

EBA/GL/2021/02

---

1. března 2021

---

## Obecné pokyny

---

podle článku 17 a čl. 18 odst. 4 směrnice (EU) 2015/849 o hloubkové kontrole klienta a faktorech, které by úvěrové a finanční instituce měly vzít v úvahu při posuzování rizika praní peněz a financování terorismu souvisejícího s jednotlivými obchodními vztahy a příležitostnými transakcemi („obecné pokyny k rizikovým faktorům praní peněz a financování terorismu“), kterými se zrušují a nahrazují obecné pokyny JC/2017/37

# 1. Povinnost dodržování pokynů a oznamovací povinnost

---

## Status těchto obecných pokynů

1. Tento dokument obsahuje obecné pokyny vydané podle článku 16 nařízení (EU) č. 1093/2010<sup>1</sup>. V souladu s čl. 16 odst. 3 nařízení Evropského parlamentu a Rady (EU) č. 1093/2010 příslušné orgány a finanční instituce vynaloží veškeré úsilí, aby se těmito obecnými pokyny řídily.
2. Obecné pokyny formulují názor orgánu EBA na náležité postupy dohledu v rámci Evropského systému dohledu nad finančním trhem nebo na to, jak by unijní právní předpisy měly být uplatňovány v konkrétní oblasti. Příslušné orgány ve smyslu čl. 4 odst. 2 nařízení (EU) č. 1093/2010, na které se tyto obecné pokyny vztahují, by s nimi měly být v souladu a začlenit je do svých postupů (např. pozměněním svého právního rámce nebo dohledových postupů), včetně případů, kdy jsou obecné pokyny zaměřeny v první řadě na instituce.

## Oznamovací povinnost

3. V souladu s čl. 16 odst. 3 nařízení (EU) č. 1093/2010 musí příslušné orgány do (07.09.2021) orgánu EBA oznámit, zda se těmito obecnými pokyny řídí nebo hodlají řídit, a v opačném případě uvést do tohoto data důvody, proč se jimi neřídí či nehodlají řídit. Neposkytnou-li příslušné orgány oznámení v této lhůtě, bude mít orgán EBA za to, že se těmito obecnými pokyny neřídí nebo nehodlají řídit. Oznámení by měla být zasílána na formuláři, který je k dispozici na internetových stránkách orgánu EBA, na adresu [compliance@eba.europa.eu](mailto:compliance@eba.europa.eu) s označením „EBA/GL/2021/02“. Oznámení by měly předkládat osoby řádně oprávněné jménem svého příslušného orgánu oznamovat, zda se těmito doporučeními řídí či nikoli. Jakoukoliv změnu stavu dodržování pokynů je rovněž nutno oznámit orgánu EBA.
4. Oznámení budou zveřejněna na webových stránkách orgánu EBA v souladu s čl. 16 odst. 3 uvedeného nařízení.

---

<sup>1</sup> Nařízení Evropského parlamentu a Rady (EU) 1093/2010 ze dne 24. listopadu 2010 o zřízení Evropského orgánu dohledu (Evropského orgánu pro bankovníctví), o změně rozhodnutí č. 716/2009/ES a o zrušení rozhodnutí Komise 2009/78/ES (Úř. věst. L 331, 15.12.2010, s. 12).

## 2. Předmět, oblast působnosti a definice

---

### Předmět

5. Tyto obecné pokyny stanovují faktory, které by podniky měly zohlednit při posuzování rizika praní peněz a financování terorismu souvisejícího s jejich obchodní činností, s obchodním vztahem nebo příležitostnou transakcí a jakoukoli fyzickou nebo právnickou osobou (dále jen „klient“). Rovněž stanovují, jak by podniky měly upravit rozsah opatření hloubkové kontroly klienta tak, aby odpovídaly míře rizika praní peněz a financování terorismu, které identifikovaly.
6. Tyto obecné pokyny se zaměřují zejména na posuzování rizik jednotlivých obchodních vztahů a příležitostných transakcí, nicméně podniky by měly tyto obecné pokyny obdobně použít v souladu s článkem 8 směrnice (EU) 2015/849 i při posuzování rizika praní peněz a financování terorismu v rámci celé své obchodní činnosti.
7. Výčet faktorů a opatření, které tyto obecné pokyny popisují, není úplný a podniky by měly případně zohlednit i další faktory a opatření.

### Oblast působnosti

8. Tyto obecné pokyny jsou určeny úvěrovým a finančním institucím uvedeným v čl. 3 odst. 1 a čl. 3 odst. 2 směrnice (EU) 2015/849 a příslušným orgánům odpovědným za dohled nad dodržováním povinností v oblasti boje proti praní peněz a financování terorismu těmito podniky.
9. Příslušné orgány by měly tyto obecné pokyny uplatňovat při posuzování toho, zda jsou strategie a postupy těchto podniků v oblasti posuzování rizik a boje proti praní peněz a financování terorismu adekvátní.
10. Příslušné orgány by měly rovněž zvážit, do jaké míry mohou tyto obecné pokyny poskytnout informace o posuzování rizika praní peněz a financování terorismu související s jejich odvětvím v rámci přístupu k dohledu založeném na posouzení míry rizika. Evropské orgány dohledu vydaly v souladu s čl. 48 odst. 10 směrnice (EU) 2015/849 obecné pokyny k dohledu založeném na posouzení rizik.
11. Dodržování evropského režimu finančních sankcí do působnosti těchto obecných pokynů nespadá.

### Definice

---

12. Pro účely těchto obecných pokynů se použijí tyto definice:

- a) „Příslušnými orgány“ se rozumí orgány příslušné pro zajištění dodržování požadavků směrnice (EU) 2015/849 podniky způsobem, jakým byla provedena do vnitrostátního práva.<sup>2</sup>
- b) „Institucemi“ se rozumí úvěrové instituce a finanční instituce specifikované v čl. 3 odst. 1 a 2 směrnice (EU) 2015/849.
- c) „Inherentním rizikem“ se rozumí míra rizika, které existuje před jeho zmírněním.
- d) „Jurisdikcemi spojenými s vyšším rizikem praní peněz a financování terorismu“ se rozumí země, které na základě posouzení rizikových faktorů stanovených v hlavě I těchto obecných pokynů vykazují vyšší riziko praní peněz a financování terorismu. Uvedené nezahrnuje „vysoce rizikové třetí země“, jejichž režimy pro boj proti praní peněz a financování terorismu vykazují strategické nedostatky, které představují významnou hrozbu pro finanční systém Unie (článek 9 směrnice (EU) 2015/849).
- e) „Vztahy nebo transakce bez osobní přítomnosti“ se rozumí jakákoliv transakce nebo vztah, kde klient není fyzicky přítomen, tedy není fyzicky přítomen na stejném fyzickém místě jako podnik nebo osoba jednající za podnik. Uvedené zahrnuje situace, kdy je totožnost klienta ověřena přes video spojení nebo podobný technický prostředek.
- f) „Příležitostnou transakcí“ se rozumí transakce, která není prováděna v rámci obchodního vztahu podle čl. 3 odst. 13 směrnice (EU) 2015/849.
- g) „Sdruženým účtem“ (tzv. „pooled account“) se rozumí bankovní účet otevřený klientem, například právníkem nebo notářem, za účelem úschovy peněz od svých klientů. Klienti, jejichž peníze budou na účtu sdruženy s dalšími prostředky, však nebudou moci přímo dát bance pokyn k uskutečnění transakce.
- h) „Zbytkovým rizikem“ se rozumí úroveň rizika, která přetrvává po zmírnění rizika.
- i) „Rizikem“ se rozumí pravděpodobnost, že dojde k praní peněz a financování terorismu, a dopad, jaký to bude mít.
- j) „Ochotou podstupovat riziko“ se rozumí úroveň rizika, kterou je instituce připravena akceptovat.
- k) „Rizikovými faktory“ se rozumí proměnné, které buď samostatně, nebo ve spojení s jinými faktory mohou zvýšit nebo snížit riziko praní peněz a financování terorismu představované jednotlivým obchodním vztahem nebo příležitostnou transakcí.
- l) „Přístupem založeným na posouzení míry rizika“ se rozumí přístup, kdy příslušné orgány a instituce identifikují, posuzují a chápou riziko praní peněz a financování terorismu, kterému jsou instituce vystaveny, a přijímají opatření v rámci boje proti

<sup>2</sup> Čl. 4 odst. 2 bod ii) nařízení (EU) 1093/2010, čl. 4 odst. 2 bod ii) nařízení (EU) 1094/2010 a čl. 4 odst. 3 bod ii) nařízení (EU) 1093/2010.

praní peněz a financování terorismu úměrná těmto rizikům.

- m) „Bankou bez fyzické přítomnosti“ se rozumí instituce podle čl. 3 odst. 17 směrnice (EU) 2015/849.
- n) „Zdrojem finančních prostředků“ se rozumí původ finančních prostředků použitých v obchodním vztahu nebo příležitostné transakci. To znamená jak činnost, ze které finanční prostředky použité v obchodním vztahu pocházejí, například z platu klienta, tak i způsob, jakým byly klientovy finanční prostředky převedeny.
- o) „Zdrojem majetku“ se rozumí původ celkového majetku klienta, například dědictví nebo úspory.

## 3. Provádění

---

### Datum použití

1. Tyto obecné pokyny se použijí tři měsíce po zveřejnění ve všech úředních jazycích EU.

## Hlava I: Obecné pokyny

---

Tyto obecné pokyny se skládají ze dvou částí. Hlava I je obecná a vztahuje se na všechny instituce. Hlava II je určena pro konkrétní odvětví. Hlava II je samostatně neúplná a je třeba ji číst společně s hlavou I.

### Obecný pokyn č. 1: Posouzení rizik: hlavní zásady pro všechny podniky

1.1. Podniky by měly důkladně znát rizika praní peněz a financování terorismu, jimž jsou vystaveny.

#### Obecné úvahy

1.2. Při plnění svých povinností stanovených ve směrnici (EU) 2015/849 by instituce měly posoudit:

- a) riziko praní peněz a financování terorismu, jemuž jsou vystaveny v důsledku povahy a složitosti své obchodní činnosti (posouzení rizik v rámci celého podniku); a
- b) riziko praní peněz a financování terorismu, jemuž jsou vystaveny v důsledku uzavření obchodního vztahu nebo provedení příležitostné transakce (individuální posouzení rizik).

Každé posouzení rizik by mělo zahrnovat dva odlišné, ale související kroky:

- a) identifikace rizikových faktorů praní peněz a financování terorismu; a
- b) posouzení rizika praní peněz a financování terorismu.

1.3. Při posuzování celkové úrovně zbytkového rizika praní peněz a financování terorismu souvisejícího s jejich obchodní činností a jednotlivými obchodními vztahy nebo příležitostnými transakcemi by podniky měly zohlednit úroveň inherentního rizika, kvalitu kontrol a další faktory snižující riziko.

1.4. Jak se uvádí v čl. 8 odst. 2 směrnice (EU) 2015/849, podniky by měly vést záznamy a zdokumentovat posouzení rizik v rámci celého podniku i případné změny provedené v tomto posouzení rizik způsobem, který podniku a příslušným orgánům umožňuje pochopit, jak bylo posouzení rizik provedeno a proč bylo provedeno určitým způsobem.

- 1.5. Podniky, které jsou úvěrovými institucemi a investičními podniky, by v této souvislosti měly přihlížet také k obecným pokynům EBA k vnitřnímu systému správy a řízení.<sup>3</sup>

## Aktualizace posouzení rizik

- 1.6. Podniky by měly zavést systémy a kontroly umožňující provádět přezkum jejich posouzení rizika praní peněz a financování terorismu souvisejícího s jejich obchodní činností a s jednotlivými obchodními vztahy, aby zajistily, že posouzení rizika praní peněz a financování terorismu je aktuální a relevantní.
- 1.7. Systémy a kontroly, které by instituce měly zavést k zajištění, že jejich individuální posouzení rizik a posouzení rizik v rámci celé činnosti instituce zůstanou nadále aktuální, by měly zahrnovat:
- a) Stanovení data v každém kalendářním roce, ke kterému bude provedena další aktualizace posouzení rizik v rámci celé činnosti instituce, a stanovení data s ohledem na míru rizika pro individuální posouzení rizik, a to tak aby se zajistilo zahrnutí nových nebo vznikajících rizik.
  - b) Pokud před takto stanoveným datem instituce zjistí, že se objevilo nové riziko praní peněz a financování terorismu nebo že došlo ke zvýšení rizika stávajícího, měla by tato zjištění co nejdříve zohlednit ve svém individuální posouzení rizik a posouzení rizik v rámci celé činnosti instituce; a
  - c) Podávání zpráv o všech problémech, které by mohly mít na posouzení rizik vliv, v průběhu rozhodného období, například interní oznámení podezřelých transakcí, nedodržování předpisů a informace od vedoucích pracovníků.
- 1.8. V rámci toho by podniky měly zajistit, aby měly zavedeny systémy a kontroly k identifikaci nově vznikajících rizik praní peněz a financování terorismu a aby mohly tato rizika posoudit a v případě potřeby je včas zahrnout do svého individuálního posouzení rizik a posouzení rizik v rámci celého podniku.
- 1.9. Systémy a kontroly, které by podniky měly zavést k identifikaci nově vznikajících rizik, by měly zahrnovat:
- a) Procesy, které zajišťují, aby byly interní informace, například informace získané v rámci průběžného sledování obchodních vztahů podniku, pravidelně posuzovány s cílem identifikovat trendy a vznikající problémy, a to jak v souvislosti s jednotlivými obchodními vztahy, tak s obchodní činností podniku.

<sup>3</sup> Obecné pokyny k vnitřnímu systému správy a řízení, EBA/GL/2017/11.



- b) Procesy, které zajišťují, aby podnik pravidelně posuzoval relevantní informační zdroje, včetně zdrojů uvedených v obecných pokynech č. 1.28 až 1.30, a to zejména:
- i. v souvislosti s individuálním posouzením rizik
    - a. varování týkající se teroristických útoků a režimy finančních sankcí nebo jejich změny, jakmile jsou vydány nebo vyhlášeny, a aby zajistil, že se na jejich základě bude jednat tak, jak je nezbytné; a
    - b. zprávy z médií, které jsou relevantní pro odvětví nebo jurisdikce, v nichž podnik vyvíjí činnost.
  - ii. v souvislosti s posouzením rizik v rámci celého podniku
    - a. varování a zprávy orgánů činných v trestním řízení;
    - b. tematické přezkumy a podobné publikace vydané příslušnými orgány; a
    - c. Procesy směřující k získání a přezkoumání informací o rizicích, zejména pak o rizicích souvisejících s novými kategoriemi klientů, zeměmi nebo zeměpisnými oblastmi, novými produkty, novými službami, novými distribučními kanály a novými systémy a kontrolami dodržování předpisů.
  - c) Jednání s dalšími zástupci odvětví a příslušnými orgány (např. kulaté stoly, konference a školení) a procesy umožňující sdělování zjištění příslušným zaměstnancům.

1.10. Podniky by při zohlednění míry rizika měly určit, jak často budou prováděna celková přezkoumání metodiky používané k posouzení rizik v rámci celého podniku a k individuálnímu posouzení rizik.

## Posouzení rizik v rámci celého podniku

1.11. Posouzení rizik v rámci celého podniku by mělo podnikům napomoci porozumět, kde jsou riziku praní peněz a financování terorismu vystaveny a na které oblasti své obchodní činnosti by se měly v boji proti praní peněz a financování terorismu zaměřit.

1.12. Za tímto účelem by podniky měly zvolit holistický přístup k rizikům praní peněz a financování terorismu, jimž jsou vystaveny, a identifikovat a posoudit riziko praní peněz a financování terorismu související s produkty a službami, které nabízejí, jurisdikcemi, v nichž působí, klienty, které získávají, a transakčními nebo distribučními kanály, které využívají při nabízení služeb svým klientům.

1.13. Podniky by měly:

- a) identifikovat rizikové faktory na základě informací z různých interních a externích zdrojů, včetně zdrojů uvedených v obecných pokynech č. 1.30 až 1.31;
  - b) vzít v úvahu relevantní rizikové faktory uvedené v hlavách I a II těchto obecných pokynů; a
  - c) zohlednit širší, kontextové faktory jako odvětvové riziko a zeměpisné riziko, které by mohly ovlivnit jejich rizikové profily, pokud jde o riziko praní peněz a financování terorismu.
- 1.14. Podniky by měly zajistit, že jejich posouzení rizik v rámci celého podniku je přizpůsobeno na míru jejich obchodnímu profilu a zohledňuje faktory a rizika specifická pro obchodní činnost podniku, ať už podnik vypracuje vlastní posouzení rizik v rámci celého podniku, nebo vypracováním posouzení rizik v rámci celého podniku pověří externí stranu. Podobně by podnik v případě, že je součástí skupiny, která vypracovává posouzení rizik pro celou skupinu, měl zvážit, zda je posouzení rizik pro celou skupinu dostatečně podrobné a konkrétní a odráží obchodní činnost podniku a rizika, kterým je vystaven v důsledku vazeb skupiny na určité země a zeměpisné oblasti, a podle potřeby posouzení rizik pro celou skupinu případně doplnit. Má-li skupina sídlo v zemi spojené s vysokou mírou korupce, podnik by měl tuto skutečnost zohlednit při posuzování rizik i v případě, že posouzení rizik pro celou skupinu o této věci mlčí.
- 1.15. Není pravděpodobné, že obecné posouzení rizika praní peněz a financování terorismu, které není přizpůsobeno konkrétním potřebám a obchodnímu modelu podniku (dále jen „standardní posouzení rizika praní peněz a financování terorismu“), nebo bezvýhradně použité posouzení rizika pro celou skupinu splní požadavky stanovené v článku 8 směrnice (EU) 2015/849.

### Proporcionalita

- 1.16. Jak se uvádí v článku 8 směrnice (EU) 2015/849, kroky, které podnik učiní za účelem identifikace a posouzení rizika praní peněz a financování terorismu ve své obchodní činnosti, musí odpovídat povaze a velikosti příslušného podniku. U malých podniků, které nenabízejí ucelené produkty nebo služby a které mají omezenou nebo pouze vnitrostátní působnost, není zapotřebí složitějšího nebo propracovanějšího posouzení rizik.

### Provádění

- 1.17. Podniky by měly
- a) posouzení rizik v rámci celého podniku zpřístupnit příslušným orgánům;

- b) přijmout opatření zajišťující, že zaměstnanci chápou posouzení rizik v rámci celého podniku a to, jak ovlivňuje jejich každodenní pracovní činnost, v souladu s čl. 46 odst. 1 směrnice (EU) 2015/849; a
- c) informovat vrcholné vedení o výsledcích posouzení rizik v rámci celého podniku a zajistit, že vrcholné vedení obdrží dostatečné informace pro pochopení rizika, jemuž je jejich obchodní činnost vystavena, a pro zaujetí stanoviska k tomuto riziku.

## **Propojení posouzení rizik v rámci celého podniku a individuálního posouzení rizik**

- 1.18. Podniky by měly zjištění ze svých posouzení rizik v rámci celého podniku využít při přípravě strategií, kontrol a postupů v oblasti boje proti praní peněz a financování terorismu v souladu s čl. 8 odst. 3 a 4 směrnice (EU) 2015/849. Podniky by měly zajistit, že jejich posouzení rizik v rámci celého podniku rovněž odráží opatření přijatá za účelem posouzení rizika praní peněz a financování terorismu souvisejícího s jednotlivými obchodními vztahy a jejich ochotu podstupovat riziko praní peněz a financování terorismu.
- 1.19. Za účelem dodržení obecného pokynu č. 1.18 a s ohledem na obecné pokyny č. 1.21 a 1.22 by podniky měly posouzení rizik v rámci celého podniku používat k určení úrovně prvotní hloubkové kontroly klienta, kterou uplatní v určitých situacích a u určitých druhů klientů, produktů, služeb a distribučních kanálů.
- 1.20. Individuální posouzení rizik by mělo být podkladem pro posouzení rizik v rámci celého podniku, avšak nemělo by jej nahrazovat.

## **Individuální posouzení rizik**

- 1.21. Podniky by měly zjistit, kterým rizikům praní peněz a financování terorismu jsou nebo by mohly být v důsledku uzavření či udržování obchodního vztahu nebo provedení příležitostné transakce vystaveny.
- 1.22. Při zjišťování rizik praní peněz a financování terorismu souvisejících s obchodním vztahem nebo příležitostnou transakcí by podniky měly zohlednit příslušné rizikové faktory, včetně toho, kdo je jejich klientem, země nebo zeměpisné oblasti, v nichž působí, konkrétní produkty, služby a transakce, které klient požaduje, a cesty, které podnik využívá k poskytování těchto produktů, služeb a transakcí.

## **Prvotní hloubková kontrola klienta**

- 1.23. Před uzavřením obchodního vztahu nebo provedením příležitostné transakce by podniky měly uplatnit prvotní hloubkovou kontrolu klienta v souladu s čl. 13 odst. 1 písm. a), b) a c) a čl. 14 odst. 4 směrnice (EU) 2015/849.

- 1.24. Prvotní hloubková kontrola klienta by měla přinejmenším zahrnovat opatření při zohlednění míry rizika s cílem:
- a) zjistit totožnost klienta a případně skutečného majitele klienta;
  - b) ověřit totožnost klienta na základě spolehlivých a nezávislých zdrojů a případně ověřit totožnost skutečného majitele, aby se podnik ujistil, zda skutečného majitele zná; a
  - c) zjistit účel a zamýšlenou povahu obchodního vztahu.
- 1.25. Podniky by měly upravit rozsah prvotních opatření hloubkové kontroly klienta při zohlednění míry rizika a s ohledem na zjištění ze svého posouzení rizik v rámci celého podniku. Pokud je riziko související s obchodním vztahem pravděpodobně nízké a v rozsahu povoleném vnitrostátními právními předpisy, mohou podniky uplatnit zjednodušená opatření hloubkové kontroly klienta. Pokud je riziko související s obchodním vztahem pravděpodobně vysoké, musí podniky uplatnit zesílená opatření hloubkové kontroly klienta.

### **Dosažení holistického přístupu**

- 1.26. Podniky by měly shromáždit dostatek informací, aby dospěly k závěru, že byly identifikovány všechny relevantní rizikové faktory na začátku obchodního vztahu, v průběhu obchodního vztahu nebo před provedením příležitostné transakce. V případě nutnosti by podniky měly uplatnit další opatření hloubkové kontroly klienta a posoudit tyto rizikové faktory tak, aby získaly ucelený pohled na riziko související s určitým obchodním vztahem nebo příležitostnou transakcí.
- 1.27. Nepředpokládá se, že by podniky pro příležitostné transakce sestavovaly úplný rizikový profil klienta.

### **Průběžná hloubková kontrola klienta**

- 1.28. Podniky by měly informace získané během obchodního vztahu použít pro účely individuálního posouzení rizik (viz „Sledování“ v obecném pokynu 4).

### **Zdroje informací**

- 1.29. Za účelem identifikace rizika praní peněz a financování terorismu by podniky měly použít informace z různých zdrojů, které jsou přístupné samostatně, nebo prostřednictvím komerčně dostupných nástrojů nebo databází, které sdružují informace z několika zdrojů.
- 1.30. Podniky by vždy měly zohlednit tyto zdroje informací:
- a) nadnárodní posuzování rizik prováděné Evropskou komisí;

- b) seznam Evropské komise obsahující vysoce rizikové třetí země;
- c) informace od vlád, například vnitrostátní posouzení rizik na úrovni vlád, politická prohlášení a varování a informativní memoranda k příslušným právním předpisům;
- d) informace od regulačních orgánů, jako jsou obecné pokyny a odůvodnění vymezená v pokutách ze strany regulačních orgánů;
- e) informace od finančních zpravodajských jednotek (FIU) a donucovacích orgánů, jako jsou zprávy o hrozbách, výstrahy a typologie; a
- f) informace získané v rámci prvotní hloubkové kontroly klienta a průběžného sledování.

1.31. K dalším zdrojům informací, které by podniky měly zohlednit, patří mimo jiné:

- a) vlastní znalosti a odborné znalosti podniků;
- b) informace od odvětvových subjektů, například typologie a informace o nově vznikajících rizicích;
- c) informace od občanské společnosti, například indexy vnímání korupce a zprávy o zemích;
- d) informace od mezinárodních normalizačních orgánů, jako jsou vzájemné hodnotící zprávy nebo právně nezávazné černé listiny, včetně těch uvedených v obecných pokynech 2.11 až 2.15;
- e) informace z věrohodných a spolehlivých volně přístupných zdrojů, jako jsou zprávy v důvěryhodných novinách;
- f) informace od věrohodných a spolehlivých komerčních organizací, například zprávy o rizicích a zpravodajská hlášení; a
- g) informace od statistických organizací a akademické obce.

1.32. Podniky by měly stanovit druh a počet zdrojů při zohlednění míry rizika a s ohledem na povahu a složitost své obchodní činnosti. Podniky by se při identifikaci rizik praní peněz a financování terorismu neměly obvykle spoléhat pouze na jeden zdroj.

## Obecný pokyn č. 2: Identifikace rizikových faktorů praní peněz a financování terorismu

- 2.1. Podniky by měly identifikovat rizikové faktory související s klienty, zeměmi nebo zeměpisnými oblastmi, produkty, službami a distribučními kanály způsobem stanoveným v těchto obecných pokynech a rovněž s přihlédnutím k neúplnému výčtu faktorů uvedenému v přílohách II a III směrnice (EU) 2015/849.
- 2.2. Podniky by měly vzít na vědomí, že výčet následujících rizikových faktorů není úplný a ani se nepředpokládá, že by podniky ve všech případech zohledňovaly všechny rizikové faktory.

## Rizikové faktory klienta

- 2.3. Při identifikaci rizik týkajících se klientů, včetně skutečných majitelů klientů, by podniky měly zohlednit riziko související s:
  - a) obchodní nebo profesní činností klienta a jeho skutečného majitele;
  - b) pověstí klienta a jeho skutečného majitele; a
  - c) povahou a chováním klienta a jeho skutečného majitele, včetně toho, zda by to mohlo ukazovat na zvýšené riziko financování terorismu.
- 2.4. Rizikové faktory, které mohou být pro zjištění rizika souvisejícího s podnikatelskou nebo profesní činností klienta nebo jeho skutečného majitele relevantní, zahrnují:
  - a) Má klient nebo skutečný majitel vazby na odvětví, která jsou běžně spojována s vyšším rizikem korupce, například stavebnictví, farmacie a zdravotnictví, obchod se zbraněmi a obrana, těžební průmysl nebo veřejné zakázky?
  - b) Má klient nebo skutečný majitel vazby na odvětví, která jsou spojena s vyšším rizikem praní peněz a financování terorismu, například některé obchodní činnosti se zaměřením na peněžní služby, kasina nebo obchodníky s drahými kovy?
  - c) Má klient nebo skutečný majitel vazby na odvětví, která operují s vysokými částkami v hotovosti?
  - d) Pokud je klient právnickou osobou, svěřenským fondem nebo jiným druhem právního uspořádání, jaký je účel jeho založení? Jaká je například povaha jeho podnikání?
  - e) Má klient nějaké politické vazby, například je osobou politicky exponovanou nebo je jeho skutečný majitel osobou politicky exponovanou? Má klient nebo skutečný majitel nějaké jiné významné vazby na politicky exponované osoby, jsou například někteří z ředitelů klienta politicky exponovanými osobami, a pokud ano, ovládají tyto politicky exponované osoby klienta nebo skutečného majitele významným způsobem? Pokud je klient nebo jeho skutečný majitel

politicky exponovanou osobou, musí podniky vždy uplatnit zesílená opatření hloubkové kontroly klienta v souladu s článkem 20 směrnice (EU) 2015/849.

- f) Má klient nebo skutečný majitel jinou významnou pozici nebo veřejné postavení na vysoké úrovni, které by mu mohlo umožnit zneužít tuto pozici k osobnímu prospěchu? Je například vyšším místním nebo regionálním veřejným činitelem se schopností ovlivňovat zadávání veřejných zakázek, členem významných sportovních orgánů s rozhodovacími pravomocemi nebo jednotlivcem, o němž je známo, že ovlivňuje vládu či jinou vysoce postavenou osobou s rozhodovacími pravomocemi?
- g) Je klient právníkou osobou podléhající vynutitelným požadavkům na zveřejnění informací, které zajišťují, aby byly spolehlivé informace o skutečném majiteli klienta veřejně dostupné, například akciovou společností kótovanou na burzách, u které je zveřejnění těchto informací podmínkou pro kótování?
- h) Je klient úvěrovou nebo finanční institucí jednajícím na svůj účet v jurisdikci s účinným režimem pro boj proti praní peněz a financování terorismu a podléhá dohledu nad dodržováním místních povinností v oblasti boje proti praní peněz a financování terorismu? Existují důkazy o tom, že klientovi byla v posledních letech v rámci dohledu udělena sankce nebo že došlo k jejímu vymáhání za nesplnění povinností v oblasti boje proti praní peněz a financování terorismu nebo požadavků na chování v širším měřítku?
- i) Je klient orgánem veřejné správy nebo státním podnikem z jurisdikce s nízkou úrovní korupce?
- j) Je pozadí klienta nebo skutečného majitele v souladu s tím, co podnik zná o jeho bývalé, současné nebo plánované obchodní činnosti, o obratu jeho podniku, o zdroji finančních prostředků a o zdroji majetku klienta nebo skutečného majitele?

2.5. Při zjišťování rizik souvisejících s pověstí klienta nebo skutečného majitele mohou být relevantní následující rizikové faktory:

- a) Existují negativní zprávy z médií nebo jiných relevantních zdrojů informací o klientovi, například existují proti klientovi nebo skutečnému majiteli nějaká obvinění ze spáchání trestné činnosti nebo terorismu? Pokud ano, jsou tyto zprávy věrohodné a spolehlivé? Podniky by měly mimo jiné určit věrohodnost obvinění s ohledem na kvalitu a nezávislost zdroje údajů a trvalost zpráv o těchto obviněních. Podniky by měly vzít v úvahu, že absence odsouzení za spáchané trestné činy nemusí nezbytně dostatečně vyloučit toho, že obvinění ze spáchání trestné činnosti jsou pravdivá.

- b) Byl klientovi, skutečnému majiteli nebo jiné veřejně známé osobě, která je s ním úzce spojena, zmrazen majetek kvůli správnímu nebo trestnímu řízení nebo obvinění z terorismu nebo financování terorismu? Má podnik důvodné podezření, že klientovi nebo skutečnému majiteli nebo jiné veřejně známé osobě, která je s ním úzce spojena, byl v minulosti majetek zmrazen?
- c) Má podnik informace o tom, že byla na klienta nebo skutečného majitele v minulosti podána oznámení o podezřelých transakcích?
- d) Má podnik nějaké interní informace o bezúhonnosti klienta nebo skutečného majitele, získané například z dlouhodobého obchodního vztahu?

2.6. Při identifikaci rizika souvisejícího s povahou a chováním klienta nebo jeho skutečného majitele mohou být relevantní následující rizikové faktory. Podniky by měly vzít v úvahu, že ne všechny tyto rizikové faktory budou od počátku patrné; mohou se projevit až po uzavření obchodního vztahu:

- a) Má klient oprávněné důvody pro neposkytnutí důkazu o své totožnosti, například kvůli tomu, že je žadatelem o azyl?
- b) Má podnik pochybnosti o pravdivosti nebo přesnosti totožnosti klienta nebo skutečného majitele?
- c) Existují náznaky, že by se klient mohl snažit vyhnout uzavření obchodního vztahu? Snaží se například klient provést jednu transakci nebo několik jednorázových transakcí, u kterých by uzavření obchodního vztahu mohlo mít větší ekonomické opodstatnění?
- d) Je vlastnická a řídicí struktura klienta transparentní a smysluplná? Je-li vlastnická a řídicí struktura klienta složitá nebo netransparentní, existují k tomu zřejmé obchodní nebo právní důvody?
- e) Vydává klient akcie na doručitele nebo má pověřené akcionáře nebo společníky?
- f) Je klient právníkou osobou nebo právním uspořádáním, které by mohlo být použito jako nástroj držby aktiv?
- g) Existuje nějaký podstatný důvod pro změny ve vlastnické a řídicí struktuře klienta?
- h) Požaduje klient provedení transakcí, které jsou složité, neobvykle nebo neočekávaně objemné, které mají neobvyklý nebo neočekávaný vzorec, jsou bez zjevného ekonomického nebo zákonného účelu nebo obchodního opodstatnění? Existují důvody k podezření, že se klient pokouší vyhnout



konkrétním limitům uvedeným v čl. 11 písm. b) směrnice (EU) 2015/849 a případně vnitrostátním právním předpisům?

- i) Požaduje klient zbytečnou nebo nepřiměřenou míru utajení? Zdráhá se klient například sdílet informace potřebné k hloubkové kontrole klienta nebo se zjevně snaží zastřít pravou povahu svého podnikání?
- j) Lze snadno vysvětlit zdroj majetku nebo finančních prostředků klienta nebo skutečného majitele, například z jeho povolání, dědictví nebo investic? Je vysvětlení věrohodné?
- k) Používá klient produkty a služby, které podle očekávání získal při prvním uzavření obchodního vztahu?
- l) Pokud klient nemá v daném státě bydliště či sídlo, mohly by být jeho potřeby lépe uspokojeny v jiném státě? Existuje ekonomický a zákonný důvod pro to, aby klient požadoval daný druh finanční služby? Podniky by měly vzít na vědomí, že článek 16 směrnice 2014/92/EU propůjčuje klientům, kteří oprávněně pobývají v Unii, právo na založení základního platebního účtu, avšak toto právo platí pouze v rozsahu, v jakém mohou úvěrové instituce dostát svým povinnostem v oblasti boje proti praní peněz a financování terorismu uvedeným v čl. 1 odst. 7 a v čl. 16 odst. 4 směrnice 2014/92/EU.

2.7. Při identifikaci rizika souvisejícího s povahou a chováním klienta nebo skutečného majitele by podniky měly věnovat pozornost rizikovým faktorům, které sice nejsou specifické pro financování terorismu, ale mohly by ukazovat na zvýšené riziko financování terorismu, zejména v situacích, kdy se vyskytují také jiné rizikové faktory financování terorismu. Za tímto účelem by podniky měly zvážit přinejmenším následující rizikové faktory:

- a) Je klient nebo skutečný majitel osobou uvedenou na seznamech osob, skupin a subjektů zapojených do teroristických činů a těch, na které se vztahují omezující opatření<sup>4</sup>, nebo je známo, že má úzké osobní nebo profesionální vazby na osoby zapsané na takových seznamech (například protože má s takovou osobou vztah nebo s ní jinak žije)?

<sup>4</sup> Viz například společný postoj Rady ze dne 27. prosince 2001 o uplatnění zvláštních opatření k boji proti terorismu (2001/931/SZBP) (Úř. věst. L 344, 28.12.2001, s. 93); nařízení Rady (ES) č. 2580/2001 ze dne 27. prosince 2001 o zvláštních omezujících opatřeních namířených proti některým osobám a subjektům s cílem bojovat proti terorismu (Úř. věst. L 344, 28.12.2001, s. 70); nařízení Rady (ES) č. 881/2002 ze dne 27. května 2002 o zavedení některých zvláštních omezujících opatřeních namířených proti některým osobám a subjektům spojeným s organizacemi ISIL (Dá'iš) a Al-Kajdá (Úř. věst. L 139, 29.5.2002, s. 9). Můžete rovněž použít mapu sankcí EU na adrese <https://www.sanctionsmap.eu/>

- b) Je klient nebo skutečný majitel osobou, o které je veřejně známo, že je vyšetřována pro teroristickou činnost, nebo která byla odsouzena za teroristickou činnost nebo o které je známo, že má úzké osobní nebo profesionální vazby na takovou osobu (například protože má s takovou osobou vztah nebo s ní jinak žije)?
- c) Provádí klient transakce vyznačující se příchozími a odchozími převody finančních prostředků ze zemí a/nebo do zemí, o kterých je známo, že v nich působí skupiny páchající teroristické trestné činy, o kterých je známo, že jsou zdroji financování terorismu, nebo na které se vztahují mezinárodní sankce? Pokud ano, je možné tyto převody snadno vysvětlit například rodinnými vazbami nebo obchodními vztahy?
- d) Je klient neziskovou organizací,
  - i. o které je veřejně známo, že její činnost nebo vedení jsou spojeny s extremismem nebo sympatizováním s terorismem? nebo
  - ii. jejíž transakční chování se vyznačuje hromadnými převody velkých objemů finančních prostředků do jurisdikcí spojených s vyšším rizikem praní peněz a financování terorismu a do vysoce rizikových třetích zemí?
- e) Provádí klient transakce vyznačující se objemnými toky peněz za krátkou dobu a zapojením neziskových organizací s nejasnými vazbami (např. mají sídlo na stejném fyzickém místě; sdílejí stejné zástupce nebo zaměstnance nebo mají více účtů pod stejnými jmény)?
- f) Převádí klient nebo zamýšlí převádět finanční prostředky osobám uvedeným v bodech a) a b)?

2.8. Kromě informačních zdrojů uvedených v obecných pokynech 1.30 a 1.31 by podniky měly věnovat zvláštní pozornost pravidelně aktualizovaným typologiím financování terorismu podle Finančního akčního výboru (FATF).<sup>5</sup>

## Země a zeměpisné oblasti

2.9. Při identifikaci rizik spojených se zeměmi a zeměpisnými oblastmi by podniky měly zohlednit riziko spojené s:

- a) jurisdikcemi, ve kterých má klient sídlo nebo bydliště a ve kterých má bydliště skutečný majitel;

<sup>5</sup> <http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-tf-risks.html>

- b) jurisdikcemi, které jsou hlavním místem podnikání klienta a skutečného majitele; a
- c) jurisdikcemi, na které mají klient a skutečný majitel relevantní osobní nebo obchodní vazby nebo kde mají finanční nebo právní zájmy.

2.10. Podniky by měly vzít v úvahu, že relativní význam rizikových faktorů jednotlivých zemí a zeměpisných oblastí je často určován povahou a účelem obchodního vztahu nebo druhem obchodní činnosti. Například:

- a) Pokud byly finanční prostředky použité v obchodním vztahu získány v zahraničí, bude relevantní zejména úroveň predikativních trestných činů praní peněz a účinnost právního systému země.
- b) Pokud byly finanční prostředky obdrženy z jurisdikcí, o nichž je známo, že v nich působí skupiny, které se dopouštějí teroristických činů, nebo pokud byly do nich zaslány, měly by podniky na základě toho, co znají o účelu a povaze obchodního vztahu zvážit, do jaké míry lze podezření očekávat nebo zda by mohlo podezření vzniknout.
- c) Pokud je klient úvěrovou nebo finanční institucí, měly by podniky věnovat zvýšenou pozornost adekvátnosti režimu pro boj proti praní peněz a financování terorismu země a účinnosti dohledu v oblasti boje proti praní peněz a financování terorismu.
- d) Pokud je klient svěřenským fondem nebo jiným druhem právního uspořádání nebo má strukturu nebo funkce podobné svěřenským fondům, jako je fiducie, fideicomiso nebo Treuhand, podniky by měly vzít v úvahu, do jaké míry země, ve které jsou klient, popřípadě skutečný majitel, registrováni, účinně dodržuje mezinárodní normy o daňové transparentnosti a sdílení informací.

2.11. Podniky by měly při určování účinnosti režimů pro boj proti praní peněz a financování terorismu jurisdikcí zohlednit tyto rizikové faktory:

- a) Byla tato země v souladu s článkem 9 směrnice (EU) 2015/849 označena Komisí za zemi, která má v režimu pro boj proti praní peněz a financování terorismu strategické nedostatky? V těchto případech by se podniky měly řídit obecnými pokyny 4.53 až 4.57.
- b) Zakazuje právo dané země provádění skupinových strategií a postupů a zejména existují situace, ve kterých by se mělo použít nařízení Komise v přenesené pravomoci (EU) 2019/758?

- c) Existují informace z více věrohodných a spolehlivých zdrojů o kvalitě kontroly prováděné jurisdikcí s ohledem na boj proti praní peněz a financování terorismu, včetně informací o kvalitě a účinnosti právního prostředí a dohledu? Příklady možných zdrojů mohou být zprávy ze vzájemného hodnocení vypracované Finančním akčním výborem (FATF) nebo regionálními orgány působícími obdobně jako Finanční akční výbor (výchozím bodem je shrnutí a hlavní zjištění a posouzení souladu s doporučeními č. 10, 26 a 27 a okamžitými výsledky č. 3 a 4), seznam jurisdikcí, které vykazují vysokou míru rizika a nespolupráce, vypracovaný Finančním akčním výborem, hodnocení Mezinárodního měnového fondu (MMF) a zprávy programů hodnocení finančního odvětví (FSAP). Podniky by měly vzít v úvahu, že členství ve Finančním akčním výboru nebo regionálních orgánech působících obdobně jako Finanční akční výbor (např. Moneyval) samo o sobě neznamená, že je režim pro boj proti praní peněz a financování terorismu jurisdikce adekvátní a účinný.

2.12. Podniky by měly vzít v úvahu, že směrnice (EU) 2015/849 neuznává „rovnocennost“ třetích zemí a že seznamy členských států EU týkající se rovnocenných jurisdikcí již nejsou nadále vedeny. V rozsahu povoleném vnitrostátními právními předpisy by podniky v souladu s těmito obecnými pokyny a přílohou II směrnice (EU) 2015/849 měly být schopny určit jurisdikce s nižší mírou rizika.

2.13. Rizikové faktory, které by podniky měly při identifikaci míry rizika financování terorismu spojené s jurisdikcí zohlednit, zahrnují:

- a) Existují informace například z trestního řízení nebo z věrohodných a spolehlivých otevřených mediálních zdrojů, které naznačují, že jurisdikce poskytuje finanční prostředky na teroristické činnosti, nebo je podporuje, ať už z oficiálních zdrojů nebo od organizovaných skupin nebo organizací v takové jurisdikci?
- b) Existují informace například z trestního řízení nebo z věrohodných a spolehlivých otevřených mediálních zdrojů, které naznačují, že skupiny páchající teroristické činy v dané zemi nebo na daném území působí?
- c) Vztahují se na jurisdikci finanční sankce, embarga nebo opatření související s terorismem, financováním terorismu nebo šířením zbraní uvalené například Organizací spojených národů nebo Evropskou unií?

2.14. Rizikové faktory, které by podniky měly při zjišťování úrovně transparentnosti a souladu s daňovými předpisy zohlednit, zahrnují:

- a) Existují informace z více než jednoho věrohodného a spolehlivého zdroje, že je země považována za jsoucí v souladu se standardy mezinárodní daňové transparentnosti a sdílení informací? Existují důkazy o tom, že příslušná

pravidla jsou účinně uplatňována v praxi? Příklady možných zdrojů mohou být zprávy Globálního fóra pro transparentnost a výměnu informací v daňových záležitostech Organizace pro hospodářskou spolupráci a rozvoj (OECD), které hodnotí jurisdikce z hlediska transparentnosti a výměny informací v oblasti daní; posouzení závazku jurisdikcí k automatické výměně informací založené na společném standardu oznamování; posouzení souladu s doporučeními Finančního akčního výboru č. 9, 24 a 25 a okamžitými výsledky č. 2 a 5 vypracovanými Finančním akčním výborem nebo regionálními orgány vyvíjejícími činnost jako Finanční akční výbor; posouzení provedená s ohledem na unijní seznam jurisdikcí nespolupracujících v daňové oblasti, a hodnocení Mezinárodního měnového fondu (např. hodnocení personálu Mezinárodního měnového fondu v extrateritoriálních finančních střediscích).

- b) Zavázala se jurisdikce k uplatňování společného standardu oznamování pro automatickou výměnu informací, který skupina G20 přijala v roce 2014, a zavedla jej účinně?
- c) Zavedla jurisdikce spolehlivý a přístupný registr skutečných majitelů?

2.15. Rizikové faktory, které by podniky měly při identifikaci rizik souvisejících s úrovní predikativních trestných činů praní peněz zohlednit, zahrnují:

- a) Existují informace z věrohodných a spolehlivých veřejných zdrojů o úrovni predikativních trestných činů praní peněz uvedených v čl. 3 odst. 4 směrnice (EU) 2015/849, například korupce, organizovaná trestná činnost, daňová trestná činnost a závažné případy podvodů? Příklady mohou být indexy vnímání korupce; zprávy zemí OECD o provádění Úmluvy OECD proti podplácení zahraničních veřejných činitelů a zpráva věnovaná celosvětové problematice drog Úřadu pro drogy a kriminalitu (OSN).
- b) Existují informace z několika věrohodných a spolehlivých zdrojů o schopnosti vyšetřovacího a soudního systému jurisdikce účinně vyšetřovat a stíhat tyto trestné činy?

## **Rizikové faktory produktů, služeb a transakcí**

2.16. Podniky by měly při identifikaci rizik souvisejících s jejich produkty, službami nebo transakcemi zohlednit rizika týkající se:

- a) úrovně transparentnosti nebo netransparentnosti, kterou produkt, služba nebo transakce poskytuje;
- b) složitosti produktu, služby nebo transakce a

c) hodnoty nebo velikosti produktu, služby nebo transakce.

2.17. Rizikové faktory, které by podniky měly zvážit při identifikaci rizika souvisejícího s transparentností produktu, služby nebo transakce, zahrnují:

- a) Do jaké míry umožňují produkty nebo služby klientovi, skutečnému majiteli či struktuře příjemců zůstat v anonymitě nebo jim usnadňují skrýt jejich totožnosti? Příklady takových produktů a služeb mohou být akcie na doručitele, svěřenské vklady, offshorové struktury a určité svěřenské fondy a právnické osoby, jako například nadace, které mohou být strukturovány takovým způsobem, aby mohly využít anonymity a umožnit jednání se společnostmi bez fyzické přítomnosti nebo společnosti mající pověřené akcionáře nebo společníky.
- b) Do jaké míry je možné, aby třetí osoba, která není součástí obchodního vztahu, udělila pokyny, například v případě určitých korespondenčních bankovních vztahů?

2.18. Rizikové faktory, které by podniky měly zvážit při identifikaci rizika souvisejícího se složitostí produktu, služby nebo transakce, zahrnují:

- a) Jak složitá je transakce a zahrnuje několik stran nebo jurisdikcí, například v případě určitých obchodních finančních transakcí? Jsou transakce přímé, například jedná se o pravidelné platby do penzijního fondu?
- b) Do jaké míry umožňují produkty nebo služby nepředpokládané platby od třetích osob nebo přijímání přeplatků? Pokud se předpokládají platby od třetích osob, zná podnik identitu těchto třetích osob, jedná se například o orgán poskytující státní podporu nebo záruky? Nebo jsou produkty a služby financovány výhradně převodem finančních prostředků z vlastního účtu klienta u jiné finanční instituce, na kterou se vztahují normy v oblasti boje proti praní peněz a financování terorismu a dohledu, které jsou srovnatelné s normami vymezenými ve směrnici (EU) 2015/849?
- c) Rozumí podnik rizikům souvisejícím s jeho novým nebo inovativním produktem či službou, zejména pokud se jedná o využití nových technologií nebo platebních metod?

2.19. Rizikové faktory, které by podniky měly zvážit při identifikaci rizika souvisejícího s hodnotou nebo velikostí produktu, služby nebo transakce, zahrnují:

- a) Do jaké míry jsou produkty nebo služby náročné na finanční prostředky v hotovosti, jako je tomu u mnoha platebních služeb, ale i některých běžných účtů?

- b) Do jaké míry usnadňují či podporují produkty nebo služby transakce vysoké hodnoty? Existují u hodnot transakcí nebo výší pojistného nějaké limity, které by mohly omezit využití produktu nebo služby pro účely praní peněz a financování terorismu?

## Rizikové faktory týkající se distribučních kanálů

2.20. Podniky by měly při identifikaci rizika souvisejícího se způsobem, jakým klient získává produkty nebo služby, které požaduje, zohlednit riziko související:

- a) mírou, do jaké je obchodní vztah veden bez osobní přítomnosti partnera; a se
- b) zprostředkovateli, jejichž služby podnik může využít, a povahou jejich vztahu s podnikem.

2.21. Podniky by měly při posuzování rizika souvisejícího se způsobem, jakým klient získává produkty nebo služby, zohlednit mnoho faktorů, například:

- a) zda je klient pro účely zjišťování totožnosti osobně přítomen. Pokud ne, zda podnik
- i. použil spolehlivou formu hloubkové kontroly klienta bez osobní přítomnosti; a
- ii. podnikl kroky k zabránění zcizení totožnosti nebo jejího zneužití.
- Podniky by v těchto situacích měly použít obecné pokyny č. 4.29 až 4.31.
- b) zda byl klient představen jinou osobou téže finanční skupiny, a pokud ano, do jaké míry se může podnik na toto představení spolehnout jako na záruku toho, že klient nevystaví podnik přílišnému riziku praní peněz a financování terorismu, a co podnik učinil pro to, aby se ujistil, že příslušná osoba ze skupiny uplatňuje na normy Evropského hospodářského prostoru (EHP) opatření hloubkové kontroly klienta v souladu s článkem 28 směrnice (EU) 2015/849;
- c) zda byl klient představen třetí osobou, například bankou, která není součástí stejné skupiny, nebo zprostředkovatelem, a pokud ano,
- i. zda se jedná o regulovanou osobu, na kterou se vztahují povinnosti v oblasti boje proti praní peněz, které jsou v souladu s povinnostmi vyplývajícími ze směrnice (EU) 2015/849, a zda je třetí osoba finanční institucí nebo její hlavní obchodní činnost nesouvisí s poskytováním finančních služeb;
- ii. zda třetí osoba uplatňuje opatření hloubkové kontroly klienta, vede záznamy podle norem EHP, podléhá dohledu v souladu s článkem 26 směrnice (EU) 2015/849, pokud jde o dodržování srovnatelných povinností v oblasti boje proti

praní peněz a financování terorismu, a zda existují náznaky, že úroveň dodržování platných právních předpisů či nařízení v oblasti boje proti praní peněz a financování terorismu dotýcnou třetí osobou je nedostatečná, například byla zprostředkovateli udělena sankce za porušení povinností v oblasti boje proti praní peněz a financování terorismu;

- iii. zda má sídlo v jurisdikci s vyšším rizikem praní peněz a financování terorismu. Pokud má třetí osoba sídlo ve vysoce rizikové třetí zemi, kterou Evropská komise označila za mající strategické nedostatky, nesmí se podniky na tuto třetí osobu spoléhat. Spoléhání se je však v rozsahu povoleném vnitrostátními právními předpisy možné za předpokladu, že zprostředkovatel je pobočkou nebo většinou vlastněným dceřiným podnikem jiného podniku usazeného v Unii a podnik je přesvědčen o tom, že zprostředkovatel plně dodržuje skupinové strategie a postupy podle článku 45 směrnice (EU) 2015/849.<sup>6</sup>
- iv. co podnik učinil pro to, aby se ujistil, že:
  - a. třetí strana vždy poskytuje nezbytné doklady totožnosti;
  - b. třetí strana na vyžádání neprodleně poskytne příslušné kopie údajů o zjišťování a ověřování totožnosti nebo elektronické údaje uvedené mimo jiné v článku 27 směrnice (EU) 2015/849;
  - c. je kvalita opatření hloubkové kontroly klienta třetí osoby taková, že se na ně lze spolehnout; a
  - d. úroveň hloubkové kontroly klienta uplatňovaná třetí stranou je přiměřená riziku praní peněz a financování terorismu souvisejícímu s obchodním vztahem, s přihlédnutím k tomu, že třetí strana bude opatření hloubkové kontroly klienta uplatňovat pro vlastní účely a případně v jiné souvislosti.
- d) zda byl klient představen prostřednictvím smluvního zástupce, tedy bez přímého kontaktu s podnikem, a do jaké míry si může být podnik jist tím, že zástupce získal dostatek informací k tomu, aby podnik svého klienta i úroveň rizika souvisejícího s obchodním vztahem znal;
- e) zda jsou využití nezávislí nebo smluvní zástupci, do jaké míry jsou do průběžného výkonu obchodní činnosti zapojení a jak to ovlivňuje znalosti podniku o klientovi a průběžné řízení rizik;

<sup>6</sup> Čl. 26 odst. 2 směrnice (EU) 2015/849.



- f) když podnik v rozsahu dovoleném vnitrostátními právními předpisy využívá externího poskytovatele služeb pro aspekty svých povinností v oblasti boje proti praní peněz a financování terorismu, zda zvažil to, zda je externí poskytovatel služeb povinnou osobou, a zda se zabýval riziky uvedenými v Obecných pokynech EBA k outsourcingu (EBA/GL/2019/02) tam, kde jsou uvedené obecné pokyny použitelné.

## Obecný pokyn č. 3: Posuzování rizika praní peněz a financování terorismu

- 3.1. Podniky by měly identifikované rizikové faktory použít k posouzení celkové úrovně rizika praní peněz a financování terorismu.

### Použití holistického přístupu

- 3.2. Podniky by měly zaujmout holistický přístup k rizikovým faktorům praní špinavých peněz a financování terorismu, které identifikovaly a které, zohledněné společně, určí úroveň rizika praní špinavých peněz a financování terorismu spojeného s obchodním vztahem, příležitostnou transakcí nebo jejich obchodní činností.
- 3.3. Podniky by měly vzít v úvahu, že pokud směrnice (EU) 2015/849 nebo vnitrostátní právní předpisy nestanoví jinak, přítomnost osamocených rizikových faktorů nezbytně nezpůsobuje u vztahu vyšší nebo nižší riziko.

### Vážené rizikové faktory

- 3.4. Při posouzení rizika praní peněz a financování terorismu se mohou podniky rozhodnout, zda budou k faktorům přistupovat odlišně v závislosti na jejich relativním významu.
- 3.5. Při vážení rizikových faktorů by podniky měly v rámci obchodního vztahu, příležitostné transakce nebo své obchodní činnosti informovaně posoudit význam různých rizikových faktorů. Často to vede k tomu, že podniky přidělují různým faktorům různá „hodnocení“; například podniky se mohou rozhodnout, zda jsou klientovy osobní vazby na jurisdikci spojenou s vyšším rizikem praní peněz a financování terorismu s ohledem na vlastnosti produktu, který požaduje, méně důležité.
- 3.6. Váha přidělená každému z těchto faktorů se v konečném důsledku bude pravděpodobně lišit podle produktu a klienta (nebo kategorie klienta) a podle podniku. Při vážení rizikových faktorů by podniky měly zajistit, aby:
- a) vážení nebylo nepřiměřeně ovlivněno pouze jedním faktorem;
  - b) hodnocení rizik nebylo ovlivněno ekonomickými nebo ziskovými důvody;

- c) vážení nevedlo k situaci, v níž žádný obchodní vztah nelze klasifikovat jako vysoce rizikový;
  - d) vážení podniku nemůže přebít ustanovení směrnice (EU) 2015/849 nebo vnitrostátních právních předpisů týkající se situací, které vždy představují vysoké riziko praní peněz; a aby
  - e) byly případně schopny nepřihlížet ke všem automaticky vytvořeným hodnocením rizik. Důvody pro rozhodnutí nepřihlédnout k těmto hodnocením by měly být řádně doloženy.
- 3.7. Pokud podnik využívá k přidělování celkových hodnocení rizik za účelem kategorizace obchodních vztahů nebo příležitostných transakcí automatizované informační systémy, které nevyvíjí interně, ale které zakoupil od externího poskytovatele, měl by chápat, jak systémy fungují a jak kombinují rizikové faktory za účelem dosažení celkového hodnocení rizik. Podnik si musí být vždy jist, že přidělená hodnocení zohledňují přístup podniku k riziku praní peněz a financování terorismu, a měl by být schopen tuto skutečnost prokázat příslušnému orgánu.

### Kategorizace rizika

- 3.8. Podnik by měl přijmout rozhodnutí o nejvhodnějším způsobu kategorizace rizika. To bude záviset na povaze a velikosti obchodní činnosti podniku a typech rizika praní peněz a financování terorismu, kterému je vystaven. Ačkoliv podniky často člení rizika na vysoká, střední a nízká, jsou možné i další kategorizace.
- 3.9. Po posouzení rizik a s přihlédnutím k inherentním rizikům i případným identifikovaným nástrojům na snižování rizika by měl podnik rozčlenit své oblasti podnikání i obchodní vztahy a příležitostné transakce podle vnímané úrovně rizika praní peněz a financování terorismu.

## Obecný pokyn č. 4: Opatření hloubkové kontroly prováděná všemi podniky

- 4.1. Posouzení rizik v rámci celého podniku a individuální posouzení rizik podniku by měla pomáhat při určování oblastí, na které by měl zaměřit své úsilí při řízení rizik praní peněz a financování terorismu, a to jak při navázání obchodního vztahu s klientem, tak po dobu trvání obchodního vztahu.
- 4.2. Podniky by měly zajistit, že jejich strategie a postupy v oblasti boje proti praní peněz a financování terorismu vycházejí z posouzení rizik a zohledňují ho.

- 4.3. Měly by rovněž zajistit, že jejich strategie a postupy v oblasti boje proti praní peněz a financování terorismu jsou snadno dostupné, uplatňované, účinné a že jim rozumí všichni příslušní zaměstnanci.
- 4.4. Při plnění své povinnosti podle článku 8 směrnice 2015/849 získat souhlas svého vrcholného vedení se strategiemi, kontrolami a postupy v oblasti boje proti praní peněz a financování terorismu by podniky měly zajistit, že vrcholné vedení má přístup k dostatečným údajům, včetně posouzení rizika praní peněz a financování terorismu v rámci celého podniku, aby mohlo zaujmout informované stanovisko k přiměřenosti a účinnosti těchto strategií a postupů a zejména strategií a postupů pro hloubkovou kontrolu klienta.

## Hloubková kontrola klienta

- 4.5. Opatření hloubkové kontroly klienta by měla pomoci podnikům lépe porozumět rizikům souvisejícím s jednotlivými obchodními vztahy a příležitostnými transakcemi.
- 4.6. Podniky musí uplatňovat všechna opatření hloubkové kontroly klienta stanovená v čl. 13 odst. 1 směrnice (EU) 2015/849, mohou však při zohlednění míry rizika stanovit rozsah každého z těchto opatření.
- 4.7. Podniky by měly ve svých strategiích a postupech jasně vymezit,
  - a) kdo je klientem a případně skutečným majitelem jednotlivých typů klientů a kategorií produktů a služeb a či totožnost je potřeba pro účely hloubkové kontroly klienta ověřit. Podniky by se měly odvolat na odvětvové pokyny v hlavě II těchto obecných pokynů obsahující bližší informace o identifikaci klientů a jejich skutečných majitelů.
  - b) co je v souvislosti s jejich obchodní činností příležitostnou transakcí a v jakém okamžiku se řada jednorázových transakcí stává obchodním vztahem namísto příležitostné transakce, přičemž zohlední faktory jako četnost nebo pravidelnost, s níž se klient vrací za účelem příležitostných transakcí, a to, do jaké míry se předpokládá, že vztah má nebo zřejmě má určité trvání. Podniky by měly vzít v úvahu, že peněžní limit stanovený v čl. 11 písm. b) směrnice (EU) 2015/849 má význam pouze do té míry, že při jeho dosažení je naprosto nutné uplatnit opatření hloubkové kontroly klienta; řada příležitostných transakcí může být obchodním vztahem i v případě, že uvedeného peněžního limitu není dosaženo;
  - c) jaká je odpovídající úroveň a druh hloubkové kontroly klienta, kterou budou vůči jednotlivým obchodním vztahům a příležitostným transakcím uplatňovat;
  - d) jak očekávají, že bude ověřena totožnost klienta, popřípadě skutečného majitele, a jak očekávají, že se určí povaha a účel obchodního vztahu;

- e) jaká úroveň sledování se má použít za jakých okolností;
- f) jak a v jakých situacích mohou být slabší formy identifikace a ověřování totožnosti nahrazeny zesíleným sledováním; a
- g) ochotu podniku podstupovat riziko.

4.8. Jak se uvádí v čl. 13 odst. 4 směrnice (EU) 2015/849, podniky by měly být schopny prokázat svému příslušnému orgánu, že daná opatření hloubkové kontroly klienta, která použily, jsou přiměřená rizikům praní peněz a financování terorismu.

### Finanční začlenění a snižování rizik

4.9. „Snižováním rizik“ se rozumí rozhodnutí podniku již nadále nenabízet služby určitým kategoriím klientů s vyšším rizikem praní peněz a financování terorismu. Vzhledem k tomu, že se riziko související s jednotlivými obchodními vztahy bude lišit, a to i v rámci jedné kategorie, uplatňování přístupu založeného na posouzení míry rizika nevyžaduje, aby podniky odmítly uzavřít nebo ukončily obchodní vztahy s celými skupinami klientů považovaných za klienty, kteří představují vyšší riziko praní peněz a financování terorismu. Podniky by měly pečlivě hledat rovnováhu mezi potřebou finančního začlenění a potřebou zmírnit riziko praní peněz a financování terorismu.

4.10. V rámci toho by podniky měly zavést příslušné strategie a postupy zohledňující míru rizika, aby zajistily, že jejich přístup k uplatňování opatření hloubkové kontroly klienta nevede k bezdůvodnému odepření přístupu oprávněným klientům k finančním službám. Má-li klient oprávněné a věrohodné důvody pro neposkytnutí tradičních forem dokladů totožnosti, podniky by měly zvážit jiné způsoby zmírňování rizika praní peněz a financování terorismu, včetně

- a) přizpůsobení úrovně a intenzity sledování tak, aby byla úměrná riziku praní peněz a financování terorismu spojenému s klientem, včetně rizika, že klient, který předložil slabší formu dokladu totožnosti, nemusí být tím, za koho se vydává; a
- b) nabízení pouze základních finančních produktů a služeb, které omezují schopnost uživatelů tyto produkty a služby zneužít pro účely finanční trestné činnosti. Tyto základní produkty a služby mohou podnikům rovněž usnadnit identifikaci neobvyklých transakcí nebo způsobů obchodování, včetně nezamýšleného použití produktu; avšak je důležité, aby případná omezení byla přiměřená a neomezovala nepřiměřeně nebo zbytečně přístup klientů k finančním produktům a službám.

- 4.11. Podniky se mohou opřít o stanovisko Evropského orgánu pro bankovníctví o uplatňování opatření hloubkové kontroly klienta na klienty, kteří jsou žadateli o azyl z vysoce rizikových třetích zemí nebo území (EBA-OP-2016-07).

### Skuteční majitelé

- 4.12. Při plnění svých povinností uvedených v čl. 13 odst. 1 písm. b) směrnice (EU) 2015/849 s cílem pochopit vlastnickou a řídicí strukturu klienta by podniky měly učinit alespoň následující kroky:

- a) Podniky by se měly zeptat klienta, kdo jsou jeho skuteční majitelé;
- b) Podniky by měly zdokumentovat získané informace.
- c) Následně by podniky měly přijmout všechna nezbytná a přiměřená opatření k ověření informací: za tímto účelem by podniky měly zvážit použití registru skutečných majitelů, je-li dostupný.
- d) Kroky b) a c) by měly být podniknuty při zohlednění míry rizika.

### Registr skutečných majitelů

- 4.13. Podniky by si měly uvědomit, že použití informací obsažených v registru skutečných majitelů samo o sobě nespĺňuje jejich povinnost přijmout přiměřená opatření zohledňující míru rizika za účelem identifikace skutečného majitele a ověření jeho totožnosti. Mohou být nutné další kroky za účelem identifikace a ověření skutečného majitele, zejména pak v případě, kdy je riziko související s obchodním vztahem zvýšené nebo pokud má podnik pochybnosti o tom, že je osoba uvedená v registru konečným skutečným majitelem.

### Kontrola jinými prostředky

- 4.14. Požadavek identifikovat skutečného majitele a učinit všechna nezbytná a přiměřená opatření k ověření jeho totožnosti se týká pouze fyzické osoby, která v konečném důsledku vlastní nebo ovládá klienta. Nicméně při plnění svých povinností podle článku 13 směrnice (EU) 2015/849 by podniky měly rovněž přijmout náležitá opatření k pochopení vlastnické a řídicí struktury klienta.
- 4.15. Opatření, která podniky přijmou za účelem pochopení klientovy vlastnické a řídicí struktury, by měla být natolik dostatečná, aby mohl být daný podnik důvodně přesvědčen, že rozumí rizikům spojeným s různými úrovněmi vlastnictví a řízení. Podniky by se měly zejména ujistit, že
- a) vlastnická a řídicí struktura klienta není zbytečně složitá nebo netransparentní; nebo

- b) složitá nebo netransparentní vlastnická a řídicí struktura má legitimní právní nebo ekonomický důvod.
- 4.16. Aby podniky dostály svým povinnostem podle čl. 33 odst. 1 směrnice (EU) 2015/849, měly by finanční zpravodajské jednotce oznámit, jestliže vlastnická a řídicí struktura klienta vzbuzuje podezření a jestliže mají důvodné podezření, že finanční prostředky mohou být výnosy z trestné činnosti nebo souvisějí s financováním terorismu.
- 4.17. Podniky by měly zvláštní pozornost věnovat osobám, které mohou vykonávat „kontrolu jinými prostředky“ podle čl. 3 odst. 6 písm. a) bodu i) směrnice (EU) 2015/849. K příkladům „kontroly jinými prostředky“, které by podniky měly zohlednit, patří mimo jiné:
- a) kontrola bez přímého vlastnictví, například prostřednictvím blízkých rodinných vztahů nebo historických či smluvních sdružení;
  - b) používání, užívání aktiv vlastněných klientem nebo prospěch z nich plynoucí;
  - c) odpovědnost za strategická rozhodnutí, která podstatným způsobem ovlivňují obchodní postupy nebo obecné směřování právnické osoby.
- 4.18. Podniky by měly rozhodnout na základě posouzení míry rizika, zda ověřit vlastnickou a řídicí strukturu klienta.

#### *Identifikace osob ve vrcholném vedení klienta*

- 4.19. Je-li klientem právnická osoba, podniky by měly vynaložit veškeré úsilí, aby identifikovaly skutečného majitele podle vymezení v čl. 3 odst. 6 písm. a) bodě i) směrnice (EU) 2015/849.
- 4.20. Podniky by se měly uchýlit k tomu, že jako skutečné majitele určí osoby ve vrcholném vedení klienta, pouze v případě, že:
- a) vyčerpaly všechny možné prostředky k identifikaci fyzické osoby, která klienta v konečném důsledku vlastní nebo ovládá;
  - b) neschopnost identifikovat fyzickou osobu, která klienta v konečném důsledku vlastní nebo ovládá, nevzbuzuje podezření z praní peněz a financování terorismu; a
  - c) ujistily se, že klientem uvedený důvod, proč fyzickou osobu, která klienta v konečném důsledku vlastní nebo ovládá, není možné identifikovat, je věrohodný.
- 4.21. Při rozhodování, která osoba ve vrcholném vedení nebo které osoby ve vrcholném vedení mají být určeny skutečným majitelem, by podniky měly zvážit, kdo má konečnou a celkovou odpovědnost za klienta a přijímá jménem klienta závazná rozhodnutí.

- 4.22. V těchto případech by podniky měly jasně zdokumentovat své důvody pro určení člena vrcholného vedení skutečným majitelem namísto identifikace skutečného majitele klienta, a musí uchovat záznamy o svém postupu<sup>7</sup>.

#### *Identifikace skutečného majitele orgánu veřejné správy nebo státního podniku*

- 4.23. Je-li klientem orgán veřejné správy nebo státní podnik, podniky by se při identifikaci osoby ve vrcholném vedení měly řídit obecnými pokyny č. 4.21 a 4.22.
- 4.24. V těchto případech a zejména v případě, že je riziko související s příslušným vztahem zvýšené, například kvůli tomu, že státní podnik je ze země spojené s vysokou mírou korupce, by podniky měly při zohlednění míry rizika podniknout takové kroky, které povedou k určení, že osoba, kterou identifikovaly jako skutečného majitele, je klientem řádně zmocněná jednat za klienta.
- 4.25. Podniky by měly rovněž řádně zvážit možnost, že osoba ve vrcholném vedení klienta může být politicky exponovanou osobou. V takovém případě musí podniky vůči dotyčné osobě ve vrcholném vedení uplatnit opatření zesílené hloubkové kontroly klienta v souladu s článkem 18 směrnice (EU) 2015/849 a posoudit, zda rozsah, ve kterém může tato politicky exponovaná osoba klienta ovlivnit, vede ke zvýšenému riziku praní peněz a financování terorismu, a zda může být nezbytné vůči klientovi uplatňovat opatření zesílené hloubkové kontroly klienta.

#### **Doložení totožnosti**

- 4.26. Při plnění povinností podle čl. 13 odst. 1 písm. a) a b) směrnice (EU) 2015/849 by podniky měly ověřit totožnost klienta, popřípadě totožnost skutečných majitelů, na základě spolehlivých a nezávislých informací a údajů získaných na dálku, elektronicky nebo v listinné podobě.
- 4.27. Podniky by měly ve svých strategiích a postupech vymežit, které informace a údaje budou pro účely hloubkové kontroly klienta považovat za spolehlivé a nezávislé. V rámci toho by podniky měly vzít v úvahu,
- a) co činí tyto údaje nebo informace spolehlivými. Podniky by měly zvážit různé míry spolehlivosti stanovené na základě
    - i. toho, v jakém rozsahu musel klient při získávání poskytnutých informací nebo údajů podstoupit určité kontroly;
    - ii. případného úředního postavení osoby nebo instituce, která tyto kontroly prováděla;

<sup>7</sup> Čl. 3 odst. 6 písm. a) bodu ii) směrnice (EU) 2015/849

- iii. úrovně záruky spojené s použitým systémem digitální identifikace; a
- iv. toho, nakolik je snadné poskytnuté informace nebo údaje o totožnosti padělat.
  - b) co činí tyto údaje nebo informace nezávislymi. Podniky by měly zvážit různé míry nezávislosti, které určí na základě toho, v jakém rozsahu osoba nebo instituce, která údaje nebo informace původně vydala nebo poskytla:
    - i. je provázána s klientem prostřednictvím přímých osobních, profesionálních nebo rodinných vazeb; a
    - ii. by mohla být klientem nepatřičně ovlivněna.

Ve většině případů by podniky měly mít možnost považovat státem a veřejnou správou vydávané informace nebo údaje za údaje poskytující nejvyšší míru nezávislosti a spolehlivosti.

- 4.28. Podniky by měly posoudit rizika spojená s jednotlivými druhy poskytnutých dokladů a použitým způsobem identifikace a ověření a zajistit, že zvolená metoda a druh odpovídá riziku praní peněz a financování terorismu souvisejícímu s klientem.

#### *Situace bez osobní přítomnosti*

- 4.29. Při plnění svých povinností podle čl. 13 odst. 1 směrnice (EU) 2015/849 by podniky v případech, kdy je obchodní vztah iniciován, navázán nebo realizován v situacích bez osobní přítomnosti nebo kdy příležitostná transakce probíhá v situacích bez osobní přítomnosti, měly:

- a) přijmout odpovídající opatření, aby se ujistily, že klient je tím, za koho se vydává; a
- b) posoudit, zda skutečnost, že vztah nebo příležitostná transakce probíhá bez osobní přítomnosti, zvyšuje riziko praní peněz a financování terorismu, a pokud ano, odpovídajícím způsobem přizpůsobit opatření hloubkové kontroly klienta. Při posuzování rizika spojeného se vztahy bez osobní přítomnosti by podniky měly zohlednit rizikové faktory uvedené v obecném pokynu č. 2.

- 4.30. Je-li riziko spojené se vztahem nebo příležitostnou transakcí bez osobní přítomnosti zvýšené, podniky by měly použít opatření zesílené hloubkové kontroly klienta v souladu s obecnými pokyny č. 4.46. Podniky by měly zejména zvážit, zda jsou vhodná zesílená opatření za účelem ověření totožnosti klienta nebo zesílené průběžné sledování vztahu.

- 4.31. Podniky by měly přihlídnout k tomu, že použití elektronických prostředků k identifikaci samo o sobě nevede ke zvýšenému riziku praní peněz a financování terorismu, zejména pak v případě, že tyto elektronické prostředky poskytují vysokou míru jistoty v souladu s nařízením (EU) 910/2014.



### *Používání inovativních technických prostředků k ověření totožnosti*

- 4.32. Směrnice (EU) 2015/849 je technologicky neutrální a podniky si mohou zvolit elektronické nebo listinné prostředky či jejich kombinaci k doložení totožnosti klientů; avšak podle čl. 13 odst. 1 písm. a) směrnice (EU) 2015/849 by se podniky měly ujistit, že daný doklad se opírá o údaje nebo informace ze spolehlivých a nezávislých zdrojů.
- 4.33. Podniky, které používají nebo hodlají používat inovativní technické prostředky k identifikaci a ověření, by měly posoudit, do jaké míry použití inovativních technických řešení může snížit nebo zvýšit rizika praní peněz a financování terorismu, zejména pak v situacích bez osobní přítomnosti. V rámci tohoto posouzení by podniky měly získat jasný přehled o:
- a) rizicích informačních a komunikačních technologií a bezpečnostních rizicích, zejména pak o riziku, že inovativní řešení může být nevhodné nebo nespolehlivé nebo by mohlo být předmětem neoprávněného zásahu;
  - b) kvalitativních rizicích, zejména o riziku, že zdroje informací použité pro účely ověření nejsou dostatečně nezávislé a spolehlivé, a tudíž nesplňují unijní nebo vnitrostátní právo; a o riziku, že rozsah ověření totožnosti zajišťovaný inovativním řešením není úměrný úrovni rizika praní peněz a financování terorismu souvisejícímu s obchodním vztahem;
  - c) právních rizicích, zejména o riziku, že poskytovatel technického řešení nedodržuje platné právní předpisy o ochraně údajů; a
  - d) rizicích podvodů týkajících se zneužití totožnosti, tedy riziku, že klient není tím, za koho se vydává. Podniky by rovněž měly zvážit riziko, že dotyčná osoba není skutečnou osobou.
- 4.34. Podniky, které namísto toho, aby vyvíjely vlastní inovativní řešení interně, používají externího poskytovatele, nadále nesou konečnou odpovědnost za splnění svých povinností v oblasti hloubkové kontroly klienta. Měly by si vyjasnit vztah s poskytovatelem inovativního řešení (např. zda se jedná o outsourcing, nebo zda je použití inovativního řešení určitou formou spoléhání se na třetí osobu v souladu s oddílem 4 směrnice (EU) 2015/849) a přijmout dostatečná opatření, aby se ujistily, že poskytovatel inovativního řešení:
- a) je registrovaný u příslušných vnitrostátních orgánů pro účely přístupu k osobním údajům a uchování osobních údajů podle právních předpisů EU

v souladu s nařízením (EU) 2016/679 (obecné nařízení o ochraně osobních údajů, GDPR)<sup>8</sup> a právními předpisy, kterými se GDPR provádí;

- b) má přístup k dostatečnému množství údajů z různých zdrojů a časových období a tyto údaje používá, přičemž přihlíží zejména k následujícím aspektům
    - i. elektronické doklady na základě klientova pasu nebudou v situaci bez osobní přítomnosti pravděpodobně postačující bez doprovodných kontrol zajišťujících, že klient je tím, za koho se vydává, a že doklad nebyl pozměněn; a
    - ii. jediný zdroj údajů nebo stavový údaj v jediném okamžiku pravděpodobně ve většině situací nebude stačit ke splnění norem pro ověření
  - c) je smluvně vázán plnit povinnosti stanovené smlouvou a závaznými právními předpisy unijního a vnitrostátního práva a ihned podnik informovat, pokud dojde ke změně; a
  - d) vykonává činnost transparentně, aby podnik vždy věděl, jaké kontroly byly provedeny, jaké zdroje byly použity, jaké byly výsledky a jak spolehlivé tyto výsledky byly.
- 4.35. Je-li externím poskytovatelem firma usazená v třetí zemi, podnik by se měl ujistit, že rozumí právním rizikům, operačním rizikům a požadavkům na ochranu údajů s tím spojeným a tato rizika účinně zmírňuje.
- 4.36. Podniky by měly být připraveny prokázat svému příslušnému orgánu, že používání konkrétního inovativního řešení je vhodné.
- 4.37. Podniky se mohou odvolat na Společné stanovisko evropských orgánů dohledu k využívání inovativních řešení v procesu hloubkové kontroly klienta z roku 2018, které tyto body blíže rozpracovává.

### Určení povahy a účelu obchodního vztahu

- 4.38. Opatření přijatá podniky s cílem určit povahu a účel obchodního vztahu by měla být úměrná riziku souvisejícímu se vztahem a dostatečná, aby podniku umožnila pochopit, kdo je klient a kdo jsou jeho skuteční majitelé. Podniky by měly alespoň učinit kroky, aby pochopily:
- a) povahu činnosti nebo podnikání klienta;
  - b) proč si klient zvolil produkty a služby podniku;

---

<sup>8</sup> Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), (Úř. věst. L 119, 4.5.2016, s. 1).

- c) hodnotu a zdroje finančních prostředků, které budou protékat přes účet;
- d) jak bude klient používat produkty a služby podniku;
- e) zda má klient jiné obchodní vztahy s dalšími částmi podniku nebo širší skupinou podniků a do jaké míry to ovlivní, jak podnik klienta chápe; a
- f) co se považuje za „běžné“ chování tohoto klienta nebo skupiny klientů.

4.39. Podniky by měly zohlednit rizikové faktory v obecných pokynech č. 2.4 až 2.6 těchto obecných pokynů.

### Zjednodušená hloubková kontrola klienta

4.40. V rozsahu, který dovolují vnitrostátní právní předpisy, mohou podniky uplatňovat opatření zjednodušené hloubkové kontroly klienta v situacích, kdy bylo riziko praní peněz a financování terorismu související s obchodním vztahem posouzeno jako nízké. Zjednodušená hloubková kontrola klienta nepředstavuje osvobození od žádných opatření hloubkové kontroly klienta; podniky však mohou upravit rozsah, dobu uskutečnění nebo typ každého nebo všech opatření hloubkové kontroly klienta způsobem odpovídajícím nízkému riziku, které identifikovaly.

4.41. Mezi opatření zjednodušené hloubkové kontroly klienta, která mohou podniky uplatnit, mimo jiné patří:

- a) přizpůsobení doby uskutečnění hloubkové kontroly klienta, pokud například požadovaný produkt nebo transakce mají vlastnosti, které omezují jejich použití pro účely praní peněz a financování terorismu, například:
  - i. ověřením totožnosti klienta nebo skutečného majitele při vzniku obchodního vztahu; nebo
  - ii. ověřením totožnosti klienta nebo skutečného majitele po překročení stanoveného limitu transakcí nebo po uplynutí přiměřené lhůty. Podniky musí zajistit, aby:
    - a. to nevedlo k faktickému osvobození od hloubkové kontroly klienta, což znamená, že podniky musí zajistit, aby totožnost klienta nebo skutečného majitele byla v konečném důsledku ověřena;
    - b. limit nebo lhůta byl stanoven na poměrně nízké úrovni (nicméně s ohledem na financování terorismu by měly podniky vzít v úvahu, že nízký limit nemusí dostatečně zmírnit riziko);

- c. měly zavedené systémy, které jim umožní zjistit, kdy byl dosažen limit nebo kdy skončila lhůta; a
  - d. neodkládaly hloubkovou kontrolu klienta nebo neprotahovaly získávání relevantních informací o klientovi, pokud by platné právní předpisy, například nařízení (EU) 2015/847 nebo ustanovení vnitrostátních právních předpisů, vyžadovaly, aby byly tyto informace získány již v samotném počátku.
- b) přizpůsobení množství získaných informací pro účely zjišťování a ověřování totožnosti nebo sledování, například:
- i. ověřením totožnosti na základě informací získaných pouze z jednoho spolehlivého, věrohodného a nezávislého dokumentu nebo zdroje údajů; nebo
  - ii. předpokládáním povahy a účelu obchodního vztahu, protože produkt je určen pouze pro jedno konkrétní použití, například zaměstnanecké penzijní pojištění nebo dárkový poukaz do nákupního střediska;
- c) přizpůsobení kvality nebo zdroje informací získaných pro účely zjišťování a ověřování totožnosti nebo sledování, například:
- i. přijetím informací získaných od klienta spíše než od nezávislého zdroje při ověřování totožnosti skutečného majitele (nicméně toto není přípustné v souvislosti s ověřováním totožnosti klienta); nebo
  - ii. spoléháním se na zdroj finančních prostředků za účelem splnění některých požadavků hloubkové kontroly klienta, pokud je riziko související se všemi aspekty vztahu velmi nízké, například jsou-li finanční prostředky platbami státní podpory nebo byly-li finanční prostředky převedeny jménem klienta z účtu firmy v EHP;
- d) přizpůsobení četnosti aktualizací hloubkové kontroly klienta a hodnocení obchodního vztahu, například jejich provedením pouze při vzniku rozhodné události, například když klient chce uzavřít smlouvu na nový produkt nebo službu nebo když je dosažen určitý limit transakce; podniky musí zajistit, aby to nevedlo k faktickému osvobození od udržování aktuálnosti informací o hloubkové kontrole klienta;
- e) přizpůsobení četnosti a intenzity sledování transakcí, například sledováním transakcí nad určitým limitem. Pokud se to podniky rozhodnou učinit, musí zajistit, aby byl limit nastaven na přiměřenou úroveň a aby měly zavedeny systémy pro identifikaci propojených transakcí, které by společně tento limit překročily.

- 4.42. Hlava II uvádí další opatření zjednodušené hloubkové kontroly klienta, která mohou mít v různých odvětvích zvláštní význam.
- 4.43. Informace, které podnik při uplatňování opatření zjednodušené hloubkové kontroly klienta získá, musí podniku umožnit, aby byl dostatečně ujištěn o tom, zda jeho posouzení, že riziko související s daným vztahem je nízké, je odůvodněné. Musí také podniku poskytnout dostatek informací o povaze obchodního vztahu za účelem zjištění veškerých neobvyklých nebo podezřelých transakcí. Zjednodušená hloubková kontrola klienta neosvobozuje instituci od povinnosti oznámit podezřelé transakce finanční zpravodajské jednotce.
- 4.44. Existují-li náznaky, že riziko nemusí být nízké, například existuje-li důvodné podezření, že dochází k pokusu o praní peněz a financování terorismu nebo má-li podnik pochybnosti o pravdivosti získaných informací, nesmí se použít zjednodušená hloubková kontrola klienta.<sup>9</sup> Použijí-li se obdobně specifické scénáře s vysokým rizikem a existuje-li povinnost provádět zesílenou hloubkovou kontrolu klienta, nesmí se použít zjednodušená hloubková kontrola klienta.

## Zesílená hloubková kontrola klienta

- 4.45. Podle článků 18 až 24 směrnice (EU) 2015/849 musí podniky uplatňovat opatření zesílené hloubkové kontroly klienta v situacích s vyšším rizikem, aby tato rizika odpovídajícím způsobem řídily a zmírňovaly. Opatření zesílené hloubkové kontroly klienta nemohou být nahrazena běžnými opatřeními hloubkové kontroly klienta, ale musí být uplatněna navíc k běžným opatřením hloubkové kontroly klienta.
- 4.46. Směrnice (EU) 2015/849 uvádí konkrétní případy, které podniky musí vždy považovat za představující vyšší riziko:
- a) je-li klient nebo skutečný majitel klienta politicky exponovanou osobou (články 20 až 24);
  - b) vstupuje-li podnik do korespondenčního vztahu, v rámci kterého jsou prováděny platby s institucí ze třetí země (článek 19);
  - c) udržuje-li podnik obchodní vztahy nebo provádí-li transakci související s vysoce rizikovými třetími zeměmi (čl. 18 odst. 1); a
  - d) všechny transakce, které jsou
    - i. složité;
    - ii. neobvykle velké;

<sup>9</sup> Čl. 11 písm. e) a f) a čl. 15 odst. 2 směrnice (EU) 2015/849.

- iii. prováděné neobvyklým způsobem; nebo
- iv. bez zjevného ekonomického nebo zákonného účelu (čl. 18 odst. 2)

4.47. Směrnice (EU) 2015/849 uvádí konkrétní opatření zesílené hloubkové kontroly klienta, která musí podniky uplatňovat:

- a) je-li klient nebo skutečný majitel klienta politicky exponovanou osobou;
- b) souvisí-li obchodní vztah nebo transakce s vysoce rizikovou třetí zemí identifikovanou Komisí v souladu s čl. 9 odst. 2 směrnice (EU) 2015/849;
- c) v případě korespondenčních vztahů souvisejících s prováděním plateb s responzenčními institucemi ze třetích zemí; a
- d) v případě všech transakcí, které jsou buď složité, neobvyklé velké, prováděné neobvyklým způsobem, nebo nemají zjevný ekonomický nebo zákonný účel.

Podniky by měly uplatňovat další opatření zesílené hloubkové kontroly klienta v situacích, kdy odpovídají riziku praní peněz a financování terorismu, které identifikovaly.

### Politicky exponované osoby

4.48. Při zavádění strategií a postupů zohledňujících míru rizika za účelem identifikace politicky exponovaných osob by podniky měly zohlednit seznam významných veřejných funkcí zveřejňovaný Komisí podle čl. 20a odst. 3 směrnice (EU) 2015/849 a zajistit identifikaci osob zastávajících tyto funkce. Tento seznam platí pro významné funkce v EU; při určování způsobu identifikace politicky exponovaných osob z třetích zemí by podniky namísto toho měly použít seznam funkcí v čl. 3 odst. 9 směrnice (EU) 2015/849 a seznam v jednotlivých případech upravit.

4.49. Podniky, které používají komerčně dostupné seznamy politicky exponovaných osob, by se měly ujistit, že informace v těchto seznamech jsou aktuální a že si podniky uvědomují omezení spojená s takovými seznamy. Podniky by měly podle potřeby přijmout další opatření, například v situacích, kdy jsou výsledky prověřování neprůkazné nebo neodpovídají očekáváním podniku.

4.50. Podniky, které zjistily, že klient nebo skutečný majitel je politicky exponovanou osobou, musí vždy:

- a) Přijmout adekvátní opatření k určení zdroje majetku a zdroje finančních prostředků, které mají být v obchodních vztazích použity, aby podnik mohl zajistit, že se nejedná o výnosy z korupce nebo jiné trestné činnosti. Opatření, která by podniky měly přijmout ke zjištění zdroje majetku a zdroje finančních prostředků politicky exponované osoby, budou záviset na míře závažnosti

vysokého rizika souvisejícího s obchodním vztahem. Podniky by měly zdroj majetku a zdroj finančních prostředků ověřit na základě spolehlivých a nezávislých údajů, dokumentů nebo informací, je-li riziko spojené se vztahem s politicky exponovanou osobou obzvláště vysoké.

- b) Získat souhlas vrcholného vedení s navázáním obchodního vztahu s politicky exponovanou osobou nebo s jeho pokračováním. Vhodná úroveň služebního postavení k podepisování by měla být určena úrovní zvýšeného rizika souvisejícího s obchodním vztahem a vrcholový manažer schvalující obchodní vztahy s politicky exponovanou osobou by měl mít dostatečné postavení a možnost dohledu k přijímání informovaných rozhodnutí v otázkách, které mají přímý dopad na rizikový profil podniku.
- c) Při posuzování toho, zda by se měl vztah s politicky exponovanou osobou schválit, by mělo rozhodnutí vrcholného vedení vycházet z úrovně rizika praní peněz a financování terorismu, kterému by byl podnik vystaven, pokud by tento obchodní vztah uzavřel, a z toho, jak je podnik schopen toto riziko účinně zvládnout.
- d) Provádět zesílené průběžné sledování jak transakcí, tak rizika souvisejícího s obchodním vztahem. Podniky by měly identifikovat neobvyklé transakce a pravidelně vyhodnocovat informace, které mají k dispozici, aby zajistily, že všechny nové nebo objevující se informace, které by mohly ovlivnit posouzení rizik, jsou zjištěny včas. Četnost průběžného sledování by měla být určena mírou vysokého rizika souvisejícího s daným vztahem.

4.51. V souladu s čl. 20 písm. b) směrnice (EU) 2015/849 podniky musí všechna tato opatření uplatnit na politicky exponované osoby, na jejich členy rodiny a známé blízké spolupracovníky a měly by upravit rozsah těchto opatření při zohlednění míry rizika.

4.52. Podniky by měly zajistit, že opatření, která ohledně politicky exponovaných osob zavedou v souladu se směrnicí (EU) 2015/849 a těmito obecnými pokyny, nevedou k tomu, že je klientům z řad politicky exponovaných osob neoprávněně odpírán přístup k finančním službám.

### Vysoce rizikové třetí země

4.53. Pokud jde o obchodní vztah nebo transakci související s vysoce rizikovými třetími zeměmi uvedenými v ustanovení čl. 9 odst. 2 směrnice (EU) 2015/849, podniky by měly zajistit, že použijí přinejmenším opatření zesílené hloubkové kontroly klienta uvedená v čl. 18a odst. 1 a v příslušných případech opatření uvedená v čl. 18a odst. 2 směrnice (EU) 2015/849.

4.54. Podniky by měly uplatňovat opatření uvedená v obecném pokynu č. 4.53 a přizpůsobit rozsah těchto opatření při zohlednění míry rizika.

- 4.55. Obchodní vztah nebo transakce vždy souvisí s vysoce rizikovou třetí zemí, jestliže
- a) finanční prostředky pocházejí z vysoce rizikové třetí země;
  - b) finanční prostředky jsou obdrženy z vysoce rizikové třetí země;
  - c) místo určení finančních prostředků se nachází ve vysoce rizikové třetí zemi;
  - d) podnik jedná s fyzickou osobou nebo právnickou osobou, která má bydliště nebo která je usazena ve vysoce rizikové třetí zemi; nebo
  - e) podnik jedná se svěřenským správcem usazeným ve vysoce rizikové třetí zemi nebo se svěřenským fondem řídicím se právním řádem vysoce rizikové třetí země.
- 4.56. Při provádění opatření hloubkové kontroly klienta nebo během obchodního vztahu by podniky měly zajistit, že uplatňují také opatření zesílené hloubkové kontroly klienta uvedená v čl. 18a odst. 1 a v příslušných případech opatření uvedená v čl. 18a odst. 2 směrnice (EU) 2015/849, když podniky zjistí, že
- a) transakce prochází vysoce rizikovou třetí zemí, například kvůli tomu, kde sídlí zprostředkující poskytovatel platebních služeb; nebo
  - b) skutečný majitel klienta má bydliště ve vysoce rizikové třetí zemi.
- 4.57. Nehledě na obecné pokyny č. 4.54 a 4.56 by podniky měly pečlivě posoudit riziko související s obchodními vztahy a transakcemi v případech, kdy
- a) je známo, že klient udržuje blízké osobní nebo profesionální vztahy s vysoce rizikovou třetí zemí; nebo
  - b) je známo, že skutečný majitel udržuje blízké osobní nebo profesionální vztahy s vysoce rizikovou třetí zemí.

V těchto situacích by podniky měly na základě posouzení rizik rozhodnout, zda použijí nebo nepoužijí opatření uvedená v článku 18a směrnice (EU) 2015/849, opatření zesílené hloubkové kontroly klienta nebo běžná opatření hloubkové kontroly klienta.

### **Korespondenční vztahy**

- 4.58. V souladu s článkem 19 směrnice (EU) 2015/849 musí podniky učinit zvláštní opatření zesílené hloubkové kontroly klienta, jestliže mají přeshraniční korespondenční vztah s responzenční institucí usazenou v třetí zemi. Podniky musí uplatňovat všechna tato opatření a přizpůsobit rozsah těchto opatření při zohlednění míry rizika.



- 4.59. Podniky by měly, pokud jde o korespondenční bankovní vztahy, vycházet z hlavy II obecných pokynů o zesílené hloubkové kontrole klienta; tyto obecné pokyny mohou být také užitečné pro podniky nacházející se v jiných korespondenčních vztazích.

### Neobvyklé transakce

- 4.60. Podniky by měly zavést adekvátní strategie a postupy pro odhalování neobvyklých transakcí nebo způsobů obchodování. Pokud podnik takové transakce odhalí, musí uplatnit opatření zesílené hloubkové kontroly klienta. Transakce mohou být neobvyklé, protože:

- a) jsou větší, než by mohl podnik běžně očekávat na základě svých znalostí o klientovi, obchodním vztahu nebo kategorii, do které klient patří;
- b) vykazují neobvyklý nebo neočekávaný způsob obchodování ve srovnání s běžnou činností klienta nebo způsobem obchodování souvisejícím s podobnými klienty, produkty nebo službami; nebo
- c) jsou velmi složité ve srovnání s jinými podobnými transakcemi souvisejícími s podobnými typy klientů, produktů nebo služeb, a podnik si není vědom žádného ekonomického důvodu nebo zákonného účelu nebo má pochybnosti o pravdivosti informací, které mu byly poskytnuty.

- 4.61. Opatření zesílené hloubkové kontroly klienta by měla podniku umožnit určit, zda tyto transakce vyvolávají podezření, a musí přinejmenším zahrnovat:

- a) přijetí náležitých a adekvátních opatření k pochopení pozadí a účelu těchto transakcí, například určení zdroje a místa určení finančních prostředků nebo dohledání více informací o obchodní činnosti klienta pro zjištění pravděpodobných důvodů, proč klient takové transakce provádí; a
- b) sledování obchodních vztahů a následných transakcí častěji a s větším zaměřením na podrobnosti. Odpovídá-li to riziku, které bylo identifikováno, může se podnik rozhodnout sledovat jednotlivé transakce.

### Další vysoce rizikové situace

- 4.62. Ve všech dalších vysoce rizikových situacích by podniky měly informovaně rozhodnout o tom, která opatření zesílené hloubkové kontroly klienta jsou pro příslušnou vysoce rizikovou situaci vhodná. Odpovídající druh zesílené hloubkové kontroly klienta, včetně rozsahu dalších požadovaných informací, a prováděného zesíleného sledování bude záviset na důvodu, pro který byla příležitostná transakce nebo obchodní vztah označen jako vysoce rizikový.

4.63. Nevyžaduje se, aby podniky uplatňovaly všechna níže uvedená opatření zesílené hloubkové kontroly klienta ve všech případech. V určitých vysoce rizikových situacích může být například vhodné zaměřit se během obchodního vztahu na průběžné zesílené sledování.

4.64. Opatření zesílené hloubkové kontroly, která by podniky měly uplatňovat, mohou zahrnovat:

a) Větší množství informací získaných pro účely hloubkové kontroly klienta, tedy:

i. Informace o totožnosti klienta nebo skutečného majitele nebo o vlastnické a řídicí struktuře klienta, aby se zajistilo, že riziku souvisejícímu s tímto vztahem je dobře porozuměno. Může sem patřit získání a posouzení informací o pověsti klienta nebo skutečného majitele a posouzení veškerých negativních tvrzení učiněných vůči klientovi nebo skutečnému majiteli. Například:

a. informace o rodinných příslušnících a blízkých obchodních partnerech;

b. informace o minulých a současných obchodních aktivitách klienta nebo skutečného majitele; a

c. vyhledávání negativních zpráv v médiích.

ii. Informace o zamýšlené povaze obchodního vztahu, aby mohl podnik zjistit, zda je povaha a účel obchodního vztahu oprávněná, a aby mohl získat úplnější rizikový profil klienta. Může to znamenat získání informací o:

a. počtu, velikosti a četnosti transakcí, které přes účet pravděpodobně projdou, aby podnik mohl zaznamenat odchylky, které by mohly vzbudit podezření (v některých případech může být vhodné vyžadovat důkazy);

b. o tom, proč klient určitý produkt nebo službu požaduje, obzvláště v případech, ve kterých není jasné, proč nemohou být potřeby klienta lépe uspokojeny jiným způsobem nebo v jiné jurisdikci;

c. místu určení finančních prostředků;

d. povaze obchodní činnosti klienta nebo skutečného majitele, aby podnik mohl lépe porozumět pravděpodobné povaze obchodního vztahu.

b) Lepší kvalita informací získaných pro účely hloubkové kontroly klienta k potvrzení totožnosti klienta nebo skutečného majitele, a to i:

- i. požadováním, aby byla první platba provedena prokazatelně jménem klienta přes účet u bankovního subjektu, na který se vztahují normy hloubkové kontroly klienta, které nejsou méně přísné než ty, které jsou stanoveny v kapitole II směrnice (EU) 2015/849; nebo
  - ii. prokázáním, že majetek a finanční prostředky klienta, které jsou použity v obchodním vztahu, nepředstavují výnosy z trestné činnosti a že zdroj majetku a finančních prostředků je v souladu s tím, co podnik ví o klientovi a povaze obchodního vztahu. V některých případech, je-li riziko související s daným vztahem obzvláště vysoké, může být ověření zdroje majetku a finančních prostředků jediným vhodným nástrojem ke zmírnění rizika. Zdroj finančních prostředků nebo majetku lze ověřit mimo jiné nahlédnutím do přiznání k DPH a dani z příjmu, kopií auditovaného účetnictví, výplatních listin, veřejných listin nebo zpráv z nezávislých médií. Podniky by měly vzít v úvahu, že i v případě finančních prostředků ze zákonné obchodní činnosti se může jednat o praní peněz nebo financování terorismu v souladu s ustanovením čl. 1 odst. 3 až 5 směrnice (EU) 2015/849.
- c) Zvýšení četnosti přezkumů, aby se zajistilo, že podnik je i nadále schopen zvládnout riziko související s jednotlivými obchodními vztahy, nebo aby se prokázalo, že vztah již nadále neodpovídá ochotě podniku podstupovat riziko, a aby bylo možné identifikovat všechny transakce, které vyžadují další přezkoumání, a to i:
- i. zvýšením četnosti přezkumů daného obchodního vztahu za účelem zjištění, zda se rizikový profil klienta změnil a zda lze riziko stále řídit;
  - ii. získáním souhlasu vrcholného vedení k zahájení nebo pokračování obchodního vztahu, aby bylo jasné, že si je vrcholné vedení vědomo rizika, kterému je podnik vystaven, a aby mohl podnik přijmout informované rozhodnutí o tom, do jaké míry je toto riziko schopen řídit;
  - iii. pravidelnějším přezkoumáváním daného obchodního vztahu s cílem zajistit, aby byly identifikovány, posouzeny a případně řešeny změny rizikového profilu klienta; nebo
  - iv. prováděním častějšího nebo pečlivějšího sledování transakcí s cílem zjistit případné neobvyklé nebo neočekávané transakce, které by mohly vzbudit podezření na praní peněz a financování terorismu. Může to znamenat i zjištění místa určení finančních prostředků nebo zjištění důvodu k uskutečnění určitých transakcí.

4.65. Hlava II uvádí další opatření zesílené hloubkové kontroly klienta, která mohou mít v různých odvětvích zvláštní význam.

## Další aspekty

- 4.66. Podniky by neměly uzavírat obchodní vztahy, nejsou-li schopny splnit své požadavky hloubkové kontroly klienta, pokud nejsou přesvědčeny o oprávněnosti účelu a povahy obchodního vztahu nebo pokud nedošly k závěru, že mohou účinně řídit riziko, že by mohly být zneužity pro účely praní peněz a financování terorismu. Jestliže takový obchodní vztah již existuje, měly by jej podniky podle případných pokynů orgánů činných v trestním řízení ukončit nebo by měly pozastavit transakce, dokud nebude možné jej ukončit.
- 4.67. Pokud mají podniky důvodné podezření, že dochází k pokusům o praní peněz a financování terorismu, musí o tom informovat své finanční zpravodajské jednotky.
- 4.68. Podniky by měly vzít v úvahu, že uplatňování přístupu založeného na posouzení míry rizika nevyžaduje, aby odmítly uzavřít obchodní vztahy s celými skupinami klientů, které spojují s vyšším rizikem praní peněz a financování terorismu, nebo je ukončily, jelikož riziko související s jednotlivými obchodními vztahy je i v rámci jedné kategorie různé.

## Sledování

- 4.69. Podle článku 13 směrnice (EU) 2015/849 by podniky měly sledovat své obchodní vztahy s klienty.
- 4.70. Sledování by mělo zahrnovat:
- sledování transakcí s cílem zajistit, že transakce odpovídají rizikovému profilu klienta, jeho finanční situaci a širšímu povědomí podniku o klientovi, a odhalit neobvyklé nebo podezřelé transakce; a
  - průběžnou aktualizaci dokumentů, údajů nebo informací, které uchovávají, aby bylo možné poznat, zda se riziko související s obchodním vztahem změnilo, a ujistit se o přesnosti informací, které jsou základem pro průběžné sledování.
- 4.71. Podniky by měly určit četnost a intenzitu sledování při zohlednění míry rizika a s přihlédnutím k povaze, velikosti a složitosti své obchodní činnosti a k úrovni rizika, jemuž jsou vystaveny.

## Sledování transakcí

- 4.72. Podniky by měly zajistit, že jejich přístup ke sledování transakcí je účinný a vhodný.
- 4.73. Účinný systém sledování transakcí se opírá o aktuální informace o klientech a měl by podniku umožnit spolehlivou identifikaci neobvyklých a podezřelých transakcí a způsobů obchodování. Podniky by měly zajistit, že mají procesy umožňující bez zbytečného prodlení přezkoumat označené transakce.

- 4.74. Vhodnost závisí na povaze, velikosti a složitosti obchodní činnosti podniku i na riziku, jemuž je podnik vystaven. Podniky by měly přizpůsobit intenzitu a četnost sledování při zohlednění míry rizika. Podniky by měly v každém případě určit,
- a) které transakce budou sledovat v reálném čase a které transakce budou sledovat ex post. V rámci toho by podniky měly určit:
    - i. které vysoce rizikové faktory nebo kombinace vysoce rizikových faktorů vždy povedou ke sledování v reálném čase; a
    - ii. které transakce spojené s vyšším rizikem praní peněz a financování terorismu jsou sledované v reálném čase, zejména pak ty, kde je riziko související s obchodním vztahem již zvýšené;
  - b) zda budou transakce sledovat manuálně nebo s použitím automatizovaného systému sledování transakcí. Podniky, které zpracovávají velký objem transakcí, by měly zvážit zavedení automatizovaného systému sledování transakcí; a
  - c) četnost sledování transakcí s přihlédnutím k požadavkům uvedeným v těchto obecných pokynech.
- 4.75. Kromě sledování jednotlivých transakcí v reálném čase a ex post a bez ohledu na použitou úroveň automatizace by podniky měly pravidelně provádět kontroly ex post na vzorku odebraném ze všech zpracovaných transakcí s cílem určit trendy, k nimž se bude přihlížet při posuzování rizika, a otestovat a podle potřeby následně zlepšit spolehlivost a vhodnost systému sledování transakcí. Podniky by k testování a zlepšení svého systému sledování transakcí měly používat také informace získané na základě obecných pokynů č. 1.29 až 1.30.

### **Aktualizace informací potřebných k hloubkové kontrole klienta**

- 4.76. Podniky musí průběžně aktualizovat informace potřebné k hloubkové kontrole klienta.<sup>10</sup>
- 4.77. Při zavádění strategií a postupů za účelem aktualizace informací potřebných k hloubkové kontrole klienta by podniky měly věnovat zvláštní pozornost tomu, že je potřeba pozorně sledovat a získat o klientovi informace, které podniku pomůžou poznat, zda došlo ke změně rizika souvisejícího s obchodním vztahem. Příkladem informací, které by podniky měly získat, je zjevná změna zdroje finančních prostředků klienta, vlastnické struktury klienta nebo chování, které soustavně neodpovídá chování nebo profilu transakcí, jež podnik očekával.
- 4.78. Změna okolností u klienta pravděpodobně povede k tomu, že bude u dotyčného klienta potřeba uplatnit opatření hloubkové kontroly klienta. V těchto situacích nemusí být nutné znovu uplatnit všechna opatření hloubkové kontroly klienta, a podniky by měly určit, která

<sup>10</sup> Čl. 14 odst. 5 směrnice o boji proti praní peněz (AMLD)

opatření hloubkové kontroly klienta uplatní, a jejich rozsah. V případech s nižším rizikem mohou podniky například při aktualizaci svých informací potřebných k hloubkové kontrole klienta vycházet z informací získaných v průběhu obchodního vztahu.

## Obecný pokyn č. 5: Vedení záznamů

- 5.1. Pro účely článků 8 a 40 směrnice (EU) 2015/849 musí podniky vést záznamy alespoň o následujícím
- informace potřebné k hloubkové kontrole klienta;
  - posouzení rizika; a
  - transakce.
- 5.2. Podniky by měly zajistit, že tyto záznamy postačují k tomu, aby se příslušnému orgánu prokázalo, že přijatá opatření jsou s ohledem na riziko praní peněz a financování terorismu přiměřená.

## Obecný pokyn č. 6: Školení

- 6.1. Podniky musí svoje zaměstnance seznámit s předpisy, které zavedly s cílem plnit povinnosti v oblasti boje proti praní peněz a financování terorismu.<sup>11</sup>
- 6.2. V rámci toho a v souladu s obecnými pokyny obsaženými v hlavě I by podniky měly učinit kroky s cílem zajistit, že zaměstnanci znají
- posouzení rizik v rámci celého podniku a to, jak ovlivňuje jejich každodenní práci;
  - podnikové strategie a postupy v oblasti boje proti praní peněz a financování terorismu a to, jak mají být uplatňovány; a
  - způsob, jak rozpoznat podezřelé nebo neobvyklé transakce a činnosti a jak v takových případech postupovat.
- 6.3. Podniky by měly zajistit, že školení v oblasti boje proti praní peněz a financování terorismu, je
- relevantní pro daný podnik a jeho obchodní činnost;
  - upravené na míru zaměstnancům a jejich konkrétní úloze;
  - pravidelně aktualizováno; a

<sup>11</sup> Čl. 46 odst. 1 směrnice (EU) 2015/849

d) účinné.

## Obecný pokyn č. 7: Přezkoumání účinnosti

- 7.1. Podniky by měly pravidelně hodnotit účinnost svého přístupu k boji proti praní peněz a financování terorismu a určit četnost a intenzitu takového hodnocení při zohlednění míry rizika a s přihlédnutím k povaze a velikosti své obchodní činnosti a k úrovni rizika praní peněz a financování terorismu, jemuž jsou vystaveny.
- 7.2. Podniky by měly zvážit, zda může být oprávněné nebo vyžadované nezávislé přezkoumání jejich přístupu.<sup>12</sup>

---

<sup>12</sup> Čl. 8 odst. 4 písm. d) směrnice (EU) 2015/849.

## Hlava II: Pokyny pro konkrétní odvětví

---

Pokyny pro konkrétní odvětví uvedené v hlavě II doplňují obecné pokyny uvedené v hlavě I těchto obecných pokynů. Je třeba je číst společně s hlavou I.

Výčet rizikových faktorů popsaný v jednotlivých odvětvových pokynech hlavy II není úplný. Podniky by měly vůči rizikům souvisejícím s danou situací zaujmout holistický přístup a vzít v úvahu, že přítomnost ojedinělých rizikových faktorů nezbytně nepře souvá obchodní vztah nebo příležitostnou transakci do vyšší či nižší kategorie rizik.

Každý odvětvový pokyn v hlavě II rovněž uvádí příklady opatření hloubkové kontroly klienta, která by podniky měly při zohlednění míry rizika uplatňovat v situacích s vysokým rizikem a v rozsahu umožněném vnitrostátními právními předpisy taktéž v situacích s nízkým rizikem. Výčet těchto příkladů není úplný a podniky by měly rozhodnout o nejvhodnějších opatřeních hloubkové kontroly klienta podle úrovně a typu rizika praní peněz a financování terorismu, které identifikovaly.



## Obecný pokyn č. 8: Odvětvové pokyny pro korespondenční vztahy

- 8.1. Obecný pokyn č. 8 obsahuje pokyny pro korespondenční bankovníctví uvedené v čl. 3 odst. 8 písm. a) směrnice (EU) 2015/849. Podniky, které nabízejí jiné korespondenční vztahy uvedené v čl. 3 odst. 8 písm. b) směrnice (EU) 2015/849, by měly tyto pokyny uplatnit ve vhodných případech.
- 8.2. Podniky by měly vzít v úvahu, že v korespondenčním bankovním vztahu poskytuje korespondenční banka bankovní služby respondenční bance, a to buď na úrovni bank, nebo jménem klienta respondenční banky. Korespondenční banka obvykle nemá s klienty respondenční banky obchodní vztah a obvykle nezná jejich totožnost ani povahu či účel související transakce, pokud tyto informace nejsou uvedeny v platebním příkazu.
- 8.3. Banky by měly zohlednit, kromě rizikových faktorů a opatření uvedených v hlavě II těchto pokynů, následující rizikové faktory a opatření.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 8.4. Faktory, které by mohly přispět ke zvýšení rizika:
  - a) Účet mohou využívat jiné respondenční banky, které mají přímý vztah s respondenční bankou, nikoliv však s korespondenční bankou ("vnoření" nebo následné zúčtování), což znamená, že korespondenční banka nepřímo poskytuje služby jiným bankám, které nejsou danou respondenční bankou.
  - b) Účet mohou využívat jiné subjekty patřící do skupiny respondenční banky, na které se nevztahuje hloubková kontrola korespondenční banky.
  - c) Služba zahrnuje otevření průběžného korespondenčního účtu, který klientům respondenční banky umožňuje provádět transakce přímo na účtu respondenční banky.
- 8.5. Faktory, které by mohly přispět ke snížení rizika:
  - a) Tento vztah je omezen na schopnosti Aplikace řízení rizik SWIFT, která je určena pro řízení komunikace mezi finančními institucemi. Ve vztahu řízeném Aplikací řízení rizik SWIFT nemá respondenční banka ani protistrana vztah k platebnímu účtu.
  - b) Banky namísto zpracovávání transakcí jménem svých klientů jednají spíše na úrovni bank, například v případě devizových služeb mezi dvěma bankami, v nichž je obchod uskutečňován na úrovni bank mezi těmito bankami a kde

vypořádání transakce nezahrnuje platbu třetí osobě. V těchto případech se transakce realizuje na vlastní účet respondenční banky.

- c) Transakce se týká prodeje, nákupu nebo zastavení cenných papírů na regulovaných trzích, například když jedná jako depozitář nebo využívá služby depozitáře s přímým přístupem, obvykle prostřednictvím místního účastníka, do systému vypořádání obchodů s cennými papíry v EU nebo mimo EU.

### Rizikové faktory klienta

#### 8.6. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Politiky boje proti praní peněz a financování terorismu respondenční banky a systémy a kontroly, které respondenční banka zavedla k jejich provádění, nejsou v souladu s požadavky uvedenými ve směrnici (EU) 2015/849.
- b) Na respondenční banku se nevztahuje adekvátní dohled v oblasti boje proti praní peněz a financování terorismu.
- c) Na respondenční banku, její mateřský podnik nebo podnik, patřící do stejné skupiny jako respondenční banka, byla v nedávné době uplatněna donucovací opatření v reakci na nedostatečné politiky a postupy v oblasti boje proti praní peněz a financování terorismu a/nebo porušování povinností v oblasti boje proti praní peněz a financování terorismu.
- d) Respondenční banka významně podniká v odvětvích, která jsou spojena s vyšším rizikem praní peněz a financování terorismu; například respondenční banka podniká v oblasti převodu finančních prostředků nebo podniká jménem některých subjektů zabývajících se poukazováním peněz nebo směnárén, s jinými státními příslušníky nebo v jiné měně, než je měna, kterou používá země, ve které má sídlo.
- e) Do vedení nebo vlastnické struktury respondenční banky je zapojena politicky exponovaná osoba, především jestliže by politicky exponovaná osoba mohla mít na respondenční banku velký vliv, jestliže pověst, bezúhonnost politicky exponované osoby nebo její vhodnost jako člena správní rady nebo osoby zastávající klíčovou funkci vyvolává obavy nebo jestliže politicky exponovaná osoba pochází z jurisdikce spojené s vyšším rizikem praní peněz a financování terorismu. Podniky by měly jurisdikcím, kde je korupce vnímána jako systémová nebo rozsáhlá, věnovat zvýšenou pozornost.
- f) Minulý průběh obchodního vztahu s respondenční bankou vyvolává obavy například proto, že objem transakcí není v souladu s očekáváním

korrespondenční banky na základě toho, co korrespondenční banka o povaze a velikosti respondenční banky zná.

- g) Respondenční banka neposkytla informace požadované korrespondenční bankou pro účely hloubkové kontroly klienta a zesílené hloubkové kontroly klienta a informace o plátcích nebo příjemcích, které jsou vyžadované na základě nařízení (EU) 2015/847. Za tímto účelem by korrespondenční banka měla zvážit kvantitativní a kvalitativní kritéria uvedená ve společných obecných pokynech JC/GL/2017/16.<sup>13</sup>

8.7. Faktory, které by mohly přispět ke snížení rizika: Korrespondenční banka dospěje k závěru, že:

- a) kontroly respondenční banky v oblasti boje proti praní peněz a financování terorismu nebyly méně přísné než kontroly vyžadované směnicí (EU) 2015/849;
- b) respondenční banka je součástí stejné skupiny jako korrespondenční banka, nemá sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu a účinně splňuje standardy skupiny v oblasti boje proti praní peněz, které nejsou méně přísné než standardy požadované směnicí EU 2015/849.

### Rizikové faktory zemí nebo zeměpisných oblastí

8.8. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Respondenční banka má sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu. Podniky by měly věnovat zvýšenou pozornost jurisdikcím
  - i. identifikovaným jako vysoce rizikové třetí země podle čl. 9 odst. 2 směrnice (EU) 2015/849;
  - ii. se zvýšenou mírou korupce a/nebo jiných predikativních trestných činů praní peněz;
  - iii. bez dostatečné kapacity právního a soudního systému ke stíhání těchto trestných činů;
  - iv. s významnou úrovní financování terorismu nebo teroristické činnosti; nebo
  - v. bez účinného dohledu nad oblastí boje proti praní peněz a financování terorismu.

<sup>13</sup> Společné obecné pokyny podle článku 25 nařízení (EU) 2015/847 k opatřením, která by měli poskytovatelé platebních služeb přijmout při zjišťování chybějících nebo neúplných informací o plátcích nebo příjemcích, a k postupům, které by měli zavést v případě převodu peněžních prostředků, u něhož chybí požadované informace, ze dne 22. září 2017.

- b) Respondenční banka významně obchoduje s klienty, kteří mají sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu.
- c) Mateřský podnik respondenční banky má ústředí v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu nebo je zapsán do obchodního rejstříku této jurisdikce.

#### 8.9. Faktory, které by mohly přispět ke snížení rizika:

- a) Respondenční banka má sídlo v členském státě EHP.
- b) Respondenční banka má sídlo ve třetí zemi, která nemá požadavky v oblasti boje proti praní peněz a financování terorismu méně přísné než požadavky stanovené směrnicí EU 2015/849, a tyto požadavky účinně uplatňuje (ačkoliv by korespondenční banky měly vzít v úvahu, že tato skutečnost je neosvobozuje od uplatňování opatření zesílené hloubkové kontroly klienta stanovených v článku 19 směrnice (EU) 2015/849).

## Opatření

8.10. Všechny korespondenční banky by u respondenční banky, která je klientem korespondenční banky, měly při zohlednění míry rizika provádět opatření hloubkové kontroly klienta stanovená v článku 13 směrnice (EU) 2015/849. To znamená, že korespondenční banky by měly:

- a) Zjistit a ověřit totožnost respondenční banky a jejího skutečného majitele. Dále by měly korespondenční banky získat dostatečné informace o obchodní činnosti a pověsti respondenční banky, aby měly jistotu v tom, že riziko praní peněz související s respondenční bankou není vysoké. Korespondenční banky by měly zejména:
  - i. získat informace o vedení respondenční banky a pro účely prevence finanční trestné činnosti zvážit význam všech vazeb, které by vedení nebo vlastníci respondenční banky mohli mít na politicky exponovanou osobu nebo jiné vysoce rizikové osoby; a
  - ii. při zohlednění míry rizika zvážit, zda by bylo získání informací o hlavní obchodní činnosti respondenční banky, typech klientů, které získává, a o kvalitě jejích systémů a kontrol v oblasti boje proti praní peněz (včetně veřejně dostupných informací o všech nedávných donucovacích opatřeních nebo trestněprávních postizích za porušení povinností v oblasti boje proti praní peněz) přiměřené. Pokud je respondenční banka pobočkou, dceřným podnikem nebo přidruženou společností, měly by korespondenční banky rovněž zohlednit postavení, pověst a kontroly v oblasti boje proti praní peněz mateřského podniku.

- b) Zjistit a zdokumentovat povahu a účel poskytované služby, jakož i povinnosti každé instituce. Může to znamenat písemné vymezení rozsahu vztahu, jaké produkty budou dodány a jaké služby budou poskytnuty a jakým způsobem a kým lze použít korespondenční bankovní facility (zda mohou například být používány jinými bankami v rámci jejich vztahu k korespondenční bance).
  - c) Sledovat obchodní vztahy, včetně transakcí, s cílem zjistit změny v rizikovém profilu korespondenční banky a odhalit neobvyklé nebo podezřelé chování, včetně činností, které nejsou slučitelné s účelem poskytovaných služeb nebo které jsou v rozporu se závazky, které byly mezi korespondenční bankou a korespondenční bankou ujednány. Pokud korespondenční banka umožňuje klientům korespondenční banky přímý přístup k účtům (např. průběžným korespondenčním účtům nebo vnořeným účtům), měla by provádět zesílené průběžné sledování daného obchodního vztahu. Vzhledem k povaze korespondenčního bankovníctví je následná kontrola standardem.
  - d) Zajistit, aby informace o hloubkové kontrole klienta, které má k dispozici, byly aktuální.
- 8.11. Korespondenční banky musí rovněž zajistit, aby korespondenční banka neumožňovala používání svých účtů bankou bez fyzické přítomnosti v souladu s článkem 24 směrnice (EU) 2015/849. Může to znamenat i požádání korespondenční banky o potvrzení, že nejedná s bankami bez fyzické přítomnosti, a kontrolu příslušných úseků v politikách a postupech korespondenční banky nebo posouzení veřejně dostupných informací, například právních předpisů, které zakazují poskytování služeb bankám bez fyzické přítomnosti.
- 8.12. Směrnice (EU) 2015/849 nepožaduje, aby korespondenční banky uplatňovaly opatření hloubkové kontroly klienta na jednotlivé klienty korespondenční banky.
- 8.13. Korespondenční banky by měly vzít v úvahu, že dotazníky hloubkové kontroly klienta poskytované mezinárodními organizacemi nejsou v běžné formě vypracovány tak, aby umožňovaly korespondenčním bankám splnit jejich konkrétní povinnosti vyplývající ze směrnice (EU) 2015/849. Při zvažování použití těchto dotazníků by měly korespondenční banky posoudit, zda jim dostatečně umožní splnit jejich povinnosti vyplývající ze směrnice (EU) 2015/849, a v případě potřeby podniknout další kroky.

### **Respondenční banky se sídlem v zemích mimo EHP**

- 8.14. Při plnění povinnosti podle článku 19 směrnice (EU) 2015/849 v případě korespondenčního vztahu souvisejícího s prováděním plateb s korespondenční institucí ze třetí země by korespondenční banka měla kromě opatření hloubkové kontroly klienta uvedených v článku 13 směrnice (EU) 2015/849 uplatnit zvláštní opatření zesílené hloubkové kontroly klienta, avšak tato opatření může přizpůsobit při zohlednění míry rizika. Ve všech ostatních situacích by podniky měly uplatnit alespoň obecné pokyny 8.10 až 8.13.

- 8.15. Korespondenční banky musí každé z těchto opatření zesílené hloubkové kontroly klienta uplatnit na respondenční banky se sídlem v zemi mimo EHP, mohou však upravit rozsah těchto opatření při zohlednění míry rizika. Pokud si je například korespondenční banka na základě adekvátního průzkumu jista tím, že respondenční banka má sídlo v třetí zemi, která má účinný režim pro boj proti praní peněz a financování terorismu s účinným dohledem nad dodržováním těchto požadavků a u které neexistuje důvodné podezření, že strategie a postupy respondenční banky v oblasti boje proti praní peněz jsou nebo byly v nedávné době považovány za nedostatečné, pak se nemusí nezbytně provádět podrobné posuzování kontrol v oblasti boje proti praní peněz respondenční banky.
- 8.16. Korespondenční banky by měly vždy opatření hloubkové kontroly klienta a zesílené hloubkové kontroly klienta a rozhodovací procesy dostatečně zdokumentovat.
- 8.17. V souladu s článkem 19 směrnice (EU) 2015/849 by přijatá opatření zohledňující míru rizika měla podnikům umožnit, aby:
- a) shromáždily dostatek informací o této respondenční instituci, aby plně porozuměly povaze jejího podnikání a zjistily rozsah, v jakém je obchodní činnost korespondenční banky vlivem podnikání respondenční banky vystavena vyššímu riziku praní peněz. Mělo by to znamenat i přijetí kroků k pochopení a posouzení povahy rizik klientské základny respondenční banky (v případě potřeby dotazováním na klienty u respondenční banky) a druhů činností, které bude respondenční banka prostřednictvím korespondenčního účtu vykonávat.
  - b) z veřejně dostupných informací zjistily, jakou má instituce pověst a jak kvalitní je dohled. To znamená, že by korespondenční banka měla posoudit, do jaké míry si může být korespondenční banka jista, že nad respondenční bankou je prováděn adekvátní dohled v oblasti plnění jejích povinností souvisejících s bojem proti praní peněz. Korespondenčním bankám může při zjišťování napomoci mnoho veřejně dostupných zdrojů, například hodnocení vypracované Finančním akčním výborem nebo programy hodnocení finančního odvětví, které obsahují oddíly o účinném dohledu.
  - c) zhodnotily kontroly prováděné respondenční institucí s ohledem na boj proti praní peněz a financování terorismu. Z toho vyplývá, že korespondenční banka by měla provést kvalitativní posouzení kontrolního rámce pro boj proti praní peněz a financování terorismu respondenční banky, a nejenom získat kopii strategií a postupů v oblasti boje proti praní peněz respondenční banky. Toto posouzení by mělo být příslušně zdokumentováno. V souladu s přístupem založeným na posouzení míry rizika, pokud je riziko obzvláště vysoké a pokud je objem korespondenčních bankovních transakcí velký, měla by korespondenční banka uvážit návštěvy na místě a/nebo provádění ověřování, aby zajistila, že jsou strategie v oblasti boje proti praní peněz účinně prováděny.

- d) získaly souhlas od vrcholného vedení vymezeného v čl. 3 odst. 12 směrnice (EU) 2015/849 před navázáním nových korespondenčních vztahů a v případě, že vyvstanou podstatná nová rizika, například v důsledku toho, že země, ve které respondenční banka sídlí, je označena jako vysoce riziková v souladu s článkem 9 směrnice (EU) 2015/849. Členem vrcholného vedení, který uděluje souhlas, by neměl být člen vedení prosazující daný vztah a čím vyšší je riziko související s tímto vztahem, tím vyšší postavení by měl člen vrcholného vedení udělující souhlas zastávat. Korespondenční banky by měly vrcholné vedení informovat o vysoce rizikových korespondenčních bankovních vztazích a krocích, které korespondenční banka přijímá, aby bylo toto riziko účinně řízeno.
- e) zdokumentovaly povinnosti každé instituce. Není-li to již upraveno ve standardní smlouvě, korespondenční banky by měly uzavřít písemnou smlouvu obsahující přinejmenším následující:
- i. produkty a služby poskytované respondenční bance,
  - ii. jak a kdo může korespondenční bankovní služby používat (např. zda je mohou používat jiné banky prostřednictvím svého vztahu s respondenční bankou) a jaké má respondenční banka povinnosti v oblasti boje proti praní peněz a financování terorismu;
  - iii. jak bude korespondenční banka sledovat vztah, aby se ujistila, že respondenční banka plní svoje povinnosti vyplývající z této smlouvy (například prostřednictvím sledování transakcí ex post);
  - iv. informace, které by měly být na žádost korespondenční banky poskytnuty respondenční bankou (zejména za účelem sledování korespondenčního vztahu), a přiměřenou lhůtu, ve které by informace měly být poskytnuty (s přihlédnutím ke složitosti platebního nebo korespondenčního řetězce).
- f) s ohledem na průběžné korespondenční účty a vnořené účty dospěly k závěru, že respondenční úvěrová nebo finanční instituce ověřila totožnost klientů, kteří mají přímý přístup k účtům korespondenční instituce, prováděla jejich průběžnou hloubkovou kontrolu a že na vyžádání je korespondenční instituce schopna poskytnout relevantní údaje o hloubkové kontrole klienta. Korespondenční banky by měly získat od respondenční banky ujištění, že relevantní údaje lze na vyžádání poskytnout.

### Respondenční banky se sídlem v zemích EHP

- 8.18. Pokud má respondenční banka sídlo v zemi EHP, článek 19 směrnice (EU) 2015/849 se nepoužije. Korespondenční banka je však i v tomto případě povinna uplatnit opatření



hloubkové kontroly klienta při zohlednění míry rizika podle článku 13 směrnice (EU) 2015/849.

- 8.19. Pokud je riziko související s respondenční bankou se sídlem v členském státě EHP zvýšené, musí korespondenční banky uplatňovat opatření zesílené hloubkové kontroly klienta v souladu s článkem 18 směrnice (EU) 2015/849. V takovém případě by měly korespondenční banky zvážit uplatnění alespoň některých opatření zesílené hloubkové kontroly klienta popsaných v článku 19 směrnice (EU) 2015/849, zejména v čl. 19 písm. a) a b).

### **Respondenční banky usazené ve vysoce rizikových třetích zemích a korespondenční vztahy související s vysoce rizikovými třetími zeměmi**

- 8.20. Korespondenční banky by měly určit, který z jejich vztahů souvisí s vysoce rizikovými třetími zeměmi identifikovanými v souladu s čl. 9 odst. 2 směrnice (EU) 2015/849.
- 8.21. Korespondenční banky by v rámci svých standardních opatření hloubkové kontroly klienta měly rovněž určit pravděpodobnost toho, že respondenční banka iniciuje transakce související s vysoce rizikovými třetími zeměmi, včetně případů, kdy významná část vlastních klientů respondenční banky udržuje relevantní profesní nebo osobní vztahy s vysoce rizikovými třetími zeměmi.
- 8.22. Při plnění svých povinností podle článku 18a by podniky měly zajistit, že rovněž uplatňují článek 13 a 19 směrnice (EU) 2015/849.
- 8.23. Není-li podle posouzení korespondenční bankou riziko praní peněz a financování terorismu vyplývající ze vztahu s respondenční bankou obzvláště vysoké, korespondenční banky by měly být schopné splnit požadavky v čl. 18a odst. 1 uplatněním článku 13 a 19 směrnice (EU) 2015/849.
- 8.24. Při plnění povinností podle čl. 18a odst. 1 písm. c) směrnice (EU) 2015/849 by korespondenční banky měly uplatňovat obecný pokyn č. 8.17 písm. c) a pečlivě posoudit vhodnost strategií a postupů respondenční banky pro stanovení zdroje finančních prostředků a majetku klientů, provést kontroly na místě nebo kontroly vzorků, nebo podle potřeby respondenční banku požádat o doložení zákonného původu zdroje majetku nebo finančních prostředků určitého klienta.
- 8.25. Vyžadují-li členské státy, aby podniky uplatňovaly další opatření v souladu s čl. 18a odst. 2, korespondenční banky by měly uplatnit jedno nebo více z následujících opatření:
- a) zvýšit četnost kontrol informací potřebných k hloubkové kontrole klienta, které o respondenční bance mají, a četnost posuzování rizika spojeného s dotyčnou respondenční bankou;



- b) požadovat podrobnější posouzení kontrol respondenční banky v oblasti boje proti praní peněz a financování terorismu. V těchto situacích s vyšším rizikem by korespondenční banky měly zvážit přezkoumání nezávislé zprávy o auditu kontrol respondenční banky v oblasti boje proti praní peněz a financování terorismu, pohovor s kontrolorem dodržování předpisů, pověření třetí strany provedením přezkumu nebo provedení kontroly na místě.
- c) požadovat zesílené a důkladnější sledování. Sledování transakcí v reálném čase je jedním z opatření zesílené hloubkové kontroly klienta, která by banky měly zvážit v situacích, kdy je riziko praní peněz a financování terorismu obzvláště zvýšené. V rámci toho by korespondenční banky měly zvážit vedení průběžného dialogu s respondenční bankou, aby lépe pochopily rizika spojená s korespondenčním vztahem a v případě potřeby umožnily rychlou výměnu smysluplných informací.
- d) požadovat zesílené sledování převodů finančních prostředků s cílem zjistit chybějící nebo neúplné informace o plátcích nebo příjemcích na základě nařízení (EU) 2015/847 a v souladu se společnými obecnými pokyny JC/GL/2017/16.<sup>14</sup>
- e) po důkladném posouzení zbytkového rizika spojeného s korespondenčním vztahem omezit obchodní vztahy nebo transakce související s vysoce rizikovými třetími zeměmi z hlediska povahy, objemu nebo způsobu platby.

---

<sup>14</sup> Společné obecné pokyny podle článku 25 nařízení (EU) 2015/847 k opatřením, která by měli poskytovatelé platebních služeb přijmout při zjišťování chybějících nebo neúplných informací o plátcích nebo příjemcích, a k postupům, které by měli zavést v případě převodu peněžních prostředků, u něhož chybí požadované informace, ze dne 22. září 2017 (JC/GL/2017/16).

## Obecný pokyn č. 9: Odvětvový pokyn pro retailové banky

- 9.1. Pro účely těchto pokynů se „retailovým bankovníctvím“ rozumí poskytování bankovních služeb fyzickým osobám a malým a středním podnikům. Produkty a službami retailového bankovníctví jsou například běžné účty, hypotéky, spořicí účty, spotřebitelské a termínované půjčky a úvěrové linky.
- 9.2. Vzhledem k povaze nabízených produktů a služeb, poměrně snadné dostupnosti a často velkému objemu transakcí a obchodních vztahů je retailové bankovníctví financováním terorismu a všemi fázemi procesu praní peněz ohroženo. Objem obchodních vztahů a transakcí souvisejících s retailovým bankovníctvím může zároveň identifikování rizika praní peněz a financování terorismu souvisejícího s jednotlivými vztahy a odhalení podezřelých transakcí velmi znesnadňovat.
- 9.3. Banky by měly zohlednit, kromě rizikových faktorů a opatření uvedených v hlavě I těchto pokynů, následující rizikové faktory a opatření. Banky, které poskytují služby iniciování plateb nebo služby informování o účtu, by měly použít také odvětvový pokyn č. 18.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 9.4. Faktory, které by mohly přispět ke zvýšení rizika:
  - a) vlastnosti produktu napomáhají anonymitě;
  - b) produkt umožňuje platby od třetích stran, které nejsou s produktem nijak spojeny, ani nebyly zjištěny předem, jelikož se takové platby neočekávaly, například v případě hypoték nebo úvěrů;
  - c) produkt nijak neomezuje obrat, přeshraniční transakce nebo podobné vlastnosti produktu;
  - d) nové produkty a nové obchodní postupy, včetně nových distribučních systémů, a použití nových nebo rozvíjejících se technologií pro nové i již existující produkty, které ještě nejsou dobře prostudovány;
  - e) úvěry (včetně hypoték) zajištěné hodnotou aktiv v jiných jurisdikcích, zejména v zemích, kde je obtížné zjistit, zda má klient na zajištění zákonný nárok, nebo kde je obtížné ověřit totožnost stran ručících za úvěr;
  - f) neobvykle velký objem nebo vysoká hodnota transakcí.
- 9.5. Faktory, které by mohly přispět ke snížení rizika:

- a) Produkt má omezené funkce, například v případě, kdy se jedná o:
  - i. spořicí produkt s pevně stanovenou dobou splatnosti s nízkými limity úspor;
  - ii. produkt, u něhož plnění nemůže být uskutečněno ve prospěch třetí osoby;
  - iii. produkt, u něhož je plnění uskutečňováno v dlouhodobém měřítku nebo za určitým účelem, jako je odchod do důchodu nebo nákup nemovitosti;
  - iv. úvěr o nízké hodnotě, včetně úvěru, jehož čerpání je podmíněno koupí určitého spotřebního zboží nebo služby; nebo
  - v. produkt o nízké hodnotě, včetně pronájmu, u kterého není právní ani majetkový nárok na majetek převeden na klienta, dokud není smluvní vztah ukončen, nebo nebude nikdy převeden.
- b) Produkt mohou využívat pouze určité kategorie klientů, například důchodci, rodiče jménem svých dětí nebo nezletilé osoby, dokud nedosáhnou plnoletého věku.
- c) Transakce musí být prováděny prostřednictvím účtu vedeného na klientovo jméno u úvěrové nebo finanční instituce, na kterou se vztahují požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky stanovené směrnicí (EU) 2015/849.
- d) Nejsou umožněny přeplatky.

### Rizikové faktory klienta

#### 9.6. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Povaha klienta, například:
  - i. Klient je podnikem, který ve velké míře využívá hotovost.
  - ii. Klient je podnikem spojeným s vyšším rizikem praní peněz, například určité subjekty zabývající se poukazováním peněz a podniky zabývající se hazardními hrami.
  - iii. Klient je podnikem spojeným s vyšším rizikem korupce, působícím například v těžebním průmyslu nebo obchodu se zbraněmi.
  - iv. Klient je neziskovou organizací, která podporuje jurisdikce spojené se zvýšeným rizikem financování terorismu.
  - v. Klient je novým podnikem bez adekvátního obchodního profilu nebo záznamů.

- vi. Klient je nerezidentem. Banky by měly vzít na vědomí, že článek 16 směrnice 2014/92/EU zakládá klientům, kteří oprávněně pobývají v Unii, právo na založení základního platebního účtu, avšak toto právo otevřít si a používat základní platební účet platí pouze v rozsahu, v jakém mohou úvěrové banky dostát svým povinnostem v oblasti boje proti praní peněz a financování terorismu, a neosvobozuje banky od jejich povinnosti identifikovat a posuzovat riziko praní peněz a financování terorismu, včetně rizika souvisejícího s klientem, který není rezidentem členského státu, ve kterém má banka sídlo.<sup>15</sup>
- vii. Skutečného majitele klienta nelze snadno identifikovat, například proto, že vlastnická struktura klienta je neobvyklá, příliš složitá nebo netransparentní nebo proto, že klient vydává akcie na doručitele.

b) Chování klienta, například:

- i. Klient se zdráhá poskytnout informace potřebné pro hloubkovou kontrolu klienta nebo vyvolává dojem, že se záměrně vyhýbá osobnímu kontaktu.
- ii. Doklad o totožnosti klienta je bez zjevného důvodu v nestandardní formě.
- iii. Chování klienta nebo objem transakcí neodpovídá očekáváním u dané kategorie klientů, ke kterým patří, nebo je neočekávané ve srovnání s informacemi, které klient poskytl při otevírání účtu.
- iv. Chování klienta je neobvyklé, klient například neočekávaně a bez rozumného vysvětlení urychluje dohodnutý splátkový kalendář buď formou jednorázových splátek, nebo předčasným ukončením smlouvy; bez zjevného důvodu činí vklady nebo požaduje výplatu bankovek s vysokou hodnotou; zvyšuje svou aktivitu po období klidového režimu nebo provádí transakce bez zjevných ekonomických důvodů.

9.7. Tento faktor by mohl přispět ke snížení rizika:

- a) Klient je dlouholetým klientem, jehož předchozí transakce nevzbuzovaly podezření nebo obavy, a požadovaný produkt nebo služba jsou v souladu s rizikovým profilem klienta.

### Rizikové faktory zemí nebo zeměpisných oblastí

9.8. Faktory, které by mohly přispět ke zvýšení rizika:

<sup>15</sup> Viz stanovisko Evropského orgánu pro bankovníctví o uplatňování opatření hloubkové kontroly klienta na klienty, kteří jsou žadateli o azyl z vysoce rizikových třetích zemí nebo území: <http://www.eba.europa.eu/documents/10180/1359456/EBA-Op-2016-07+%28Opinion+on+Customer+Due+Diligence+on+Asylum+Seekers%29.pdf>

- a) Finanční prostředky klienta plynou z osobních nebo obchodních vazeb na jurisdikce spojené s vyšším rizikem praní peněz a financování terorismu.
- b) Příjemce se nachází v jurisdikci související s vyšším rizikem praní peněz a financování terorismu. Podniky by měly věnovat zvýšenou pozornost jurisdikcím, o nichž je známo, že financují nebo podporují teroristické aktivity nebo že v nich působí skupiny páchající teroristické činy, a jurisdikcím, na něž se vztahují finanční sankce, embarga nebo opatření související s terorismem, financováním terorismu nebo šířením zbraní.

9.9. Tento faktor by mohl přispět ke snížení rizika:

- a) Země spojené s transakcí mají režim pro boj proti praní peněz a financování terorismu, který není méně přísný než režim vyžadovaný směrnici (EU) 2015/849, a jsou spojeny s nízkou úrovní predikativních trestných činů.

### Rizikové faktory související s distribučními kanály

9.10. Faktory, které by mohly přispět ke zvýšení rizika:

- a) obchodní vztahy bez osobní přítomnosti partnera, pokud neexistují náležitá dodatečná bezpečnostní opatření – například elektronické podpisy, elektronické identifikační certifikáty vydané v souladu s nařízením (EU) č. 910/2014 a kontroly za účelem odhalení podvodů týkajících se zneužití totožnosti;
- b) spoléhání se na opatření hloubkové kontroly klienta třetí osoby v situacích, kdy banka nemá s dotyčnou třetí osobou dlouhodobý vztah;
- c) nové distribuční kanály, které ještě nebyly vyzkoušeny.

9.11. Tento faktor by mohl přispět ke snížení rizika:

- a) Produkt je dostupný pouze pro klienty, kteří splňují konkrétní kritéria způsobilosti stanovená vnitrostátními orgány veřejné moci, jako v případě příjemců státní podpory nebo určitých spořicíh produktů pro děti registrované v určitém členském státě.

## Opatření

9.12. Pokud banky používají k identifikaci rizika praní peněz a financování terorismu spojeného s jednotlivými obchodními vztahy nebo příležitostnými transakcemi a k odhalení podezřelých transakcí automatizované systémy, měly by zajistit, aby tyto systémy odpovídaly účelům podle kritérií stanovených v hlavě I. Použití automatizovaných

informačních systémů by nikdy nemělo být považováno za náhradu ostražitosti zaměstnanců.

### Zesílená hloubková kontrola klienta

9.13. Pokud je riziko související s obchodním vztahem nebo příležitostnou transakcí vysoké, musí banky uplatňovat opatření zesílené hloubkové kontroly klienta v souladu s článkem 18 směrnice (EU) 2015/849. Mezi tato opatření patří:

- a) Ověření totožnosti klienta a skutečného majitele na základě více než jednoho spolehlivého a nezávislého zdroje.
- b) Zjištění a ověření totožnosti ostatních akcionářů či společníků, kteří nejsou skutečnými majiteli klienta nebo fyzickými osobami, které mají pravomoc používat účet nebo dávat pokyny týkající se převodu finančních prostředků nebo převodu cenných papírů.
- c) Získání více informací o klientovi a povaze a účelu daného obchodního vztahu s cílem vypracovat úplnější profil klienta, například vyhledáváním negativních zpráv v otevřených zdrojích nebo médiích nebo ze zpravodajských hlášení třetích osob. Příklady typu informací, které mohou banky požadovat, zahrnují:
  - i. povahu podnikání nebo zaměstnání klienta;
  - ii. zdroj majetku klienta a zdroj finančních prostředků klienta, který je zapojen do obchodního vztahu, aby měly banky jistotu, že je legální;
  - iii. účel transakce, včetně případného místa určení finančních prostředků klienta;
  - iv. informace o všech vazbách, které by klient mohl mít na jiné jurisdikce (ústředí, provozní zařízení, pobočky apod.) a osoby, které by mohly ovlivnit jeho činnost; nebo
  - v. pokud má klient sídlo v jiné zemi, proč požaduje služby retailového bankovníctví mimo svou domovskou jurisdikci.
- d) Zvýšení četnosti sledování transakcí.
- e) Častější přezkumy a případné aktualizace informací a dokumentace. Pokud je riziko související s tímto vztahem obzvláště vysoké, měly by banky vyhodnocovat daný obchodní vztah každý rok.

9.14. Pokud jde o obchodní vztahy nebo transakce související s vysoce rizikovými třetími zeměmi, banky by se měly řídit obecnými pokyny v hlavě I.

### Zjednodušená hloubková kontrola klienta

9.15. V situacích s nízkým rizikem a v rozsahu, který dovolují vnitrostátní právní předpisy, mohou banky uplatňovat opatření zjednodušené hloubkové kontroly klienta, která mohou zahrnovat:

- a) u klientů, na které se vztahuje zákonný licenční a regulační režim, ověření totožnosti prokázáním, že se na klienta tento režim vztahuje, například prostřednictvím vyhledávání ve veřejném rejstříku regulačního orgánu;
- b) ověření totožnosti klienta a případně jeho skutečného majitele při uzavření obchodního vztahu v souladu s čl. 14 odst. 2 směrnice (EU) 2015/849;
- c) za předpokladu, že platba čerpaná z účtu samostatným nebo společným jménem klienta u regulované úvěrové nebo finanční instituce v zemi EHP splňuje požadavky stanovené v čl. 13 odst. 1 písm. a) a b) směrnice (EU) 2015/849;
- d) přijetí jiných dokladů k prokázání totožnosti, které splňují kritérium nezávislého a spolehlivého zdroje dle čl. 13 odst. 1 písm. a) směrnice (EU) 2015/849, například dopis od vládní agentury nebo jiného spolehlivého veřejného orgánu klientovi, má-li klient přiměřené důvody pro neposkytnutí standardního dokladu totožnosti a za předpokladu, že neexistují důvody k podezření;
- e) aktualizace informací hloubkové kontroly klienta pouze v případě konkrétních rozhodných událostí, například požaduje-li klient nový produkt nebo produkt s vyšším rizikem, nebo při změnách v chování nebo v transakčním profilu klienta, které naznačují, že riziko související s tímto vztahem již není nízké.

### Sdružené účty („pooled accounts“)

9.16. Pokud si klient banky otevře „sdružený účet“ za účelem správy finančních prostředků, které patří jeho klientům, měla by banka uplatnit opatření hloubkové kontroly klienta v plném rozsahu a jednat s jeho klienty jako se skutečnými majiteli finančních prostředků držených na sdruženém účtu a ověřit jejich totožnost.

9.17. Pokud existují náznaky, že riziko související s daným obchodním vztahem je vysoké, musí banky podle potřeby uplatnit opatření zesílené hloubkové kontroly klienta stanovená v článku 18 směrnice (EU) 2015/849.

9.18. Nicméně v rozsahu, který dovolují vnitrostátní právní předpisy, a pokud je riziko související s obchodním vztahem nízké a za podmínek uvedených níže, může banka uplatnit opatření zjednodušené hloubkové kontroly klienta za předpokladu, že:

- a) Klient je podnikem, na který se vztahují povinnosti v oblasti boje proti praní peněz a financování terorismu v zemi EHP nebo ve třetí zemi s režimem pro boj proti praní peněz a financování terorismu, které nejsou méně přísné než povinnosti uložené směrnicí (EU) 2015/849, a podléhá účinnému dohledu nad dodržováním těchto požadavků.
- b) Klient není podnikem, nýbrž jinou povinnou osobou, na kterou se vztahují povinnosti v oblasti boje proti praní peněz a financování terorismu v zemi EHP a která podléhá účinnému dohledu nad dodržováním těchto požadavků.
- c) Riziko praní peněz a financování terorismu související s obchodním vztahem je nízké mimo jiné dle posouzení bankou obchodní činnosti klienta, typů klientů, na které se obchodní činnost klienta zaměřuje, a jurisdikce, které obchodní činnost klienta podléhá;
- d) banka je přesvědčena o tom, že klient uplatňuje přísná opatření hloubkové kontroly klienta zohledňující míru rizika na své vlastní klienty a skutečné majitele svých klientů (banka může přijmout opatření zohledňující míru rizika, aby posoudila přiměřenost klientových strategií a postupů hloubkové kontroly klienta, například přímým jednáním s daným klientem); a
- e) banka přijala kroky zohledňující míru rizika, aby se ujistila, že klient poskytuje informace o hloubkové kontrole klienta a dokumenty týkající se jeho klientů, kteří jsou skutečnými majiteli finančních prostředků držných na sdruženém účtu okamžitě na vyžádání, například zahrnutím příslušných ustanovení do smlouvy s klientem nebo ověřováním schopnosti klienta poskytovat na vyžádání informace o hloubkové kontrole klienta.

9.19. Pokud jsou splněny podmínky pro uplatňování zjednodušené hloubkové kontroly klienta na sdružené účty, mohou opatření zjednodušené hloubkové kontroly klienta banky zahrnovat:

- a) zjištění a ověření totožnosti klienta, včetně skutečných majitelů klienta (nikoliv však klientových klientů);
- b) posouzení účelu a zamýšlené povahy obchodního vztahu; a
- c) průběžné sledování obchodního vztahu.

### **Klienti, kteří nabízejí služby týkající se virtuálních měn**

9.20. Podniky by měly vzít v úvahu skutečnost, že kromě poskytovatelů podílejících se na směnárenských službách mezi virtuální měnou a měnami s nuceným oběhem a poskytovatelů virtuálních peněženek, kteří jsou povinnými osobami podle směrnice (EU) 2015/849, zůstává vydávání nebo držení virtuálních měn podle vymezení v čl. 3 odst. 18



směrnice (EU) 2015/849 v EU do značné míry neregulované, což zvyšuje rizika praní peněz a financování terorismu. Podniky se mohou odvolat na zprávu EBA o kryptoaktivech z ledna 2019.

- 9.21. Při navazování obchodního vztahu s klienty, kteří poskytují služby týkající se virtuálních měn, by podniky v rámci svého posouzení rizika praní peněz a financování terorismu spojeného s klientem měly zvážit riziko praní peněz a financování terorismu spojeného s virtuálními měnami.
- 9.22. Podniky by měly za obchodní činnosti související s virtuálními měnami považovat mimo jiné následující:
- a) provozování platformy pro obchodování s virtuálními měnami, která provádí směnu mezi měnou s nuceným oběhem a virtuální měnou;
  - b) provozování platformy pro obchodování s virtuálními měnami, která provádí směnu mezi virtuálními měnami;
  - c) provozování platformy pro obchodování s virtuálními měnami, která umožňuje přímé (peer-to-peer) transakce;
  - d) poskytování služeb virtuální peněženky;
  - e) zařízení „prvotní nabídky kryptoměny“ (ICO), související poradenství nebo prospěch z prvotní nabídky kryptoměny.
- 9.23. Za účelem zmírnění úrovně rizika praní peněz a financování terorismu spojeného s těmito klienty by banky neměly uplatňovat opatření zjednodušené hloubkové kontroly klienta. Podniky by v rámci svých opatření hloubkové kontroly klienta měly přinejmenším:
- a) zahájit s klientem dialog, jehož účelem je pochopit povahu obchodní činnosti a související rizika praní peněz a financování terorismu;
  - b) kromě ověření totožnosti skutečných majitelů klienta provést hloubkovou kontrolu vrcholného vedení, pokud se liší od skutečných majitelů, včetně zohlednění případných nepříznivých informací;
  - c) pochopit, do jaké míry tito klienti u svých klientů na základě zákonné povinnosti nebo dobrovolně uplatňují vlastní opatření hloubkové kontroly klienta.
  - d) zjistit, zda je klient registrován nebo licencován v členském státě EHP nebo ve třetí zemi, a vyhodnotit přiměřenost režimu dotyčné třetí země pro boj proti praní peněz a financování terorismu;

- e) zjistit, zda jsou podniky používající prvotní nabídky kryptoměny ve formě virtuálních měn k získání peněžních prostředků legitimní a případně regulované.

9.24. V případě zvýšeného rizika spojeného s těmito klienty by banky měly uplatnit opatření zesílené hloubkové kontroly klienta v souladu s hlavou I.

## Obecný pokyn č. 10: Odvětvový pokyn pro vydavatele elektronických peněz

- 10.1. Obecný pokyn č. 10 obsahuje pokyny pro vydavatele elektronických peněz definované v čl. 2 odst. 3 směrnice 2009/110/ES. Míra rizika praní peněz a financování terorismu související s elektronickými penězi podle vymezení v čl. 2 odst. 2 směrnice 2009/110/ES závisí především na vlastnostech jednotlivých produktů elektronických peněz a na tom, do jaké míry vydavatelé elektronických peněz využívají jiných osob k distribuci a zpětné výměně elektronických peněz jejich jménem v souladu s čl. 3 odst. 4 směrnice 2009/110/ES.
- 10.2. Podniky, které vydávají elektronické peníze, by měly, vedle rizikových faktorů a opatření uvedených v hlavě I těchto obecných pokynů, zohlednit následující rizikové faktory a opatření. Podniky, jejichž povolení zahrnuje poskytování obchodních činností, jako jsou služby iniciování plateb a služby informování o účtu, by se měly rovněž řídit odvětvovým pokynem č. 18. V tomto ohledu může být také relevantní odvětvový pokyn č. 11 pro subjekty zabývající se poukazováním peněz.

### Rizikové faktory

#### Rizikové faktory produktů

- 10.3. Vydavatelé elektronických peněz by měli zohlednit riziko praní peněz a financování terorismu související s:
- a) limity;
  - b) způsobem financování; a
  - c) prospěšností a obchodovatelností.
- 10.4. Faktory, které by mohly přispět ke zvýšení rizika:
- a) Limity: produkt umožňuje
    - i. platby, nabití nebo zpětnou výměnu o vysoké hodnotě nebo neomezené hodnotě, včetně výběru hotovosti;
    - ii. vysoký počet plateb, nabití nebo zpětných výměn, včetně výběru hotovosti;
    - iii. ukládání vysokých nebo neomezených částek finančních prostředků na produkt/účet elektronických peněz.
  - b) Způsob financování: produkt může být

- i. dobíjen anonymně, například za hotovost; získání elektronických peněz nebo produktů elektronických peněz, na které se vztahuje osvobození podle článku 12 směrnice (EU) 2015/849;
  - ii. financován z plateb od nezjištěných třetích osob;
  - iii. financován prostřednictvím jiných produktů elektronických peněz.
- c) Prospěšnost a obchodovatelnost: produkt
- i. umožňuje transfery plateb mezi osobami;
  - ii. je přijímán jako platební prostředek velkým počtem obchodníků nebo prodejních míst;
  - iii. je vyvinut tak, aby byl přijímán jako platební prostředek obchodníky obchodujícími se zbožím a službami spojenými s vysokým rizikem finanční trestné činnosti, například hazardních her poskytovaných online;
  - iv. lze využít pro přeshraniční transakce nebo v různých jurisdikcích;
  - v. je vyvinut pro použití jinými osobami než klientem, například některé produkty partnerských karet (nikoliv však dárkové poukazy o nízké hodnotě);
  - vi. umožňuje výběr hotovosti o vysoké hodnotě.

#### 10.5. Faktory, které by mohly přispět ke snížení rizika:

- a) Limity: produkt
- i. stanovuje nízké limity pro platby, nabití nebo zpětnou výměnu, včetně výběru hotovosti (podniky by však měly vzít v úvahu, že nízký limit nemusí postačovat ke snížení rizika financování terorismu);
  - ii. omezuje počet plateb, nabití nebo zpětných výměn, včetně výběru hotovosti v daném období;
  - iii. omezuje množství finančních prostředků, které lze kdykoliv na produkt/účet elektronických peněz ukládat.
- b) Financování: produkt
- i. vyžaduje, aby finanční prostředky na nákup nebo opětovné nabití byly ověřitelně čerpány z účtu vedeného pod samostatným nebo společným jménem klienta u úvěrové nebo finanční instituce EHP;

- c) Prospěšnost a obchodovatelnost: produkt
- i. neumožňuje nebo přísně omezuje výběr hotovosti;
  - ii. lze použít pouze na domácím trhu;
  - iii. je přijímán omezeným počtem obchodníků nebo prodejních míst, jejichž obchodní činnost je vydavateli elektronických peněz známa;
  - iv. je vyvinut tak, aby omezoval jeho využívání obchodníky obchodujícími se zbožím a službami, které jsou spojeny s vysokým rizikem finanční trestné činnosti;
  - v. je přijímán jako platební prostředek u omezených typů služeb nebo produktů s nízkým rizikem.

### Rizikové faktory klienta

#### 10.6. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Klient nakupuje několik produktů elektronických peněz od stejného vydavatele, často produkt opětovně nabíjí nebo provádí několik hotovostních výběrů za krátkou dobu a bez ekonomického důvodu; jsou-li distributoři (nebo zástupci, kteří vystupují jako distributoři) sami povinnými subjekty, platí to i pro produkty elektronických peněz od různých vydavatelů zakoupené od stejného distributora.
- b) Transakce klienta jsou vždy těsně pod limity hodnot/transakcí.
- c) Zdá se, že produkt používá několik lidí, jejichž totožnost není vydavateli známa (produkt je například používán z několika IP adres najednou).
- d) Často se mění identifikační údaje klienta, například adresa bydliště nebo IP adresa nebo propojené bankovní účty.
- e) Produkt se nepoužívá pro účely, pro které byl určen, je například používán v zámorí, přičemž byl navržen jako dárkový poukaz nákupního střediska.

#### 10.7. Tento faktor by mohl přispět ke snížení rizika:

- a) Produkt je k dispozici pouze určitým kategoriím klientů, například příjemcům sociálních dávek nebo zaměstnancům společnosti, která je vydává k pokrytí výdajů na obchodní činnost.

### Rizikové faktory související s distribučními kanály

#### 10.8. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Distribuce on-line a distribuce bez osobní přítomnosti partnera a bez určitých bezpečnostních opatření, jako jsou elektronické podpisy, elektronické identifikační prostředky splňující kritéria stanovená v nařízení (EU) č. 910/2014 a opatření za účelem odhalení podvodů týkajících se zneužití totožnosti.
- b) Distribuce prostřednictvím zprostředkovatelů, kteří sami nejsou povinnými osobami podle směrnice (EU) 2015/849 nebo případně podle vnitrostátních právních předpisů, pokud vydavatel elektronických peněz:
  - i. spoléhá na zprostředkovatele, aby vykonával některé povinnosti vydavatele elektronických peněz v oblasti boje proti praní peněz a financování terorismu;
  - ii. není přesvědčen o tom, že zprostředkovatel má zavedeny adekvátní systémy a kontroly v oblasti boje proti praní peněz a financování terorismu; a
  - iii. segmentace služeb, to znamená poskytování služeb elektronických peněz několika provozně nezávislými poskytovateli služeb bez řádného dohledu a koordinace.

10.9. Podniky by před podepsáním distribuční smlouvy s obchodníkem měly pochopit povahu a účel obchodní činnosti obchodníka, aby se ujistily, že zboží a poskytované služby jsou zákonné, a posoudily riziko praní peněz a financování terorismu související s obchodní činností obchodníka. V případě on-line obchodníka by podniky měly také učinit kroky, aby pochopily, jaký typ klientů tento obchodník přitahuje, a určily očekávaný objem a velikost transakcí, a mohly tak rozpoznat podezřelé nebo neobvyklé transakce.

### **Rizikové faktory zemí nebo zeměpisných oblastí**

10.10. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Příjemce se nachází v jurisdikci související s vyšším rizikem praní peněz a financování terorismu a/nebo je produkt vydán nebo financován finančními prostředky ze zdrojů v takové jurisdikci. Podniky by měly věnovat zvýšenou pozornost jurisdikcím, o nichž je známo, že financují nebo podporují teroristické aktivity nebo že v nich působí skupiny páchající teroristické činy, a jurisdikcím, na něž se vztahují finanční sankce, embarga nebo opatření související s terorismem, financováním terorismu nebo šířením zbraní.

## **Opatření**

### **Opatření hloubkové kontroly klienta**

10.11. Podniky by měly uplatňovat opatření hloubkové kontroly klienta na:

- a) majitele elektronického peněžního účtu nebo produktu; a
- b) další držitele karet. Jsou-li produkty spojeny s více kartami, podniky by měly určit, zda uzavřely jeden obchodní vztah nebo více obchodních vztahů a zda by další držitelé karet mohli být skutečnými majiteli.

10.12. Vnitrostátní právní předpisy mohou stanovit osvobození od zjišťování a ověřování totožnosti klientů a skutečných majitelů a posouzení povahy a účelu obchodního vztahu u některých produktů elektronických peněz v souladu s článkem 12 směrnice (EU) 2015/849.

10.13. Podniky by měly vzít v úvahu, že osvobození podle článku 12 směrnice (EU) 2015/849 se nevztahuje na povinnost provádět průběžné sledování transakcí a obchodních vztahů, ani je neosvobozuje od povinnosti zjistit a oznámit podezřelé transakce; to znamená, že by podniky měly zajistit, aby získaly dostatek informací o svých klientech nebo o typech klientů, na které se jejich produkty budou zaměřovat, aby mohly provádět smysluplné průběžné sledování obchodních vztahů.

10.14. Mezi příklady typů systémů sledování, které by podniky měly zavést, patří:

- a) systémy sledování transakcí, které odhalují odchylky nebo podezřelé vzorce chování, včetně neočekávaného použití produktu způsobem, pro nějž nebyl určen; podnik může být schopen produkt deaktivovat buď manuálně, nebo prostřednictvím čipu, dokud se nepřesvědčí o tom, že důvody k podezření neexistují;
- b) systémy, které odhalují nesrovnalosti mezi předloženými a zjištěnými informacemi, například mezi předloženými informacemi o zemi původu a elektronicky zaznamenanou IP adresou;
- c) systémy, které porovnávají předložené údaje s údaji z jiných obchodních vztahů a které tak mohou identifikovat vzorce, například stejný nástroj financování nebo stejné kontaktní údaje;
- d) systémy, které odhalují, zda je produkt používán obchodníky obchodujícími se zbožím a službami, které jsou spojeny s vysokým rizikem finanční trestné činnosti;
- e) systémy, které spojují elektronické peněžní produkty se zařízeními nebo IP adresami pro webové transakce.

### Zesílená hloubková kontrola klienta

10.15. V souladu s článkem 18a by vydavatelé elektronických peněz měli u vztahů nebo transakcí souvisejících s vysoce rizikovými třetími zeměmi uplatňovat opatření zesílené hloubkové kontroly klienta stanovená v tomto ohledu v hlavě I.

10.16. Mezi příklady opatření zesílené hloubkové kontroly klienta, který by podniky měly uplatňovat ve všech ostatních vysoce rizikových situacích, patří:

- a) získávání dalších informací o klientech při zjišťování totožnosti, například o zdroji finančních prostředků;
- b) uplatňování dalších opatření při ověřování totožnosti z většího rozsahu spolehlivých a nezávislých zdrojů (např. porovnání podle on-line databází) s cílem ověřit totožnost klienta nebo skutečného majitele;
- c) získávání dalších informací o zamýšlené povaze obchodního vztahu, například dotazováním klientů na jejich podnikání nebo na jurisdikci, do níž hodlají elektronické peníze převádět;
- d) získávání informací o obchodníkovi/příjemci, zejména v případě, kdy má vydavatel elektronických peněz důvodné podezření, že jsou jeho produkty používány k nákupu nezákonného zboží nebo zboží, které je dovoleno od určité věkové hranice;
- e) provádění kontrol za účelem odhalení podvodů týkajících se zneužití totožnosti, aby bylo zajištěno, že klient je osobou, kterou tvrdí, že je;
- f) provádění zesíleného sledování vztahů s klienty a jednotlivých transakcí;
- g) zjištění zdroje a/nebo místa určení finančních prostředků.

### **Zjednodušená hloubková kontrola klienta**

10.17. V rozsahu, který dovolují vnitrostátní právní předpisy, mohou podniky zvážit uplatnění zjednodušené hloubkové kontroly klienta na produkty elektronických peněz s nízkým rizikem, které nejsou osvobozeny podle článku 12 směrnice (EU) 2015/849.

10.18. V rozsahu, který dovolují vnitrostátní právní předpisy, patří mezi příklady opatření zjednodušené hloubkové kontroly klienta, která mohou podniky uplatňovat v situacích s nízkým rizikem, například:

- a) odložení ověření totožnosti klienta nebo skutečného majitele na určitý pozdější den po uzavření vztahu nebo do překročení určitého (nízkého) peněžního limitu (podle toho, která ze skutečností nastane dříve). Peněžní limit by neměl být vyšší než 150 EUR, jestliže produkt není dobíjecí nebo může být používán v jiných jurisdikcích nebo pro přeshraniční transakce;



- b) ověření totožnosti klienta na základě platby provedené z účtu vedeného pod samostatným nebo společným jménem klienta nebo z účtu, u něhož může klient prokázat, že je pod kontrolou regulované úvěrové nebo finanční instituce v EHP;
- c) ověření totožnosti na základě menšího počtu zdrojů;
- d) ověření totožnosti na základě méně spolehlivých zdrojů;
- e) použití alternativních metod k ověření totožnosti;
- f) předpokládání povahy a zamýšleného účelu obchodního vztahu, je-li to zřejmé, například v případě některých dárkových poukazů, na které se nevztahuje osvobození podle „uzavřené smyčky“ nebo „uzavřené sítě“;
- g) snížení intenzity sledování, dokud není dosaženo určitého peněžního limitu. Vzhledem k tomu, že průběžné sledování je v průběhu vztahu s klientem důležitým prostředkem pro získání více informací o rizikových faktorech klienta (viz výše), měl by být tento limit jak pro jednotlivé transakce, tak pro transakce, které se zdají být v průběhu 12 měsíců propojeny, nastaven na úroveň, kterou podnik vyhodnotil jako nízko rizikovou jak pro účely financování terorismu, tak pro účely praní peněz.

## Obecný pokyn č. 11: Odvětvový pokyn pro subjekty zabývající se poukazováním peněz

- 11.1. Subjekty zabývající se poukazováním peněz jsou platební instituce, instituce elektronických peněz nebo úvěrové instituce, které jsou v souladu se směrnicí (EU) 2015/2366 oprávněny poskytovat a provádět platební služby v celé EU. Podniky jsou v tomto odvětví různorodé a mohou to být jednotlivé podniky i složití řetězoví provozovatelé.
- 11.2. Mnoho subjektů zabývajících se poukazováním peněz využívá k poskytování platebních služeb zástupce jednající jejich jménem. Zástupci často poskytují platební služby na podporu své hlavní obchodní činnosti a nemohou být podle platných právních předpisů v oblasti boje proti praní peněz a financování terorismu sami povinnými osobami; rovněž jejich odborné znalosti v oblasti boje proti praní peněz a financování terorismu mohou být omezené.
- 11.3. Povaha poskytované služby může subjekty zabývající se poukazováním peněz vystavit riziku praní peněz a financování terorismu. Je to způsobeno jednoduchostí a rychlostí transakcí, jejich celosvětovým dosahem a jejich častým hotovostním charakterem. Z povahy této platební služby navíc vyplývá, že subjekty zabývající se poukazováním peněz často spíše provádějí příležitostné transakce, než by uzavírali obchodní vztahy se svými klienty, z čehož vyplývá, že jejich znalost rizika praní peněz a financování terorismu souvisejícího s klienty může být omezená.
- 11.4. Subjekty zabývající se poukazováním peněz by měly, kromě rizikových faktorů a opatření uvedených v hlavě I těchto obecných pokynů, zohlednit následující rizikové faktory a opatření. Podniky, jejichž povolení zahrnuje poskytování obchodních činností, jako jsou služby iniciování plateb a služby informování o účtu, by se měly rovněž řídit odvětvovým pokynem č. 18.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 11.5. Faktory, které by mohly přispět ke zvýšení rizika:
  - a) produkt umožňuje transakce o vysoké hodnotě nebo neomezené hodnotě;
  - b) produkt nebo služba má celosvětový dosah;
  - c) transakce je prováděna hotovostně nebo je financována s využitím anonymních elektronických peněz, včetně elektronických peněz, na které se vztahuje osvobození podle článku 12 směrnice (EU) 2015/849;

- d) převody jsou prováděny jedním nebo více plátcí v různých zemích místnímu příjemci.

11.6. Tento faktor by mohl přispět ke snížení rizika:

- a) finanční prostředky použité při převodu pocházejí z účtu vedeného na jméno plátce u úvěrové nebo finanční instituce v EHP.

### Rizikové faktory klienta

11.7. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Obchodní činnost klienta:
  - i. Klient vlastní nebo provozuje podnik, který zpracovává velký objem hotovosti.
  - ii. Podnikání klienta má složitou vlastnickou strukturu.
  - iii. Činnost klienta by mohla být spojena s financováním terorismu, protože se o něm veřejně ví, že sympatizuje s extremismem, nebo se o něm ví, že je napojen na skupinu organizované trestné činnosti.
- b) Chování klienta:
  - i. Potřeby klienta by mohly být lépe uspokojeny jinak, například proto, že subjekt zabývající se poukazováním peněz není pro klienta nebo obchodní činnost klienta místním subjektem.
  - ii. Zdá se, že klient jedná jménem někoho jiného, například na klienta dohlíží jiná osoba nebo jsou spatřeny poblíž místa, ve kterém se transakce provádí, nebo klient čte pokyny z poznámek.
  - iii. Chování klienta není z ekonomického hlediska zjevně smysluplné, například klient bez námitek akceptuje nevýhodný směnný kurz nebo vysoký poplatek, požaduje transakci v měně, která není oficiálně nabízena nebo běžně používána v jurisdikci, kde se klient a/nebo příjemce transakce nachází, požaduje nebo poskytuje velký objem měny v nízké nebo vysoké nominální hodnotě.
  - iv. Transakce klienta se vždy pohybují těsně pod platnými limity, včetně limitu hloubkové kontroly klienta pro příležitostné transakce podle čl. 11 písm. b) směrnice (EU) 2015/849 a limitu 1 000 EUR stanoveného v čl. 5 odst. 2 nařízení (EU) 2015/847.<sup>16</sup> Podniky by měly vzít na vědomí, že limit uvedený v čl. 5 odst. 2

<sup>16</sup> Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006.

nařízení (EU) 2015/847 se vztahuje pouze na transakce, které nejsou financovány hotovostí nebo anonymními elektronickými penězi.

- v. Klient využívá služby neobvyklým způsobem, například odesílá peníze sobě samému nebo přijímá peníze poslané jím samotným nebo odesílá peníze okamžitě po jejich obdržení.
- vi. Zdá se, že klient nemá o příjemci mnoho informací nebo se tyto informace zdráhá poskytnout.
- vii. Několik klientů podniku převádí finanční prostředky stejnému příjemci nebo se zdá, že mají stejné identifikační údaje, například adresu nebo telefonní číslo.
- viii. Příchozí transakce není doplněna o požadované informace o plátcí nebo příjemci.
- ix. Odeslaná nebo přijatá částka neodpovídá příjmu klienta (je-li znám).
- x. Zvýšení objemu nebo počtu transakcí nesouvisí s obvyklým způsobem, jako je převod mzdy nebo kulturní oslavy.
- xi. Klient poskytuje nejednotné biografické údaje nebo identifikační doklady obsahující nejednotné informace.

#### 11.8. Faktory, které by mohly přispět ke snížení rizika:

- a) Klient je dlouholetým klientem podniku, jehož chování v minulosti nevyvolávalo podezření a neexistovaly žádné náznaky, že by se riziko praní peněz a financování terorismu mohlo zvýšit.
- b) Převáděná částka je nízká; podniky by však měly vzít v úvahu, že nízké částky samy o sobě nepostačují k tomu, aby riziko financování terorismu zmírňovaly.

#### **Rizikové faktory související s distribučními kanály**

#### 11.9. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Neexistují žádná omezení týkající se nástroje financování, například u hotovosti nebo plateb z produktů elektronických peněz, na které se vztahuje osvobození podle článku 12 směrnice (EU) 2015/849, bankovních převodů nebo šeků.
- b) Použitý distribuční kanál umožňuje určitou míru anonymity.
- c) Služba je poskytována zcela on-line bez adekvátních bezpečnostních opatření.
- d) Služba poukazování peněz je poskytována prostřednictvím zástupců, kteří:
  - i. zastupují více než jeden subjekt;

- ii. mají ve srovnání s jinými zástupci v podobných lokalitách neobvyklé obraty, například neobvykle vysoké nebo nízké objemy transakcí, neobvykle velké hotovostní transakce nebo vysoký počet transakcí, které se pohybují těsně pod limitem hloubkové kontroly klienta, nebo vyvíjejí obchodní činnost mimo běžnou pracovní dobu;
  - iii. obchodují z velké části s plátcí nebo příjemci z jurisdikcí spojených s vyšším rizikem praní peněz a financování terorismu;
  - iv. uplatňují politiky v oblasti boje proti praní peněz a financování terorismu platné pro celou skupinu nepřehledným nebo rozporuplným způsobem; nebo
  - v. nepocházejí z finančního sektoru a vykonávají další obchodní činnost jako své hlavní podnikání.
- e) Služba poukazování peněz je poskytována prostřednictvím široké sítě zástupců v různých jurisdikcích.
- f) Služba poukazování peněz je poskytována prostřednictvím příliš složitého platebního řetězce, například s velkým počtem zprostředkovatelů působících v různých jurisdikcích, nebo umožňujícího (formální a neformální) vypořádací systémy, které není možné vysledovat.

#### 11.10. Faktory, které by mohly přispět ke snížení rizika:

- a) Zástupci jsou sami regulovanými finančními institucemi.
- b) Služba může být financována pouze převody z účtu vedeného na jméno klienta u úvěrové nebo finanční instituce v EHP nebo na účet, u něhož může klient prokázat, že jej ovládá.

#### **Rizikové faktory zemí nebo zeměpisných oblastí**

#### 11.11. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Plátce nebo příjemce se nachází nebo transakce je prováděna z IP adresy nacházející se v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu. Podniky by měly věnovat zvýšenou pozornost jurisdikcím, o nichž je známo, že financují nebo podporují teroristické aktivity nebo že v nich působí skupiny páchající teroristické činy, a jurisdikcím, na něž se vztahují finanční sankce, embarga nebo opatření související s terorismem, financováním terorismu nebo šířením zbraní.
- b) Příjemce má bydliště v jurisdikci, která nemá žádný oficiální bankovní sektor, nebo jej má méně rozvinutý, z čehož vyplývá, že při provádění platby by mohly být využívány neoficiální služby poukazování peněz, například systém hawala.

- c) Protistrana podniku se nachází v třetí zemi [spojené s vyšším rizikem praní peněz a financování terorismu]
- d) Plátce nebo příjemce se nachází ve vysoce rizikové třetí zemi.

## Opatření

11.12. Jelikož je velká část obchodní činnosti subjektů zabývajících se poukazováním peněz primárně založena na transakcích, měly by podniky zvážit, které systémy sledování a kontroly zavedou, aby zajistily, že odhalí pokusy o praní peněz a financování terorismu, a to i v případě neúplných nebo chybějících informací hloubkové kontroly klienta o klientovi z důvodu neuzavřeného obchodního vztahu. Při analýze vhodných systémů sledování by se subjekty zabývajících se poukazováním peněz měly ujistit, že odpovídají velikosti a složitosti obchodní činnosti a objemu transakcí.

11.13. Podniky by měly v každém případě zavést:

- a) systémy pro identifikaci propojených transakcí, včetně těch, které mohou být podle jejich strategií a postupů obchodním vztahem, jako jsou systémy pro identifikaci řady transakcí nižších než 1 000 EUR, které mají stejného plátce a příjemce a určité trvání;
- b) systémy pro zjišťování, zda jsou transakce od různých klientů určeny pro stejného příjemce;
- c) systémy umožňující v co největší míře zjistit zdroje finančních prostředků, jejich a místo určení;
- d) systémy umožňující plně vysledovat transakce i počet subjektů zapojených do platebního řetězce;
- e) systému umožňující identifikovat, zda je převod uskutečňován do vysoce rizikové třetí země nebo obdrženo z vysoce rizikové třetí země; a
- f) systémy umožňující zajistit, aby do celého platebního řetězce mohly zasahovat pouze subjekty oprávněné k poskytování služeb poukazování peněz.

11.14. Pokud je riziko související s příležitostnou transakcí nebo obchodním vztahem vysoké, měly by podniky uplatňovat zesílenou hloubkovou kontrolu klienta v souladu s hlavou I, včetně případného zesíleného sledování transakcí (např. zvýšení četnosti nebo nižší limity). Pokud je naopak riziko související s příležitostnou transakcí nebo obchodním vztahem nízké a v rozsahu povoleném vnitrostátními právními předpisy, mohou podniky uplatňovat opatření zjednodušené hloubkové kontroly klienta v souladu s hlavou I.

11.15. V souladu s článkem 18a směrnice (EU) 2015/849 by subjekty zabývající se poukazováním peněz měly u vztahů nebo transakcí souvisejících s vysoce rizikovými třetími zeměmi uplatňovat opatření zesílené hloubkové kontroly klienta stanovená v tomto ohledu v hlavě I.

### Využívání služeb zástupců

11.16. Subjekty zabývající se poukazováním peněz, které k poskytování platebních služeb využívají služeb zástupců, by měly mít informace o tom, kdo jsou jejich zástupci podle vymezení v článku 19 směrnice (EU) 2015/2366. V důsledku toho by subjekty zabývající se poukazováním peněz měly při zohlednění míry rizika přijmout a uplatňovat příslušné strategie a postupy, aby omezily riziko praní peněz nebo financování terorismu, kterému jejich zástupci mohou být vystaveni nebo k němu zneužiti:

- a) Zjištěním totožnosti osoby, která je majitelem zástupce nebo která zástupce ovládá, je-li zástupcem právnická osoba, aby se zajistilo, že riziko praní peněz a financování terorismu, kterému je v důsledku využití služeb zástupce subjekt zabývající se poukazováním peněz vystaven, nebylo vysoké.
- b) Získáním důkazů v souladu s požadavky čl. 19 odst. 1 písm. c) směrnice (EU) 2015/2366 o tom, že vedoucí pracovníci a další osoby odpovědné za řízení zástupce jsou způsobilými a vhodnými osobami, a posouzením jejich čestnosti, bezúhonnosti a pověsti. Každé šetření, které subjekt zabývající se poukazováním peněz provede, by mělo být přiměřené povaze, složitosti a míře rizika praní peněz a financování terorismu a vyplývat z platebních služeb poskytovaných zástupcem, a mělo by být založeno na postupech hloubkové kontroly klienta subjektu zabývajícího se poukazováním peněz.
- c) Přijetím přiměřených opatření k zajištění, aby interní kontroly v oblasti boje proti praní peněz a financování terorismu zástupců byly odpovídající po celou dobu trvání vztahu se zástupcem, například sledováním několika transakcí zástupce nebo přezkoumáním kontrol zástupců na místě. Pokud se interní kontroly v oblasti boje proti praní peněz a financování terorismu zástupců od kontrol subjektů zabývajících se poukazováním peněz odlišují, například proto, že zástupce zastupuje více než jeden subjekt, nebo proto, že je zástupce povinnou osobou v oblasti boje proti praní peněz a financování terorismu podle platných právních předpisů, měl by subjekt zabývající se poukazováním peněz riziko posoudit a řídit, jelikož by tyto rozdíly mohly mít vliv na dodržování předpisů v oblasti boje proti praní peněz a financování terorismu jím samotným i zástupcem.
- d) Poskytováním školení v oblasti boje proti praní peněz a financování terorismu tak, aby zástupci měli dostatečné znalosti o příslušných rizicích praní peněz a financování terorismu a kvalitě kontrol v oblasti boje proti praní peněz

a financování terorismu dle očekávání subjektu zabývajcího se poukazováním peněz.



## Obecný pokyn č. 12: Odvětvový pokyn týkající se správy majetku

- 12.1. Správa majetku představuje poskytování bankovních a jiných finančních služeb jednotlivcům s vysokým čistým jměním a jejich rodinám nebo podnikům. Je také známa pod pojmem soukromé bankovníctví. Klienti podniků zabývajících se správou majetku mohou očekávat, že jim pracovníci pro oblast vztahů s klienty poskytnou služby na míru, které zahrnují například bankovníctví (např. běžné účty, hypotéky a devizové služby), správu investic a poradenství, svěřenské služby, služby úschovy, pojištění, administrativní služby, daňové plánování a plánování majetku a souvisejících zařízení, včetně právní podpory.
- 12.2. Řada znaků obvykle spojovaných se správou majetku, jako jsou bohatí a vlivní klienti; transakce a portfolia o velmi vysoké hodnotě; ucelené produkty a služby, včetně investičních produktů na míru; a očekávání zachování důvěrnosti a mlčenlivosti může znamenat vyšší riziko praní peněz ve srovnání s obvyklými znaky retailového bankovníctví. Služby podniků zabývajících se správou majetku mohou být obzvláště náchylné ke zneužití ze strany klientů, kteří chtějí zatajit původ svých finančních prostředků nebo se například vyhnout placení daní ve své domovské jurisdikci.
- 12.3. Podniky by v tomto odvětví měly, vedle rizikových faktorů a opatření uvedených v hlavě I těchto obecných pokynů, zohlednit následující rizikové faktory a opatření. V tomto ohledu mohou být také relevantní odvětvové pokyny č. 9, 14 a 17 v hlavě I.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 12.4. Faktory, které by mohly přispět ke zvýšení rizika:
- a) klienti požadující vysoké částky hotovosti nebo jiné kapitálové investice, například do drahých kovů;
  - b) transakce o velmi vysoké hodnotě;
  - c) finanční dohody zahrnující jurisdikce spojené s vyšším rizikem praní peněz a financování terorismu (podniky by měly věnovat zvýšenou pozornost zemím, v jejichž kultuře je zakotveno bankovní tajemství nebo které nedodržují standardy mezinárodní daňové transparentnosti);
  - d) úvěry (včetně hypoték) zajištěné hodnotou aktiv v jiných jurisdikcích, zejména v zemích, kde je obtížné zjistit, zda má klient na zajištění zákonný nárok, nebo kde je obtížné ověřit totožnost stran ručících za úvěr;

- e) využívání složitých obchodních struktur, například svěřenských fondů a soukromých investičních nástrojů, zejména pokud je nejasná totožnost konečného skutečného majitele;
- f) obchodní činnost je uskutečňována ve více zemích, zejména pokud je zapotřebí většího počtu poskytovatelů finančních služeb;
- g) přeshraniční ujednání, jsou-li aktiva uložena nebo spravována v jiné finanční instituci, buď z téže finanční skupiny, nebo mimo skupinu, zejména pokud má druhá finanční instituce sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu. Podniky by měly věnovat zvýšenou pozornost jurisdikcím spojeným s vyšší mírou predikativních trestných činů, nedostatečným režimem pro boj proti praní peněz a financování terorismu nebo nedostatečnými standardy mezinárodní daňové transparentnosti.

### Rizikové faktory klienta

#### 12.5. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Klienti s příjmem a/nebo majetkem působící ve vysoce rizikových odvětvích, například v odvětví zbrojním, těžebním, ve stavebnictví, v odvětví hazardních her nebo jako soukromí vojenští dodavatelé.
- b) Klienti, vůči kterým byla vznesena věrohodná obvinění z nezákonného jednání.
- c) Klienti, kteří vyžadují neobvykle vysokou míru zachování důvěrnosti nebo mlčenlivosti.
- d) Klienti, jejichž jednání týkající se výdajů nebo transakcí znesnadňuje zavedení „normálních“ nebo očekávaných vzorců chování.
- e) Velmi bohatí a vlivní klienti, včetně klientů v postavení významné veřejné osoby, klientů s bydlištěm v jiné zemi a politicky exponovaných osob. Pokud je klient nebo skutečný majitel klienta politicky exponovanou osobou, musí podniky vždy v souladu s články 18 až 22 směrnice (EU) 2015/849 uplatnit zesílenou hloubkovou kontrolu klienta.
- f) Klient vyžaduje, aby podnik klientovi umožnil poskytnutí produktu nebo služby třetí osobou bez zjevného obchodního nebo ekonomického důvodu.

### Rizikové faktory zemí nebo zeměpisných oblastí

#### 12.6. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Obchodní činnost se uskutečňuje v zemích, v jejichž kultuře je zakotveno bankovní tajemství, nebo které nedodržují standardy mezinárodní daňové transparentnosti.
- b) Klient žije v jurisdikci spojené s vyšším rizikem praní peněz nebo financování terorismu, nebo jeho finanční prostředky pocházejí z činností prováděných v této jurisdikci.

## Opatření

12.7. Zaměstnanec, který řídí vztah podniku s klientem v oblasti správy jeho majetku (řídící pracovník pro vztahy s klienty), obvykle hraje při posuzování rizika klíčovou úlohu. Úzký kontakt řídícího pracovníka pro vztahy s klientem usnadní shromažďování informací, které umožní plnohodnotnější představu o účelu a povaze podnikání klienta (např. zjištění zdroje majetku klienta, místa určení finančních prostředků, proč by složité nebo neobvyklé dohody přesto mohly být hodnověrné a zákonné, nebo proč by mohla být vhodná další bezpečnostní opatření). Tento úzký kontakt však může také vést ke střetu zájmů, pokud se řídící pracovník pro vztahy s klientem příliš sblíží, a to na úkor snahy podniku o řízení rizika finanční trestné činnosti. V důsledku toho je rovněž zapotřebí zavést odpovídající nezávislý dohled nad hodnocením rizika, který může být zajištěn například oddělením dodržování předpisů a vrcholným vedením.

### Zesílená hloubková kontrola klienta

12.8. V souladu s článkem 18a by podniky měly u vztahů nebo transakcí souvisejících s vysoce rizikovými třetími zeměmi uplatňovat opatření zesílené hloubkové kontroly klienta stanovená v tomto ohledu v hlavě I.

- a) Získání a ověření většího počtu informací o klientech než při situacích se standardní mírou rizika a jejich pravidelné přezkoumávání a aktualizace, a to jak pravidelně, tak na základě zásadních změn profilu klienta. Podniky by měly provádět přezkumy při zohlednění míry rizika a provádět přezkumy u klientů s vyšším rizikem alespoň jednou ročně, nicméně pokud to riziko vyžaduje, pak častěji. Tyto postupy mohou zahrnovat postupy pro zaznamenávání všech návštěv v prostorách klientů, ať již v jejich bydlišti nebo v místě podnikání, včetně všech změn profilu klienta nebo jiných informací, které by mohly ovlivnit posouzení rizik, které z těchto návštěv vyplývají.
- b) Zjištění zdroje majetku a finančních prostředků; pokud je riziko obzvláště vysoké a/nebo pokud má podnik pochybnosti o zákonném původu finančních prostředků, může být ověření zdroje majetku a finančních prostředků jediným příslušným nástrojem pro zmírnění rizika. Zdroje finančních prostředků nebo majetku lze ověřit mimo jiné nahlédnutím do:

- i. originálu nebo ověřené kopie dokladu o mzdě novějšího data;
  - ii. písemného potvrzení o ročním platu podepsaného zaměstnavatelem;
  - iii. originálu nebo ověřené kopie smlouvy o prodeji, například investic nebo společnosti;
  - iv. písemného potvrzení o prodeji podepsaného advokátem nebo právním zástupcem;
  - v. originálu nebo ověřené kopie závěti nebo soudem potvrzené poslední vůle;
  - vi. písemného potvrzení o dědictví podepsaného advokátem, právním zástupcem, svěřenským správcem nebo vykonavatelem závěti;
  - vii. internetového vyhledávání v obchodním rejstříku společností k potvrzení prodeje společnosti.
  - viii. Provádění většího rozsahu kontrol a hloubkových kontrol u obchodních vztahů, než je běžné u poskytování obvyklých finančních služeb, například v oblasti retailového bankovníctví nebo správy investic.
- c) Zjištění místa určení finančních prostředků.

## Obecný pokyn č. 13: Odvětvový pokyn pro poskytovatele financování obchodu

- 13.1. Financováním obchodu se rozumí správa platby za účelem usnadnění pohybu zboží (a poskytování služeb) v tuzemsku nebo přes hranice. Při přepravě zboží na mezinárodní úrovni je dovozce vystaven riziku, že zboží nedorazí, zatímco vývozce je vystaven riziku, že nedorazí platba. Aby se tato rizika zmírnila, mnoho nástrojů financování obchodu využívá během transakcí bank.
- 13.2. Financování obchodu může mít mnoho různých forem. Mezi ně patří:
- a) Transakce „otevřeného účtu“: jedná se o transakce, při kterých kupující provede platbu poté, co obdrží zboží. Jedná se o nejběžnější způsob financování obchodu, ale bankám, které provádí převod finančních prostředků, často není známa obchodní povaha transakce. Banky by se při řízení rizik souvisejících s těmito transakcemi měly řídit pokyny uvedenými v hlavě I.
  - b) Dokumentární akreditivy, které mají mnoho podob a jsou vhodné pro různé situace: dokumentární akreditiv je finanční nástroj vytvořený bankou, který zaručuje platbu stanovenému příjemci (obvykle vývozci) po předložení určitých „vyhovujících“ dokumentů uvedených v úvěrových podmínkách (např. důkaz o tom, že zboží bylo odesláno).
  - c) Dokumentární inkasa: dokumentárním inkasem se rozumí proces, během něhož „inkasní“ banka vybere platbu nebo akceptovanou směnku od dovozce zboží, aby následně zaslala platbu vývozci. Inkasní banka jako protiplnění dovozci zašle příslušné obchodní dokumenty (které obdrží od vývozce, obvykle prostřednictvím jeho banky).
- 13.3. Na jiné produkty financování obchodu, například forfaiting nebo strukturované financování nebo rozsáhlejší činnosti, například projektové financování, se působnost těchto odvětvových pokynů nevztahuje. Banky nabízející tyto produkty by se měly řídit obecnými pokyny uvedenými v hlavě I.
- 13.4. Produkty financování obchodu mohou být zneužity pro účely praní peněz a financování terorismu. Kupující se například může dohodnout s prodávajícím na zkeslení ceny, druhu, kvality nebo množství zboží za účelem převodu finančních prostředků nebo hodnoty mezi zeměmi.
- 13.5. Banky by měly vzít v úvahu, že Mezinárodní obchodní komora vypracovala standardy, jako Jednotné zvyklosti a pravidla pro dokumentární akreditivy (č. 600), tedy soubor pravidel vztahujících se na finanční instituce vydávající dokumentární akreditivy, kterými se řídí používání dokumentárního akreditivu a dokumentárního inkasa, nevztahují se však na

záležitosti týkající se finanční trestné činnosti. Banky by měly vzít na vědomí, že tyto standardy nemají právní sílu a jejich použití neznamená, že banky nemusí plnit své právní a regulační povinnosti v oblasti boje proti praní peněz a financování terorismu.

- 13.6. Podniky by v tomto odvětví měly, vedle rizikových faktorů a opatření uvedených v hlavě I těchto obecných pokynů, zohlednit následující rizikové faktory a opatření. V tomto ohledu může být také relevantní odvětvový pokyn č. 8 v hlavě II.

## Rizikové faktory

- 13.7. Banky, které jsou zapojeny do transakcí financování obchodu, mají často přístup pouze k části informací o transakci a jejích účastnících. Obchodní dokumentace může být různorodá a banky nemusí mít dostatek odborných znalostí týkajících se různých typů obchodní dokumentace, kterou obdrží. Může to identifikaci a posouzení rizika praní peněz a financování terorismu znesnadnit.

- 13.8. Banky by nicméně měly použít zdravý rozum a odborný úsudek, aby posoudily, do jaké míry mohou informace a dokumentace, které mají k dispozici, vyvolat obavy nebo podezření ohledně praní peněz a financování terorismu.

- 13.9. Banky by měly v co největší míře zohlednit následující rizikové faktory:

### Rizikové faktory transakcí

- 13.10. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Transakce je neobvykle vysoká vzhledem k tomu, co je o předchozí oblasti podnikání a obchodní aktivitě klienta známo.
- b) Transakce je značně strukturovaná, roztržitá nebo složitá, dotýká se mnoha stran, bez zjevného legitimního důvodu.
- c) V situacích, kdy se předpokládají dokumenty v originále, jsou bez rozumného vysvětlení použity kopie dokumentů.
- d) V dokumentech jsou výrazné nesrovnalosti, například mezi popisem druhu, množství nebo kvality zboží v klíčových dokladech (tj. fakturách, dokladech o pojištění a přepravních dokladech) a skutečně dodaným zbožím v rozsahu, v jakém je tato skutečnost známa.
- e) Druh, množství a hodnota zboží neodpovídá informacím banky o obchodní činnosti kupujícího.

- f) Zboží, které je předmětem obchodu, představuje vyšší riziko z hlediska praní peněz, například ceny některých komodit mohou výrazně kolísat, což může ztěžovat odhalení fiktivních cen.
- g) Sjednaná hodnota zboží nebo zásilky je nadměrně nebo nedostatečně pojištěná nebo je použito několik pojištění v rozsahu, v jakém je tato skutečnost známa.
- h) Zboží, které je předmětem obchodu, vyžaduje vývozní licence, jako je zvláštní vývozní povolení pro zboží dvojího užití, tedy zboží, software a technologie, které je možné používat pro civilní i vojenské účely.
- i) Obchodní dokumentace není v souladu s platnými právními předpisy nebo standardy.
- j) Cena za jednotku se zdá být, na základě toho, co banka o zboží a obchodu zná, neobvyklá.
- k) Transakce je neobvyklá jiným způsobem, například dokumentární akreditiv je často bezdůvodně pozměňován nebo zboží je bez zjevného obchodního důvodu odesláno přes jinou jurisdikci.
- l) Obchodované zboží je určeno osobě nebo do země, která je předmětem sankcí, embarga nebo podobných opatření vydaných například Uníí nebo Organizací spojených národů, nebo na podporu takové osoby nebo země.

#### 13.11. Faktory, které by mohly přispět ke snížení rizika:

- a) Nezávislí inspektoři ověřili kvalitu a množství zboží a přítomnost nezbytných dokladů a povolení.
- b) Transakce se týkají zavedených protistran, které již v minulosti spolu obchodovaly a u nichž byla v minulosti provedena hloubková kontrola.

### Rizikové faktory klienta

#### 13.12. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Transakce a/nebo zúčastněné strany, kterých se transakce týká, neodpovídají tomu, co banka o předchozí činnosti nebo oblasti podnikání klienta zná (např. zboží, které je dodáváno, nebo množství dodávaného zboží jsou v rozporu s tím, co je o obchodní činnosti dovozce nebo vývozce známo).
- b) Existují náznaky, že kupující a prodávající by mohli skrytě spolupracovat, například:

- i. kupující i prodávající jsou ovládáni stejnou osobou;
  - ii. podniky, jichž se transakce týká, mají stejnou adresu, uvedou pouze adresu registrovaného zástupce nebo mají jiné nesrovnalosti v adresách;
  - iii. kupující je ochoten nebo má zájem přijmout nebo nebrat v úvahu nesrovnalosti v dokumentaci.
- c) Klient není schopen nebo se zdráhá k transakci předložit příslušnou dokumentaci.
  - d) Klientovi dělá problémy vysvětlit důvod celého vývozního procesu nebo klient není schopen vysvětlit obsah a význam souvisejících dokumentů vztahujících se k dokumentárnímu akreditivu nebo dokumentárnímu inkasu.
  - e) Právní struktura kupujícího neumožňuje identifikovat vlastníky nebo kupující k zastupování práv a zájmů kupujícího používá zástupce nebo třetí strany.

#### 13.13. Faktory, které by mohly přispět ke snížení rizika:

- a) Klient je stávajícím klientem, jehož obchodní činnost je bankám dobře známa a jehož transakce je s touto činností v souladu.

#### **Rizikové faktory zemí nebo zeměpisných oblastí**

#### 13.14. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Země, které se transakce týká (včetně země, z níž zboží pochází, do níž je zboží určeno nebo přes kterou je zboží přepravováno, nebo v níž má některá strana transakce sídlo), nemá zavedeny devizové kontroly. Zvyšuje se tak riziko, že skutečný účel transakce je v rozporu s místními právními předpisy vyvážet měnu.
- b) Země, jíž se transakce týká, má vyšší míru predikativních trestných činů (souvisejících například s obchodem s narkotiky, pašováním nebo paděláním) nebo má zóny volného obchodu.
- c) Transakce je prováděna pod záštitou státních nebo mezinárodních organizací nebo nadací na podporu obětí přírodní katastrofy nebo osob postižených válečným konfliktem nebo občanskými nepokoji.

#### 13.15. Faktory, které by mohly přispět ke snížení rizika:

- a) Obchod je uskutečňován v rámci EU/EHP.



- b) Země, jichž se transakce týká, mají režim pro boj proti praní peněz a financování terorismu, který není méně přísný než požadavky uvedené ve směrnici (EU) 2015/849, a jsou spojovány s nízkou mírou predikativních trestných činů.

## Opatření

- 13.16. Banky musí provádět hloubkovou kontrolu klienta u strany, která zadává platební příkaz. V praxi většina bank přijímá pokyny pouze od stávajících klientů a širší obchodní vztah, který banka s klientem má, může napomoci bance při provádění hloubkové kontroly.
- 13.17. Pokud banka poskytuje klientovi služby financování obchodu, měla by v rámci svého postupu hloubkové kontroly přijmout kroky směřující k porozumění obchodní činnosti svého klienta. Mezi příklady informací, které banka může získat, patří informace o zemích, se kterými klient obchoduje, o používaných obchodních trasách, o zboží, s nímž obchoduje, s kým klient obchoduje (kupující, dodavatelé atd.), zda klient využívá služeb zástupců nebo třetích osob, a pokud ano, kde mají sídlo. Mělo by to bankám napomoci porozumět, kdo je jejich klientem, a odhalit neobvyklé či podezřelé transakce.
- 13.18. Pokud je banka korespondenční bankou, musí vůči korespondenční instituci uplatnit opatření hloubkové kontroly klienta. Korespondenční banky by se měly řídit odvětvovým pokynem č. 8 pro korespondenční bankovníctví.

### Zesílená hloubková kontrola klienta

- 13.19. V souladu s článkem 18a by podniky měly u vztahů nebo transakcí souvisejících s vysoce rizikovými třetími zeměmi uplatňovat opatření zesílené hloubkové kontroly klienta stanovená v tomto ohledu v hlavě I.
- 13.20. V jiných situacích s vyšším rizikem musí banky rovněž uplatnit opatření zesílené hloubkové kontroly klienta. V rámci toho by banky měly zvážit, zda by nebylo vhodné provést u transakce samotné a ostatních stran podílejících se na transakci (včetně stran, které nejsou klienty) důkladnější hloubkovou kontrolu.
- 13.21. Kontroly ostatních stran, kterých se transakce týká, mohou obsahovat:
- a) Přijetí kroků k lepšímu porozumění vlastnictví nebo pozadí ostatních stran, kterých se transakce týká, zejména pokud mají sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu, nebo pokud obchodují s vysoce rizikovým zbožím. Mohou sem spadat kontroly obchodních rejstříků a informačních zdrojů třetích osob a průzkumy veřejně dostupných zdrojů na internetu.
  - b) Získání více informací o finanční situaci zúčastněných stran.

#### 13.22. Kontroly transakcí mohou obsahovat:

- a) využití zdrojů údajů třetích stran nebo údajů z veřejně dostupných zdrojů, například Mezinárodního námořního úřadu (jako jsou výstražná oznámení, nákladní listy, přepravní a cenové kontroly) nebo bezplatné služby sledování kontejnerové přepravy k ověření poskytnutých informací a k ověření legálnosti účelu transakce;
- b) zvážení na základě odborného úsudku, zda ceny zboží jsou po obchodní stránce přiměřené, zejména ve vztahu k obchodovaným komoditám, pro něž lze získat spolehlivé a aktuální informace o cenách;
- c) ověření, že hmotnosti a objemy přepravovaného zboží odpovídají přepravní metodě.

13.23. Jelikož jsou dokumentární akreditivy i dokumentární inkasa z velké části založeny na listinných dokladech a jsou doprovázeny dokumenty souvisejícími s obchodem (například fakturami, nákladními listy a manifesty), automatizované sledování transakcí nemusí být proveditelné. Banka, zpracovávající dokumentaci, by měla tyto dokumenty posoudit z hlediska jejich souladu s obchodními podmínkami transakce a požadovat od zaměstnanců, aby na základě odborných znalostí a úsudku posoudili, zda některé neobvyklé rysy transakce vyžadují použití opatření zesílené hloubkové kontroly klienta nebo zda vyvolávají podezření na praní peněz a financování terorismu.

#### **Zjednodušená hloubková kontrola klienta**

13.24. V případě kontrol běžně prováděných bankami za účelem odhalení podvodů a zajištění, aby transakce odpovídala standardům stanoveným Mezinárodní obchodní komorou, se v praxi neuplatní opatření zjednodušené hloubkové kontroly klienta ani v situacích s nižším rizikem.

## Obecný pokyn 14: Odvětvový pokyn pro životní pojišťovny

- 14.1. Produkty životního pojištění jsou vytvořeny za účelem finanční ochrany pojistníka proti riziku nejisté budoucí události, například smrti, nemoci či „přežití úspor“ v důchodu (riziku dlouhověkosti). Ochrana je poskytována ze strany pojistitele, který sdružuje finanční rizika, s nimiž se mnoho různých pojistníků potýká. Produkty životního pojištění lze také koupit ve formě investičních produktů nebo produktů pro účely důchodového zabezpečení.
- 14.2. Produkty životního pojištění jsou poskytovány prostřednictvím různých distribučních kanálů klientům, kteří mohou být fyzickými nebo právníckými osobami či právními uspořádáními. Příjemcem plnění může být pojistník nebo jmenovaná či určená třetí osoba; příjemce může být rovněž během doby trvání smlouvy změněn a původnímu příjemci plnění by tak plnění nebylo vyplaceno.
- 14.3. Většina produktů životního pojištění je vytvořena na dlouhé období a některé produkty jsou vypláceny pouze při ověřitelné události, jako je smrt nebo odchod do důchodu. To znamená, že mnoho produktů životního pojištění není dostatečně flexibilní, aby se za účelem praní peněz stalo první možností. Stejně jako u jiných produktů finančních služeb však existuje riziko, že by finanční prostředky sloužící k zakoupení životního pojištění mohly pocházet z trestné činnosti.
- 14.4. Podniky by v tomto odvětví měly, vedle rizikových faktorů a opatření uvedených v hlavě I těchto obecných pokynů, zohlednit následující rizikové faktory a opatření. V tomto ohledu mohou být také relevantní odvětvové pokyny č. 12 a 16 uvedené v hlavě II. Pokud jsou využívání zprostředkovatelé, budou relevantní rovněž rizikové faktory distribučních kanálů uvedené v hlavě I.
- 14.5. Nicméně zprostředkovatelé by mohli využít i těchto pokynů.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 14.6. Faktory, které by mohly přispět ke zvýšení rizika:
  - a) Flexibilita plateb, produkt například umožňuje:
    - i. platby od třetích stran, které nejsou známy;
    - ii. platby pojistného o vysoké hodnotě nebo neomezené hodnotě, přeplatky nebo velké množství plateb pojistného o nižší hodnotě;
    - iii. platby v hotovosti.

- b) Snadný přístup k nashromážděným finančním prostředkům; produkt například umožňuje kdykoliv za omezený poplatek nebo platbu částečné výběry nebo předčasné ukončení smlouvy.
- c) Obchodovatelnost, produkt například může být:
  - i. obchodován na sekundárním trhu;
  - ii. použit jako zajištění úvěru.
- d) Anonymita, produkt například usnadňuje nebo umožňuje anonymitu klienta.

14.7. Mezi faktory, které mohou přispět ke snížení rizika, patří: Produkt:

- a) je vyplacen pouze v případě předem stanovené události, například smrti, nebo ke konkrétnímu dni, například životní pojištění spojené s úvěrem, týkající se spotřebitelských a hypotečních úvěrů, které je vypláceno pouze v případě smrti pojištěné osoby;
- b) bez nároku na odbytné;
- c) bez investičního prvku;
- d) neumožňuje režim plateb od třetích osob;
- e) vyžaduje, aby byly celkové investice omezeny na nízkou hodnotu;
- f) je životní pojistkou s nízkým pojistným;
- g) umožňuje pouze pravidelné platby pojistného o nízké hodnotě, například bez možnosti přeplatků;
- h) je dostupný pouze prostřednictvím zaměstnavatelů, například důchodový systém, penzijní připojištění nebo obdobný systém, kdy jsou příspěvky zaměstnanců hrazeny prostřednictvím srážky ze mzdy a pravidla systému neumožňují postoupení účasti člena podle tohoto systému;
- i) nelze vyplatit v krátkodobém ani střednědobém horizontu, například důchodové systémy bez možnosti předčasného ukončení smlouvy;
- j) nelze použít jako zajištění;
- k) neumožňuje platby v hotovosti;
- l) obsahuje podmínky omezující dostupnost finančních prostředků, které musí být pro získání daňové úlevy splněny.

## Rizikové faktory klienta a příjemce plnění

### 14.8. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Povaha klienta, například:
  - i. právnické osoby, jejichž struktura znesnadňuje zjistit totožnost skutečného majitele;
  - ii. klient nebo skutečný majitel klienta je politicky exponovanou osobou;
  - iii. příjemce plnění pojistky nebo skutečný majitel tohoto příjemce plnění je politicky exponovanou osobou;
  - iv. věk klienta není pro daný typ požadovaného produktu obvyklý (např. klient je velmi mladý nebo velmi starý);
  - v. smlouva neodpovídá výši majetku klienta;
  - vi. povolání nebo činnosti klienta jsou považovány za pravděpodobně napojené na praní peněz, například proto, že je známo, že ve velké míře využívají hotovostní prostředky nebo jsou vystaveni vysokému riziku korupce;
  - vii. smlouva je upsána „správcem“, například svěřenské společnosti jednající jménem klienta;
  - viii. pojistníkem a/nebo příjemcem plnění je společnost s pověřenými akcionáři nebo společníky a/nebo akciemi na doručitele.
- b) Chování klienta:
  - i. Například pokud jde o smlouvu:
    - a. klient často převádí smlouvu na jiného pojistitele;
    - b. častá a neodůvodněná předčasná ukončení smluv, zejména pokud jsou peněžní prostředky vypláceny na různé bankovní účty;
    - c. klient často nebo neočekávaně využívá doby „na podívání se“ / lhůty „na rozmyšlenou“ zejména v případech, kdy jsou peněžní prostředky vypláceny zdánlivě nespřízněné třetí osobě;
    - d. klient vynakládá vysoké částky, aby dosáhl předčasného ukončení produktu;

- e. klient převede smlouvu na zdánlivě nespřízněnou třetí osobu;
  - f. požadavek klienta na změnu nebo zvýšení pojistné částky a/nebo částek pojistného je neobvyklý nebo neúměrný.
- ii. Například pokud jde o příjemce plnění:
- a. pojistitel je informován o změně příjemce plnění až při požadavku na vyplacení;
  - b. klient mění doložku ve prospěch třetí osoby a určuje zjevně nespřízněnou třetí osobu;
  - c. pojistitel, klient, skutečný majitel, příjemce plnění nebo skutečný majitel příjemce plnění se nacházejí v různých jurisdikcích.
- iii. Například pokud jde o platby:
- a. klient používá neobvyklé platební metody, například hotovost nebo strukturované měnové nástroje nebo jiné formy platebních prostředků umožňující anonymitu;
  - b. platby z různých bankovních účtů bez vysvětlení;
  - c. platby od bank, které nejsou usazeny v zemi, kde má klient bydliště;
  - d. klient hradí neočekávané a časté nebo vysoké přeplatky;
  - e. platby přijaté od nespřízněných třetích osob;
  - f. vyšší příspěvky do důchodového systému při blížícím se dni odchodu do důchodu.

14.9. Faktory, které by mohly přispět ke snížení rizika. Jestliže je životní pojištění vlastněné společností, klient je:

- a) úvěrová nebo finanční instituce, na kterou se vztahují požadavky v oblasti boje proti praní peněz a financování terorismu a nad kterou je vykonáván dohled za

účelem dodržování těchto požadavků způsobem stanoveným směrnicí (EU) 2015/849;

- b) orgán veřejné správy nebo státní podnik v jurisdikci EHP.

### **Rizikové faktory související s distribučními kanály**

14.10. Faktory, které by mohly přispět ke zvýšení rizika:

- a) prodeje bez osobní přítomnosti partnera, například prodeje on-line, prodeje přes poštu nebo telefon, bez odpovídajících bezpečnostních opatření, jako jsou elektronické podpisy nebo elektronické identifikační prostředky, které jsou v souladu s nařízením (EU) č. 910/2014;
- b) dlouhé řetězce zprostředkovatelů;
- c) služby zprostředkovatele jsou využívány za neobvyklých okolností (např. při nezdůvodněné zeměpisné vzdálenosti).

14.11. Faktory, které by mohly přispět ke snížení rizika:

- a) Zprostředkovatelé jsou pojistiteli, který je ujištěn o tom, že uplatňují opatření hloubkové kontroly klienta přiměřená riziku souvisejícímu se vztahem a odpovídajícím požadavkům směrnice (EU) 2015/849, dobře známi.
- b) Produkt je dostupný pouze zaměstnancům některých společností, které uzavřely smlouvu s pojistitelem o poskytování životního pojištění svým zaměstnancům, například v rámci zaměstnaneckých benefitů.

### **Rizikové faktory zemí nebo zeměpisných oblastí**

14.12. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Pojstitel, klient, skutečný majitel, příjemce plnění nebo skutečný majitel příjemce plnění mají sídlo v jurisdikcích spojených s vyšším rizikem praní peněz nebo financování terorismu nebo jsou s ním spojováni. Podniky by měly věnovat zvýšenou pozornost jurisdikcím bez účinného dohledu nad plněním povinností v oblasti boje proti praní peněz a financování terorismu.
- b) Pojistné je hrazeno z účtů vedených u finančních institucí usazených v jurisdikcích spojených s vyšším rizikem praní peněz a financování terorismu. Podniky by měly věnovat zvýšenou pozornost jurisdikcím bez účinného dohledu nad plněním povinností v oblasti boje proti praní peněz a financování terorismu.

- c) Zprostředkovatel má sídlo v jurisdikcích spojených s vyšším rizikem praní peněz nebo financování terorismu, nebo na ně má vazby. Podniky by měly věnovat zvýšenou pozornost jurisdikcím bez účinného dohledu nad plněním povinností v oblasti boje proti praní peněz a financování terorismu.

#### 14.13. Faktory, které by mohly přispět ke snížení rizika:

- a) Země podle věrohodných zdrojů, například vzájemných hodnocení nebo podrobných hodnotících zpráv, mají účinné systémy boje proti praní peněz a financování terorismu.
- b) Země podle věrohodných zdrojů mají nízkou míru korupce a jiné trestné činnosti.

## Opatření

14.14. Ustanovení čl. 13 odst. 5 směrnice (EU) 2015/849 stanoví, že v případě životního pojištění musí podniky uplatňovat opatření hloubkové kontroly klienta nejen u klienta a skutečného majitele, ale i u příjemců plnění, jakmile jsou identifikováni nebo určeni. To znamená, že podniky musí:

- a) získat jméno příjemce plnění, jestliže je jako příjemce plnění identifikována fyzická nebo právnická osoba nebo právní uspořádání; nebo
- b) získat další informace, aby zajistily, že v okamžiku výplaty plnění je zjištěna totožnost příjemců plnění, jestliže jsou příjemci plnění skupinou osob nebo jsou určeni na základě určitých charakteristik. Jestliže jsou například jako příjemci plnění označeni „má budoucí vnoučata“, měl by pojistitel získat informace o potomcích pojistníka.

14.15. Podniky musí ověřit totožnost příjemců plnění nejpozději v okamžiku výplaty plnění.

14.16. Jestliže má podnik informaci o tom, že životní pojištění bylo postoupeno třetí osobě, která hodnotu pojistky obdrží, musí zjistit totožnost skutečného majitele v okamžiku postoupení.

14.17. V souladu s čl. 13 odst. 6 směrnice (EU) 2015/849 by podniky v případech, kdy jsou obmyšlenými svěřenských fondů nebo podobných právních uspořádání určeni na základě příslušnosti k určité kategorii nebo na základě určitých vlastností, měly získat dostatek informací, aby se ujistily, budou schopny zjistit totožnost obmyšlených v okamžiku výplaty výnosů nebo v okamžiku, kdy obmyšlení uplatní svá nabytá práva.

## Zesílená hloubková kontrola klienta



14.18. V souladu s článkem 18a by podniky měly u vztahů nebo transakcí souvisejících s vysoce rizikovými třetími zeměmi uplatňovat opatření zesílené hloubkové kontroly klienta stanovená v tomto ohledu v hlavě I. Ve všech ostatních vysoce rizikových situacích mohou být vhodná následující opatření zesílené hloubkové kontroly klienta:

- a) Pokud klient využije doby „na podívání se“ / lhůty „na rozmyšlenou“ mělo by být pojistné vráceno na bankovní účet klienta, z něhož byly finanční prostředky uhrazeny. Podniky by měly před vrácením finančních prostředků zajistit, aby byla ověřena totožnost klienta v souladu s článkem 13 směrnice (EU) 2015/849, obzvláště je-li pojistné vysoké, nebo jeví-li se okolnosti jako neobvyklé. Podniky by měly také posoudit, zda zrušení nevzbuzuje ohledně transakce podezření a zda by nebylo vhodné předložit zprávu o podezřelých aktivitách.
- b) Za účelem zvýšení znalostí podniku o klientovi, skutečném majiteli, příjemci plnění nebo skutečném majiteli příjemce plnění, plátcích a příjemcích třetích stran mohou být přijaty i další kroky. Například:
  - i. Neuplatnění odchylky uvedené v čl. 14 odst. 2 směrnice (EU) 2015/849, která stanoví osvobození od hloubkové kontroly klienta předem;
  - ii. ověření totožnosti dalších relevantních osob, včetně plátců a příjemců třetích stran, před uzavřením obchodního vztahu;
  - iii. získání dalších informací pro zjištění zamýšlené povahy obchodního vztahu;
  - iv. získání dalších informací o klientovi a pravidelnější aktualizace identifikačních údajů klienta a skutečného majitele;
  - v. liší-li se plátce od klienta, zjištění důvodu, proč tomu tak je;
  - vi. ověření totožnosti podle více než jednoho spolehlivého a nezávislého zdroje;
  - vii. zjištění zdroje majetku a zdroje finančních prostředků klienta, například z údajů o zaměstnání a mzdových údajů, výsledku dědického řízení nebo rozvodového vypořádání;
  - viii. je-li to možné, zjištění totožnosti příjemce plnění a ověření jeho totožnosti na počátku obchodního vztahu namísto vyčkávání, až je identifikován nebo určen, s přihlédnutím k tomu, že se příjemce plnění může během doby trvání smlouvy změnit;
  - ix. zjištění a ověření totožnosti skutečného majitele příjemce plnění;
  - x. v souladu s články 20 a 21 směrnice (EU) 2015/849 přijetí opatření ke zjištění, zda je klient politicky exponovanou osobou, a přijetí odpovídajících opatření ke

zjištění, zda je příjemce plnění nebo skutečný majitel příjemce plnění politicky exponovanou osobou v okamžiku postoupení celé pojistky nebo její části nebo nejpozději v době výplaty plnění;

- xi. vyžadování, aby byla první platba uskutečněna prostřednictvím účtu vedeného na jméno klienta u banky, na kterou se vztahují opatření hloubkové kontroly klienta, které nejsou méně přísné než požadavky dle směrnice (EU) 2015/849.

14.19. Článek 20 směrnice (EU) 2015/849 vyžaduje, aby v případech, kdy je riziko spojeno se vztahem s politicky exponovanou osobou vysoké, neměly podniky uplatňovat pouze opatření hloubkové kontroly klienta v souladu s článkem 13 směrnice, ale rovněž před výplatou plnění informovat vrcholné vedení, aby mohlo zaujmout informované stanovisko k riziku praní peněz a financování terorismu spojenému s danou situací a rozhodnout o nejvhodnějších opatřeních ke zmírnění tohoto rizika; kromě toho musí podniky uplatňovat zesílenou hloubkovou kontrolu klienta v rámci celého obchodního vztahu.

14.20. Podniky by měly:

- a) získat další informace o obchodním vztahu, aby bylo možné pochopit povahu vztahu mezi klientem/pojištěnou osobou a příjemcem plnění a vztahu mezi plátcem a příjemcem plnění, pokud plátcem není klientem/pojištěnou osobou; a
- b) posílit kontrolu zdroje finančních prostředků.

14.21. Je-li příjemcem plnění politicky exponovaná osoba, která je výslovně jmenována, podniky by neměly s provedením zesílené kontroly celého obchodního vztahu čekat až na výplatu pojistného plnění.

14.22. Může být vyžadováno častější a podrobnější sledování transakcí (včetně případného zjištění zdroje finančních prostředků).

### Zjednodušená hloubková kontrola klienta

14.23. Následující opatření by mohla vést ke splnění některých požadavků na hloubkovou kontrolu klienta v situacích s nízkým rizikem (v rozsahu umožněném vnitrostátními právními předpisy):

- a) Podniky by mohly považovat ověření totožnosti klienta za splněné na základě platby provedené z účtu, o kterém je podnik ubezpečen, že je veden na samostatné nebo společné jméno klienta u úvěrové instituce regulované v EHP.
- b) Podniky by mohly považovat ověření totožnosti příjemce plnění ze smlouvy za splněné na základě platby provedené na účet, o kterém je podnik ubezpečen, že je veden na jméno příjemce plnění u úvěrové instituce regulované v EHP.



## Obecný pokyn č. 15: Odvětvový pokyn pro investiční podniky

- 15.1. Investiční podniky podle vymezení v čl. 4 odst. 1 bodě 1 směrnice 2014/65/EU by při poskytování nebo provádění investičních služeb nebo činností podle vymezení v čl. 4 odst. 1 bodě 2 směrnice 2014/65/EU měly kromě těch uvedených v hlavě I těchto obecných pokynů zvážit následující rizikové faktory a opatření. V tomto ohledu může být také relevantní odvětvový pokyn č. 12.
- 15.2. Při plnění svých povinností vyplývajících ze směrnice (EU) 2015/849 by podniky v tomto odvětví měly zohlednit, že:
- riziko praní peněz a financování terorismu v tomto odvětví je dáno především rizikem spojeným s klienty, kterým investiční podniky poskytují služby; a
  - vzhledem k povaze činností vykonávaných investičními podniky mohou být podniky vystaveny predikativním trestným činům, jako je zneužívání trhu, které mohou vést k praní peněz a financování terorismu.

### Rizikové faktory

#### Rizikové faktory produktů, služeb nebo transakcí

- 15.3. Faktory, které by mohly přispět ke zvýšení rizika:
- transakce jsou vzhledem k profilu klienta neobvykle vysoké;
  - dohody o vypořádání jsou nestandardní nebo se zdají být mimořádné;
  - jsou používány zrcadlové obchody nebo transakce související s cennými papíry pro přepočty měn, které se jeví jako neobvyklé nebo nemají zjevný obchodní nebo ekonomický účel;
  - produkt nebo služba jsou strukturované tak, že to může ztěžovat identifikaci klientů; jsou možné platby od třetích osob.
- 15.4. Faktory, které by mohly přispět ke snížení rizika:
- Na produkt nebo službu se vztahují povinné požadavky týkající se transparentnosti a/nebo zveřejnění informací.

#### Rizikové faktory klienta

- 15.5. Faktory, které by mohly přispět ke zvýšení rizika:
- Chování klienta, například:

- i. důvod investice postrádá zjevný ekonomický účel;
- ii. klient požaduje zpětný odkup nebo vyplacení dlouhodobé investice během krátké doby od počáteční investice nebo před datem vyplacení bez jasného důvodu, především vede-li to k finanční ztrátě nebo zaplacení vysokých transakčních poplatků;
- iii. klient požaduje během krátké doby opakovaný nákup a prodej akcií bez zjevné strategie nebo ekonomického důvodu;
- iv. neochota poskytnout informace týkající se hloubkové kontroly klienta o klientovi a skutečném majiteli;
- v. časté změny informací týkajících se hloubkové kontroly klienta nebo platebních údajů;
- vi. klient převádí finanční prostředky, které převyšují finanční prostředky potřebné pro tuto investici, a žádá o vrácení přeplatků;
- vii. okolnosti, za kterých klient využívá lhůty „na rozmyšlenou“ vzbuzují podezření;
- viii. používá několika účtů bez předchozího oznámení, zejména pokud jsou tyto účty vedeny v několika nebo vysoce rizikových jurisdikcích;
- ix. klient si přeje strukturovat vztah tak, aby se zapojilo více stran v různých jurisdikcích, například pověřené společnosti, především jestliže jsou tyto jurisdikce spojeny s vyšším rizikem praní peněz a financování terorismu.

b) Povaha klienta, například:

- i. klientem je společnost, svěřenský fond nebo jiné právní uspořádání, jehož struktura nebo funkce se podobají svěřenským fondům, se sídlem v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu (podniky by měly věnovat zvýšenou pozornost jurisdikcím, které nedodrží standardy mezinárodní daňové transparentnosti a sdílení informací);
- ii. klient je investičním subjektem, jenž neprovádí žádnou hloubkovou kontrolu klienta, nebo ji provádí pouze v omezené míře;
- iii. klient je neregulovaným investičním subjektem třetí strany;
- iv. vlastnická a řídicí struktura klienta je netransparentní;

- v. klient nebo skutečný majitel je politicky exponovanou osobou nebo má jiné vysoké postavení, které by mu mohlo umožnit zneužít svého postavení k osobnímu prospěchu;
  - vi. klient je neregulovanou pověřenou společností s neznámými akcionáři nebo společníky.
- c) Obchodní činnost klienta, například finanční prostředky klienta plynou z obchodní činnosti v odvětvích, která jsou spojena s vyšším rizikem finanční trestné činnosti, jako je stavebnictví, léčiva a zdravotnictví, obchod se zbraněmi a obrana, těžební průmysl nebo veřejné zakázky.

15.6. Faktory, které by mohly přispět ke snížení rizika:

- a) Klient je institucionálním investorem, jehož postavení bylo ověřeno vládou agenturou EHP, například prostřednictvím důchodového systému schváleného vládou.
- b) Klientem je orgán veřejné správy z jurisdikce EHP.
- c) Klientem je finanční instituce usazené v jurisdikci EHP.

**Rizikové faktory související s distribučními kanály**

15.7. Faktory, které by mohly přispět ke zvýšení rizika:

- a) složitý řetězec přijímání a předávání příkazů;
- b) složitý distribuční řetězec investičních produktů;
- c) obchodní systém má členy nebo účastníky nacházející se ve vysoce rizikových jurisdikcích.

**Rizikové faktory zemí nebo zeměpisných oblastí**

15.8. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Investor nebo jeho uschovatel má sídlo v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu.
- b) Finanční prostředky pocházejí z jurisdikce spojené s vysokou mírou rizika praní peněz a financování terorismu.

## Opatření

- 15.9. Při přípravě strategií a postupů v oblasti boje proti praní peněz a financování terorismu v souladu s povinnostmi vyplývajícími ze směrnice (EU) 2015/849 by podniky v tomto odvětví měly zohlednit, že v závislosti na druhu vykonávané činnosti se na ně budou vztahovat pravidla, podle kterých musejí o svých klientech shromáždit rozsáhlé informace. V takovém případě by měly zvážit, do jaké míry mohou být informace získané pro účely splnění směrnice o trzích finančních nástrojů II (MiFID II) a nařízení o infrastruktuře evropských trhů (EMIR) ve standardních situacích použity také ke splnění jejich povinností týkajících se hloubkové kontroly klienta.
- 15.10. Investiční manažeři by zejména měli mít o svých klientech dobré znalosti, které jim pomohou stanovit vhodná investiční portfolia. Shromážděné informace budou podobné těm, které podniky získávají pro účely boje proti praní peněz a financování terorismu.
- 15.11. Podniky by měly v rizikovějších situacích dodržovat pokyny zesílené hloubkové kontroly klienta stanovené v hlavě I. V případech, kdy je riziko související s obchodním vztahem vysoké, by podniky navíc měly:
- a) zjistit a případně ověřit totožnost hlavních investorů klienta podniku, pokud je klient neregulovaným investičním subjektem třetí strany;
  - b) chápat důvod každé platby nebo převodu na účet nebo z účtu neověřené třetí osoby.
- 15.12. V rozsahu povoleném vnitrostátními právními předpisy mohou investiční manažeři uplatňovat pokyny zjednodušené hloubkové kontroly klienta stanovené v hlavě I v situacích s nízkým rizikem.

## Obecný pokyn č. 16: Odvětvový pokyn pro poskytovatele investičních fondů

- 16.1. Poskytování investičních fondů se může týkat několika stran, například správce fondu, jmenovaných poradců, depozitáře a pověřených uschovatelů, registrátorů a v některých případech hlavních makléřů. Obdobně může být do distribuce podílů fondu zapojeno také několik stran, například smluvní zástupce, správce majetku s diskrečním a konzultačním přístupem, poskytovatelé služeb a nezávislí finanční poradci.
- 16.2. Typ a počet stran zapojených do procesu distribuce fondu závisí na povaze fondu a může ovlivnit množství informací, které fond o svých klientech a investorech zná. Fond nebo, pokud fond sám není povinnou osobou, správce fondu je odpovědný za plnění povinností v oblasti boje proti praní peněz a financování terorismu, ačkoliv povinnosti fondu v oblasti hloubkové kontroly klienta mohou vykonávat jedna nebo více dalších stran za určitých podmínek.
- 16.3. Investiční fondy mohou být zneužity osobami nebo subjekty pro účely praní peněz a financování terorismu:
- a) Retailové fondy jsou často distribuovány bez osobní přítomnosti partnera; dostupnost těchto fondů je obvykle snadná a poměrně rychlá a podíly v těchto fondech mohou být převáděny mezi různými stranami.
  - b) Alternativní investiční fondy, například hedgeové fondy, realitní fondy a soukromé kapitálové fondy, mívají obvykle menší počet investorů, kteří mohou být soukromými i institucionálními investory (penzijní fondy, fondy fondů). Tyto fondy, které jsou určeny pro omezený počet osob s vysokým čistým jměním nebo fondy rodinného majetku, mohou představovat pro účely praní peněz a financování terorismu podstatně vyšší riziko zneužití než retailové fondy, jelikož je u investorů pravděpodobnější, že budou schopni vykonávat nad majetkem fondu kontrolu. Pokud investoři nad těmito aktivy vykonávají kontrolu, jsou tyto fondy soukromými subjekty držby aktiv, která jsou označena jako faktor znamenající potenciálně vyšší riziko uvedený v příloze III směrnice (EU) 2015/849.
  - c) Bez ohledu na často střednědobou až dlouhodobou povahu investic, která může atraktivnost těchto produktů pro účely praní peněz snižovat, mohou přesto být pro oblast praní peněz atraktivní z důvodu své schopnosti růstu a vytváření příjmu.
- 16.4. Tento odvětvový pokyn se zaměřuje na:



- a) investiční fondy obchodující se svými akciemi nebo podíly podle čl. 3 odst. 2 písm. d) směrnice (EU) 2015/849; a
- b) správce fondů v případech, kdy investiční fond není zapsán v obchodním rejstříku.

Ostatní subjekty, které se podílejí na poskytování nebo distribuci podílů fondu, například zprostředkovatelé, musejí plnit své vlastní povinnosti hloubkové kontroly klienta a měly by se podle potřeby řídit příslušnými kapitolami těchto obecných pokynů.

Pro fondy a správce fondů by mohly být rovněž relevantní i odvětvové pokyny č. 8, 14 a 15.

## Rizikové faktory

### Rizikové faktory produktů, služeb nebo transakcí

16.5. Faktory, které by mohly přispět ke zvýšení rizika souvisejícího s fondem:

- a) Fond je určen pro omezený počet jednotlivců nebo fondů rodinného majetku, například soukromý fond nebo fond s jediným investorem.
- b) Je možné upisovat ve prospěch fondu a následně investice okamžitě vyplatit, aniž by to investorovi způsobilo vysoké administrativní náklady.
- c) S podíly nebo akciemi fondu je možné obchodovat, aniž by musel být v době obchodování informován fond nebo správce fondu;
- d) Informace o investorovi jsou známy několika subjektům.

16.6. Faktory, které by mohly přispět ke zvýšení rizika souvisejícího s upisováním:

- a) Upisování se týká účtů nebo třetích osob v několika jurisdikcích, zejména pokud jsou tyto jurisdikce spojeny s vysokým rizikem praní peněz a financování terorismu definovaným v obecných pokynech č. 2.9 až 2.15 hlavy I.
- b) Upisování se týká třetích upisovatelů nebo příjemců, především neočekávaných.

16.7. Faktory, které by mohly přispět ke snížení rizika souvisejícího s fondem:

- a) Nejsou možné platby třetím osobám a od třetích osob.
- b) Fond je otevřen pouze drobným investorům s omezenými investicemi.

### Rizikové faktory klienta

16.8. Faktory, které by mohly přispět ke zvýšení rizika: Chování klienta je neobvyklé, například:

- a) Odůvodnění investice postrádá zjevnou strategii nebo ekonomický účel nebo klient investuje v rozporu se svou celkovou finanční situací, pokud jsou tyto skutečnosti fondu nebo správci fondu známy.
- b) Klient požaduje opakovaný nákup a/nebo prodej podílových jednotek nebo akcií během krátké doby od počáteční investice nebo před datem vyplacení bez jasné strategie nebo důvodu, především vede-li to k finanční ztrátě nebo zaplacení vysokých transakčních poplatků.
- c) Klient převádí finanční prostředky, které převyšují hodnotu potřebnou pro investici, a žádá o vrácení přeplatků.
- d) Klient používá několik účtů bez předchozího oznámení, zejména pokud jsou tyto účty vedeny v několika jurisdikcích nebo jurisdikcích spojených s vyšším rizikem praní peněz a financování terorismu.
- e) Klient si přeje strukturovat vztah tak, aby se zapojilo více stran v různých jurisdikcích, například neregulované pověřené společnosti, především jestliže jsou tyto jurisdikce spojeny s vyšším rizikem praní peněz a financování terorismu.
- f) Klient náhle bez odůvodnění mění místo vypořádání, například vlivem změny svého bydliště.

16.9. Faktory, které by mohly přispět ke snížení rizika:

- a) klientem je institucionální investor, jehož postavení bylo ověřeno vládou agenturou z EHP, například vládou schváleným důchodovým systémem;
- b) klientem je podnik, na který se vztahují požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky dle směrnice (EU) 2015/849.

### **Rizikové faktory související s distribučními kanály**

16.10. Faktory, které by mohly přispět ke zvýšení rizika:

- a) složité distribuční kanály, které omezují dohled fondu nad svými obchodními vztahy a omezují jeho schopnost sledovat transakce, fond například využívá velké množství dílčích distributorů k distribuci ve třetích zemích;
- b) distributor se nachází v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu definovaným v obecné části těchto obecných pokynů.

#### 16.11. Faktory, které by mohly přispět ke snížení rizika:

- a) Fond akceptuje pouze určitý typ investorů s nízkým rizikem, například regulované podniky provádějící investování na bázi hlavní činnosti (např. životní pojišťovny) nebo podnikové důchodové systémy.
- b) Podíly ve fondu lze koupit a vyplatit pouze prostřednictvím podniku, na který se vztahují požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky dle směrnice EU 2015/849.

#### Rizikové faktory zemí nebo zeměpisných oblastí

#### 16.12. Faktory, které by mohly přispět ke zvýšení rizika:

- a) Finanční prostředky klientů nebo skutečných majitelů pocházejí z jurisdikcí spojených s vyšším rizikem praní peněz a financování terorismu, zejména jsou-li spojeny s vyšší mírou predikativních trestných činů v oblasti praní peněz.
- b) Klient požaduje, aby investice byla vyplacena na účet v úvěrové instituci nacházející se v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu.

### Opatření

16.13. Opatření, která by fondy nebo správci fondů měli přijmout za účelem splnění svých povinností týkajících se hloubkové kontroly klienta, budou záviset na tom, jak klient nebo investor (pokud investor není klientem) do fondu vstupuje. Fondy nebo správci fondů by měli rovněž při zohlednění míry rizika přijmout opatření ke zjištění a ověření totožnosti případných fyzických osob, kteří klienta v konečném důsledku vlastní nebo ovládají (nebo jejichž jménem se transakce provádějí), například požádáním potenciálního klienta při jeho první žádosti o připojení se k fondu o informaci, zda investuje svým jménem nebo zda je zprostředkovatelem investujícím jménem jiné osoby.

#### 16.14. Klient je:

- a) fyzická nebo právnická osoba, která přímo nakupuje podíly nebo akcie fondu na svůj vlastní účet, a nikoliv jménem jiných skrytých investorů; nebo
- b) podnik, který v rámci své hospodářské činnosti přímo nakupuje podíly nebo akcie svým jménem a vykonává kontrolu nad investicemi ku konečnému prospěchu jedné nebo několika třetích osob, které nad investicemi nebo investičními rozhodnutími nemají kontrolu; nebo
- c) podnik, například finanční zprostředkovatel, který jedná svým vlastním jménem a je zapsán v registru akcií/podílů fondu, ale jedná na účet a podle určitých

pokynů jedné nebo několika třetích osob (např. protože je finanční zprostředkovatel pověřenou osobou, makléřem, provozovatelem sdruženého/souhrnného účtu více klientů nebo provozovatelem podobného pasivního uspořádání); nebo

- d) klient podniku, například klient finančního zprostředkovatele, kdy podnik není zapsán v registru akcií/podílů fondu (např. protože investiční fond využívá služeb finančního zprostředkovatele k distribuci akcií nebo podílů fondu a investor nakupuje podíly nebo akcie prostřednictvím podniku a je zapsán v registru akcií nebo podílů fondu).

### Zesílená hloubková kontrola klienta

16.15. V situacích popsaných v obecných pokynech 16.14 písm. a) a b) by měla být fondem nebo správcem fondu ve vysoce rizikových situacích přijata opatření zesílené hloubkové kontroly klienta, například:

- a) získání dalších informací o klientech, například o pověsti a zázemí klienta, před uzavřením obchodního vztahu;
- b) přijetí dalších kroků k dalšímu ověření získaných dokumentů, údajů nebo informací;
- c) získání informací o zdroji finančních prostředků a/nebo zdroji majetku klienta a skutečného majitele klienta;
- d) požadování, aby platba zpětného odkupu byla provedena prostřednictvím původního účtu použitého k investici nebo účtu, jež je veden na samostatné nebo společné jméno klienta;
- e) zvýšení četnosti a intenzity sledování transakcí;
- f) požadování, aby první platba byla provedena prostřednictvím platebního účtu vedeného na samostatné nebo společné jméno klienta u úvěrové nebo finanční instituce regulované v EHP nebo u regulované úvěrové nebo finanční instituce ve třetí zemi uplatňující požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky dle směrnice (EU) 2015/849;
- g) získání souhlasu vrcholného vedení v okamžiku první transakce;
- h) zesílené sledování vztahů s klienty a jejich jednotlivých transakcí.

16.16. V situacích popsaných v obecném pokynu 16.14 písm. c), pokud je riziko zvýšené, zejména pokud je fond určen pro omezený počet investorů, musí se uplatnit opatření zesílené

hloubkové kontroly klienta, která mohou zahrnovat opatření stanovená v obecném pokynu 16.15 výše.

16.17. Jestliže má finanční zprostředkovatel sídlo v třetí zemi a navázal s fondem nebo správcem fondu vztah podobný korespondenčnímu bankovníctví, opatření popsaná v obecných pokynech č. 16.20 a 16.21 se nepoužijí. V takových případech by podniky při plnění svých povinností vyplývajících z článku 19 směrnice (EU) 2015/849 měly vůči zprostředkovateli uplatnit opatření zesílené hloubkové kontroly klienta uvedené v odvětvovém pokynu č. 8. 14 až 8.17.

16.18. V situacích popsaných v obecném pokynu 16.14 písm. d), pokud je riziko zvýšené, zejména pokud je fond určen pro omezený počet investorů, musí se uplatnit opatření zesílené hloubkové kontroly klienta, která mohou zahrnovat opatření stanovená v obecném pokynu 16.15 výše.

### Zjednodušená hloubková kontrola klienta

16.19. V situacích popsaných v obecných pokynech 16.14 písm. a) a 16.14 písm. b) v situacích s nižším rizikem, v rozsahu povoleném vnitrostátními právními předpisy, a za předpokladu, že finanční prostředky jsou ověřitelně převáděny na platební účet nebo z platebního účtu vedeného na samostatné nebo společné jméno klienta u úvěrové nebo finanční instituce regulované v EHP, je příkladem opatření zjednodušené hloubkové kontroly klienta, které může fond nebo správce fondu přijmout, využití zdroje finančních prostředků ke splnění některých požadavků hloubkové kontroly klienta.

16.20. V situacích popsaných v obecném pokynu 16.14 písm. c), je-li finanční zprostředkovatel klientem fondu nebo správcem fondu, by měl fond nebo správce fondu vůči finančnímu zprostředkovateli uplatňovat při zohlednění míry rizika opatření hloubkové kontroly klienta. Fond nebo správce fondu by měl rovněž při zohlednění míry rizika přijmout opatření ke zjištění a ověření totožnosti investorů souvisejících s finančním zprostředkovatelem, jelikož by tito investoři mohli být skutečnými majiteli finančních prostředků investovaných prostřednictvím zprostředkovatele. V rozsahu povoleném vnitrostátními právními předpisy mohou fondy nebo správci fondů v situacích s nízkým rizikem uplatňovat opatření zjednodušené hloubkové kontroly klienta podobná opatřením uvedeným v hlavě I obecných pokynů za těchto podmínek:

- a) Na finančního zprostředkovatele se vztahují povinnosti v oblasti boje proti praní peněz a financování terorismu v jurisdikci EHP nebo ve třetí zemi, která má požadavky v oblasti boje proti praní peněz a financování terorismu neméně přísné než požadavky dle směrnice (EU) 2015/849.
- b) Nad finančním zprostředkovatelem je vykonáván účinný dohled z hlediska dodržování těchto požadavků.

- c) Fond nebo správce fondu přijal při zohlednění míry rizika kroky k zajištění toho, aby riziko praní peněz a financování terorismu související s obchodním vztahem bylo nízké, a to mimo jiné na základě posouzení obchodní činnosti finančního zprostředkovatele, druhů klientů, kterým finanční zprostředkovatel poskytuje služby, a jurisdikcí, kterých se obchodní činnost zprostředkovatele týká, ze strany fondu nebo správce fondu.
- d) Fond nebo správce fondu přijal při zohlednění míry rizika kroky k zajištění toho, aby zprostředkovatel uplatňoval přísná opatření při zohlednění míry rizika hloubkové kontroly klienta vůči svým vlastním klientům a skutečným majitelům svých klientů. V rámci toho by měl fond nebo správce fondu přijmout opatření při zohlednění míry rizika k posouzení adekvátnosti strategií a postupů zprostředkovatele v oblasti hloubkové kontroly klienta, například na základě veřejně dostupných informací o dodržování předpisů ze strany zprostředkovatele nebo o přímé spolupráci se zprostředkovatelem.
- e) Fond nebo správce fond přijal kroky při zohlednění míry rizika k zajištění, že zprostředkovatel poskytne informace o hloubkové kontrole klienta a dokumenty o souvisejících investorech okamžitě na vyžádání, například zahrnutím příslušných ustanovení do smlouvy se zprostředkovatelem nebo testováním schopnosti zprostředkovatele poskytovat informace hloubkové kontroly klienta na vyžádání.

16.21. V situacích popsaných v obecném pokynu 16.14 písm. d) by měl fond nebo správce fondu při zohlednění míry rizika uplatňovat opatření hloubkové kontroly klienta vůči konečnému investorovi jakožto klientovi fondu nebo správce fondu. Ke splnění svých povinností v oblasti hloubkové kontroly klienta se může fond nebo správce fondu spoléhat na zprostředkovatele v souladu s podmínkami stanovenými v kapitole II oddílu 4 směrnice (EU) 2015/849, které se na ně vztahují.

16.22. V rozsahu povoleném vnitrostátními právními předpisy mohou fondy nebo správci fondů uplatňovat opatření zjednodušené hloubkové kontroly klienta v situacích s nízkým rizikem. Jsou-li splněny podmínky uvedené v obecném pokynu 16.20, mohou opatření zjednodušené hloubkové kontroly klienta znamenat, že fond nebo správce fondu získá údaje o totožnosti z registru akcií fondu a informace uvedené v čl. 27 odst. 1 směrnice (EU) 2015/849, které musí fond nebo správce fondu obdržet od zprostředkovatele v přiměřené lhůtě. Fond nebo správce fondu by měl tuto lhůtu stanovit v souladu s přístupem založeným na posouzení míry rizika.

## Obecný pokyn č. 17 Odvětvový pokyn pro regulované platformy skupinového financování

- 17.1. Pro účely tohoto odvětvového pokynu se použijí a měly by se uplatnit následující definice uvedené v čl. 2 odst. 1 nařízení (EU) 2020/1503: „služba skupinového financování“, „platforma skupinového financování“, „poskytovatel služeb skupinového financování“, „vlastník projektu“ a „investor“. Tento odvětvový pokyn se odkazuje na „klienty“ ve smyslu pojmu „klient“ vymezeného v čl. 2 odst. 1 písm. g) téhož nařízení.
- 17.2. Poskytovatelé služeb skupinového financování by měli rozpoznat rizika vyplývající z toho, že platformy skupinového financování nejsou omezovány hranicemi a klienti poskytovatelů služeb skupinového financování se mohou nacházet kdekoliv na světě, včetně vysoce rizikových jurisdikcí. Poskytovatelé služeb skupinového financování by měli znát své klienty, aby předešli používání svých platform skupinového financování k financování fiktivních investičních projektů z nezákonných finančních prostředků nebo aby předešli zneužívání pro účely financování terorismu, kdy je udán fiktivní důvod pro nikdy nerealizovaný projekt skupinového financování a finanční prostředky ze skupinového financování jsou následně použity k financování teroristického útoku.
- 17.3. Poskytovatelé služeb skupinového financování by měli kromě rizikových faktorů a opatření uvedených v hlavě I zvážit ty uvedené v tomto odvětvovém pokynu. Poskytovatelé služeb skupinového financování, kteří poskytují investiční služby, by se měli rovněž řídit odvětvovým pokynem č. 16.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 17.4. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika:
- a) Poskytovatel služeb skupinového financování vybírá finanční prostředky prostřednictvím platformy skupinového financování, ale umožní pozdější následné předání, včetně obchodních modelů, kdy:
    - i. peněžní prostředky jsou vybírány na neurčený projekt a následně ponechány na účtu investora, dokud není projekt určen; nebo
    - ii. peněžní prostředky jsou vybírány, ale mohou být vráceny investorům, není-li dosaženo cíle získávání finančních prostředků nebo neobdrží-li peněžní prostředky vlastník projektu.

- b) Poskytovatel služeb skupinového financování povoluje předčasný zpětný odkup investic, předčasné splacení úvěrů nebo další prodej investic nebo úvěrů na sekundárních trzích.
- c) Poskytovatel služeb skupinového financování neomezuje velikost, objem nebo hodnotu transakcí, nabití nebo zpětný odkup probíhající prostřednictvím platformy skupinového financování nebo výši finančních prostředků uložených na účtech jednotlivých investorů.
- d) Poskytovatel služeb skupinového financování umožňuje investorům provádět platbu ve prospěch vlastníka projektu prostřednictvím platformy skupinového financování s použitím nástrojů, které jsou mimo oblast působnosti jakéhokoli regulačního režimu nebo na které se vztahují méně přísné požadavky v oblasti boje proti praní peněz a financování terorismu než požadavky dle směrnice (EU) 2015/849.
- e) Poskytovatel služeb skupinového financování přijímá investice v hotovosti od investorů nebo povoluje prostřednictvím platformy skupinového financování výběry hotovosti investorům, kteří jsou fyzickými osobami nebo neregulovanými právníckými osobami.
- f) Poskytovatel služeb skupinového financování umožňuje investorům nebo věřitelům finanční páku, zvýhodněný zpětný odkup nebo zaručenou návratnost.
- g) Poskytovatel služeb skupinového financování nepotvrzuje svůj závazek zpětného odkupu cenných papírů a není stanovena lhůta tohoto odkupu.
- h) Pro jiné než kapitálové nástroje nejsou srozumitelně stanoveny nominální úroková sazba, datum, od něhož jsou úroky splatné, data úrokových plateb, datum splatnosti a příslušný výnos.
- i) Poskytovatel služeb skupinového financování umožňuje provádění plateb přes platformu skupinového financování ve virtuálních měnách.
- j) Poskytovatel služeb skupinového financování umožňuje investorům a vlastníkům projektu mít na platformě skupinového financování více účtů, které nejsou svázány s konkrétními projekty skupinového financování.
- k) Poskytovatel služeb skupinového financování umožňuje na platformě skupinového financování převody mezi investory nebo vlastníky projektu.

17.5. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke snížení rizika:



- a) Poskytovatel služeb skupinového financování vyžaduje, aby finanční prostředky určené k investování, zpětnému odkupu, půjčování nebo splacení byly ověřitelně čerpány z účtu nebo zaslány na účet vedený na samostatné nebo společné jméno klienta u úvěrové nebo finanční instituce nebo platební instituce povolené v souladu se směrnicí (EU) 2015/2366, na které se vztahují požadavky v oblasti boje proti praní peněz a financování terorismu, jež nejsou méně přísné než požadavky dle směrnice (EU) 2015/849.
- b) Poskytovatel služeb skupinového financování stanovuje pro investice, půjčování, zpětný odkup a splacení probíhající přes platformu skupinového financování nízké limity z hlediska výše peněžních prostředků a počtu plateb.
- c) Poskytovatel služeb skupinového financování vyžaduje pevnou nebo delší dobu držení investic nebo dobu splacení úvěrů získaných přes platformu skupinového financování.
- d) Poskytovatel služeb skupinového financování omezuje výši finančních prostředků, které je možné v určitém okamžiku mít na jakémkoli účtu na platformě skupinového financování.
- e) Poskytovatel služeb skupinového financování využívá technologie k rozpoznání toho, zda investoři nebo vlastníci projektu používají VPN nebo jiné technologie skrývající skutečnou polohu a zařízení při používání platformy skupinového financování.
- f) Poskytovatel služeb skupinového financování neumožňuje vytvoření více účtů na platformě skupinového financování.

### Rizikové faktory klienta

17.6. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a) Povaha nebo chování klienta jsou neobvyklé, například:
  - i. Důvod investice nebo úvěru postrádá zjevnou strategii nebo ekonomický účel.
  - ii. Investor žádá o zpětné vyplacení investice v krátké lhůtě od prvotní investice.
  - iii. Investor žádá o zvýhodněné podmínky nebo fixní návratnost investice.

- iv. Investor nebo vlastník projektu převádí na platformu finanční prostředky, které převyšují částku potřebnou pro projekt/úvěr, a pak žádá o vrácení přeplatků;
  - v. Investorem nebo vlastníkem projektu je fyzická osoba nebo právnická osoba spojená s vyššími úrovněmi rizik praní peněz;
  - vi. Vlastník projektu, neočekávaně nebo bez rozumného vysvětlení, urychluje dohodnutý harmonogram zpětného odkupu/splácení prostřednictvím jednorázových plateb nebo předčasného ukončení; nebo
  - vii. Zdá se, že vlastník projektu se zdráhá poskytnout informace o projektu nebo iniciativě usilující o skupinové financování.
  - viii. Zdroj finančních prostředků pro investici je nejasný a investor se zdráhá tuto informaci na žádost poskytovatele služeb skupinového financování poskytnout. Míra investovaných aktiv převyšuje objem odhadovaných likvidních aktiv investora. Investované finanční prostředky jsou vypůjčené.
  - ix. Investor nemá bydliště nebo sídlo v zemi platformy skupinového financování nebo investování, ani nemá žádné jiné napojení na tuto zemi.
  - x. Investor nebo vlastník projektu je politicky exponovanou osobou.
  - xi. Investor odmítá poskytnout požadovanou hloubkovou kontrolu klienta.
- b) Investor nebo vlastník projektu převádí virtuální měnu.
  - c) Investor nebo vlastník projektu jsou spojováni s negativními zprávami.
  - d) Na investora nebo vlastníka projektu jsou uvaleny sankce.

### **Rizikové faktory související s distribučními kanály**

17.7. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika

- a) Poskytovatel služeb skupinového financování provozuje platformu skupinového financování zcela on-line bez adekvátních bezpečnostních opatření, jako jsou

elektronická identifikace osoby používající elektronické podpisy nebo elektronické prostředky identifikace splňující nařízení (EU) č. 910/2014.

- b) Klienti jsou získáváni bez osobní přítomnosti přes platformu skupinového financování bez jakýchkoli zavedených bezpečnostních opatření.
- c) Poskytovatel služeb skupinového financování vykonává činnost mimo jakýkoliv regulační režim, a tudíž nemusí existovat opatření, která by jinak sloužila k rozpoznání a zmírnění potenciálního používání platformy skupinového financování pro účely praní peněz a financování terorismu. Uvedeným není dotčeno uplatnění obecného pokynu č. 11.

17.8. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke snížení rizika:

- a) Poskytovatel služeb skupinového financování používá úvěrovou instituci nebo finanční instituci k nakládání s penězi nebo pro služby poukazování peněz. Popřípadě si poskytovatel služeb skupinového financování otevře u regulované úvěrové instituce nebo finanční instituce účet na vlastní jméno, přes který protékají peněžní transakce mezi vlastníky projektu a investory.
- b) Poskytovatel služeb skupinového financování provozující platformu skupinového financování je oprávněn jako platební instituce na základě směrnice (EU) 2015/2366 nebo jako zástupce platební instituce oprávněné na základě směrnice (EU) 2015/2366 a přímo zpracovává peněžní transakce mezi investory a vlastníky projektu. Uvedeným není dotčeno uplatnění obecného pokynu č. 11.
- c) Investoři a vlastníci projektu se osobně setkali nebo byli představeni regulovaným finančním zprostředkovatelem (úvěrovou institucí nebo investičním podnikem), jenž u všech klientů (vlastníků projektu a investorů) provádí úplnou hloubkovou kontrolu klienta.

### **Rizikové faktory zemí nebo zeměpisných oblastí**

17.9. Poskytovatel služeb skupinového financování by měl vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a) Poskytovatel služeb skupinového financování má celosvětovou působnost a spojuje investory, vlastníky projektu a projekty z různých jurisdikcí.
- b) Finanční prostředky plynou z osobních nebo obchodních vazeb na jurisdikci, kterou důvěryhodné zdroje označují za jurisdikci s významnou úrovní korupce

nebo jiné trestné činnosti, jako je terorismus, praní peněz, výroba a dodávky nedovolených drog, či jiné predikativní trestné činy.

- c) Vlastník projektu, investor nebo jejich případní příslušní skuteční majitelé se nacházejí v jurisdikci spojené s vyššími riziky praní peněz a financování terorismu nebo v jurisdikci bez účinného dohledu v oblasti boje proti praní peněz a financování terorismu. Poskytovatelé služeb skupinového financování by měli věnovat zvýšenou pozornost jurisdikcím, o nichž je známo, že financují nebo podporují teroristické aktivity nebo že v nich působí skupiny páchající teroristické činy, a jurisdikcím, na něž se vztahují finanční sankce, embarga nebo opatření (vydaná například Evropskou unií nebo Organizací spojených národů) související s terorismem, financováním terorismu nebo šířením zbraní.

## Opatření

- 17.10. Poskytovatelé služeb skupinového financování, kteří jsou povinnými osobami jako platební instituce oprávněné na základě směrnice (EU) 2015/2366, nebo jednají jako zástupce platební instituce oprávněné na základě směrnice (EU) 2015/2366, by měli příslušná opatření v odvětvovém pokynu č. 11 uplatňovat i na své služby skupinového financování.
- 17.11. Poskytovatelé služeb skupinového financování, kteří jsou povinnými osobami jako investiční podniky oprávněné na základě směrnice (EU) 2014/65, by měli příslušná opatření v odvětvovém pokynu č. 15 uplatňovat i na své služby skupinového financování.
- 17.12. Poskytovatelé služeb skupinového financování, kteří jsou povinnými osobami jako úvěrové instituce oprávněné na základě směrnice (EU) 2013/36, by měli příslušná opatření v odvětvovém pokynu č. 9 uplatňovat i na své služby skupinového financování.
- 17.13. Podnik, který je oprávněný jako poskytovatel služeb skupinového financování podle vnitrostátního práva a na který se vztahují vnitrostátní právní předpisy v oblasti boje proti praní peněz a financování terorismu, by měl uplatňovat tento odvětvový pokyn a další relevantní odvětvové pokyny obdobně, aby se nad poskytovateli služeb skupinového financování usazenými v Unii zajistil harmonizovaný a účinný dohled v oblasti boje proti praní peněz a financování terorismu.

## Hlubková kontrola klienta

- 17.14. Poskytovatelé služeb skupinového financování by měli opatření hlubkové kontroly klienta v souladu s hlavou I uplatňovat na všechny své klienty, ať už se jedná o investory, nebo vlastníky projektu.
- 17.15. Poskytovatelé služeb skupinového financování, kteří se při vybírání finančních prostředků od klientů nebo při převádění finančních prostředků klientům spoléhají na úvěrové instituce nebo finanční instituce, by se měli řídit rizikovými faktory souvisejícími s distribučními

kanály v hlavě I a zejména by se měli ujistit, že tyto úvěrové instituce nebo finanční instituce zavedly vhodná opatření hloubkové kontroly klienta.

### Zesílená hloubková kontrola klienta

17.16. Pokud je riziko související s příležitostnou transakcí nebo obchodním vztahem vysoké, platforma poskytovatele služeb skupinového financování by měla uplatňovat následující opatření zesílené hloubkové kontroly klienta:

- a) získání dalších informací od klientů provádějících transakce na příslušné platformě, například informací o jejich investičním záměru a zkušenostech, pozadí a pověsti, před uzavřením obchodního vztahu (například vyhledáváním v otevřených zdrojích nebo negativních zpráv v médiích nebo z informačních zpráv třetích osob s cílem vypracovat úplnější profil klienta);
- b) přijetí dalších kroků k dalšímu ověření získaných dokumentů, údajů nebo informací;
- c) získání informací o zdroji finančních prostředků klientů a jejich skutečných majitelích;
- d) požadování, aby platba zpětného odkupu nebo splátky byla provedena prostřednictvím původního účtu použitého k investici nebo účtu, jenž je veden na samostatné nebo společné jméno dotyčných klientů;
- e) zvýšení četnosti a intenzity sledování transakcí;
- f) požadování, aby první platba investice nebo úvěru byla provedena prostřednictvím platebního účtu vedeného na samostatné nebo společné jméno dotčené osoby u úvěrové nebo finanční instituce regulované v EHP nebo u regulované úvěrové nebo finanční instituce ve třetí zemi uplatňující požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky dle směrnice (EU) 2015/849;
- g) získání souhlasu vrcholného vedení v okamžiku transakce, kdy klienti používají platformu poprvé;
- h) zesílené sledování vztahů s klienty a jejich jednotlivých transakcí.

### Zjednodušená hloubková kontrola klienta

17.17. V situacích s nízkým rizikem a v rozsahu, který dovolují vnitrostátní právní předpisy, mohou platformy skupinového financování uplatňovat opatření zjednodušené hloubkové kontroly klienta, která mohou zahrnovat:

- a) ověření totožnosti klienta a případně jeho skutečného majitele při uzavření obchodního vztahu v souladu s čl. 14 odst. 2 směrnice (EU) 2015/849; nebo
- b) za předpokladu, že platba čerpaná z účtu samostatným nebo společným jménem klienta u regulované úvěrové nebo finanční instituce v zemi EHP splňuje požadavky stanovené v čl. 13 odst. 1 písm. a) a b) směrnice (EU) 2015/849.

## Obecný pokyn č. 18: Odvětvový pokyn pro poskytovatele služeb iniciování platby a poskytovatele služeb informování o účtu

18.1. Při uplatňování tohoto obecného pokynu by podniky měly vzít v úvahu definice v čl. 4 odst. 18 a 19 směrnice (EU) 2015/2366, podle kterých:

- a) poskytovatelem služeb iniciování platby je poskytovatel platebních služeb vykonávající služby iniciování platby, jimiž se podle vymezení v čl. 4 odst. 15 směrnice (EU) 2015/2366 rozumí služby k iniciování platebního příkazu na žádost uživatele platebních služeb ve vztahu k platebnímu účtu vedenému u jiného poskytovatele platebních služeb;
- b) poskytovatelem služeb informování o účtu je poskytovatel platebních služeb nabízející služby informování o účtu, jimiž se podle vymezení v čl. 4 odst. 16 směrnice (EU) 2015/2366 rozumí služby on-line, jejichž cílem je poskytnout konsolidované informace o jednom nebo více platebních účtech uživatele platebních služeb vedených buď u jiného poskytovatele platebních služeb, nebo u více než jednoho poskytovatele platebních služeb.

18.2. Podniky by měly zohlednit skutečnost, že přestože jsou poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu povinnými osobami podle směrnice (EU) 2015/849, s nimi spojené inherentní riziko praní peněz a financování terorismu je omezené vzhledem k tomu, že:

- a) poskytovatelé služeb iniciování platby jsou sice součástí platebního řetězce, ale sami neprovádějí platební transakce a nedrží finanční prostředky uživatelů platebních služeb;
- b) poskytovatelé služeb informování o účtu nejsou součástí platebního řetězce a nedrží finanční prostředky uživatele platebních služeb.

18.3. Při nabízení služeb iniciování platby nebo služeb informování o účtu by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli společně s hlavou I zohlednit ustanovení tohoto odvětvového pokynu.

## Rizikové faktory

### Rizikové faktory klienta

18.4. Při posuzování rizika praní peněz a financování terorismu by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli vzít v úvahu alespoň následující faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a) V případě poskytovatelů služeb iniciování platby: Klient převádí z různých platebních účtů stejnému příjemci finanční prostředky, které dohromady představují vysokou

částku, bez jasného ekonomického nebo zákonného důvodu nebo které u poskytovatele služeb iniciování platby vzbuzují důvodné podezření, že se klient snaží vyhnout určitým limitům pro sledování transakcí;

- b) V případě poskytovatelů služeb informování o účtu: klient převádí z různých platebních účtů stejnému příjemci finanční prostředky nebo dostává od stejného plátce na různé platební účty finanční prostředky, které dohromady představují vysokou částku, bez jasného ekonomického nebo zákonného důvodu, nebo které u poskytovatele služeb informování o účtu vzbuzují důvodné podezření, že se klient snaží vyhnout určitým limitům pro sledování transakcí.

### Rizikové faktory související s distribučními kanály

- 18.5. Při posuzování rizik praní peněz a financování terorismu se poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu mohou odvolat na stanovisko evropských orgánů dohledu k využívání inovativních řešení v procesu hloubkové kontroly klienta (JC 2017 81).

### Rizikové faktory zemí nebo zeměpisných oblastí

- 18.6. Při posuzování rizik praní peněz a financování terorismu by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli vzít v úvahu alespoň následující faktory, které mohou potenciálně přispět ke zvýšení rizika, zejména pak v případech, kdy klient k provádění plateb používá více účtů vedených u různých poskytovatelů platebních služeb spravujících účet:

- a) V případě poskytovatelů služeb iniciování platby: klient iniciuje platbu do jurisdikce spojené s vyšším rizikem praní peněz a financování terorismu, do vysoce rizikové třetí země nebo osobě, o které je známo, že má vazby na tyto jurisdikce.
- b) V případě poskytovatelů služeb informování o účtu: Klient dostává finanční prostředky z jurisdikcí nebo posílá finanční prostředky do jurisdikcí spojených s vyšším rizikem praní peněz a financování terorismu, do vysoce rizikové třetí země nebo osobě, o které je známo, že má vazby na tyto jurisdikce, nebo klient spojuje platební účty vedené na jméno různých osob ve více než jedné jurisdikci.

- 18.7. Při posuzování rizik praní peněz a financování terorismu by poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby měli vzít v úvahu následující faktory, které mohou potenciálně přispět ke snížení rizika:

- a) V případě poskytovatelů služeb iniciování platby: klient iniciuje platební transakce do členské země EHP nebo do třetí země, která uplatňuje požadavky v oblasti boje proti praní peněz a financování terorismu, které nejsou méně přísné než požadavky dle směrnice (EU) 2015/849.
- b) V případě poskytovatelů služeb informování o účtu: platební účty klienta jsou vedeny v členské zemi EHP.



## Opatření

### 18.8. Klient je:

- a) V případě poskytovatelů služeb iniciování platby: klient je fyzickou nebo právnickou osobou, která má platební účet a požaduje iniciování platebního příkazu z tohoto účtu. V konkrétním případě, kdy má poskytovatel služeb iniciování platby obchodní vztah ve smyslu čl. 3 odst. 13 směrnice (EU) 2015/849 týkající se nabízení služeb iniciování platby s příjemcem, a ne s plátcem, a plátce používá příslušného poskytovatele služeb iniciování platby k iniciování jediné nebo jednorázové transakce příslušnému příjemci, klient poskytovatele služeb iniciování platby je pro účely těchto obecných pokynů příjemcem, a ne plátcem. Uvedeným není dotčen článek 11 směrnice (EU) 2015/849 a hlava I těchto obecných pokynů, zejména pak v souvislosti s příležitostnými transakcemi, a povinnosti poskytovatelů služeb iniciování platby podle směrnice (EU) 2015/2366 a dalších platných právních předpisů EU.
- b) V případě poskytovatelů služeb informování o účtu: klient je fyzickou nebo právnickou osobou, která má s poskytovatelem služeb informování o účtu smlouvu. Může se jednat o fyzickou nebo právnickou osobou, která je majitelem platebních účtů.

18.9. Poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu by měli přijmout odpovídající opatření k identifikaci a posouzení rizika praní peněz a financování terorismu souvisejícího s jejich obchodní činností. Za tímto účelem by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli vzít v úvahu všechny údaje, které mají k dispozici. Druh údajů, které mají k dispozici, bude záviset mimo jiné na konkrétní službě nabízené klientovi, na výslovném souhlasu uživatele platebních služeb a na tom, které údaje jsou nezbytné k poskytnutí služeb, a to v souladu s čl. 66 odst. 3 písm. f) a čl. 67 odst. 2 písm. f) směrnice (EU) 2015/2366.

18.10. S ohledem na článek 11 směrnice (EU) 2015/849 by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli určit rozsah opatření hloubkové kontroly klienta při zohlednění míry rizika, s přihlédnutím ke všem údajům, které mají k dispozici s výslovným souhlasem uživatele platebních služeb, a údajům, které jsou nezbytné k poskytnutí služeb, a to v souladu s čl. 66 odst. 3 písm. f) a čl. 67 odst. 2 písm. f) směrnice (EU) 2015/2366. Ve většině případů nízká míra inherentního rizika spojeného s těmito obchodními modely znamená, že se bude běžně provádět zjednodušená hloubková kontrola klienta. V těchto případech nízkého rizika, pokud je uplatňování opatření zjednodušené hloubkové kontroly klienta zakázáno nebo omezeno vnitrostátními předpisy, mohou poskytovatelé služeb informování o účtu a poskytovatelé služeb iniciování platby odpovídajícím způsobem přizpůsobit opatření hloubkové kontroly klienta a uplatnit obecný pokyn č. 18.15.

18.11. Sledování: V rámci svých procesů hloubkové kontroly klienta by poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu měli zajistit, že jejich systémy v oblasti boje proti praní peněz a financování terorismu jsou nastaveny tak, že upozorňují na neobvyklou nebo podezřelou transakční aktivitu, s přihlédnutím ke všem údajům, které

mají k dispozici s výslovným souhlasem uživatele platebních služeb, a údajům, které jsou nezbytné k poskytnutí služeb, a to v souladu s čl. 66 odst. 3 písm. f) a čl. 67 odst. 2 písm. f) směrnice (EU) 2015/2366. Poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu by k odhalení neobvyklé transakční aktivity měli používat vlastní nebo externí typologie.

### **Hlubková kontrola klienta**

18.12. Poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu by měli u svých klientů uplatňovat opatření hloubkové kontroly klienta v souladu s hlavou I.

18.13. Podle článku 13 směrnice (EU) 2015/849 by se poskytovatel služeb informování o účtu měl při přidání každého účtu zeptat klienta nebo jinými způsoby ověřit, zda se jedná o jeho vlastní účet, sdílený účet nebo účet právnické osoby, k němuž má klient přístup na základě zmocnění (např.: účet sdružení, firemní účet).

### **Zesílená hloubková kontrola klienta**

18.14. V situacích s vyšším rizikem by podniky měly uplatňovat opatření zesílené hloubkové kontroly klienta uvedená v hlavě I.

### **Zjednodušená hloubková kontrola klienta**

18.15. Podniky by vždy měly znát jméno svého klienta. Poskytovatelé služeb iniciování platby a poskytovatelé služeb informování o účtu mohou zvážit uplatnění zjednodušené hloubkové kontroly klienta, jako je:

- a) spoléhání se na zdroj finančních prostředků jako na doklad totožnosti klienta, jsou-li známé údaje o platebním účtu klienta a je-li platební účet veden u poskytovatele platebních služeb regulovaného v EHP;
- b) odložení ověření totožnosti klienta na určité pozdější datum po uzavření vztahu. V tomto případě by podniky měly zajistit, že jejich strategie a postupy určují okamžik, kdy se hloubková kontrola klienta použije;
- c) předpokládání povahy a účelu obchodního vztahu;

## Obecný pokyn č. 19: Odvětvový pokyn pro podniky vykonávající činnosti směnáren

- 19.1. Podniky poskytující směnářské služby by měly spolu s hlavou I přihlédnout k ustanovením uvedeným v tomto obecném pokynu.
- 19.2. Podniky by měly vzít v úvahu inherentní rizika směnářských služeb, v důsledku kterých mohou být vystaveny významným rizikům praní peněz a financování terorismu. Podniky by si měly uvědomovat, že tato rizika vyplývají z jednoduchosti transakcí, jejich rychlosti a častého hotovostního charakteru. Podniky by rovněž měly přihlédnout k tomu, že jejich znalost rizika praní peněz a financování terorismu spojeného s klientem může být omezená kvůli tomu, že namísto uzavření obchodního vztahu obvykle provádí příležitostné transakce.

### Rizikové faktory

#### Rizikové faktory produktů, služeb a transakcí

- 19.3. Podniky by měly vzít v úvahu následující faktory, které mohou potenciálně přispět ke zvýšení rizika:
- a) Transakce je neobvykle velká v absolutním vyjádření nebo ve srovnání s ekonomickým profilem klienta;
  - b) Transakce nemá zjevný ekonomický nebo finanční účel;
- 19.4. Podniky by měly vzít v úvahu následující faktory, které mohou potenciálně přispět ke snížení rizika:
- a) Směňovaná částka je nízká; podniky by však měly vzít v úvahu, že nízké částky samy o sobě nepostačují k tomu, aby riziko financování terorismu zmírňovaly;

#### Rizikové faktory klienta

- 19.5. Podniky by měly vzít v úvahu následující faktory, které mohou potenciálně přispět ke zvýšení rizika:
- a) Chování klienta:
    - i. transakce klienta jsou těsně pod platným limitem pro hloubkovou kontrolu klienta, zejména pak v případě, kdy jsou transakce časté nebo probíhají během krátké doby;
    - ii. klient nemůže poskytnout nebo neposkytne informace o původu finančních prostředků;

- iii. klient požaduje výměnu velkých částek v cizí měně, která není směnitelná nebo není často používána;
- iv. klient vyměňuje velké množství bankovek s nízkou nominální hodnotou v jedné měně za bankovky s vyšší nominální hodnotou v jiné měně; nebo naopak.
- v. Chování klienta není z ekonomického hlediska smysluplné;
- vi. Klient ve stejný den navštíví více poboček stejného podniku (je-li to podniku známo);
- vii. Klient se ptá na limit pro identifikaci anebo odmítá odpovědět na běžné nebo obvyklé otázky;
- viii. Klient převádí finanční prostředky v jedné cizí měně do jiné cizí měny;
- ix. Výměna velkých částek nebo časté výměny, které nesouvisí s obchodní činností klienta;
- x. Měna prodávaná klientem neodpovídá zemi jeho státní příslušnosti nebo bydliště;
- xi. Vzhledem ke své poloze klient bez logického vysvětlení kupuje měnu z neobvyklého místa;
- xii. Klient kupuje měnu, která neodpovídá tomu, co je známo o cílové zemi klienta;
- xiii. Klient kupuje nebo prodává vysokou částku v měně z jurisdikce spojené se zvýšenou mírou predikativních trestných činů praní peněz nebo teroristické činnosti;

b) Obchodní činnost klienta:

- i. Obchodní činnost klienta je spojena s vyšším rizikem praní peněz a financování terorismu, například kasina, nákup/prodej drahých kovů a drahokamů, obchodník se sběrnými surovinami;

### **Rizikové faktory související s distribučními kanály**

19.6. Podniky by měly vzít v úvahu následující faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a) Služba je poskytována zcela on-line bez adekvátních bezpečnostních opatření.
- b) Služby jsou poskytovány prostřednictvím sítě zástupců.

## Rizikové faktory zemí nebo zeměpisných oblastí

19.7. Podniky by měly vzít v úvahu následující faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a) Směnárna se nachází v jurisdikci spojené s vyšším rizikem praní peněz a financování terorismu.

## Opatření

19.8. Jelikož je tato obchodní činnost primárně založena na transakcích, měly by podniky zvážit, které systémy sledování a kontroly zavedou, aby zajistily, že jsou schopny odhalit pokusy o praní peněz a financování terorismu, a to i v případě neúplných nebo chybějících informací hloubkové kontroly klienta o klientovi. Tento systém sledování by se měl přizpůsobit objemu obchodní činnosti a vystavení riziku.

## Hloubková kontrola klientů

19.9. Podniky by ve svých interních strategiích a postupech měly jasně vymežit, v jakém okamžiku by u příležitostných klientů měly provést hloubkovou kontrolu klienta. Uvedené by mělo zahrnovat:

- a) situaci, kdy transakce nebo identifikované propojené transakce dosahují částky nejméně 15 000 EUR nebo případného nižšího vnitrostátního limitu. Strategie a postupy by měly jasně vymežovat, v jakém okamžiku se řada jednorázových transakcí stává obchodním vztahem, přičemž se přihlédne ke specifickým činnostem podniku (tj. k průměrné běžné velikosti jednorázové transakce u obvyklé klientely).
- b) situaci, kdy existuje podezření na praní peněz nebo financování terorismu.

19.10. Podniky by měly v každém případě zavést systémy a kontroly podle obecného pokynu 4.7 písm. b) za účelem:

- a) identifikace propojených transakcí (například s cílem zjistit, zda se stejný klient během krátké doby obrací na více poboček);
- b) přiměřeného a účinného sledování transakcí s ohledem na velikost podniku, počet jeho poboček, velikost a objem transakcí; druh vykonávaných činností, distribučních kanálů a rizik identifikovaných při posouzení rizik v rámci celého podniku.

## Zesílená hloubková kontrola klienta

19.11. Pokud je riziko související s příležitostnou transakcí nebo obchodním vztahem vysoké, měly by podniky uplatňovat zesílenou hloubkovou kontrolu klienta v souladu s hlavou I, včetně

případného zesíleného sledování transakcí (např. zvýšení četnosti nebo nižší limity), získání dalších informací o povaze a účelu obchodní činnosti nebo o zdroji finančních prostředků klienta.

### Zjednodušená hloubková kontrola klienta

19.12. V situacích s nízkým rizikem by podniky v rozsahu, který dovolují vnitrostátní právní předpisy, měly zvážit uplatnění zjednodušené hloubkové kontroly klienta, jako je:

- a) odložení ověření totožnosti klienta na určité pozdější datum po uzavření vztahu.
- b) ověření totožnosti klienta na základě platby provedené z účtu vedeného pod samostatným nebo společným jménem klienta u úvěrové nebo finanční instituce regulované v EHP.

## Obecný pokyn č. 20: Odvětvový pokyn pro podnikové financování

- 20.1. Podniky poskytující služby podnikového financování (tzv. corporate finance) by měly vzít v úvahu inherentní rizika praní peněz a financování terorismu související s touto činností a měly by si uvědomit, že tato činnost vychází z blízkých poradenských vztahů, zejména s podnikovými klienty a dalšími subjekty, jako jsou potenciální strategičtí investoři.
- 20.2. Při nabízení služeb podnikového financování by podniky měly uplatnit ustanovení hlavy I, a dále pak ustanovení uvedená v tomto obecném pokynu. V tomto ohledu mohou být také relevantní odvětvové pokyny č. 12, 15 a 16.

### Rizikové faktory

#### Rizikové faktory klienta a příjemce plnění

- 20.3. Při nabízení služeb podnikového financování by podniky měly vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika:
- a) vlastnická struktura klienta je bez zjevného obchodního nebo zákonného důvodu netransparentní. Jsou-li například vlastnická práva nebo kontrola svěřeny jiným subjektům, jako jsou svěřenské fondy nebo sekuritizační jednotka pro speciální účel podle vymezení v čl. 2 odst. 2 nařízení (EU) 2017/2402;
  - b) podnikové struktury nebo transakce jsou složité, například dlouhý řetězec holdingových společností s použitím krycích společností, nebo netransparentní, a to bez zjevného rozumného obchodního účelu;
  - c) neexistuje důkaz, že klient obdržel pověření nebo souhlas vrcholného vedení dostatečné úrovně pro uzavření smlouvy;
  - d) existuje málo nezávislých způsobů ověření totožnosti klienta;
  - e) existuje podezření na porušení povinností, například podvod s cennými papíry nebo obchodování zasvěcených osob.
- 20.4. Při nabízení služeb podnikového financování by podniky měly vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke snížení rizika. Klient je:
- a. orgánem veřejné správy nebo státním podnikem z jurisdikce s nízkou úrovní korupce; nebo
  - b. úvěrovou nebo finanční institucí z jurisdikce s účinným režimem pro boj proti praní peněz a financování terorismu a podléhá dohledu nad dodržováním povinností v oblasti boje proti praní peněz a financování terorismu.

### Rizikové faktory zemí nebo zeměpisných oblastí

20.5. Při nabízení služeb podnikového financování by podniky měly vzít v úvahu následující rizikové faktory, které mohou potenciálně přispět ke zvýšení rizika:

- a. klient nebo skutečný majitel má sídlo v jurisdikcích spojených s vyšším rizikem praní peněz nebo financování terorismu, nebo na ně má vazby. Podniky by měly věnovat zvýšenou pozornost jurisdikcím s vysokou mírou korupce.

### Opatření

20.6. Poskytovatelé podnikového financování budou vzhledem k povaze obchodní činnosti přirozeně shromažďovat rozsáhlé informace pro hloubkovou kontrolu; podniky by měly z těchto informací vycházet pro účely související s bojem proti praní peněz a financování terorismu.

### Zesílená hloubková kontrola klienta

20.7. Pokud je riziko související s obchodním vztahem nebo příležitostnou transakcí vysoké, podniky by měly uplatňovat opatření zesílené hloubkové kontroly klienta, jako jsou:

- a) další kontroly vlastnické a řídicí struktury klientů, skutečných majitelů a zejména případných vazeb klienta s politicky exponovanými osobami a toho, do jaké míry tyto vazby ovlivňují riziko praní peněz a financování terorismu související s obchodním vztahem;
- b) posouzení bezúhonnosti statutárních orgánů, akcionářů a dalších osob významně zapojených do obchodní činnosti klienta a transakce podnikového financování;
- c) ověření totožnosti dalších vlastníků nebo ovládajících osob právnické osoby;
- d) určení zdroje a povahy finančních prostředků nebo aktiv vložených všemi stranami transakce, je-li to vhodné pak na základě dokladů a záruk od příslušných třetích stran.
- e) další kontroly s cílem určit finanční situaci podnikového klienta;
- f) používání jiných než listinných forem důkazů, například schůzky s důvěryhodnými osobami, které dotyčné fyzické osoby znají; například s bankéři, auditory nebo právními poradci. Podniky by měly zvážit, zda důkazy postačují k prokázání toho, že klient správně uvedl svoji osobní a finanční



situaci. Při používání jiných než listinných důkazů by měly být vedeny záznamy uvádějící, na jakém základě byla rozhodnutí přijímána;

- g) hloubkové kontroly klienta zohledňující míru rizika a prováděné u jiných stran finančního ujednání s cílem získat dostatečné podklady pro pochopení povahy transakce. Rizika praní peněz totiž pro podnik nemusejí představovat pouze její klienti, ale také strany transakce, s nimiž podnik nemá přímý obchodní vztah. Podniky by měly zohlednit skutečnost, že se může jednat o tyto strany:
- i. cíl převzetí nebo fúze klientského podniku;
  - ii. potenciální nebo skuteční investoři podnikového klienta;
  - iii. právnické osoby, ve kterých má podnik významný vlastnický podíl (ale s nimiž nemá širší obchodní vztah);
  - iv. potenciální budoucí klienti;
  - v. v sekuritizačních transakcích podle vymezení v čl. 2 odst. 1 nařízení (EU) 2017/2402: zástupci jednající za sekuritizační jednotku pro speciální účel (kteří mohou, ale nemusí být regulovaným podnikem);
- h) podniky nabízející služby podnikového financování by měly uplatňovat zesílené průběžné sledování. V tomto ohledu by podniky používající automatizované sledování transakcí měly toto sledování spojit s know-how a odbornými znalostmi zaměstnanců vykonávajících tuto činnost. Výsledkem tohoto zesíleného sledování by měla být jasná představa, proč klient vykonává určitou transakci nebo činnost; za tímto účelem by podniky měly zajistit, že jejich zaměstnanci používají svoje znalosti o klientovi a to, co by za daných okolností bylo běžné, k odhalení neobvyklých nebo potenciálně podezřelých aspektů;
- i) jestliže se podílí na emisi cenných papírů, podnik by měl potvrdit, že třetí strany účastnící se prodeje sekuritizovaných nástrojů nebo transakcí investorům mají dostatečná vlastní ujednání hloubkové kontroly klienta;
  - j) pokud jde o rizika praní peněz a financování terorismu spojená se sekuritizovanými nástroji nebo transakcí, podnik by měl znát související ekonomický účel ujednání, včetně úrovně hloubkové kontroly vhodné pro různé strany ujednání, včetně těch, s nimiž podnik nemá přímý obchodní vztah.

## Zjednodušená hloubková kontrola klienta

- 20.8. Podniky by měly pro účely zjednodušené hloubkové kontroly klienta použít informace, které mají díky tomu, že se činnost v oblasti podnikového financování odehrává na základě navázaných vztahů, a vzhledem k rozsahu transakcí a potřebě posoudit úvěrové riziko a riziko ztráty dobré pověsti související s ujednáními v oblasti podnikového financování.
- 20.9. Jestliže podniky jednají se zprostředkovateli, kteří spravují účty primárně ve prospěch jejich příslušných klientů, podniky by měly použít odvětvový pokyn č. 16.