy:

- existuje situace, která se týká vysoké hodnoty nebo je neobvyklá a/nebo
- pokud riziko a/nebo rizikový profil spojený se zákazníkem a povaha obchodního vztahu zavdává příčinu k provedení dodatečných opatření, aby bylo možné obchodní vztah později náležitě monitorovat.

Pokud je Zákazník právnickou osobou, Společnost kromě výše uvedeného identifikuje i Zákazníka:

- **oblast činnosti,** přičemž Společnost musí pochopit, čím se Zákazník zabývá a hodlá zabývat v rámci obchodního vztahu a jak to odpovídá účelu a povaze obchodního vztahu obecně a zda je to přiměřené, srozumitelné a věrohodné;
- **platební praktiky,** včetně zemí, ze kterých jsou platby přijímány a do kterých jsou prováděny, předpokládaná doba trvání obchodního vztahu, rozsah a způsoby používání hotovosti a kryptoměn, platební kanály (pobočka, internetová banka, platby kartou) atd;
- **hlavní obchodní partneři,** kde Společnost musí identifikovat, kdo jsou hlavní partneři Zákazníka, se kterými budou uzavírány transakce v deklarované oblasti činnosti a s deklarovaným objemem činnosti.

Oblast činnosti, platební postupy a hlavní obchodní partneři musí odpovídat profilu zkušeností zástupce zákazníka (nebo klíčových osob) a/nebo skutečného vlastníka. Společnost tedy musí určit, odkud pochází kapacita, schopnosti, dovednosti a znalosti (obecně zkušenosti) zástupce a/nebo Skutečného majitele, aby mohl působit v této oblasti činnosti, s těmito objemy obchodů a s těmito hlavními obchodními partnery.

Kromě výše uvedených opatření může společnost v rámci pochopení účelu a povahy prováděné transakce zjistit zdroj a původ finančních prostředků použitých v transakci (transakcích), jak je popsáno níže.

Zjištění vlastnické a řídící struktury zákazníka

Společnost zjistí vlastnickou a řídící strukturu zákazníka, který je právnickou osobou, na základě dokumentů vydaných příslušným orgánem nebo institucí, které obsahují informace o výše uvedených skutečnostech. Společnost rovněž uplatní postup zjišťování, zda se na osobu v této struktuře vztahují Sankce, stanovený v kapitole Provádění sankcí těchto Pokynů.

Sledování obchodního vztahu

Společnost sleduje navázané obchodní vztahy, u nichž jsou zavedena následující opatření průběžné hloubkové kontroly (ODD):

- zajištění pravidelné aktualizace dokumentů, údajů nebo informací shromážděných v rámci uplatňování opatření náležité péče a v případě spouštěcích událostí, tj. především údajů o zákazníkovi, jeho zástupci (včetně práva na zastoupení) a skutečném majiteli, jakož i o účelu a povaze obchodního vztahu;
- průběžné sledování obchodního vztahu, které zahrnuje transakce prováděné v rámci obchodního vztahu s cílem zajistit, aby transakce odpovídaly znalostem Společnosti o zákazníkovi, jeho aktivitách a rizikovém profilu;
- identifikace zdroje a původu finančních prostředků použitých při transakci (transakcích).

Společnost pravidelně **kontroluje a aktualizuje dokumenty, údaje a informace** shromážděné v rámci provádění opatření CDD. Pravidelnost kontrol musí vycházet z rizikového profilu zákazníka a kontroly musí probíhat minimálně:

- jednou za půl roku pro zákazníka s vysoce rizikovým profilem;
- jednou ročně pro zákazníka se středně rizikovým profilem;
- jednou za dva roky pro zákazníky s nízkým rizikem.

Shromážděné dokumenty, údaje a informace se musí také zkontrolovat, zda nedošlo k události, která indikuje potřebu aktualizovat shromážděné dokumenty, údaje a informace.

V rámci **průběžného sledování obchodního vztahu** Společnost sleduje transakce uzavírané v průběhu obchodního vztahu tak, aby mohla určit, zda uzavírané transakce odpovídají informacím, které byly o Zákazníkovi dříve známy (tj. tomu, co Zákazník deklaroval při navázání obchodního vztahu nebo co se dozvěděl v průběhu obchodního vztahu).

Společnost rovněž sleduje obchodní vztah, aby zjistila činnost zákazníka nebo skutečnosti, které naznačují trestnou činnost, praní peněz nebo financování terorismu nebo jejichž souvislost s praním peněz nebo financováním terorismu je pravděpodobná, včetně komplikovaných, vysoce hodnotných a neobvyklých transakcí a transakčních vzorců, které nemají žádný rozumný nebo zřejmý ekonomický nebo legitimní účel nebo které nejsou charakteristické pro specifické rysy daného obchodu. V průběhu obchodního vztahu Společnost průběžně vyhodnocuje změny v činnosti Zákazníka a posuzuje, zda tyto změny mohou zvýšit míru rizika spojeného se Zákazníkem a obchodním vztahem, což vyvolává potřebu uplatnit opatření EDD.

V rámci průběžného sledování obchodních vztahů společnost uplatňuje následující opatření:

- screening, tj. sledování transakcí v reálném čase;
- monitorování, tj. pozdější analýza transakcí.

Cílem **screeningu** je identifikovat**:**

- podezřelé a neobvyklé transakce a jejich vzorce;
- transakce překračující stanovené prahové hodnoty;

- politicky exponované osoby a okolnosti týkající se mezinárodních sankcí.

Kontrola transakcí se provádí automaticky a zahrnuje následující opatření:

- stanovené prahové hodnoty pro transakce zákazníka v závislosti na rizikovém profilu zákazníka a odhadovaném obratu transakcí vykázaných zákazníkem;
- bodování peněženek s virtuální měnou, kam bude virtuální měna zaslána v souladu s objednávkou zákazníka;
- bodování peněženek s virtuální měnou, ze kterých je virtuální měna přijímána.

Pokud Zákazník zadá příkaz k transakci, která přesahuje stanovenou hranici, nebo k transakci do peněženky virtuální měny s vysokým rizikem (např. peněženky spojené s podvody, trestnou činností apod.), bude transakce manuálně schválena Zaměstnancem, který před schválením přistoupí k nutnosti uplatnit případná další opatření CDD (např. uplatnění opatření EDD, dotaz na zdroj a původ finančních prostředků nebo dotaz na další informace týkající se transakce).

Při **sledování transakcí** zaměstnanec posuzuje transakce s cílem odhalit činnosti a transakce, které:

- odchýlit od toho, co lze důvodně očekávat na základě provedených opatření CDD, poskytovaných služeb, informací poskytnutých zákazníkem a dalších okolností (např. překročení odhadovaného obratu transakcí, zasílání virtuální měny pokaždé do nové peněženky s virtuální měnou, objem transakcí překračující limit);
- bez odchylky podle předchozího odstavce lze předpokládat, že je součástí praní peněz nebo financování terorismu;
- může ovlivnit hodnocení rizikového profilu zákazníka.

V případě zjištění výše uvedené skutečnosti je zaměstnanec povinen informovat MPSV a odložit jakoukoli transakci Zákazníka až do rozhodnutí MPSV o této skutečnosti.

Kromě výše uvedeného musí MLRO pravidelně (alespoň jednou týdně) kontrolovat transakce společnosti, aby zajistil, že:

- zaměstnanci společnosti řádně plnili výše uvedené povinnosti;
- neexistují transakce a vzorce transakcí, které jsou komplikované, mají vysokou hodnotu a jsou neobvyklé a nemají žádný rozumný nebo zřejmý ekonomický nebo legitimní účel nebo nejsou charakteristické svými specifickými rysy.

Společnost v případě potřeby **identifikuje zdroj[9] a původ[10] prostředků** použitých v transakci (transakcích). Potřeba identifikovat zdroj a původ finančních prostředků závisí na předchozích aktivitách zákazníka a na dalších známých informacích. Identifikace zdroje a původu prostředků použitých v transakci se tedy provádí v následujících případech:

[9] **zdroj finančních prostředků** použitých v transakci je důvod, vysvětlení a základ (právní vztah a jeho obsah), proč byly finanční prostředky převedeny.

[10] **původem finančních prostředků** použitých v transakci je činnost, kterou byly finanční prostředky vydělané nebo přijaté.

- transakce překračují limity stanovené Společností;
- pokud transakce neodpovídají dříve známým informacím o zákazníkovi;
- pokud Společnost chce nebo by měla důvodně považovat za nezbytné posoudit, zda transakce odpovídají informacím, které byly o Zákazníkovi dříve známy;
- pokud má společnost podezření, že transakce naznačují trestnou činnost, praní peněz nebo financování terorismu nebo že je pravděpodobná souvislost transakcí s praním peněz nebo financováním terorismu, včetně komplikovaných, vysoce hodnotných a neobvyklých transakcí a vzorců transakcí, které nemají žádný rozumný nebo zřejmý ekonomický nebo legitimní účel nebo nejsou charakteristické pro specifické rysy daného podnikání.

OPATŘENÍ ZESÍLENÉ HLOUBKOVÉ KONTROLY

Kromě opatření CDD uplatňuje společnost opatření zesílené hloubkové kontroly (EDD) s cílem řídit a zmírnit zjištěné riziko praní peněz a financování terorismu, které je vyšší než obvykle.

Společnost uplatňuje opatření EDD vždy, když:

- rizikový profil zákazníka vykazuje vysokou míru rizika;
- po identifikaci zákazníka nebo ověření předložených informací vzniknou pochybnosti o pravdivosti předložených údajů, pravosti dokladů nebo identifikaci skutečného majitele;
- zákazník je PEP;
- země původu zákazníka je vysoce rizikovou třetí zemí nebo transakce souvisí s vysoce rizikovou třetí zemí.

Před uplatněním opatření EDD se zaměstnanec společnosti ujistí, že obchodní vztah nebo transakce jsou vysoce rizikové a že takovému obchodnímu vztahu nebo transakci lze přisoudit vysokou míru rizika. Především však zaměstnanec před uplatněním opatření EDD posoudí, zda jsou přítomny výše popsané znaky, a uplatní je jako nezávislé důvody (tj. každý z identifikovaných faktorů umožňuje uplatnění opatření EDD ve vztahu k zákazníkovi).

Při uplatňování opatření EDD je třeba dodržovat následující dodatečná a relevantní opatření náležité péče:

- shromažďování dodatečných dokumentů a ověřování dodatečně předložených informací po identifikaci zákazníka a skutečného majitele na základě dodatečných dokumentů, údajů nebo informací pocházejících z důvěryhodného a nezávislého zdroje;
- shromáždění dodatečných informací o účelu a povaze obchodního vztahu nebo transakce a ověření předložených informací na základě dodatečných dokumentů, údajů nebo informací, které pocházejí ze spolehlivého a nezávislého zdroje[2];.

[2] toto opatření se uplatní vždy, když Společnost přijde do styku s rizikovou třetí zemí prostřednictvím zákazníka nebo transakce.

- shromáždění dalších informací a dokumentů týkajících se skutečného provedení transakcí uskutečněných v rámci obchodního vztahu s cílem vyloučit zdánlivost transakcí;
- shromažďování dalších informací a dokumentů za účelem identifikace zdroje a původu finančních prostředků použitých v transakci uskutečněné v obchodním vztahu, aby se vyloučila zdánlivost transakcí;
- provedení první platby související s transakcí prostřednictvím účtu, který byl otevřen na jméno zákazníka účastnícího se transakce v úvěrové instituci registrované nebo s místem podnikání ve smluvním státě Evropského hospodářského prostoru nebo v zemi, kde platí požadavky rovnocenné požadavkům směrnice Evropského parlamentu a Rady (EU) 2015/849;
- uplatnění opatření náležité péče ve vztahu k zákazníkovi nebo jeho zástupci, přičemž se nachází na stejném místě jako zákazník nebo jeho zástupce;
- shromažďování dalších informací o zákazníkovi a jeho skutečném vlastníkovi, včetně identifikace všech vlastníků zákazníka, včetně těch, jejichž podíl je nižší než 25 %;[2]
- shromažďování informací o původu finančních prostředků a majetku zákazníka a jeho skutečného majitele; 3.[2,]
- zlepšení sledování obchodního vztahu zvýšením počtu a četnosti uplatňovaných kontrolních opatření a výběrem ukazatelů transakcí nebo vzorců transakcí, které jsou dodatečně ověřovány;[2,3]
- je provedena analýza digitálního dojmu zákazníka na internetu (vyhledávání v nepříznivých médiích);
- získání souhlasu generálního ředitele pro transakce s novými a stávajícími zákazníky;[2,3]

Výši opatření EDD a jejich rozsah určuje zaměstnanec, který tato opatření uplatňuje. Zaměstnanec je povinen oznámit uplatněná opatření EDD do 2 pracovních dnů od zahájení uplatňování opatření EDD zasláním příslušného oznámení na MPSV.

V případě uplatnění opatření EDD monitoruje společnost obchodní vztah častěji než obvykle a nejpozději každých šest měsíců přehodnocuje rizikový profil zákazníka.

ZJEDNODUŠENÁ OPATŘENÍ HLOUBKOVÉ KONTROLY

Opatření zjednodušené hloubkové kontroly (SDD) mohou být uplatněna v případech, kdy rizikový profil zákazníka ukazuje na nízké riziko a kdy bylo v souladu s hodnocením rizik Společností zjištěno, že za těchto okolností je riziko praní špinavých peněz nebo financování terorismu nižší než obvykle.

V rámci opatření SDD společnost provede alespoň následující:

- ověřit, že opatření SDD mohou být použita v souladu s platnými právními předpisy;
- provést identifikaci zákazníka, jak je uvedeno výše;
- identifikovat skutečného vlastníka, jak je uvedeno výše;

- provádí další činnosti v rámci identifikace a kontroly zákazníka v rozsahu nezbytném pro účinné řízení rizik.

VÝJIMKY PRO NEPROVEDENÍ HLOUBKOVÉ KONTROLY.

Společnost neprovádí CDD/EDD nebo jeho část, pokud:

- provedení CDD/EDD nebo jeho části by pravděpodobně zmařilo nebo ohrozilo vyšetřování podezřelé transakce; nebo
- společnost dostane od FAÚ pokyn neprovádět CDD/EDD nebo jeho část z důvodu, že by provedení kontroly mohlo zmařit nebo ohrozit vyšetřování podezřelé transakce nebo probíhající trestní řízení.

PROVÁDĚNÍ SANKCÍ

Po nabytí účinnosti, změně nebo ukončení Sankcí Společnost ověří, zda osoby ve vlastnické struktuře Zákazníka, Zákazník nebo osoba, která s nimi hodlá mít obchodní vztah nebo transakci, není subjektem Sankcí. Pokud Společnost zjistí, že osoba, na kterou se vztahují Sankce, nebo že transakce, kterou hodlá uskutečnit nebo uskutečňuje, je v rozporu se Sankcemi, Společnost uplatní Sankce a neprodleně o tom informuje FAÚ.

Postup pro identifikaci předmětu sankcí a transakce porušující sankce

Společnost použije k ověření vztahu zákazníka k sankcím alespoň jeden z následujících zdrojů (databází):

- Konsolidovaný seznam sankcí EU;
- Konsolidovaný seznam sankcí OSN.

Společnost ověří vztah Zákazníka k Sankcím v rámci výše popsaného procesu identifikace Zákazníka.

Kromě výše uvedených zdrojů může Společnost využít i jiné zdroje na základě rozhodnutí Zaměstnance, který uplatňuje opatření CDD.

K ověření, zda se jména osob, která vyplynou z šetření, shodují s osobami uvedenými v oznámení obsahujícím sankce, se použijí jejich osobní údaje, jejichž hlavními charakteristikami jsou v případě právnické osoby její název nebo ochranná známka, rejstříkový kód nebo datum registrace a v případě fyzické osoby její jméno a osobní kód nebo datum narození.

Za účelem zjištění totožnosti osob uvedených v příslušném právním aktu nebo oznámení, které jsou totožné s osobami zjištěnými na základě dotazu z databází, musí Společnost provést analýzu jmen osob zjištěných na základě dotazu na základě možného vlivu faktorů zkreslujících osobní údaje (např. přepis cizích jmen, jiné pořadí slov, záměna diakritiky nebo zdvojených písmen apod.).Společnost bude výše uvedené ověření provádět průběžně v rámci navázaného obchodního vztahu vždy při aktualizaci výše uvedených sankčních seznamů ze strany příslušných orgánů.

Pokud má Zaměstnanec pochybnosti o tom, že se na určitou osobu vztahují Sankce, neprodleně o tom informuje MLRO nebo generálního ředitele. V takovém případě MLRO generálního ředitele rozhodne, zda si od dané osoby vyžádá nebo získá další údaje, nebo zda své podezření neprodleně oznámí FAÚ.

Společnost si především sama opatřuje další informace o osobě, která je s ní v obchodním vztahu nebo s ní provádí úkon, jakož i o osobě, která s ní hodlá navázat obchodní vztah, provést úkon nebo jednání, přičemž upřednostňuje informace z důvěryhodného a nezávislého zdroje. Pokud z nějakého důvodu takové informace nejsou k dispozici, společnost se dotáže osoby, která je s ní v obchodním vztahu nebo s ní provádí transakci či úkon, jakož i osoby, která s ní hodlá navázat obchodní vztah, provést transakci či úkon, zda informace pochází z důvěryhodného a nezávislého zdroje, a odpověď posoudí.

Akce při identifikaci subjektu sankcí nebo transakce porušující sankce

Pokud se Zaměstnanec dozví, že Zákazník, který je v obchodním vztahu nebo provádí transakci se Společností, jakož i osoba, která hodlá navázat obchodní vztah nebo provést transakci se Společností, je předmětem Sankcí, je povinen neprodleně informovat MPSV nebo generálního ředitele o identifikaci subjektu Sankcí, o pochybnostech o něm a o přijatých opatřeních.

MPSV nebo generální ředitel odmítne uzavřít obchod nebo řízení, přijme opatření stanovená v zákoně o uložení nebo výkonu sankcí a neprodleně oznámí FAÚ své pochybnosti a přijatá opatření.

Při identifikaci subjektu sankcí je nutné určit opatření, která jsou přijímána za účelem sankcionování této osoby. Tato opatření jsou popsána v právním aktu, kterým se sankce provádějí, proto je nutné přesně určit, jaká sankce je vůči dané osobě uplatňována, aby bylo zajištěno zákonné a správné uplatňování opatření.

ODMÍTNUTÍ TRANSAKCE NEBO OBCHODNÍHO VZTAHU A JEJICH UKONČENÍ.

Společnost nesmí navazovat obchodní vztahy a navázaný obchodní vztah nebo transakce se ukončí v případě, že:

- společnost má podezření na praní špinavých peněz nebo financování terorismu;
- společnost není schopna přijmout a provést žádné z požadovaných opatření CDD, včetně případů, kdy:
    - zákazník odmítne předložit informace nebo doklady pro identifikaci zákazníka nebo jeho zástupce;
    - zákazník nespolupracuje při uplatňování opatření CDD;
    - není možné zákazníka identifikovat nebo zkontrolovat z jiného důvodu;
- Společnost má pochybnosti o pravdivosti informací poskytnutých Zákazníkem nebo o pravosti předložených dokumentů;
- původ finančních prostředků nebo jiného majetku zákazníka, který je PEP, použitého v obchodním vztahu nebo transakci, není Společnosti znám;

- zákazník, jehož kapitál tvoří akcie na doručitele nebo jiné cenné papíry na doručitele, chce navázat obchodní vztah;
- zákazník, který je fyzickou osobou, za níž stojí jiná, skutečně prospěšná osoba, chce navázat obchodní vztah (podezření, že je použita krycí osoba);
- rizikový profil zákazníka se stal nepřiměřeným rizikovému apetitu společnosti (tj. úroveň rizikového profilu zákazníka je "zakázaná").

Výše uvedené se nepoužije, pokud společnost oznámila FAU navázání obchodního vztahu, transakci nebo pokus o transakci v souladu s níže uvedeným postupem a obdržela od FAU konkrétní pokyn k pokračování obchodního vztahu, navázání obchodního vztahu nebo transakce.

V případě ukončení obchodního vztahu v souladu s touto kapitolou převede Společnost aktiva Zákazníka v přiměřené lhůtě, pokud možno však nejpozději do jednoho měsíce od ukončení, a to jako celek na účet otevřený u úvěrové instituce, která je registrována nebo má sídlo ve smluvním státě Evropského hospodářského prostoru nebo v zemi, kde se uplatňují požadavky odpovídající požadavkům stanoveným v příslušných směrnicích Evropského parlamentu a Rady. Ve výjimečných případech mohou být aktiva převedena na jiný účet než účet zákazníka nebo vydána v hotovosti, a to tak, že o tom FAÚ informuje se všemi relevantními a dostatečnými informacemi nejméně 7 pracovních dnů předem a za podmínky, že FAÚ nevydá jiný příkaz. Bez ohledu na příjemce peněžních prostředků je minimální informací uvedenou v anglickém jazyce v platebních údajích o převodu prostředků Zákazníka to, že převod souvisí s mimořádným ukončením vztahu se Zákazníkem.

OHLAŠOVACÍ POVINNOST

Zjistí-li společnost v souvislosti se svou činností podezřelou transakci, oznámí to bez zbytečného odkladu FAÚ. Vyžadují-li to okolnosti případu, zejména hrozí-li nebezpečí z prodlení, oznámí Společnost podezřelou transakci ihned po jejím zjištění.

Minimální charakteristiky podezřelých transakcí jsou uvedeny v příslušné příloze těchto pokynů.

Společnost rovněž podá FAÚ oznámení o podezřelém obchodu vždy, když neprovede CDD/EDD nebo jeho část na základě výjimky pro neprovedení hloubkové kontroly (popsané v kapitole CDD těchto Pokynů).

Pokud vznikne potřeba výše uvedeného hlášení, musí zaměstnanec, kterému se tato potřeba stala známou, o tom neprodleně informovat MPSV. MPSV přijme rozhodnutí a zašle příslušnou zprávu FAÚ.

Zpráva se zasílá v souladu s pokyny vydanými FAÚ, a to písemně, v listinné podobě doporučeným dopisem nebo elektronicky způsobem, který zajistí důvěrnost předávaných údajů.

V oznámení podezřelé transakce Společnost uvede identifikační údaje osoby, které se oznámení týká, identifikační údaje všech ostatních účastníků transakce, které jsou v době oznámení k dispozici, informace o významných okolnostech transakce a veškeré další informace, které by mohly být relevantní pro její posouzení z hlediska opatření proti praní peněz nebo financování terorismu.

Pokud je oznámení podáváno v souvislosti s osvobozením od provádění CDD, společnost v oznámení rovněž uvede:

- okolnosti a důvody neprovedení CDD nebo jeho části v rozsahu, který umožňuje posoudit vhodnost tohoto postupu;
- konkrétní postup v rámci CDD nebo jeho část, kterou společnost neprovedla.

Společnost odloží transakci zákazníka, u které bylo FAÚ podáno oznámení. Společnost má právo provést transakci nejdříve 24 hodin po odeslání oznámení podezřelého FAU, pokud nejpozději neposkytla jiné pokyny.

Společnost, její organizační složka, generální ředitel, MPSV a Zaměstnanec nesmí informovat osobu, jejího skutečného majitele, zástupce nebo třetí osobu o oznámení, které na ně bylo podáno FAÚ, o plánu podat takové oznámení nebo o vzniku oznámení, jakož i o příkazu FAÚ nebo o zahájení trestního řízení. Po splnění příkazu učiněného FAÚ může společnost informovat osobu o tom, že FAÚ omezil nakládání s účtem této osoby nebo že jí bylo uloženo jiné omezení.

POVINNOST ŠKOLENÍ

Společnost zajišťuje, aby její zaměstnanci, její dodavatelé a další osoby, které se podílejí na podnikání na obdobném základě a které plní pracovní úkoly důležité pro předcházení zneužití podnikání k praní peněz nebo financování terorismu (dále jen "příslušné osoby"), měli pro tyto pracovní úkoly odpovídající kvalifikaci. Při přijímání nebo zaměstnávání příslušné osoby se její kvalifikace prověřuje v rámci procesu přijímání/jmenování, a to tak, že se kromě obvyklého získávání referencí provádí i prověrka zahrnující výpisy z rejstříku trestů, která se dokumentuje pomocí zvláštního standardního formuláře posuzujícího vhodnost zaměstnance.

V souladu s požadavky platnými pro Společnost na zajištění vhodnosti příslušných osob Společnost dbá na to, aby tyto osoby byly průběžně školeny a informovány tak, aby byly schopny plnit povinnosti Společnosti v souladu s platnými právními předpisy. Prostřednictvím školení je zajištěno, že tyto osoby mají znalosti v oblasti AML/CFT v přiměřeném rozsahu s ohledem na úkoly a funkci dané osoby. Školení musí poskytovat především informace o všech nejnovějších metodách praní peněz a financování terorismu a rizicích z nich vyplývajících.

Toto školení se týká příslušných částí obsahu platných pravidel a předpisů, hodnocení rizik Společnosti, Směrnic a postupů Společnosti a informací, které by měly těmto Příslušným osobám usnadnit odhalení podezření na praní peněz a financování terorismu. Školení je strukturováno na základě rizik identifikovaných prostřednictvím politiky hodnocení rizik.

Obsah a četnost školení je přizpůsoben úkolům a funkci dané osoby v otázkách týkajících se opatření proti praní peněz a financování terorismu. Pokud jsou pokyny nějakým způsobem aktualizovány nebo změněny, obsah a četnost školení se odpovídajícím způsobem upraví.

Školení nových zaměstnanců zahrnuje seznámení s obsahem platných pravidel a předpisů, politikou společnosti v oblasti hodnocení rizik, těmito pokyny a dalšími příslušnými postupy.

Zaměstnanci a generální ředitel jsou průběžně školeni pod záštitou MLRO v souladu s následujícím plánem školení:

- periodicita: nejméně jednou ročně pro generálního ředitele. Nejméně jednou ročně pro zaměstnance a zapojené relevantní osoby.
- rozsah: přezkoumání platných pravidel a předpisů, směrnic společnosti a dalších příslušných postupů. Konkrétní informace týkající se nových/aktualizovaných prvků v platných pravidlech a předpisech. Zpráva a výměna zkušeností týkajících se transakcí přezkoumávaných od předchozího školení.

Kromě výše uvedeného jsou příslušné osoby průběžně informovány o nových trendech, vzorcích a metodách a jsou jim poskytovány další informace důležité pro předcházení praní peněz a financování terorismu.

Uskutečněné školení je třeba elektronicky zdokumentovat a potvrdit podpisem příslušné osoby. Tato dokumentace by měla obsahovat obsah školení, jména účastníků a datum školení.

SHROMAŽĎOVÁNÍ A UCHOVÁVÁNÍ ÚDAJŮ

Společnost prostřednictvím osoby (vč. zaměstnanců, generálního ředitele a MLRO), která jako první obdrží příslušné informace nebo dokumenty, je povinna je zaevidovat a uchovat:

- veškeré informace a kopie dokumentů shromážděné v rámci procesu identifikace zákazníka, jakož i veškeré změny a úpravy těchto údajů;
- informace a kopie dokumentů získaných v rámci CDD;
- informace o tom, kdo a kdy provedl první identifikaci zákazníka;
- záznamy o postupu při posuzování a určování rizikového profilu zákazníka, včetně výběru vhodných opatření přijatých vůči zákazníkovi a posouzení skutečností souvisejících s podáním oznámení o podezřelém obchodu;
- v případě, že má Zákazník zástupce, originál nebo ověřenou kopii plné moci nebo číslo jednací rozhodnutí soudu o ustanovení zástupce;
- informace o okolnostech odmítnutí navázání obchodního vztahu ze strany společnosti;
- okolnosti odmítnutí navázání obchodního vztahu z podnětu Zákazníka, pokud odmítnutí souvisí s uplatněním opatření CDD Společností;
- informace o všech provedených operacích za účelem identifikace osoby účastnící se transakce nebo skutečného majitele zákazníka;
- informace o okolnostech ukončení obchodního vztahu v souvislosti s nemožností uplatnit opatření CDD.
- každé datum nebo období transakce a popis obsahu transakce;
- informace sloužící jako základ pro výše uvedené oznamovací povinnosti;
- údaje o podezřelých nebo neobvyklých transakcích nebo okolnostech, o kterých nebyl FAÚ informován.

Kromě výše uvedených informací společnost eviduje každou částku transakce, měnu a číslo účtu.

Výše uvedené údaje se uchovávají po dobu 10 let od ukončení obchodního vztahu nebo dokončení transakce. Údaje související s plněním oznamovací povinnosti musí být uchovávány po dobu 5 let od splnění oznamovací povinnosti.

Dokumenty a údaje musí být uchovávány tak, aby bylo možné vyčerpávajícím způsobem a neprodleně reagovat na dotazy FAÚ nebo v souladu s právními předpisy jiných dozorových orgánů, vyšetřovacích orgánů nebo soudu.

Společnost uplatňuje všechna pravidla ochrany osobních údajů na základě požadavků vyplývajících z platných právních předpisů. Společnost smí zpracovávat osobní údaje získané při provádění CDD pouze za účelem prevence praní špinavých peněz a financování terorismu a údaje nesmí být dále zpracovávány způsobem, který nesplňuje účel, například pro marketingové účely.

Společnost po uplynutí této lhůty uchovávané údaje vymaže, pokud právní předpisy upravující danou oblast nestanoví jiný postup. Na základě příkazu příslušného dozorového úřadu mohou být údaje důležité pro předcházení, odhalování nebo vyšetřování praní peněz nebo financování terorismu uchovávány po delší dobu, nejdéle však po dobu pěti let od uplynutí první lhůty.

VNITŘNÍ KONTROLA PROVÁDĚNÍ POKYNŮ

Plnění Pokynů interně kontroluje generální ředitel nebo zaměstnanec pověřený generálním ředitelem výkonem příslušných funkcí (dále v této kapitole - pracovník interní kontroly). Pracovník pro vnitřní kontrolu musí disponovat potřebnými kompetencemi, nástroji a přístupem k relevantním informacím ve všech strukturálních útvarech Společnosti.

Pracovník pro vnitřní kontrolu vykonává funkce vnitřní kontroly alespoň v těchto oblastech:

- soulad společnosti se stanovenou politikou hodnocení rizik a rizikovým apetitem;
- Provádění opatření CDD;
- provádění sankcí;
- povinnost společnosti odmítnout transakci nebo obchodní vztah a jejich ukončení;
- ohlašovací povinnost společnosti vůči FAÚ;
- povinnost společnosti absolvovat školení týkající se požadavků AML/CFT;
- povinnost společnosti shromažďovat a uchovávat údaje.

Přesná opatření pro provádění vnitřní kontroly stanoví vnitřní kontrolor a musí odpovídat velikosti společnosti a povaze, rozsahu a úrovni složitosti poskytovaných činností a služeb. Útvary vnitřní kontroly musí zohlednit alespoň výše uvedené oblasti zkoumání. Vnitřní kontrolní opatření se provádějí v době stanovené pracovníkem pro vnitřní kontrolu s jím stanovenou četností, nejméně jednou měsíčně, pokud povaha opatření výslovně nestanoví jinak.

Výsledky provádění vnitřních kontrolních opatření (dále v této kapitole - údaje o vnitřní kontrole) se ukládají odděleně od ostatních údajů a uchovávají se po dobu 10 let. K údajům o vnitřní kontrole mají přístup pouze členové správní rady a pracovník pro vnitřní kontrolu. Pracovník pro vnitřní kontrolu může poskytnout přístup k údajům o vnitřní kontrole dalším zaměstnancům nebo třetím stranám (např. poradcům, auditorům apod.) pouze s předchozím souhlasem

představenstva. Osoby, které mají přístup k údajům vnitřní kontroly, je nesmí nikomu zpřístupnit bez předchozího souhlasu představenstva.

Údaje o vnitřní kontrole se ukládají v chronologickém pořadí a ve formátu, který umožňuje jejich analýzu a srozumitelné propojení s dalšími relevantními údaji.

Pracovník pro vnitřní kontrolu předkládá zprávu o vnitřní kontrole představenstvu nejméně jednou za čtvrtletí a valné hromadě akcionářů společnosti nejméně jednou ročně. Předkládaná zpráva o vnitřní kontrole musí obsahovat alespoň následující údaje:

- období výkonu vnitřní kontroly;
- jméno a pozici osoby provádějící vnitřní kontrolu;
- popis provedených interních kontrolních opatření;
- výsledky vnitřní kontroly;
- obecné závěry z provedené vnitřní kontroly;
- zjištěné nedostatky, které byly odstraněny v období výkonu vnitřní kontroly;
- zjištěné nedostatky, které nebyly ke konci období výkonu vnitřní kontroly odstraněny;
- opatření, která je třeba provést k odstranění zjištěných nedostatků.

Správní rada přezkoumá předloženou zprávu o vnitřní kontrole a přijme k ní usnesení. O podstatě tohoto usnesení je informován pracovník vnitřní kontroly ve formátu, který lze reprodukovat písemně. Z tohoto důvodu je správní rada povinna:

- analyzovat výsledky provedené vnitřní kontroly;
- provést opatření k odstranění zjištěných nedostatků.

Společnost musí nejméně jednou ročně a v následujících případech přezkoumat a v případě potřeby aktualizovat postup vnitřní kontroly:

- poté, co Evropská komise zveřejnila výsledky celoevropského hodnocení rizik praní peněz a financování terorismu (k dispozici na internetových stránkách Evropské komise http://ec.europa.eu);
- po zveřejnění výsledků národního hodnocení rizik praní peněz a financování terorismu;
- po obdržení pokynu od FAÚ k posílení příslušných postupů vnitřní kontroly;
- v případě významných událostí nebo změn v řízení a činnosti společnosti.

Hodnocení rizik a ochota riskovat

Cílem zavedení vnitřních kontrolních opatření pro dodržování stanovené politiky hodnocení rizik (včetně stanoveného rizikového apetitu) je prověření následujících okolností:

- Společnost zavádí a používá při poskytování služeb zákazníkům přístup založený na riziku (např. opatření CDD prováděná v souladu s úrovní rizika);
- Společnost určila faktory, které ovlivňují vznik rizik praní peněz a financování terorismu, a určila, které faktory jsou relevantní;

- Společnost stanovila a posoudila ML/TF všech služeb, které poskytuje;
- Společnost sestavuje rizikový profil zákazníka před provedením transakce nebo vytvořením obchodního vztahu;
- Společnost pravidelně aktualizuje rizikový profil zákazníka;
- Společnost dodržuje stanovený rizikový apetit;
- Společnost vede záznamy o všech incidentech v souladu se zavedenou politikou hodnocení rizik;
- politika hodnocení rizik byla v průběhu loňského roku přezkoumána a neexistují žádné informace o tom, že by MLRO vyžadovalo dřívější přezkoumání.

Zavedení opatření hloubkové kontroly zákazníka

Cílem zavedení vnitřních kontrolních opatření pro dodržování opatření CDD Společností je prověření následujících okolností:

- Společnost uplatňuje opatření CDD předepsaná Pokyny u všech příslušných zákazníků;
- společnost shromažďuje řádné dokumenty a informace při uplatňování opatření CDD;
- společnost řádně ověřuje údaje a dokumenty shromážděné při uplatňování opatření CDD;
- společnost uplatňuje příslušnou úroveň opatření CDD (např. opatření EDD atd.);
- společnost uplatňuje vhodná opatření EDD u konkrétních zákazníků (např. PEP, vysoce riziková země atd.);
- společnost provádí identifikaci zákazníků v souladu se stanoveným postupem;
- společnost řádně identifikuje zástupce (zástupce) zákazníků;
- společnost řádně identifikuje skutečné vlastníky zákazníků;
- společnost řádně identifikuje status PEP zákazníků;
- společnost řádně identifikuje účel a povahu obchodního vztahu nebo transakce;
- společnost řádně sleduje obchodní vztahy se zákazníky.

Provádění sankcí

Cílem zavedení vnitřních kontrolních opatření pro dodržování sankcí ze strany Společnosti je prověření následujících okolností:

- Společnost uplatňuje postup pro identifikaci subjektu Sankcí nebo transakce porušující Sankce;
- společnost provede opatření, pokud identifikuje subjekt sankcí nebo transakci porušující sankce.

Povinnost odmítnout transakci nebo obchodní vztah a jejich ukončení

Cílem zavedení vnitřních kontrolních opatření pro dodržování povinnosti Společnosti odmítnout transakci nebo obchodní vztah a jejich ukončení je prověření následujících okolností:

- Společnost odmítne transakci nebo obchodní vztah, pokud je to v souladu s Pokyny povinné;
- společnost odmítne nebo ukončí transakci nebo obchodní vztah, pokud je to v souladu s Pokyny povinné.

Oznamovací povinnost

Cílem zavedení vnitřních kontrolních opatření pro splnění oznamovací povinnosti Společnosti je prověření následujících okolností:

- společnost zasílá FAU zprávy a informace, pokud to vyžadují pokyny (včetně příslušných pokynů FAU);
- hlášení zaslaná FAU jsou vyplněna v souladu s pokyny FAU.

Povinnost školení

Cílem zavedení interních kontrolních opatření pro plnění povinnosti školení v oblasti AML/CTF je prověření následujících okolností:

- všichni zaměstnanci (včetně MLRO a generálního ředitele) absolvovali příslušné školení;
- každý zaměstnanec (včetně MLRO a generálního ředitele) absolvoval školení za posledních 360 dní.

Povinnost shromažďování a uchovávání údajů

Cílem zavedení interních kontrolních opatření pro dodržování povinnosti shromažďování a uchovávání údajů je prověření následujících okolností:

- všechny údaje, které mají být uloženy v souladu s Pokyny (dále v této kapitole jen "uložené údaje"), byly řádně uloženy v chronologickém pořadí a ve formátu, který umožňuje jejich analýzu a srozumitelné propojení uložených údajů s jinými relevantními údaji;
- přístup k uloženým údajům mají pouze zaměstnanci (včetně MLRO a generálního ředitele) nebo oprávněné třetí strany;
- všechny příslušné lodní deníky jsou vedeny v souladu s pokyny;
- uložená data v elektronickém formátu mají zálohu;
- uložená data v jiných formátech (např. na papíře) mají zálohu v elektronické podobě;
- jsou uložené údaje neodvolatelně vymazány v souladu s Pokyny.

PŘÍLOHY

Název přílohy	Popis dokumentu
1. Politika hodnocení rizik	Stanovuje zásady pro řízení rizik ve společnosti (včetně hodnocení rizik a rizikových faktorů), pokud jde o rizika praní špinavých peněz a financování terorismu.

	Obsahuje vlastní přílohy.
2. Požadavky na monitorování obchodních vztahů	Stanoví opatření, která se použijí v průběhu sledování obchodního vztahu (opatření ODD).
3. Protokol transakcí	Stanovuje soubor údajů, které se mají ukládat o každé transakci se zákazníkem.
4. Protokol školení	Návrh dokumentu podepíše zaměstnanec (zaměstnanci) po provedení příslušného školení.
5. Zpráva MLRO představeni	Formulář zprávy, který MLRO čtvrtletně poskytuje generálnímu řediteli.
6. FAU & další pokyny	Obsahuje pokyny vydané FAÚ a dalšími orgány (FATF).
7. Seznam zdrojů	Pro uplatnění opatření CDD/EDD lze použít neúplný seznam zdrojů.
8. Ukazatele podezřelých transakcí	Obsahuje neúplný seznam indikátorů podezřelých transakcí.

TABULKA ŘÍZENÍ VERZÍ

Verze	Datum schválení	Změny Popis
1.0	10.12.2024	První vydání