

Politica de combatere a spălării banilor şi a finanţării terorismului



Iunie 2023

1. Domeniul de aplicare al politicii

Spălarea de bani este participarea la orice tranzacție care urmărește să ascundă sau să deghizeze natura sau originea fondurilor derivate din activitățile ilegale. Spălarea de bani implică nu numai veniturile traficului de droguri, ci și fonduri legate de alte activități ilegale, inclusiv fraude, corupție, criminalitate organizată, terorism și multe alte crime. În general, spălarea de bani constă din trei etape:

- Plasarea: introducerea numerarului provenit din activități ilegale / penale în instituții financiare sau nefinanciare.
- Stratificarea: separarea încasărilor activităților infracționale își formează sursa prin utilizarea unor straturi de tranzacții financiare complexe. Aceste straturi sunt concepute pentru a împiedica traseul de audit, pentru a deghiza originea fondurilor și pentru a oferi anonim.
- Integrarea: plasarea veniturilor spălate în economie în așa fel încât acestea să reintre în sistemul financiar ca fonduri aparent legitime.

Această politică este elaborată și actualizată periodic de către Ofiterul de Management al Riscurilor /Ofițer de conformitate și de către Ofiterul de Prevenire și Combatere a Spălării Banilor al TeleTrade - DJ International Consulting Ltd (Compania) pe baza principiilor generale instituite de Consiliul de Administrație al Companiei în legătură cu prevenirea spălării banilor și finanțării terorismului.

Aceasta politica se aplică tuturor angajaților Companiei și are ca obiectiv să stabilească roluri și responsabilități cheie pentru membrii personalului, precum și să asigure respectarea legislației următoare:

- LEGEA PENTRU PREVENIREA ȘI COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI Nr. 188 (I) / 2007 din 2007-2019 precum și modificare a LEGII Nr.22 (I) 2021 (Legea)
- DIRECTIVA (UE) 2018/843 din 30 mai 2018 de modificare a DIRECTIVEI (EU) 2015/849 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului
- DIRECTIVA DI144-2007-08 din 2012, DIRECTIVA DI144-2007-08 (A) OF 2016 AND DIRECTIVA DI144-2007-08 (B) OF 2016, DIRECTIVA RAD157/2019 actualizata de RAD125/2020 a COMISIEI de SECURITATI si SCHIMB DIN CIPRU (CySEC) pentru PREVENȚIA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISTICE (Directiva AML)
- Orice alte directive, circulare și linii directoare emise de Comisia de Securități și Schimb din Cipru (CySEC), Unitatea de combatere a spălării banilor (MOKAS) , recomandările Grupul de Acțiune Financiară Internațională (" Recomandările FATF "), Orientările ESA și orice altă autoritate încredințată de sarcina de a combate spălarea banilor.

Compania a stabilit principii și proceduri pentru prevenirea spălării banilor și combaterea finanțării terorismului, în conformitate cu profilul de risc al produselor, serviciilor, clienților și locațiilor geografice ale acesteia.

Toate amendamentele și / sau modificările versiunii actuale a politicii trebuie să fie aprobate de Consiliul de administrație al companiei.

2. Politica de acceptare a clienților

Înțelegerea inadecvată a profilului și scopului activității investiționale a clientului poate expune Companie la o serie de riscuri. Pentru a minimiza aceste riscuri, Compania a elaborat Politica de Acceptare a Clienților.

3. Abordare bazată pe riscuri

Compania aplică măsuri și proceduri adecvate, pe o abordare bazată pe riscuri, astfel încât să își concentreze efortul în acele domenii în care riscul de spălare de bani și finanțare a terorismului pare să fie mai mare. Această abordare va permite Companiei să atribuie clienților săi următoarele categorii de risc:

- Clienți cu risc ridicat
- Clienți cu risc mediu
- Categoriile cu risc scăzut

4. Managementul riscului dinamic

Managementul riscurilor este un proces continuu, realizat în mod dinamic. Evaluarea riscului nu este un eveniment izolat cu o durată limitată. Activitățile clientului se schimbă, precum și serviciile și instrumentele financiare furnizate de companie. Același lucru se întâmplă și cu instrumentele financiare și tranzacțiile utilizate pentru spălarea banilor sau finanțarea terorismului.

5. Cunoașterii clientelei (KYC)

Metoda principală pentru prevenirea spălării banilor este prin efectuarea procedurilor “ Cunoaște-ți clientul ”. Cu cunoștințe minuțioase despre clienți, contrapartide și originea fondurilor clientului, poate fi identificat un comportament neobișnuit sau suspect, inclusiv identități false, tranzacții neobișnuite, schimbarea comportamentului sau a altor indicatori în care poate apărea spălarea.

Compania efectuează identificarea obligatorie a fiecărui Client și verificarea identității fiecărui Client și, după caz, a beneficiarilor reali înainte de stabilirea unei relații de afaceri sau de efectuarea tranzacției.

5.1 Stabilirea identificării pentru clienții individuali

Identitatea va fi stabilită pentru satisfacția Companiei prin referire la documentele oficiale de identitate sau la alte dovezi care pot fi adecvate în circumstanțele, inclusiv, fără limitare: numele complet; data nasterii; origine; starea civilă; numele soției / soțului, dacă este căsătorit; numele părinților; adresa completă, inclusiv numărul de telefon și codul orașului; ocupație; informații despre venituri și situația financiară.

Documentele de identificare trebuie să fie valabile la momentul stabilirii relației de afaceri.

Dovada identității potențialului client trebuie să fie sub forma unei copii adevărate sau a unei copii:

- a) Pașaport sau carte de identitate națională dacă potențialul client nu are pașaport

b) Dovada reședinței - acest document poate fi sub forma unei facturi de utilități (factură electrică, apă sau telefon fix, factură de internet la domiciliu), factură fiscală a autorității locale, o scrisoare de confirmare emisă de municipalitate, extras bancar sau alt document echivalent care arată numele complet al clientului potențial (nu poate fi soție / soț/ numele altui membru al familiei) și ar trebui datat în ultimele 6 luni. Cu condiția să existe o explicație rezonabilă, o dovadă de reședință emisă în numele părintelui potențialului client (mama / tatăl) sau soțul/sotia poate fi acceptată, cu toate acestea, ar trebui primite documente suplimentare pentru stabilirea relației, cum ar fi certificatul de naștere, certificatul de căsătorie.

În funcție de țara de origine, Compania poate solicita documente suplimentare și va fi luată în considerare de la caz la caz, în urma unei abordări bazate pe riscuri de către AMLCO și directori.

Compania aplică proceduri suplimentare de identificare a clienților și de diligență cuvenită pentru clienții care prezintă un nivel ridicat de risc pentru spălarea banilor sau finanțarea terorismului și sunt clasificate de către Companie ca fiind risc ridicat conform Politicii de Acceptare a Clienților.

Compania va urma următoarele măsuri pentru a verifica identitatea clienților care nu sunt față în față:

- 1) Atunci când este posibil, se stabilește un contact direct și personal cu potențialul client. Membrul personalului companiei sau unitățile sale organizaționale la distanță, care s-a întâlnit cu clientul în persoană și i-a verificat identitatea, confirmă o întâlnire față în față în profilul clientului în software-ul CRM;
- 2) Contact telefonic cu clientul de la reședința sau biroul său, înainte de stabilirea unei relații de afaceri sau a tranzacției ocazionale, pe un număr de telefon furnizat de potențialul client;
- 3) Contact cu clientul prin e-mail la o adresă de e-mail furnizată de potențialul client.

Compania poate aplica, de asemenea, următoarele metode de verificare suplimentare:

- a) Prima plată a operațiunilor se realizează printr-un cont deschis pe numele clientului cu o instituție de credit care operează și este licențiată într-un stat membru al UE sau într-o țară terță, care impune cerințe pentru combaterea spălării banilor echivalente cu cele din Directiva UE;
- b) Apel video cu potențialul client. Se prevede că un potențial client, a cărui identitate a fost verificată mai jos, nu poate depune o sumă peste € 2.000 pe an, indiferent de numărul de conturi pe care le păstrează la Companie, cu excepția cazului în care se ia o măsură suplimentară conform alineatului de mai sus pentru a-i verifica identitatea. În acest caz, Compania monitorizează atât suma depozitului clientului, cât și riscul de spălare de bani sau finanțare a terorismului, de asemenea, avertizează clientul în mod corespunzător și în timp util pentru procedura de mai sus, pentru a obține consimțământul expres al clientului înainte de începerea acestuia.;
- c) Solicitarea ca documentele de identificare să fie furnizate sub formă de copii autentice certificate ale originalelor. Certificarea se poate face prin:

- un terț, cum ar fi, contabil sau avocat, cu condiția ca măsuri suplimentare/ proceduri sunt aplicate conform alineatului **Utilizarea a unei terța parte pentru identificarea clientului și pentru diligența cuvenită a prezentei politici;**
- o autoritate sau o persoană competentă care, în conformitate cu dispozițiile relevante din legile țării lor, este responsabilă să certifice autenticitatea documentelor sau informațiilor.

6. Monitorizarea continuă

Compania efectuează analize ale înregistrărilor existente și examinează tranzacțiile și activitățile clientilor întreprinse pe parcursul relației de afaceri, să se asigure că tranzacțiile efectuate sunt în concordanță cu cunoștințele companiei despre client, profilul de afaceri și de risc, inclusiv acolo unde este necesar, verificarea sursei și originii fondurilor creditate în conturi.

Compania se asigură că înregistrările de identificare ale clienților ' rămân complet actualizate cu toate datele și informațiile de identificare relevante pe toată durata relației de afaceri. Compania examinează și verifică, în mod regulat, validitatea și adecvarea datele de identificare și informațiile a clientilor pe care le păstrează, în special cele referitoare la clienții cu risc ridicat.

7. Raportarea tranzacțiilor suspecte către MOKAS

Tranzacții suspecte

Tranzacțiile suspecte sunt tranzacții sau alte activități care nu au un scop aparent legal sau nu sunt genul în care un anumit client ar fi în mod normal așteptat să se angajeze, iar Compania nu cunoaște nicio explicație rezonabilă pentru tranzacție sau activitate după examinarea faptelor disponibile, inclusiv contextul și scopul posibil al tranzacției sau activității. Compania, în cazurile în care există o încercare de a se executa tranzacții care cunoaște sau suspectează că sunt legate de spălarea banilor sau finanțarea terorismului, raportează, prin intermediul AMLCO, suspiciunea sa către MOKAS.

8. Păstrarea Evidentelor

Compania trebuie să pastreze evidența pentru următoarele:

- Documente de identificare a clienților obținute
- Orice documente / informații suplimentare obținute în timpul relației
- Toate rapoartele World-Check si Accuity World de conformitate efectuate pentru client, precum și toate rezultatele pentru screening-ul pe listele de sancțiuni.
- Detalii despre toate tranzacțiile comerciale relevante efectuate pentru clienți

pentru o perioadă de cinci (5) ani după încheierea relației de afaceri cu clientul sau după data unei tranzacții ocazionale.

Aceste informații pot fi utilizate ca dovezi în orice investigație ulterioară de către autorități. Evidentele păstrate furnizează probe de audit în timpul oricărei investigații ulterioare. În practică, unitățile de afaceri ale Companiei vor face în mod obișnuit înregistrări ale lucrărilor efectuate pentru clienți în cursul activității normale, iar aceste înregistrări ar trebui arhivate.