DATUM: 3. 7. 2023

Dohledový benchmark č. 2/2023

K provádění kontroly klienta prostřednictvím systému k monitoringu transakcí

Česká národní banka (dále jen „ČNB“) vykonává mj. kontrolní činnost v oblasti prevence legalizace výnosů z trestné činnosti a financování terorismu u povinných osob, vůči nimž vykonává dohled. Tento benchmark se primárně vztahuje na úvěrové instituce – banky (dále jen „povinná osoba“ nebo „banka“), nicméně jej lze vhodně a přiměřeně aplikovat i na další subjekty finančního trhu úměrně jejich velikosti a struktuře poskytovaných produktů a služeb.

Obsah dohledového benchmarku:

Relevantní právní úprava

Klíčové předpisy a vybraná ustanovení

- Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „AML zákon“)
  - zejména ustanovení § 9, § 9a, § 15, § 18 odst. 1, § 21 odst. 1, § 21a
- Vyhláška č. 67/2018 Sb., o některých požadavcích na systém vnitřních zásad, postupů a kontrolních opatření proti legalizaci výnosů z trestné činnosti, ve znění vyhlášky č. 253/2021 Sb. (dále jen „AML vyhláška“)
  - zejména ustanovení § 8 odst. 1, § 9 odst. 2 písm. a), § 17 odst. 2, § 17a, § 18
- Vyhláška č. 163/2014 Sb., o výkonu činnosti bank, spořitelních a úvěrních družstev a obchodníků s cennými papíry, ve znění pozdějších předpisů (dále jen „vyhláška č. 163/2014 Sb.“)
- Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů a navazující právní předpisy v podobě sankcí stanovených přímo použitelnými právními předpisy Evropské unie (dále jen „EU“), vydanými příslušnými orgány EU a publikovanými v Úředním věstníku EU, a příslušná výkladová stanoviska Evropské komise k těmto nařízením[1]
- Zákon č. 1/2023 Sb., o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon)

Vybrané metodické pokyny, hodnocení rizik a uznávané AML/CFT standardy

- Basel Committee on Banking Supervision: Guidelines – Sound management of risks related to money laundering and financing of terrorism
- FATF – Risk-based Approach Guidance for the Securities Sector
- EBA/GL/2021/02 – Obecné pokyny podle čl. 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 (dále jen „EBA/GL/2021/02“)
- EBA/GL/2019/04 – Obecné pokyny EBA pro řízení rizik v oblasti IKT a bezpečnosti
- EBA/GL/2019/02 – Obecné pokyny EBA k outsourcingu
- Sdělení ČNB o obecných pokynech EBA k outsourcingu[2]
- Finanční analytický úřad (dále jen „FAÚ“) - Zpráva o druhém kole procesu národního hodnocení rizik praní peněz a financování terorismu[3]

---

1 https://ec.europa.eu/info/business-economy-euro/banking-and-finance/international-relations/restrictive-measures-sanctions_en.

2 https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/obecne-pokyny-evropskych-organu-dohledu/Sdeleni-CNB-o-obecnych-pokynech-EBA-k-outsourcingu/.

3 Cílem procesu národního hodnocení rizik (NRA) je ve spolupráci se všemi zainteresovanými subjekty posoudit rizika praní peněz a financování terorismu v České republice a zpracovat o tom zprávu. Proces koordinuje Finanční analytický úřad a řídí se při tom příslušnou metodikou Finančního akčního výboru (Financial Action Task Force, FATF), pátou

Účel a obecné předpoklady

Tento dohledový benchmark reaguje na vybraná, zejména opakovaná, kontrolní zjištění v systému preventivních opatření, která musí povinná osoba uplatňovat v zájmu účinné implementace postupů k provádění průběžné kontroly klienta prostřednictvím pravidelného monitoringu transakcí[4] (dále jen „AML monitoring“).

AML monitoring je nedílnou součástí komplexního systému předpokladů a opatření v boji proti praní špinavých peněz a financování terorismu a synergicky doplňuje další opatření, jakými jsou např. povinnost identifikace, kontrola klienta[5], pravidelné školení, archivace, rekonstruovatelnost procesů apod. Kromě výše uvedeného je systém tvořen rovněž vzájemnými vazbami mezi dalšími nezbytnými opatřeními (zejména se jedná o výpočet rizikovosti klienta/produktů či transakcí[6], kontroly v oblasti mezinárodních sankcí), a proto AML monitoring předpokládá jejich vzájemné propojení. Zavedení, provázání a uplatňování těchto souvisejících opatření je klíčové pro odhalování a šetření podezřelých obchodů.

V textu uvedená upozornění cílí zejména do následujících oblastí:

- **Předpisová základna**
  Kapitola upozorňuje zejména na nedostatky v oblasti systému vnitřních zásad a rizikově orientovaného přístupu. Součástí jsou také upozornění k metodikám upravujícím prováděcí praxi.

- **Výkon AML monitoringu transakcí a technické předpoklady**
  Kapitola se zabývá vlastním nastavením AML monitoringu a mj. klade důraz na správně technicky nastavený a fungující systém AML monitoringu, jako jeden z předpokladů pro celkovou způsobilost řídicího a kontrolního systému (dále též „ŘKS“).[7] S ohledem na tuto skutečnost je zde silná provázanost s požadavky vyplývajícími z oblasti dohledu nad informačními systémy / informačními technologiemi (dále též „IS/IT“). Požadavky v oblasti IS/IT tedy synergicky doplňují požadavky kladené na AML monitoring.[8]

- **Procesní postupy**
  Upozornění v kapitole míří na pracovní postupy vyhodnocování rizika podezřelosti transakcí, a to včetně navazujících procesů. V rámci AML monitoringu využívají povinné osoby obvykle semi-automatizovaná řešení, a to jak na komerční bázi či interně vyvinuté (tzv. in-house). V případě splnění parametrických podmínek daných jednotlivými detekčními scénáři jsou generovány tzv. alerty (upozornění), které následně prošetřují příslušní zaměstnanci povinné osoby (nebo osoby podílející se na činnosti povinné osoby v rámci tzv. outsourcingu)

AML směrnicí a AML zákonem. Aktuální veřejná verze je publikována na webových stránkách: https://www.financnianalytickyurad.cz/narodni-hodnoceni-rizik.

4 Termín „transakce“ je pro účely tohoto dokumentu používán ve smyslu „obchod“ podle ustanovení § 4 odst. 1 AML zákona. V kontextu AML monitoringu u úvěrových a finančních institucí, zejména pak bank, se termín „transakce“ v tomto kontextu v praxi používá, a proto jej zavádí i tento dokument.

5 Kontrola klienta ve smyslu širšího pojetí, tedy v relevantních případech včetně zjištění vlastnické a řídicí struktury klienta, zjištění totožnosti skutečného majitele apod.

6 A to ať již jednotlivých nebo sledu / souboru transakcí v jejich vzájemné provázanosti v kontextu dané situace (např. chování klienta, struktura obchodního případu, strukturování transakcí apod.).

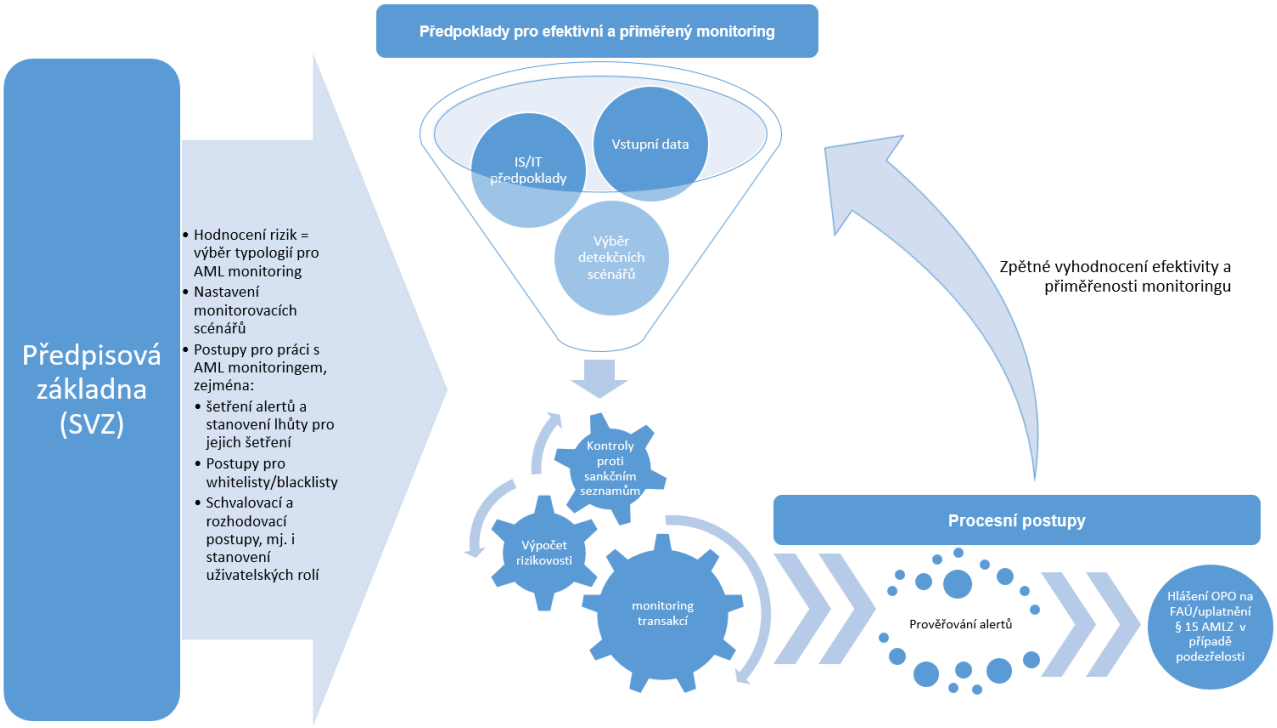
7 ŘKS ve smyslu vyhlášky č. 163/2014 Sb.

8 Tato kapitola je tedy určena pro AML / compliance officery jako benchmark pro to, co by mělo být nastaveno (měli vyžadovat) v rámci povinné osoby ze strany útvarů majících v gesci IS/IT problematiku.

odpovědní za agendu prevence legalizace výnosů z trestné činnosti a financování terorismu (dále jen „AML“).

- **Nové trendy**
  Upozornění na oblasti, kde je nutné vyhodnocovat specifická rizika s ohledem na využití nových technologií, zejména pak za využití prvků umělé inteligence, tzv. AI.

Zjednodušeně lze celkovou koncepci AML monitoringu zobrazit následovně:



I. Předpoklady předpisové základny a rizikově orientovaného přístupu

AML zákon ve spojení s AML vyhláškou explicitně ukládá povinnost monitorovat transakce a upravuje i některé další aspekty AML monitoringu. Základní pilíř této povinnosti představuje ustanovení § 9 odst. 2 písm. d) AML zákona[9], které stanoví povinnost průběžného sledování obchodního vztahu a obchodů prováděných v průběhu daného vztahu. Průběžné sledování obchodního vztahu a jednotlivých obchodů je nutné vykonávat v rozsahu potřebném k posouzení rizika praní peněz a financování terorismu (dále jen „ML/FT“)[10]. Ustanovení § 21 odst. 5 AML zákona dále povinné osobě ukládá, aby postupy pro provádění kontroly klienta stanovila tak, aby odpovídaly ML/FT riziku v závislosti na typu klienta, produktu aj.

9 Rovněž i ustanovení § 9a odst. 3 písm. c) AML zákona, blíže viz kapitola Risk Based Approach.
10 Ustanovení § 9 odst. 3 AML zákona.

i. Risk Based Approach

Právní úprava v oblasti AML ve svém souhrnu tvoří základ pro povinné uplatnění tzv. rizikově orientovaného přístupu (Risk Based Approach – RBA, dále i „RBA“). RBA, tak jak je definován zejména v rámci ustanovení § 21 odst. 5 AML zákona (především písm. d)) a § 5 AML vyhlášky, vyžaduje, aby povinné osoby přijaly vhodné kroky k identifikaci a posouzení ML/FT rizika, a přitom vzaly v úvahu rizikové faktory týkající se jejich klientů, země/zemí původu, produktů, služeb, transakcí, či dodavatelských kanálů. Tyto kroky přitom mají být přímo úměrné povaze a velikosti povinné osoby. V návaznosti na identifikovaná rizika musí mít povinné osoby nastavené postupy, kontrolní mechanismy a procedury k řízení, resp. efektivní kontrole ML/FT rizik, která jsou identifikována na úrovni EU, národního hodnocení rizik a hodnocením rizik dané povinné osoby.

AML vyhláška v ustanovení § 8 odst. 1 stanoví, že opatření obsažená ve vnitřním systému povinné osoby musí být vůči klientovi nastavena takovým způsobem, který zajistí, mj. aby byla schopna účinně řídit rizika a identifikovat případný podezřelý obchod. V rámci takových opatření má povinná osoba zavést a uplatňovat postupy, mezi něž mj. patří i rozsah a četnost prováděných opatření kontroly klienta[11]. U klientů se zvýšeným rizikem v souladu s RBA pak ustanovení § 9a odst. 3 písm. c) AML zákona a § 9 odst. 2 písm. a) AML vyhlášky požadují zesílené monitorování obchodního vztahu a obchodů v jeho rámci. Zesílené monitorování pak lze zpravidla chápat jako častější monitorování transakcí rizikového subjektu s nižšími přednastavenými limity.

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy:

- **Rizikově orientovaný přístup není průběžně přizpůsobován měnícím se podmínkám produktového, klientského, transakčního portfolia nebo distribučních kanálů, tedy obecně situacím, které jsou zejména součástí systému vnitřních zásad** (dále též jen „SVZ“ nebo „předpisová základna“[12]) **a hodnocení rizik povinné osoby, v důsledku čehož je povinná osoba mj. vystavena riziku porušení ustanovení § 4 odst. 4, 5 a 7 AML vyhlášky.**

ii. Systém vnitřních zásad a hodnocení rizik

Povinná osoba vypracuje SVZ podle ustanovení § 21 AML zákona. **SVZ je souhrnným dokumentem sdružujícím postupy a opatření povinné osoby** v rozsahu, ve kterém provádí činnosti podléhající působnosti AML zákona**, které jsou připraveny na základě hodnocení rizik.**[13]

Povinnost zavést příslušná systematická opatření v rámci SVZ lze rovněž dovozovat z AML vyhlášky. AML vyhláška dále stanoví, že tato opatření musí být současně zpětně rekonstruovatelná[14]. Požadavek rekonstruovatelnosti je obsažen v ustanovení § 16 odst. 3 AML zákona a dále rozveden v ustanovení § 18 odst. 2 AML vyhlášky. Tato ustanovení společně stanoví povinnost řádné dokumentace obchodního vztahu a jednotlivých obchodů, a to způsobem a v rozsahu, který zajistí jejich dostatečnou průkaznost. Jedno z takových opatření, které musí

[11] Ustanovení § 8 odst. 2 písm. b) AML vyhlášky.
[12] Tento benchmark používá termín „systém vnitřních zásad“ ve smyslu AML zákona (ustanovení § 21 odst. 2) a AML vyhlášky (ustanovení § 4). Systém vnitřních zásad je ucelený systém všech předpisů, postupů, vnitřních kontrol, metodických pokynů, procesů a systémových opatření, které má povinná osoba pro účely boje proti praní špinavých peněz a financování terorismu nastaveny.
[13] Ustanovení § 21a AML zákona.
[14] Ustanovení § 18 odst. 1 AML vyhlášky.

povinná osoba přijmout, je i interní metodika pro oblast AML monitoringu, jež představuje součást SVZ povinné osoby, který dále vhodně doplňuje.[15]

S ohledem na shora uvedené ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy povinná osoba:

- **Nedostatečně rozpracuje svou předpisovou základnu, která nestanovuje pracovní / metodické postupy pro AML monitoring, jako jsou např. postupy pro:**
  - **vyhodnocování scénářů k detekci podezřelých obchodů,**
  - **stanovování výše detekčních limitů, tzv. „thresholdů“[16],**
  - **aktualizace parametrických seznamů (seznam zemí, produktů, platebních kódů apod.),**
  - **ověřování datové věty, která je rozhodná pro výpočet alertu (tj. zda data, kterými se plní výpočetní model, jsou úplná, správná a aktuální),**
  - **šetření alertů (včetně jejich prioritizace, kterou se řídí zpracovávání většího množství alertů),**
  - **zařazování subjektů na tzv. „whitelist“.[17]**
- **Nedochází k průběžné aktualizaci hodnocení rizik[18] povinné osoby a v případě změn není dostatečně upraven systém vnitřních zásad.**

II. Předpoklady pro efektivní a přiměřený AML monitoring transakcí

i. Data a detekční scénáře

V této oblasti je kladen **důraz zejména na integritu a kvalitu vstupních dat** o všech relevantních typech transakcí, chování klienta, povaze obchodního vztahu[19] a indikátorů ML/FT rizik k vyhodnocení potenciální rizikovosti.

---

15 Z dohledové praxe plyne poznatek, že v „hlavním / zastřešujícím“ předpise SVZ bývá jen velmi stručná zmínka o AML monitoringu, případně zde zmínka o AML monitoringu zcela chybí. Z tohoto „hlavního / zastřešujícího“ předpisu SVZ však často není zřejmé, zda takto podrobně rozpracovaný metodický předpis na AML monitoring vůbec existuje. S ohledem na tuto skutečnost je vhodné, aby povinné osoby zmiňovaly odkaz na metodický předpis upravující AML monitoring již v „hlavním / zastřešujícím“ předpise SVZ. Senzitivní informace, jako jsou např. detailní postupy pro nastavení detekčních scénářů, včetně určení detekčních limitů (tzv. „thresholdů“), je z povahy věci součástí SVZ, nicméně přesto lze očekávat, že tyto informace budou dostupné pouze vymezenému okruhu pověřených osob (tzv. princip „need to know“). V takovýchto případech se může jednat pouze o referenci v rámcovém AML předpisu na specifický dokument, manuál či metodiku, kterou má k dispozici pouze útvar zajišťující činnosti v oblast AML/CFT (samozřejmě s možností přezkumu vnitřním auditem apod.).

16 Např. interní analytický dokument, který by odůvodňoval konkrétní nastavení limitů v kontextu dané povinné osoby. Příkladem neobezřetného přístupu je situace, kdy (i) nejvyšší transakce klientů fyzických osob za poslední rok je 1 000 000 Kč a limit scénáře sledující neobvyklou nadlimitní platbu je nastaven na hodnotu 5 000 000 Kč (ii) nastavení limitů nezohledňuje specifika daného klientského segmentu, typicky např. rozdíl středních a velkých podniků (obecně tzv. SME a LARGE CORP) či přímo informace poskytnuté klientem v rámci kontroly klienta, a to ať již vstupní či průběžné.

17 Vysvětlení termínu „whitelist“ a proces „whitelistování“ jsou dále rozvedeny v části „Postupy pro šetření alertů, zařazení na whitelisty“ tohoto benchmarku.

18 Ustanovení § 21a AML zákona.

19 Např. povaha obchodního vztahu, délka jeho trvání apod., v rámci něhož jsou transakce realizovány.

Předpokladem výkonu AML monitoringu je **průběžné, včasné a kvalitní vyhodnocování efektivity jednotlivých detekčních scénářů, včetně nastavení příslušných detekčních parametrů** (např. limitů na transakce) tak, aby odpovídaly aktuálním rizikům v kontextu hodnocení rizik a RBA.[20]

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy:

- **Není uplatňován relevantní přístup k datové čistotě a integritě, a tedy data, která jsou základem pro výkon AML monitoringu, postrádají platnost, správnost nebo úplnost. Výsledkem tohoto stavu je značná chybovost v detekci klientského nebo transakčního rizika, byť často v rámci sofistikovaného a nákladného řešení.**

- **Datové nedostatky vznikají při vstupní nebo pravidelné kontrole klienta, kdy tato není provedena vůbec nebo není provedena v takovém rozsahu, který by zabezpečoval dostatečné porozumění AML rizikům asociovaných s klientem. Jedná se např. o klienty typu finanční instituce či klienty typu advokát / notář při provádění úschov peněz prostřednictvím tzv. úschovních účtů, u kterých často povinným osobám chybí znalost struktury klientského portfolia, které tito klienti obsluhují, kvality jimi prováděných AML kontrol a obecně jejich předpisové základny.**

- **Nastavení detekčních scénářů nereflektuje doporučované standardy, nepřihlíží k výsledkům vlastní prováděcí praxe.**

- **V důsledku uplatňování jednotného limitu detekčního scénáře / detekčních scénářů pro všechny povinné osoby v rámci skupiny (tedy i mezinárodně působící) nedochází k zohlednění lokálních specifik daného trhu / produktu / skupin klientů apod.**

ii. Interní převody mezi účty téhož klienta či mezi klienty v rámci dané povinné osoby

ČNB se při výkladu ustanovení § 4 odst. 1 AML zákona přiklání k výkladové praxi, kdy pojmem obchod je myšleno jakékoliv nakládání s majetkem klienta, tedy i jakákoliv transakce. Tento názor je podpořen i ustálenou výkladovou praxí, např. „*Obecný pojem ‚obchod´ pro potřeby LegVTrČ označuje jakékoli jednání, kterým by případně mohlo dojít k legalizaci výnosů. Nejedná se tedy zásadně jen o klasickou obchodní transakci se stranou prodávající a kupující, za obchod jsou pro účely tohoto zákona považovány například i přesuny mezi jednotlivými účty téhož majitele. Definici pojmu obchod naopak nenaplňuje nakládání s majetkem povinné osoby – vždy musí jít o nakládání s majetkem jiné osoby. Obchod v LegVTrČ není posuzován podle směru ‚od klienta´ nebo ‚ke klientovi´; jedná se vždy o obchod, například v oblasti hazardních her se za obchod považuje jak vklad, tak výhra.*“[21]. Postupy AML monitoringu může povinná osoba aplikovat i na interní převody mezi účty téhož klienta či mezi účty různých klientů vedených v rámci jedné povinné osoby. V této souvislosti rovněž postupuje v souladu s RBA a může tedy na základě předchozího vyhodnocení určit pouze některé typy interních převodů s vyšším rizikem a na ty AML monitoring uplatňovat.[22]

---

[20] Tyto procesy musejí být i zpětně rekonstruovatelné ve smyslu ustanovení § 18 AML vyhlášky.

[21] Markéta Hlavinová, Viktor Kabeš, Jaroslava Pilíková. Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Komentář. 3. Vydání. Praha. C.H.Beck, 2022, k ustanovení § 4 AML zákona.

[22] Lze tedy předpokládat, že pokud k tomuto nejsou zjištěny další rizikové faktory, není nutné sledovat např. převod z účtu téhož klienta na spořicí / termínovaný účet, tzv. cashpooling nebo tzv. over-night účet apod. Za relevantní situace lze

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy povinná osoba v rámci AML monitoringu nesleduje, resp. nebere v potaz, při vyhodnocovaní interní převody mezi účty téhož klienta či mezi účty různých klientů vedených v rámci jedné povinné osoby[23] (tzv. interní převody). V důsledku takto aplikovaného nastavení jsou tyto platby prakticky vyřazeny z AML monitoringu.

iii. Nebankovní finanční instituce v pozici klienta povinné osoby

Podle Národního hodnocení rizik[24] nebankovní finanční instituce (zejména poskytovatelé platebních a směnárenských služeb) patří mj. i v důsledku globalizace obchodu a rozvoje digitalizace, mezi sektory, které jsou vysoce zranitelné vůči riziku ML/FT, a představují tedy zvýšené riziko v podobě vyšší materializace jednotlivých ML/FT typologií. Toto riziko musí být v rámci RBA doprovázeno zesílenými opatřeními, která jej dostatečně zmírňují. Z tohoto důvodu je při uzavírání obchodního vztahu s těmito klienty a v jeho průběhu nutné uplatňovat zesílenou kontrolu klienta s ohledem na ustanovení § 9a odst. 1 AML zákona, respektive ustanovení § 9 AML vyhlášky, za účelem hlubšího porozumění danému obchodnímu vztahu.

Hlavním rizikem je zde realizace transakcí klientů klienta, lze tedy hovořit o tzv. „nested" účtech. Pro povinné osoby, jejichž klientem je finanční instituce, je riziko obdobné riziku tzv. korespondenčního bankovnictví. AML monitoring proto musí být způsobilý efektivně detekovat rizika spojená s těmito specifickými typy klientů – nebankovními finančními institucemi.[25]

Povinná osoba by měla při kontrole klientů typu nebankovní finanční instituce vycházet nejen z informací obecného charakteru, ale zejména získávat informace dostatečné k porozumění podstaty a účelu obchodního vztahu s těmito klienty, tzn. porozumění rizikovému apetitu těchto klientů, kteří jsou rovněž povinnou osobou v intencích AML zákona. Povinná osoba by měla disponovat v případě tohoto typu klientů informacemi, jakým způsobem tito klienti řídí ML/FT rizika svých klientů, tzn. informacemi o:

- kvalitě uplatňovaných pravidel a postupů v oblasti AML[26],
- obchodním modelu (mj. i v kontextu toho, zda je očekávatelně realizovatelný),
- možných obchodech, které svým klientům nabízí (typy produktů/služeb),

považovat např. převody mezi účty téže osoby, která má současně vedeny účty jako fyzická osoba – spotřebitel a fyzická osoba – podnikatel.

23 Rizikové indikátory mohou být mj. i v rámci převodů téže ekonomicky spjaté skupiny (ESS) či ekonomicky spjaté skupiny osob (ESSO).

24 Viz např. dokument „*Zpráva o druhém kole procesu národního hodnocení rizik praní peněz a financování terorismu*" uveřejněný na webových stránkách FAÚ: https://www.financnianalytickyurad.cz/informace-o-druhem-kole-narodniho-hodnoceni-rizik.

25 V této souvislosti je vhodné rovněž upozornit na definici skutečného majitele ve smyslu ustanovení § 4 odst. 4 písm. b) AML zákona - tzv. „skutečného majitele transakce". Skutečným majitelem se pro účely tohoto zákona rozumí fyzická osoba, za kterou se obchod provádí, kdy v souladu s ustanovením § 9 odst. 2 písm. b) AML zákona by povinná osoba měla znát totožnost skutečného majitele včetně skutečného majitele transakce. Jedná se tedy o upozornění na tuto zákonnou povinnost, jako jednu z možností v rámci provedení zesílené kontroly klienta v případě zvýšeného rizika či prověřování potenciálně podezřelého obchodu u jednotlivé/vybrané transakce či vzájemně souvisejících transakcí.

26 Zdrojem informací může být např. SVZ (pokud jej klient poskytne dobrovolně v plném znění), vybrané části SVZ (které budou relevantní pro posouzení klientem uplatňovaných opatření) nebo klientem vhodně popsané shrnutí opatření, která uplatňuje (případně formou zápisu z jednání s klientem, kde by se toto probralo v potřebném detailu). Tzv. Wolfsbergský AML dotazník je vhodnou formou doplnění informací o klientovi, nicméně neměl by být jediným zdrojem informací a povinná osoby by měla učinit další vhodné kroky k získání a ověření potřebných informací v rámci provedení kontroly klienta.

- struktuře portfolia klientů, kterým daná nebankovní finanční instituce poskytuje své služby, za účelem vyhodnocení vztahu k rizikové zemi původu[27],
- destinacích, z / do kterých budou směřovat platby (v kontextu možného výskytu ML/FT rizikových zemí),
- očekávaných objemech plateb a
- tom, jakým způsobem řídí rizika spojená s prováděním mezinárodních sankcí apod.

V důsledku provádění transakcí klienta může být povinná osoba mj. vystavena riziku provádění transakcí, které by jinak považovala za vysoce rizikové či přímo nepřijatelné v kontextu svého risk apetitu, resp. RBA. AML monitoring by měl být způsobilý sledovat transakce takovým způsobem, že vyjma kontrol oproti sankčním seznamům, bude využívat povinnou osobou získané informace z provedené kontroly klienta, a to minimálně struktury či kumulace transakcí na úrovni klienta (např. zda transakce odpovídají deklarovanému objemu/struktuře, či nejsou realizovány vůči jiné než klientem deklarované zemi apod.). Další linií obrany je mj. i úzká spolupráce s daným klientem, resp. jeho pracovníky odpovědnými za oblast AML.

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy AML monitoring nedisponuje specifickými detekčními scénáři, které umožňují včas a efektivně detekovat podezřelosti u klientů nebankovních finančních institucí při zohlednění relevantních rizikových faktorů a informací z provedené kontroly klienta (např. očekávané objemy / počty transakcí vs. skutečně realizované počty / objemy).

iv. Investiční nástroje

Kontrola klienta ve smyslu ustanovení § 9 AML zákona zahrnuje všechny obchody (transakce) realizované klientem. Provádění pravidelné kontroly klienta prostřednictvím AML monitoringu se tedy vztahuje i na tzv. oblast investičních obchodů. ČNB se v praxi setkává se situací, kdy povinné osoby mají v rámci AML monitoringu, tedy „hlavního“ AML systému, nastaven monitoring pouze na transakce na běžném (platebním) účtu klienta. V potaz tedy nejsou brány již jednotlivé transakce (obchody) uskutečňované s tzv. investičními nástroji ve smyslu ustanovení § 3 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů (dále jen „ZPKT“) (dále jen „investiční nástroj“). Zpravidla jsou přezkoumávány pouze příchozí a odchozí platby (či finální součty z jednotlivých provedených obchodů) s investičními nástroji ve prospěch běžného platebního účtu klienta. Takovýto způsob AML monitoringu sám o sobě nemůže plnit hlavní úlohu ve smyslu provádění kontroly klienta za účelem detekce potenciálně podezřelých obchodů. Právě ono shora uvedené nastavení scénáře není schopno detekovat podezřelou aktivitu včas a neumožní povinné osobě zabránit provedení obchodu v případě, že se jedná o podezřelý obchod, ale maximálně upozorní až na sekundární projevy rizikovosti bez možnosti včas aktivně jednat.

Smyslem kontroly klienta v rámci obchodního vztahu je posoudit obchodní vztah v jeho celku, tedy zda dává smysl, odpovídá rizikovému profilu klienta a nevykazuje znaky rizikovosti, resp. podezřelosti. Vstupní a výstupní kontrola prostředků s ohledem na jejich původ je samozřejmě důležitá, ale v kontextu shora uvedeného je nutné brát zřetel i na monitoring případného nestandardního jednání klienta v rámci obchodního vztahu jako celku, tedy i v rámci dílčích

[27] Tedy tak, aby se povinná osoba nevystavovala riziku, že by prováděla zprostředkovaně platby pro skupiny klientů se vztahem k vybraným rizikovým zemím s ohledem na její vlastní hodnocení rizik (např. v podobě opatření, že klient nebude přes povinnou osobu realizovat transakce svých klientů se vztahem k vybrané zemi v podobě bydliště / pobytu či státní příslušnosti).

indikátorů rizikovosti při provádění jednotlivých obchodů / pokynů s investičními nástroji. Příklady rizikovosti a rizikových typologií lze nalézt např. v níže uvedených dokumentech, zejména v podobě uznávaných standardů a doporučení:

- Hodnocení rizik provedené bankou,
- Národní hodnocení rizik,
- Nadnárodní hodnocení rizik na evropské úrovni,
- Uznávané AML standardy, zejména pak
  - FATF (2018), Guidance for a Risk-Based Approach for the Securities Sector,
  - EBA/GL/2021/02, zejména
    - Obecný pokyn č. 12: Odvětvový pokyn týkající se správy majetku,
    - Obecný pokyn č. 15: Odvětvový pokyn pro investiční podniky,
    - Obecný pokyn č. 16: Odvětvový pokyn pro poskytovatele investičních fondů.

Povinné osoby zpravidla částečně nahrazují AML monitoring specializovanými aplikacemi, které dle povinností stanovených regulatorním rámcem Market Abuse Regulation (MAR) jsou primárně určeny k detekci jiných rizik, např. obchody typu „wash trade“[28], „painting the tape“[29] apod. Smyslem těchto systémů tedy není naplnění AML povinností, a proto ani ze své podstaty nejsou určeny pro řízení a vyhodnocování ML/FT rizika.

Dostatečná účinnost automatizovaného AML monitoringu v oblasti obchodů s investičními nástroji je podmíněna jeho schopností porovnávat klientem realizované transakce v jejich celku, tedy jak ty na běžném účtu, tak ty související s investičními nástroji. Bez takto fungující detekce potenciální podezřelosti nelze zajistit identifikaci všech ML rizikových transakcí, resp. identifikaci nesrovnalosti s informacemi získanými povinnou osobou. Konkrétně se jedná zejména o níže uvedené informace, kterými povinná osoba disponuje a vyhodnocuje na úrovni klienta mj. i v kontextu ustanovení § 7 AML vyhlášky jakožto informace jí známé:

oblast AML:

- riziková kategorie klienta,
- informace získané z provedené vstupní a průběžné kontroly klienta[30], majetkové poměry klienta (zejména zdroj peněžních prostředků, povolání / předmět činnosti klienta, jeho pravidelný příjem), běžné a očekávané obraty na „klasickém / běžném“ účtu;

oblast poskytování investičních služeb, např. informace v praxi obecně získávané zejména prostřednictvím tzv. investičního dotazníku[31] v rámci plnění vybraných regulatorních požadavků úpravy kapitálového trhu pro účely:

- plnění povinností při nabízení nebo doporučování investičního nástroje zákazníkovi ve smyslu ustanovení § 12bb ZPKT a § 15c ZPKT a dalších (tzv. řízení produktů dle směrnice MiFID II neboli „product governance“) a

[28] Jedná se o provádění transakcí, aniž by při ní fakticky došlo ke změně skutečného vlastníka finančního nástroje. Např. rozhodnutí ČNB, vedené pod č. j. 2010/5287/570, ke sp. zn. Sp/2009/188/573, ze dne 11. 6. 2010, ve věci účastníka řízení Patria Finance, a. s., nebo rozhodnutí ČNB, vedené pod č. j. 2010/2786/110, ke sp. zn. Sp/2009/165/573, ze dne 11. 6. 2010, ve věci účastníka řízení Raiffeisenbank, a. s., veřejně dostupné na webových stránkách ČNB.

[29] Jedná se o situaci, při které investor současně prodává a nakupuje stejné finanční nástroje a vytváří tím uměle aktivitu.

[30] Ve smyslu ustanovení § 9 a § 9a AML zákona a dále rozvedených požadavků v rámci AML vyhlášky.

[31] Případně jiným vhodným způsobem.

- vyžadování informací od zákazníků ve smyslu ustanovení § 15i ZPKT a § 15h ZPKT za účelem posouzení přiměřenosti a vhodnosti investiční služby pro daného zákazníka (vybrané části viz příloha č. 1)[32].

v. IS/IT předpoklady

Předmětem IS/IT pozornosti jsou všechny AML IS/IT procesy, zejména pak procesy změnového řízení a rozvoje softwarových systémů, bezpečnostního monitoringu, bezpečnostních a provozních incidentů s dopadem do funkčností AML, přístupových práv a ochrany informací[33], provozu informačních systémů a kontinuity podnikání. Oblast IS/IT se řídí u bank zejména ustanovením § 11 bod 2. a body 10. až 21. přílohy č. 6 vyhlášky č. 163/2014 Sb. a dále Obecnými pokyny EBA pro řízení rizik v oblasti IKT a bezpečnosti.

Sledovanými předpoklady jsou zejména:

- **Dostatečná míra rekonstruovatelnosti klíčových částí procesů v oblasti IS/IT – minimálně v oblasti definice a nasazování nových verzí / funkčností (včetně funkčností generování AML alertů), provozních kroků jako vypínání a zapínání funkčností, změn přístupových práv, bezpečnostního monitoringu a bezpečnostních incidentů atd.**
- **Definovaný a efektivní proces změnového řízení a rozvoje IS/IT – všechny funkční a nefunkční požadavky jsou osobou odpovědnou za oblast AML monitoringu[34] jasně specifikované, otestované a akceptované.**
- **Funkční monitoring důležitých událostí systémů používaných pro AML monitoring, zejména změny přístupových práv, změn verzí softwaru, změn ve spuštění jednotlivých AML funkčností a AML procedur a dále událostí definovaných jako bezpečnostní incidenty a propagace těchto incidentů do celého procesu práce s bezpečnostními incidenty.**
- **Definovaná a implementovaná architektura a integrace IS/IT systémů v oblasti AML monitoringu, která bere v úvahu požadavky kontinuity podnikání (tzv. BCM) a je efektivní pro plnění požadavků AML monitoringu, mimo jiné s externími systémy jako např. externí databáze/registry. Typicky se jedná o sankční seznamy (veřejně dostupné i komerční, které obsahují rozšířené sady dat) a další zdroje k prověřování negativních informací či stanovení rizikovosti prověřovaných subjektů, např. CRIF, základní registry, BRKI, NRKI, Solus.**
- **Implementovaný systém řízení přístupových oprávnění v IS/IT systémech s principy need-to-know a oddělení neslučitelných rolí.**

---

[32] ČNB dále upozorňuje na další povinnosti spojené s vyplňováním investičního dotazníku zákazníkem, které jsou synergické s plněním požadavků v oblasti AML. Jedná se zejména o povinnost (i) kontrolovat konsistenci odpovědí mezi sebou, (ii) kontrolovat spolehlivost odpovědí mezi jednotlivými dotazníky – tím se rozumí např. odhalení opakovaného účelového vyplňování investičního dotazníku se záměrem dosáhnout na žádoucí investiční profil, (iii) zajistit, že informace nejsou zjevně zastaralé, nepřesné či neúplné – mít nastavenou dobu, po jejímž uplynutí musí zákazník investiční dotazník aktualizovat, vč. upozornění zákazníka, že je potřebné získané informace aktualizovat v případě, že dojde k materiální změně skutečného stavu.

[33] Např. DLP (Data Loss Prevention).

[34] Též označováno jako tzv. Business Owner.

- **Efektivní řízení outsourcingu v případě využívání outsourcingu pro IS/IT AML. Funkční identifikace, sledování, vyhodnocování outsourcingu[35] včetně uchopení dopadů v případě události kontinuity podnikání (selhání dodavatele) a ochrany dat.**
- **Efektivně implementované zálohování tak, aby splňovalo požadavky kontinuity podnikání, ale též podporovalo rekonstruovatelnost, zejména možnost rekonstrukce hlášených alertů v definovaném časovém okamžiku (toto je možné řešit i jinak např. vhodnou archivací). Podpora rekonstruovatelnosti alertů se týká nejen vedení záznamu vygenerování alertů, ale také historie zpracování těchto alertů.**
- **Na IS/IT systémy je nutno z pohledu kontinuity podnikání hledět jako na klíčový systém v souladu s napojenými okolními systémy jako online transakční systémy a datový sklad (tzv. DWH).**
- **Zajištění a udržování integrity dat pro efektivní práci v oblasti AML. V případě využívání různých jazyků a znakových sad zajistit kompatibilní a efektivní využívání kódování, kódových tabulek a transliterace textových informací tak, aby nedocházelo ke ztrátě nebo zmatení informací např. u názvů a adres klientů.**
- **Udržovat aktuální rizikovou analýzu IS/IT systémů pro oblasti AML.**

III. Předpoklady pro oblast procesních postupů

i. Lhůty pro generování a šetření alertu

Smyslem ustanovení § 21 odst. 1 AML zákona[36] především je, aby zavedené a uplatňované postupy byly odpovídající a měly tak způsobilost a schopnost naplnit svůj účel, tj. zmírňovat rizika ML/FT a efektivně jim předcházet. Systém vnitřních zásad, který nebude mít tuto základní vlastnost a předpoklad, nebude tedy způsobilý zmírňovat rizika ML/FT a efektivně jim předcházet. Takové předcházení rizikům vyžaduje pro-aktivní přístup, nikoliv re-aktivní přístup.[37]

Základním předpokladem pro AML monitoring je primárně zavedení a uplatňování postupů pro včasnou detekci, prošetření a oznámení podezřelých obchodů FAÚ podle ustanovení § 18 odst. 1 AML zákona tak, aby ve svém celku bylo dosaženo smyslu a účelu AML zákona, tedy aby v případě potřeby bylo možné peněžní prostředky včas zajistit.[38]

Z požadavků stanovených AML vyhláškou, zejména pak z ustanovení § 17a, jednoznačně vyplývá, že povinná osoba musí účinně monitorovat transakce tak, aby mohla odhalit a prošetřit případná podezření v přiměřené lhůtě. Z AML vyhlášky rovněž vyplývá, že povinná osoba musí zavést

---

35 Ve smyslu EBA/GL/2019/02 – EBA Guidelines on outsourcing.

36 Ustanovení § 21 odst. 1 AML zákona stanoví: „*Povinná osoba **zavede a uplatňuje odpovídající strategie a postupy vnitřní kontroly a komunikace ke zmírňování a účinnému řízení rizik** legalizace výnosů z trestné činnosti a financování terorismu identifikovaných v hodnocení rizik podle § 21a a k naplnění dalších povinností stanovených tímto zákonem*“.

37 To vše samozřejmě kontinuálně při zachování RBA, z něhož je zřejmé, že některé typologie jsou prováděny před jejich provedením (ex-ante), např. kontroly transakcí oproti sankčním seznamům, a jiné zase po jejich provedení (ex-post), např. kumulace hotovostních transakcí.

38 ČNB rovněž upozorňuje na doplňující ustanovení § 15 AML zákona, které v rámci šetření alertu slouží nejen jako nástroj povinné osoby k získání potřebných informací a podkladů, ale též v případech existence pochybností o pravdivosti informací, kdy oznámení dle ustanovení § 18 odst. 1 AML zákona bývá realizováno i v kombinaci s uplatněním zmiňovaného ustanovení § 15 AML zákona.

vyhledávání informací automatizovaným způsobem, leda že je nepřiměřené její velikosti či povaze obchodní činnosti (viz ustanovení § 17 odst. 2 AML vyhlášky). V případě bank nelze s ohledem na jejich velikost a komplexnost uvažovat o možnosti jiné, než o zpracování pomocí automatizovaných systémů.

Jednou z klíčových vlastností takového systému pak musí být odpovídající nastavení lhůt pro generování alertů a jejich následné prošetření. Postup zpracování alertu zahrnuje všechny fáze jeho existence: vygenerování, prioritizaci, šetření, uzavření. Prošetřování je pak spjaté s prioritizací alertů na základě RBA. Obecně lze uvést, že okamžik zahájení šetření alertů a rovněž i délka šetření alertů, by měly odpovídat rizikovosti sledované typologie, ve spojení s rizikovostí daného klienta / obchodu. K tomuto je nutné uvést, že lhůta pro šetření alertů začíná běžet jeho vlastním vygenerováním, nikoliv „otevřením“ (přiřazením příslušnému pracovníkovi). Alert, který je generovaný scénářem sledujícím denní či týdenní historii transakcí, předpokládá zpracování bezodkladně či maximálně v řádu dnů. Alert, který je generovaný scénářem sledujícím delší historii transakcí (týdny, měsíce) či komplexněji podmínky (např. změna cash-flow, toky v rámci ESS/ESSO[39]), předpokládá zpracování do měsíce.

Lhůta zpracování alertu je ovlivňována řadou skutečností. Příkladem lze uvést situaci, kdy je klient vyzván k součinnosti, např. doložení dokumentů, ale z objektivních důvodů je nemůže obratem doložit, např. je na dovolené / pracovní cestě v zahraničí.[40] Poté se může lhůta pro šetření adekvátně prodloužit. Tyto důvody objektivně mohou ztížit či dokonce znemožnit včasné uzavření alertu. Pokud se tak stane, je nutné, aby nastalé překážky včasného zpracování alertu byly součástí záznamu šetření (uzavření), a to včetně popisu kroků vynaloženého úsilí o jejich překonání.

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy:

- **Samotné vygenerování alertu probíhá bez rozdílu situací (detekčních scénářů dle sledovaných typologií) v tzv. dávkách (batch), zpravidla až po týdnech či až 30 dnech. Jedná se o situace, kdy je již fakticky naplněna podmínka detekčního scénáře pro vygenerování příslušného alertu, nicméně tento je k prověření vygenerován a předán hromadně v rámci jednotlivé dávky.**
- **Jsou stanoveny extrémně nepřiměřeně dlouhé lhůty pro samotné šetření jednotlivých alertů, zpravidla v řádech desítek až stovek dní.[41] Takovéto situace jsou vytvořeny zejména v případech povinných osob, které jsou součástí mezinárodně působící skupiny, kde je vytvořen systém tzv. investigačních center (hubů), do kterých je outsourcováno samotné šetření, přičemž každá další investigační úroveň (level) má stanovenu dílčí lhůtu pro šetření. Právě součet těchto dílčích lhůt může v konečném důsledku vytvářet předpoklad pro nepřiměřeně dlouhé šetření, tedy časového okamžiku od provedení samotné transakce či sledu transakcí v důsledku čehož se z AML**

[39] Rizikové indikátory mohou být mj. i v rámci převodů téže ekonomicky spjaté skupiny (ESS) či ekonomicky spjaté skupiny osob (ESSO).

[40] Dalšími objektivními důvody mohou být např. situace (i) nemoc klienta nebo odpovědných zaměstnanců právnické osoby (zde ovšem za podmínky řádné funkce řízení rizik za účelem předpokladu očekávatelné míry zastupitelnosti); (ii) odpověď klienta vyvolá další otázky a je třeba dotaz opakovat / zpřesnit; (iii) existence veřejných zdrojů, které mohou potvrdit informace o transakci nebo získané od klienta, ale lze je ověřit až s určitým časovým zpožděním (např. zápisy do katastru nemovitostí); (iv) prodleva způsobená čekáním na odpověď (zejména ze zahraničí).

[41] V praxi lze samozřejmě očekávat přípustnou odchylku od stanovených lhůt v odůvodnitelných situacích, viz příklad uvedený v textu výše.

monitoringu do jisté míry stává pouhé „papírové cvičení“, které nebere na zřetel zákonem sledovaný smysl a účel daných opatření.

ii. Postupy pro šetření alertů, zařazení na whitelisty

Prosté a mechanické zavedení systému hlášení podezřelých transakcí, resp. identifikace alertů, či zařazení klientů či jednotlivých účtů klienta na tzv. „whitelist“[42], bez ohledu na další navazující činnosti povinné osoby a alespoň základní formalizaci daných postupů, vede ve svém důsledku k systému, který neplní svoji funkci a stěží může představovat naplnění zákonného požadavku a účinné opatření, které je způsobilé řídit ML/FT rizika a přispívat k cíli sledovanému AML zákonem, tj. bránit legalizaci výnosů z trestné činnosti a financování terorismu (srov. ustanovení § 1 AML zákona).

Přístup povinné osoby založený na ad hoc subjektivním posouzení situace nelze považovat za dostatečný. Tento přístup mj. vytváří nepřiměřenou zátěž na AML systém v rámci povinné osoby, a to zejména s ohledem na absenci dané metodiky, která by jednoznačně stanovovala daná pravidla tak, aby mohla být adekvátně přezkoumatelná a i vynutitelná vůči jednotlivým zaměstnancům povinné osoby. Smyslem a účelem není zvyšovat nepřiměřeně zátěž v podobě „byrokratických“ interních metodik, které mají do detailu popisovat každou možnou situaci, ale to, aby byly alespoň v základních rysech definovány základní postupy. Je očekávatelné, že každý jednotlivý případ (tzv. alert) má svá specifika. Lze tedy očekávat jistou míru odchylky, ale právě tato musí být určitelná a rekonstruovatelným způsobem ověřitelná. Součástí pravidel a postupů pro šetření alertů by měla být rovněž metodika, která by stanovovala priority pro jejich šetření. Tedy takový postup, který by adekvátně zohledňoval RBA, kdy lze důvodně očekávat, že šetření bude započato od klientů/transakcí, které představují vyšší riziko, a končit u klientů/transakcí s nejmenším rizikem.[43]

Omezení AML monitoringu u subjektů či transakcí, tzv. „whitelistování“, je obecně přípustné ve smyslu zjednodušené kontroly klienta dle ustanovení § 13 AML zákona.[44] V praxi se z technologického pohledu jedná o standardní funkcionalitu většiny systémů. O používání whitelistování lze uvažovat za předpokladu, že systémové opatření sloužící k řízení AML/CFT je adekvátní a dostatečně robustní tak, aby bylo možné uvažovat o individuálních a konkrétních odchylkách od nastaveného systému (nikoliv plošné vyřazování skupin klientů). Takovéto postupy musí být ale vždy doprovázeny jak metodikou (viz předchozí část), tak odůvodněním v kontextu řízení rizik, a zejména pak souvisejícími kontrolními mechanismy pro pravidelnou kontrolu odůvodnitelnosti dané výjimky.[45] Tyto procesy musejí být i zpětně rekonstruovatelné ve smyslu ustanovení § 18 AML vyhlášky. Pokud tedy řídicí a kontrolní systém kontrolované osoby v oblasti AML/CFT takovéto předpoklady splňuje, lze na whitelist zařadit jednotlivé klienty či účty klientů.

---

42 Tj. interní seznam subjektů, které jsou automaticky vyřazeny z monitoringu.

43 Nicméně i u klientů s nejmenším rizikem by měly být lhůty nastaveny v kontextu kapitoly „Lhůty pro šetření a generování alertů“ tohoto dohledového benchmarku.

44 Whitelistování v mezích zjednodušené identifikace a kontroly klienta nelze zaměňovat s výjimkou z identifikace a kontroly klienta ve smyslu ustanovení § 13a AML zákona. V rámci zjednodušené identifikace a kontroly klienta je tedy stále dána povinnost provádět kontrolu, a to v přesně stanoveném (omezeném) rozsahu s ohledem na rizika spojená s produktem a klientem.

45 Pravidelná revize by měla mj. včas odhalit výskyt ML/FT rizikového faktoru, který by znemožňoval ponechání na whitelistu.

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup mj. situace, kdy součástí SVZ nejsou formalizované postupy pro:

- **šetření jednotlivých alertů a pořadí jejich šetření, jež by bralo v potaz RBA;**
- **zařazování subjektů do výjimek z AML monitoringu, tzv. „whitelistování", (nepostačí pouhé nastavení v rámci dané aplikace/systému) včetně řádného odůvodnění a schválení odpovídající danému riziku a pravidelné přezkoumávání odůvodněnosti aplikace zjednodušené kontroly formou tzv. „whitelistování".**

iii. Uzavření alertu

Každý alert představuje potenciálně podezřelý obchod, který je třeba prověřit, vyhodnotit a uzavřít. Součástí uzavření je pak příslušné vyjádření, tj. uvést, zda a proč byla podezřelost obchodu v daném případě vyloučena či nikoliv a uvést informaci o případných dalších opatřeních (např. neuskutečnění obchodu, podání oznámení podezřelého obchodu ve smyslu AML zákona). Vyjádření k uzavření pomáhá povinné osobě zajistit rekonstruovatelnost postupů a procesů, jak je požadováno AML zákonem i vyhláškou[46].

S ohledem na shora uvedené tedy ČNB považuje za nedostatečně obezřetný přístup, pokud:

- **Z alertu nelze zpětně rekonstruovat důvod a okolnosti způsobu jeho vyřešení, tedy včetně alertů uzavřených bez podání oznámení podezřelého obchodu nebo bez aplikace ustanovení § 15 AML zákona, tj. neuskutečnění obchodu.[47]**

IV. AML monitoring s využitím umělé inteligence (AI)

ČNB vnímá trend zavádění technologií, které využívají umělé inteligence (tzv. „AI") a přínosů z nich plynoucích. Jedná se nejen o úspory v rámci personálních kapacit nutných např. v kontextu narůstajících objemů alertů, ale zejména o potenciální přínos spočívající v kvalitě detekce jednotlivých podezřelostí[48], kde je možné více zacílit na individuální prvky v rámci každého jednotlivého klienta. ČNB obecně zastává pozici tzv. technologické neutrality, a tedy ani v oblasti AML se nebrání zavádění systémů s využitím AI.[49] Současné využití je poměrně široké, počínaje nástroji pro vstupní kontrolu klienta, prioritizaci jednotlivých alertů, které stále šetří jednotliví pracovníci povinné osoby až po plně automatizované šetření alertů, která jsou následně verifikována. Jako každá technologie, mají i systémy využívající AI svá úskalí a rizika, která je potřeba detekovat, řídit a vytvořit k nim adekvátní opatření.

---

46 Ustanovení § 16 odst. 3 AML zákona a § 18 AML vyhlášky.

47 Typickým nedostatkem je v případě uzavření alertu pouhé uvedení poznámky „OK" bez dalšího vysvětlení.

48 Z poznatků ČNB v kontextu dohledové praxe, diskusí a v rámci tzv. „AML komunity" a mj. i z vyjádření komerčních subjektů vyplývá, že i velmi kvalitně odladěný AML systém postavený na tzv. rule-based scénářích vykazuje efektivitu cca 10 %. Příkladem lze uvést např. „*Worldwide banks manually review millions of financial crime monitoring alerts per month with almost 95% of the alerts raised being 'non-suspicious'.*" https://home.kpmg/xx/en/home/services/advisory/risk-consulting/fighting-financial-crime/transaction-monitoring.html.

49 Obecně i AML zákon a AML vyhláška jsou svou povahou technologicky neutrální, mj. i ve vztahu k AML monitoringu.

V případě použití prvků AI považuje ČNB za obezřetný přístup následující:

- **Ověření kvality vstupních, tzv. učících dat, na kterých se bude provádět prvotní kalibrace (nastavení) AI.**[50]
- **Dostatečná míra srozumitelnosti a rekonstruovatelnosti rozhodovacích procesů učiněných AI. Výsledek procesu, např. důvody pro vyhodnocení alertu, musí být zpětně vysledovatelné. Obecně je tato problematika označována jako „self-explainable AI".**
- **Možnost průběžné kalibrace modelu AI. Jedná se zejména o situace, kdy dojde k relativně rychlé změně okolností/chování v daném segmentu.**[51]
- **K implementaci systémů s prvky AI dochází v působnosti IT týmů a ve spolupráci s útvarem řízení rizik. Systémy umělé inteligence musí obsahovat jasnou projektovou dokumentaci (ve smyslu zavedení/implementace nástroje). Strojové učení zahrnuje testování a průběžné aktualizování.**
- **Je řešena otázka tzv. „programové předpojatosti" v rozhodování systému. Předpokladem je mitigace rizika vyplývající z okolnosti, že systémy AI se učí ze souboru dat, na kterých byly „vyškoleny", a v závislosti na způsobu, jakým k tomuto sestavení došlo, existuje možnost, že soubor dat bude odrážet předpoklady nebo předsudky. Tyto předsudky pak mohou ovlivnit rozhodování systému a vést k neodůvodněné diskriminaci.**
- **Udržovat maximální transparentnost systému. Je nutné, aby uživatel systému byl schopen vysvětlit pravidla fungování AI a ty bylo možné průběžně ověřovat pro správnost nastavení resp. jejich fungování, nikoli, aby se jednalo o tzv. „black box".**

Závěr

ČNB očekává, že povinná osoba v kontextu shora uvedených předpokladů přijme takové postupy a opatření v oblasti AML monitoringu, kterými zajistí účinnou prevenci legalizace výnosů z trestné činnosti a financování terorismu včetně efektivního detekování potenciálně podezřelých obchodů, které ji v konečném důsledku nebudou vystavovat rizikům včasného neoznámení podezřelého obchodu.

[50] Jedná se např. o problematiku tzv. „datových kotev" které si AI při učení vytvoří. Příklad špatné kalibrace (učících dat) – systém měl poznat ze souborů fotografií zvířat vlka. Systém vykazoval 98% úspěšnost. Posléze se zjistilo, že vlka poznal vždy kvůli tomu, že na pozadí obrázku s vlkem byl sníh. Pokud se sníh odstranil, úspěšnost poznání vlka kleslo na 50 %.

[51] Příkladem může být nástup pandemie, v důsledku čehož dojde k celospolečenským změnám, tedy i ke změnám v chování jednotlivých klientů. Příkladem větší výběr hotovosti (nástup pandemie, nejistota), zvýšené platby na e-shopech / platebními kartami (práce v režimu „homeoffice", obchodníci vyžadují pouze bezkontaktní platby apod.). Opačným příkladem může být situace, kdy podnik v době tzv. „lock-downu" vykazoval stále stejné hotovostní tržby.

Příloha č. 1 - Vybrané části požadavků směrnice MiFID II pro účely: (i) řízení produktů (tzv. product governance) a (ii) posouzení vhodnosti

Vhodnost	Product governance
čl. 54+ čl. 55 Nařízení 2017/565 + Obecné pokyny ESMA	*čl. 18 Obecných pokynů ESMA*
	Typ zákazníků, jimž je produkt určen: Podnik by měl vymezit, jakému typu zákazníků je produkt určen. Toto vymezení by mělo být provedeno na základě kategorizace zákazníků podle směrnice MiFID II jako „neprofesionálního zákazníka“, „profesionálního zákazníka“ a „způsobilé protistrany“.
Znalosti v oblasti investic: typy služeb, obchodů a finančních nástrojů, které zákazník zná. **Zkušenosti** v oblasti investic: povaha, objem a frekvence obchodů s finančními nástroji, které zákazník provádí, a doba, po kterou jsou prováděny. **Vzdělání a povolání** nebo relevantní dřívější povolání zákazníka či potenciálního zákazníka.	**Znalosti a zkušenosti**: Podnik by měl vymezit znalosti, které by cíloví zákazníci měli mít o jednotlivých prvcích, jako jsou: relevantní typ produktu, vlastnosti produktu nebo znalosti v tematicky souvisejících oblastech, které pomáhají produkt pochopit. Například u strukturovaných produktů se složitým výnosovým profilem by podniky mohly vymezit, že by cíloví investoři měli vědět, jak tento typ produktu funguje, a měli by znát pravděpodobné výsledky produktu. Pokud jde o zkušenosti, podnik by mohl popsat rozsah praktických zkušeností cílových zákazníků s prvky, jako jsou: relevantní typ produktů, relevantní vlastnosti produktů nebo zkušenosti v tematicky souvisejících oblastech. Podnik by mohl například vymezit dobu, po kterou by měli být zákazníci aktivní na finančních trzích. V některých případech mohou být znalosti a zkušenosti na sobě vzájemné závislé (tj. investor s omezenými nebo nulovými zkušenostmi by mohl být způsobilým cílovým zákazníkem, jestliže jsou jeho chybějící zkušenosti nahrazeny rozsáhlými znalostmi).
Finanční zázemí, včetně schopnosti nést ztráty: informace o finanční situaci zákazníka nebo potenciálního zákazníka zahrnují údaje o zdroji a výši jeho pravidelných příjmů, jeho aktiv, včetně likvidních aktiv, investic a nemovitostí, a o jeho pravidelných finančních závazcích.	**Finanční situace se zaměřením na schopnost nést ztráty**: Podnik by měl v procentuálním vyjádření vymezit rozsah ztrát, které by cíloví zákazníci měli být schopní a ochotní nést (například od minimálních ztrát k úplné ztrátě), a měl by vymezit, zda existují jakékoliv další platební závazky, které mohou překročit investovanou částku (například výzvy k dodatkové úhradě). Uvedené je rovněž možné vyjádřit jako maximální podíl aktiv, který by měl být investován.
Investiční cíle, včetně tolerance k riziku: informace o investičních cílech zákazníka nebo potenciálního zákazníka zahrnují údaje o době, po kterou chce zákazník investici držet, jeho preferencích týkajících se podstoupení rizik, o jeho rizikovém profilu a o účelech investice.	**Riziková tolerance a slučitelnost poměru rizika a výnosů produktu s cílovým trhem:** Podnik by měl vymezit obecný postoj, který by cíloví zákazníci měli ve vztahu k rizikům investice mít. Základní postoje vůči riziku by měly být rozřazeny do jednotlivých kategorií (například „rizikově orientovaný nebo spekulativní“, „vyvážený“, „konzervativní“) a měly by být jasně popsány. Vzhledem k tomu, že jednotlivé podniky v řetězci mohou mít odlišné přístupy k vymezení rizika, podnik by měl jasně stanovit kritéria, která musí být splněna při kategorizaci zákazníka tímto způsobem. Při plnění tohoto požadavku by podniky měly v relevantních případech používat ukazatel rizik stanovený nařízením o strukturovaných retailových investičních produktech a pojistných produktech s investiční složkou (PRIIP) nebo směrnicí o SKIPCP.
	Cíle a potřeby zákazníků: Podnik by měl vymezit investiční cíle a potřeby cílových zákazníků, které má produkt splňovat, včetně širších finančních cílů cílových zákazníků nebo celkové strategie, kterou se při investování řídí. Například by mohl být zmíněn očekávaný investiční horizont (počet let, po které má být investice držena). Tyto cíle lze „doladit“ vymezením konkrétních aspektů investice a očekávání cílových zákazníků. Konkrétní cíle a potřeby zákazníků, které má produkt splňovat, se mohou pohybovat od konkrétních k obecnějším. Produkt může být například navržen tak, aby odpovídal potřebám určité věkové skupiny, byl daňově efektivní na základě země, kde mají zákazníci daňový domicil, nebo byl navržen se zvláštními vlastnostmi produktu tak, aby případně splňoval určité investiční cíle, jako je „měnová ochrana“, „zelené investice“, „etické investice“ atd.