****

****

**S.I.HAL s.r.o.**

ANTI MONEY-LAUNDERING(AML)

&

KNOW YOUR CUSTOMER(KYC)

 **Politika platformy Smartex.info proti praní špinavých peněz**

1. **Definice AML politiky a některé definice**

Smyslem této politiky společnosti S.I.Hal s.r.o. (dále jen "společnost") je zakázat a aktivně provádět prevenci praní špinavých peněz a jakoukoli činnost, která napomáhá praní špinavých peněz nebo financování teroristické nebo trestné činnosti. Společnost se zavazuje k dodržování předpisů AML v souladu s platnými právními předpisy ČR.
SPOLEČNOST vyžaduje, aby její zaměstnanci, zaměstnanci a přidružené subjekty dodržovali tyto standardy při předcházení používání svých produktů a služeb pro účely praní špinavých peněz.Společnost používá některých složitějších technik pro zajišťování bezpečnosti, tuto činnost vykonává v zájmu udržení dobrých vztahů s partnerskými finančními institucemi a dobré reputace před partnery a zákazníky. Informace o zákaznících jsou neveřejné, jsou skladovány dle zákonů o ochraně osobních údajů a nejsou vydány jinak než na základě zákonné pravomoci příslušného orgánu.

Pro účely této politiky je praní špinavých peněz obecně definováno jako zapojení do aktů určených k utajení nebo maskování skutečného původu výnosů z trestné činnosti, aby se zdálo, že protiprávní výnos pochází z legitimního původu nebo představuje legitimní majetek.

Praní peněz obecně probíhá ve třech fázích.

1. Peněžní prostředky nejprve vstupují do peněžního systému ve fázi "umístění", kde peněžní prostředky získané z trestné činnosti jsou přeměněny na měnové nástroje, jako jsou peněžní příkazy nebo cestovní šeky, nebo uloženy na účty ve finančních institucích.
2. Ve fázi "vrstvení" se prostředky převádějí nebo přesouvají na jiné účty nebo jiné finanční instituce, aby dále oddělily peníze od svého trestného původu.
3. Ve fázi "integrace" jsou finanční prostředky znovu zavedeny do ekonomiky a využívány k nákupu oprávněných aktiv nebo k financování jiných trestných činností nebo legitimních podniků.

Financování terorismu nemusí zahrnovat výnosy z trestné činnosti, ale spíše pokus o utajení původu nebo zamýšleného využití finančních prostředků, které budou později použity pro kriminální účely.

Každý zaměstnanec společnosti, jehož povinnosti souvisejí s poskytováním produktů a služeb společnosti a které se přímo či nepřímo zabývá klientelem společnosti, očekává, že bude znát požadavky platných zákonů a předpisů, které ovlivňují jeho pracovní povinnosti, a je kladnou povinností takového zaměstnance, aby tyto povinnosti vždy plnil způsobem, který splňuje požadavky příslušných zákonů a předpisů.

Každý zaměstnanec i vnitřní partner společnosti tuto politiku podepíše sám za sebe svým jménem nebo ji akceptuje při registraci

Aby bylo zajištěno provádění této obecné politiky, vedení společnosti vytvořilo a udržuje průběžný program za účelem zajištění souladu s příslušnými zákony a předpisy a předcházení praní špinavých peněz. Tento program usiluje o koordinaci specifických regulačních požadavků v celé skupině v rámci konsolidovaného rámce, aby bylo možné účinně minimalizovat riziko vystavení platformy praní špinavých peněz a financování terorismu

1. **Odhad rizika**

Posouzení rizika vystavení problému praní špinavých peněz ve všech vztazích se zákazníky musí být dokončeno pomocí standardního modelu rizikové klasifikace společnosti. Každý uživatel má svůj vlastní "rizikový rating", který není veřejný. V případě, že uživatelé vykazují neobvyklý rating, jsou povini se podrobit nezbytným opatření - deklarovat zdroj finančních prostředků. V opačném případě je ukončena spolupráce s uživatelem, zavedení uživatele na černou listinu a případně předání informací dalším orgánům, vyžaduje-li to zákon nebo příslušný orgán na základě zákonné pravomoce.

1. **Podezřelá činnost**

Existují náznaky podezřelých aktivit, které naznačují praní špinavých peněz. Ty jsou běžně označovány jako "Red flag" (červená vlajka 🡪 symbol pro podezřelou aktivitu)

Pokud je zjištěna červená vlajka, bude provedena dodatečná náležitá péče před přijetím požadavků klienta nebo poskytováním služeb. Červená vlajka neboli red flag nemusí nutně znamenat trestnou činnost uživatele. Red flag není definována zákonem, jedná se pouze o instrumenty, se kterými společnost pracuje v rámci udržení dobré reputace před regulátory. Red flag je pouhým důvodem pro zvýšenou pozornost společnosti. Společnost bude pracovat takovým způsobem, aby s informacemi pracovala efektivně.

Příklady „červených vlajek“ jsou:

* Zákazník vykazuje mimořádné obavy ohledně politik AML, zejména pokud jde o jeho totožnost, druh podnikání a majetek, nebo se zdráhá nebo odmítá odhalit jakékoli informace týkající se podnikatelských činností nebo poskytne nereálné, padělané nebo podezřelé identifikační nebo obchodní doklady.
* Zákazník se chce zapojit do transakcí, které nemají obchodní smysl nebo zjevnou investiční strategii, nebo jsou v rozporu s uvedenou obchodní strategií zákazníka.
* Informace poskytnuté zákazníkem, které identifikují oprávněný zdroj peněžních prostředků, jsou nepravdivé, zavádějící nebo podstatně nesprávné.
* Zákazník se odmítne na žádost identifikovat nebo neoznačí legitimní zdroj svých prostředků a jiných aktiv.
* Zákazník (nebo osoba veřejně spojená se zákazníkem) má sporné zázemí nebo je předmětem zpravodajství o možných trestních, občanských nebo regulačních porušováních.
* Zákazník projevuje nedostatečnou pozornost ohledně rizik, nesmyslným poplatkům nebo jiným transakčním nákladům
* Zdá se, že zákazník jedná jako zástupce nezveřejněné jistiny, ale odmítá nebo se zdráhá, bez oprávněných obchodních důvodů, poskytnout informace nebo jiným způsobem vyhýbat se této osobě nebo subjektu.
* Zákazník má potíže s popisem povahy svého podnikání nebo nemá obecné znalosti o svém oboru.
* Zákazník se pokouší provádět časté nebo velké vklady měny, trvá na tom, že obchoduje pouze s peněžními ekvivalenty.
* Bez ohlášení nebo jasného důvodu má zákazník více účtů pod jedním jménem nebo více názvy, s velkým počtem přenosů mezi účty nebo třetími stranami.
* Účet zákazníka má nevysvětlitelnou nebo náhlou aktivitu, zejména u účtů, které neměly nebo neměly žádné předchozí aktivity.
* Účet zákazníka má jakékoliv množství bankovních převodů třetím osobám, které nejsou ve spojení, v rozporu s Obchodními podmínkami a s oprávněným obchodním účelem zákazníka.
* Účet zákazníka má bankovní převody, které mají zjevný obchodní účel pro zemi identifikovanou jako rizikovou pro praní špinavých peněz nebo pro financování ilegálních aktivit
* Účet zákazníka označuje velké či časté bankovní převody, které byly okamžitě zrušeny šekovou nebo debetní kartou bez jakéhokoli zjevného obchodního účelu.
* Zákazník provádí nadměrné převody mezi nesouvisejícími účty bez jakéhokoli zjevného obchodního účelu.
* Zákazník požaduje, aby byla transakce zpracována tak, aby se zabránilo běžným požadavkům firmy na dokumentaci.
* Jiná činnost zákazníka nebo jeho chování vypovídá o jeho působení v trestné činnosti nebo porušování zákonů
1. **Identifikace zákazníka**

Společnost bude dokumentovat a udržovat písemné postupy pro identifikaci zákazníků (dále jen "ověření"), které umožní vytvořit přiměřené přesvědčení, že společnost zná skutečnou identitu svých zákazníků.

Není-li společnost schopna ověřit totožnost zákazníka v přiměřené lhůtě po vyzvednutí služby nebo otevírání účtu, budou tyto služby pozastaveny a účet bude uzavřen. Takový účet a služby budou předmětem zvýšené péče, dokud nebude ověřena totožnost zákazníka nebo bude účet zrušen a služby pozastaveny.

Společnost nutně neověřuje každého zákazníka, ověřuje pouze takové, u kterých uzná ověření za nutné na základě red flag nebo na zálkadě příslušných zákonů. V rámci ČR se společnost bude řídit zákonem 253/2008 Sb. Proti legalizaci výnosů z trestné činnosti a financování terorizmu, v platném znění a znění pozdějších předpisů.

1. **Ověření a proces KYC pro fyzické osoby**

Pro fyzické osoby by měly být případně získány následující informace:

* Křestní jméno a příjmení a všechna jiná jména používaná (například rodné jméno).
* Správná adresa trvalého bydliště (je třeba získat úplnou adresu, není dostatečné číslo poštovní schránky).
* Telefonní číslo, faxové číslo a e-mailová adresa.
* Datum a místo narození.
* Národnost.
* Cestovní průkaz / řidičský průkaz nebo jiný vládní doklad s fotografií a jménem
* Zaměstnání, veřejná funkce a / nebo jméno zaměstnavatele.
* Úřední osobní identifikační číslo nebo jiný jedinečný identifikátor, který je obsažen v nezaniklém úředním dokladu (např. Pas, průkaz totožnosti, povolení k pobytu, záznamy o sociálním zabezpečení, řidičský průkaz) s fotografií zákazníka.
* Zdroj bohatství (dodatečná informace v případě dodatečných otázek ze strany společnosti).

Společnost ověří tyto informace nejméně jednou z následujících metod:

* Potvrzení data narození z úředního dokumentu (např. Rodný list, cestovní pas, průkaz totožnosti, záznamy o sociálním zabezpečení).
* Potvrzení trvalé adresy (např. Účet za služby, daňový výměr, bankovní výpis, dopis od veřejného orgánu).
* Kontaktujte zákazníka telefonicky, dopisem nebo e-mailem, abyste potvrdili informace poskytnuté po otevření účtu
1. **Ověřování a proces KYC pro právnické osoby**

Základními principy identifikace zákazníků pro fyzické osoby platí stejná aplikace pro identifikaci zákazníků pro všechny právnické osoby. Pokud se jedná o identifikaci a ověřování fyzických osob, musí být výše uvedené pokyny pro tyto osoby stejné. Základní úroveň KYC pro právnickou osobu zahrnuje KYC pro fyzickou osobu.

U právnických osob (tj. Společností a partnerství) je třeba získat následující dodatkové informace k KYC pro fyzickou osobu, které je zastupitelem společnosti:

* Název instituce.
* Hlavní místo podnikatelské činnosti instituce.
* poštovní adresa instituce.
* Kontaktní telefonní a faxová čísla.
* Některá forma oficiálního identifikačního čísla, je-li k dispozici (např. Daňové identifikační číslo).
* originál nebo ověřená kopie osvědčení o zakládání a stanov a stanov.
* Povaha a účel podnikání a jeho legitimita.

Tyto informace by měly být ověřeny alespoň jednou z následujících metod:

* U zavedených právnických osob - přezkoumání kopie poslední zprávy a účtů (auditované, pokud jsou k dispozici).
* Proveďte vyhledávání společností a / nebo jiné obchodní dotazy, abyste zjistili, že instituce nebyla, nebo není v procesu, že byla rozpuštěna, zrušena, zrušena nebo ukončena.
* Využít nezávislý proces ověřování informací, například přístup k veřejným a soukromým databázím.
* Získat předchozí bankovní reference.
* Návštěva právnické osoby, pokud je to možné.
* Kontaktování právnické osoby telefonicky, poštou nebo e-mailem.
1. **Monitorování aktivity klienta**

Monitorování transakcí a činností musí být prováděno po celou dobu vztahu s klientem, aby bylo zajištěno, že transakce a prováděná činnost jsou v souladu s klienty KYC, jejich podnikání, zdrojem finančních prostředků a zdrojem bohatství. Monitorování složitých, neobvyklých a velkých transakcí nebo neobvyklých vzorů transakcí musí být přezkoumáno a zaznamenáno písemně. Tyto zkoušky jsou založeny na pozadí a účelu těchto transakcí. Společnost transakce monitoruje v rámci nezbytných zákonů.

1. **Řízení**

Kontrola je řízena na základě vyžádání příslušného orgánu, finanční instituce nebo v případě červené vlajky. V takovém příapdě je zákazník povinen vysvětlit všechny kroky spojené s kontrolou.

V případě, že společnost je kontrolována bankovní institucí, společnost nenese odpovědnost za to, jak dlouho to může trvat. V případě kontroly ze strany třetí strany (která může zmrazit zákazníkovi peníze - jakoukoli bankovní instituci), když zákazník odmítne kontrolu (prostředky odmítnout poskytnout zdroj peněžních prostředků nebo účel transakce) a společnost nebude moci vysvětlit partnerovi potřebné údaje o transakci, peníze mohou být drženy touto třetí stranou až do vysvětlení situace. Zákazník souhlasí s tím, že společnost nese odpovědnost za tyto problémy (protože v takový moment nemá žádný nástroj ke změně).

1. **Uchovávání dat**

Databáze s informacemi o činnosti platformy se uchovává elektronicky prostřednictvím zabezpečeného online úložiště.

Každý klient má složku vytvořenou pod svým uživatelským jménem v administraci provozovatele. Veškerá dokumentace KYC a protokoly o kontrole zabezpečení jsou uloženy v podsložce pro dokumentaci. Dokumentace týkající se platebních transakcí je uložena v další podsložce pro platby a přehledy.

Dokumentace je neveřejná a je přístupná pouze pověřeným orgánům na zákonné officiální vyžádání nebo provozovateli ro účel ověření klienta. Další informace o uchovávání dat jsou poznamenány v přehledu o ochraně osobních údajů.