POLITICA DE COMBATERE A SPĂLĂRII BANILOR, DE COMBATERE A FINANȚĂRII TERORISMULUI ȘI MĂSURILE DE SANCȚIONARE

28 noiembrie 2024

I. INTRODUCERE

1. Scopul prezentei politici privind măsurile de combatere a spălării banilor ("**AML**"), de combatere a finanțării terorismului ("**CFT**") și a sancțiunilor este de a se asigura că **''Octogon Gas & Logistics S.R.L.''** ("**Societatea**") dispune de politici interne pentru a preveni utilizarea activității sale pentru spălarea banilor și finanțarea terorismului și de politici interne pentru punerea în aplicare a sancțiunilor internaționale.

2. Aceste politici au fost adoptate pentru a se asigura că societatea respectă normele și reglementările stabilite în:

   - Legea nr. 129/2019 privind prevenirea și combaterea spălării banilor și finanțării terorismului;

   - DIRECTIVA (UE) 2018/843 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 30 mai 2018 de modificare a Directivei (UE) 2015/849 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului și de modificare a Directivelor 2009/138/CE și 2013/36/UE (AMLD5).

3. Prezenta politică este supusă revizuirii de către conducerea societății cel puțin o dată pe an. Propunerea de revizuire și revizuirea prezentei politici pot fi programate mai des, dacă este necesar.

4. Prezenta politică este acceptată și aprobată prin hotărârea conducerii societății.

II. DEFINIȚII

1. **Compania** înseamnă persoana juridică cu următoarele date:

   - numele companiei: **Octogon Gas & Logistics S.R.L.;**
   - numărul de înregistrare: **J13/3470/2008;**
   - adresa: **Constanța, Bulevardul Mamaia nr. 182;**
   - e-mail: **office@octogon-gl.ro**

2. **Politica** - prezentul document, inclusiv toate anexele prevăzute mai sus. Politica include, printre altele, politica de evaluare a riscurilor a societății cu privire la abordarea pentru riscurile de ML/TF.

3. **Spălarea banilor** ("**Spălarea banilor**") înseamnă, conform prevederilor legale române din Legea nr. 129/ 2019, articolul 49:

   - schimbul sau transferul de bunuri, cunoscând că aceste bunuri provin din infracțiuni, în scopul de a ascunde sau deghiza originea ilicită a acestor bunuri sau de a ajuta persoana care a comis infracțiunea din care provin bunurile să se sustragă urmăririi penale, procesului sau pedepsei;
   - ascunderea sau disimularea adevăratei naturi, surse, locații, dispoziții, mișcări, circulația, proprietatea sau drepturile cu privire la bunuri, știind că aceste bunuri sunt produsul infracțiunii;
   - achiziționarea, deținerea sau utilizarea unui bun de către o altă persoană decât subiectul activ al infracțiunii din care provine bunul, cunoscând că acest bun provine din infracțiune.

4. **Finanțarea terorismului** (TF) înseamnă obținerea sau punerea la dispoziție, în mod direct sau indirect, de fonduri, legale sau ilegale, cu intenția ca acestea să fie utilizate sau știind că urmează să fie utilizate, în totalitate sau în parte, pentru comiterea de acte de terorism sau pentru sprijinirea unei entități teroriste, constituie finanțarea terorismului constituie infracțiunea de finanțare a terorismului, în sensul legislației aplicabile.

5. **Sancțiunile** reprezintă un instrument esențial al politicii externe menit să sprijine menținerea sau restabilirea păcii, a securității internaționale, a democrației și a statului de drept, respectarea drepturilor omului și a dreptului internațional sau realizarea altor obiective ale Cartei Organizației Națiunilor Unite sau ale politicii externe și de securitate comune a Uniunii Europene. Sancțiunile includ:

   - sancțiuni internaționale care sunt impuse unui stat, teritoriu, unitate teritorială, regim, organizație, asociație, grup sau persoană printr-o rezoluție a Consiliului de

Securitate al Organizației Națiunilor Unite, o decizie a Consiliului Uniunii Europene sau orice altă legislație care impune obligații României;

- sancțiuni ale Guvernului României, care reprezintă un instrument de politică externă ce poate fi impus în plus față de obiectivele specificate în clauza anterioară în scopul protejării securității sau intereselor României.

Sancțiunile internaționale pot interzice intrarea în stat a unei persoane care face obiectul unei sancțiuni internaționale, pot restricționa comerțul internațional și tranzacțiile internaționale și pot impune alte interdicții sau obligații.

Subiectul sancțiunilor este orice persoană fizică sau juridică, entitate sau organism, desemnat în actul juridic care impune sau pune în aplicare sancțiunile, în privința căruia se aplică sancțiunile.

6. **Clientul** înseamnă o persoană fizică sau juridică care are o relație de afaceri cu societatea sau o persoană fizică sau juridică cu care societatea încheie o tranzacție ocazională.

7. **Prin beneficiar real** se înțelege o persoană fizică care, profitând de influența sa, efectuează o tranzacție, un act, o acțiune, o operațiune sau o etapă sau exercită controlul într-un alt mod asupra unei tranzacții, a unui act, a unei acțiuni, a unei operațiuni sau a unei etape sau asupra unei alte persoane și în interesul, în beneficiul sau pe contul căreia se efectuează o tranzacție sau un act, o acțiune, o operațiune sau o etapă. În cazul unei persoane juridice, beneficiarul real este o persoană fizică a cărei participație directă sau indirectă sau suma tuturor participațiilor directe și indirecte în persoana juridică depășește 25 %, inclusiv participațiile sub formă de acțiuni sau alte forme de acțiuni la purtător.

8. **Angajatul** înseamnă angajatul companiei, inclusiv persoanele care sunt implicate în aplicarea prezentei politici în cadrul companiei.

9. **Relația de afaceri** înseamnă o relație care se stabilește în urma încheierii unui contract pe termen lung de către societate în cadrul activităților economice sau profesionale în scopul furnizării unui serviciu sau al distribuirii acestuia într-un alt mod sau care nu se bazează pe un contract pe termen lung, dar pentru care o anumită durată ar putea fi așteptată în mod rezonabil la momentul stabilirii contactului și în timpul căreia societatea efectuează în mod repetat tranzacții separate în cadrul activităților economice sau profesionale în timp ce furnizează un serviciu.

10. **Tranzacția ocazională** înseamnă tranzacția efectuată de societate în cursul activităților economice sau profesionale în scopul furnizării unui serviciu sau vânzării de bunuri sau distribuirii acestora în alt mod către client în afara unei relații de afaceri stabilite.

11. **PEP** înseamnă o persoană fizică care îndeplinește sau a îndeplinit funcții publice importante și cu privire la care persistă riscuri conexe.

III. PRINCIPII PENTRU STRUCTURA ȘI GESTIONAREA SOCIETĂȚII

1. Structura organizatorică a societății trebuie să corespundă dimensiunii acesteia și naturii, domeniului de aplicare și nivelului de complexitate al activităților și serviciilor sale furnizate, inclusiv nivelul de risc și riscurilor aferente, și trebuie să fie structurată în conformitate cu principiul celor trei linii de apărare. Structura organizațională a societății trebuie să corespundă înțelegerii complete a riscurilor potențiale și gestionării acestora. Lanțurile de raportare și subordonare ale societății trebuie să fie asigurate astfel încât toți angajații să își cunoască locul în structura organizațională și să își cunoască sarcinile de lucru.

2. **Conducerea a societății**

2.1. Conducerea societății este purtătoarea culturii de conformitate cu cerințele de prevenire a spălării banilor și a finanțării terorismului, garantând că membrii săi și angajații societății își desfășoară activitatea într-un mediu în care sunt pe deplin conștienți de cerințele de prevenire a spălării banilor și a finanțării terorismului și de obligațiile asociate acestor cerințe, iar considerentele de risc relevante sunt luate în considerare într-o măsură adecvată în procesele decizionale ale societății.

2.2. Conducerea societății poartă responsabilitatea finală pentru măsurile luate pentru a preveni utilizarea serviciilor societății pentru spălarea banilor sau finanțarea terorismului. Aceștia asigură supravegherea și sunt responsabili pentru:

- stabilirea și menținerea proceselor, procedurilor, riscurilor și proceselor de control AML[1] ;
- adoptarea prezentei politici și a altor orientări și instrucțiuni interne;
- stabilirea liniilor directoare ale societății pentru măsurile de combatere a spălării banilor;
- alocarea de resurse suficiente pentru a asigura punerea în aplicare efectivă a politicii și a altor documente conexe și pentru a menține organizația;
- asigurarea faptului că toți angajații relevanți urmează o formare anuală în domeniul AML.

3. **Prima linie de apărare - angajații**

3.1. Prima linie de apărare are rolul de a aplica măsurile de due diligence cu ocazia relațiilor de afaceri și a tranzacțiilor ocazionale și de a aplica măsurile de due diligence în timpul relațiilor

[1] Pentru simplificarea prezentei politici, "AML" include și prevenirea finanțării terorismului și punerea în aplicare a sancțiunilor.

de afaceri. Prima linie de apărare cuprinde unitățile structurale și angajații societății cu ale căror activități sunt asociate riscuri și care trebuie să identifice și să evalueze aceste riscuri, caracteristicile lor specifice și domeniul lor de aplicare și care gestionează aceste riscuri prin intermediul activităților lor obișnuite, în primul rând prin aplicarea măsurilor de due diligence. Riscurile care decurg din activitățile și prestarea de servicii de către societate aparțin primei linii de apărare. Ei sunt managerii (proprietarii) acestor riscuri și responsabili pentru acestea.

3.2. Angajații societății trebuie să acționeze cu prudența și competența așteptate de la ei și în conformitate cu cerințele stabilite pentru funcțiile lor, pornind de la interesele și obiectivele societății, și să se asigure că sistemul financiar și spațiul economic al țării nu sunt utilizate pentru spălarea banilor și finanțarea terorismului. Societatea ia măsuri pentru a evalua aptitudinile angajaților înainte ca aceștia să înceapă să lucreze, cu instruirea corespunzătoare.

3.3. Din motivele menționate mai sus, angajații sunt obligați să:

- să adere la toate cerințele descrise în prezenta politică și în alte documente conexe;
- colectează informațiile necesare despre clienți în conformitate cu funcția și responsabilitățile lor;
- să raporteze conducerii societății informații, situații, activități, tranzacții sau tentative de tranzacții care sunt neobișnuite pentru orice tip de serviciu sau relație cu clienții, indiferent de valoare, indiferent dacă tranzacția a fost sau nu finalizată fără întârziere;
- să nu informeze sau să nu informeze în alt mod clienții dacă aceștia sau alți clienți fac sau pot face obiectul unui raport sau dacă un raport a fost sau poate fi depus;
- să urmeze cursurile de formare corespunzătoare în materie de combatere a spălării banilor, necesare pentru postul ocupat de angajat.

4. A doua linie de apărare - gestionarea riscurilor și conformitatea

4.1. A doua linie de apărare constă în funcțiile de gestionare a riscurilor și de conformitate. Aceste funcții pot fi, de asemenea, îndeplinite de aceeași persoană sau unitate structurală, în funcție de dimensiunea societății și de natura, domeniul de aplicare și nivelul de complexitate al activităților lor și al serviciilor furnizate, inclusiv apetitul la risc și riscurile care decurg din activitățile societății.

4.2. Obiectivul funcției de conformitate este de a garanta că societatea respectă legislația în vigoare, orientările și alte documente și de a evalua efectul posibil al oricăror modificări ale mediului juridic sau de reglementare asupra activităților societății și asupra cadrului de

conformitate. Sarcina conformității este de a ajuta prima linie de apărare, în calitate de proprietari ai riscurilor, să definească locurile în care riscurile se manifestă (de exemplu, analiza tranzacțiilor suspecte și neobișnuite, pentru care angajații din domeniul conformității au competențele profesionale și calitățile personale necesare etc.) și de a ajuta prima linie de apărare să gestioneze eficient aceste riscuri. A doua linie de apărare nu se implică în asumarea de riscuri.

4.3. Politica privind riscurile este pusă în aplicare, iar cadrul de gestionare a riscurilor este controlat de funcția de gestionare a riscurilor. Executantul funcției de gestionare a riscurilor se asigură că toate riscurile sunt identificate, evaluate, măsurate, monitorizate și gestionate și informează unitățile corespunzătoare ale societății cu privire la acestea. Executantul funcției de administrare a riscurilor în scopul combaterii spălării banilor efectuează, în principal, supravegherea respectării nivelului de risc, supravegherea toleranței la risc, supravegherea identificării modificărilor riscurilor, efectuează o trecere în revistă a riscurilor asociate și îndeplinește alte sarcini legate de administrarea riscurilor.

5. **A treia linie de apărare - auditul intern**

5.1. A treia linie de apărare este reprezentată de funcția de audit intern independentă și eficientă. Funcția de audit intern poate fi îndeplinită de unul sau mai mulți angajați, de unitatea structurală a societății cu funcțiile relevante sau de o parte terță care furnizează societății serviciul relevant.

5.2. Angajații, unitatea structurală a societății sau terțul care îndeplinește funcția de audit intern trebuie să aibă competența, instrumentele și accesul la informațiile relevante necesare în toate unitățile structurale ale societății. Metodele de audit intern trebuie să respecte dimensiunea societății, natura, domeniul de aplicare și nivelul de complexitate ale activităților și serviciilor furnizate, nivelul risc și riscurile care decurg din activitățile societății.

5.3. Decizia de a efectua un audit intern este luată printr-o rezoluție a conducerii societății, care trebuie să evalueze necesitatea efectuării unui audit intern cel puțin o dată pe an.

IV. PRINCIPII DE APLICARE A MĂSURILOR DE CUNOAȘTERE A CLIENTELEI

1. Măsurile de precauție privind clientela (CDD) sunt necesare pentru verificarea identității unui client nou sau existent, ca o monitorizare continuă, bazată pe riscuri, a relației de afaceri cu clientul. Măsurile de precauție privind clientela constau în 3 niveluri, inclusiv măsuri simplificate și măsuri consolidate de precauție privind clientela, după cum se specifică mai jos.

2. **Principii fundamentale**

2.1. Măsurile CDD sunt luate și aplicate în măsura necesară, având în vedere profilul de risc al clientului și alte circumstanțe, în următoarele cazuri:

- la stabilirea relației de afaceri și la monitorizarea continuă a relației de afaceri;
- la executarea sau medierea tranzacției (tranzacțiilor) ocazionale în afara relației de afaceri, în cazul în care valoarea tranzacției (tranzacțiilor) depășește 15 000 de euro (sau o sumă egală în alte active) pe o perioadă de până la un an;
- în urma verificării informațiilor colectate în timpul aplicării măsurilor de diligență necesară sau în cazul în care există îndoieli cu privire la suficiența sau veridicitatea documentelor sau datelor colectate anterior, în timpul actualizării datelor relevante;
- în caz de suspiciune de spălare a banilor sau de finanțare a terorismului, indiferent de orice derogări, excepții sau limite prevăzute în prezenta politică și în legislația aplicabilă.

2.2. Societatea nu stabilește sau menține relația de afaceri și nu efectuează tranzacții dacă:

- societatea nu este în măsură să ia și să aplice niciuna dintre măsurile CDD necesare;
- societatea are suspiciuni că serviciile sau tranzacțiile societății vor fi utilizate pentru spălarea banilor sau finanțarea terorismului;
- nivelul de risc al clientului sau al tranzacției nu este conform cu riscurile asumate de societate.

2.3. În cazul primirii de informații în limbi străine în cadrul implementării CDD, societatea poate solicita traducerea documentelor într-o altă limbă aplicabilă societății. Utilizarea traducerilor ar trebui evitată în situațiile în care documentele originale sunt elaborate într-o limbă aplicabilă societății.

2.4. Realizarea CDD este un proces care începe cu punerea în aplicare a măsurilor CDD. Atunci când acest proces este finalizat, clientul atribuie un nivel de risc individual documentat, care va sta la baza măsurilor de monitorizare și care este urmărit și actualizat atunci când este necesar.

2.5. Societatea a aplicat măsurile CDD în mod adecvat în cazul în care societatea are convingerea profundă că a respectat obligația de a aplica măsurile de precauție. Principiul rezonabilității este respectat în luarea în considerare a convingerii interne. Aceasta înseamnă că, la aplicarea măsurilor CDD, societatea trebuie să dobândească cunoștințele, înțelegerea și convingerea că a colectat suficiente informații despre client, activitățile clientului, scopul relației de afaceri și al tranzacțiilor efectuate în cadrul relației de afaceri, originea fondurilor etc., astfel încât să înțeleagă clientul și activitățile (de afaceri) ale acestuia, luând astfel în considerare nivelul de risc al clientului, riscul asociat relației de afaceri și natura acestei relații. Un astfel de nivel de afirmare trebuie să permită identificarea tranzacțiilor complicate, de mare valoare și neobișnuite și a tiparelor de tranzacții care nu au un scop

economic sau legitim rezonabil sau evident sau care nu sunt caracteristice caracteristicilor specifice ale activității în cauză.

3. **Serviciile furnizate**

3.1. Principala activitate economică a societății este reprezentată de serviciile de încărcare și descărcare GPL.

3.2. Verificarea informațiilor utilizate pentru identificarea clientului

3.3. Verificarea informațiilor pentru identificarea clientului înseamnă utilizarea datelor dintr-o sursă credibilă și independentă pentru a confirma că datele sunt adevărate și corecte, confirmând, de asemenea, dacă este necesar, că datele legate direct de client sunt adevărate și corecte. Aceasta înseamnă, printre altele, că scopul verificării informațiilor este de a obține asigurări că clientul care dorește să stabilească relația de afaceri este persoana care pretinde a fi.

3.4. Identificarea față în față (întâlnire personală cu clientul) sau identificarea prin mijloace informatice (utilizarea unui sistem de identificare electronică de încredere) este considerată a fi verificarea credibilă și independentă a informațiilor obținute în cursul identificării.

3.5. În situațiile care nu sunt specificate în metodele de identificare menționate mai sus, sursa credibilă și independentă (trebuie să existe cumulativ) este verificarea informațiilor obținute în cursul identificării:

- care provine din două surse diferite;
- în cazul în care clientul trimite o fotografie a imaginii faciale a clientului și a documentului de identitate utilizat pentru identificare imediat înainte de transmiterea datelor, iar societatea se asigură că fotografia a fost făcută recent;
- care a fost emisă de (documente de identitate) sau primită de la o terță parte sau de la un loc care nu are niciun interes sau legătură cu clientul sau cu societatea, adică care este neutru (de exemplu, informațiile obținute de pe internet nu sunt astfel de informații, deoarece acestea provin adesea chiar de la client sau veridicitatea și independența lor nu pot fi verificate);
- a căror veridicitate și independență pot fi determinate fără obstacole obiective, iar veridicitatea și independența sunt inteligibile și pentru o terță parte neimplicată în relația de afaceri; și
- datele incluse în care sau obținute prin care sunt actualizate și relevante, iar societatea poate obține asigurări cu privire la acest lucru (iar asigurarea poate fi obținută în anumite cazuri și pe baza celor două clauze anterioare).

4. **Aplicarea măsurilor simplificate de due diligence (nivel 1)**

4.1. Procedura simplificată de due diligence (SDD) se aplică în cazul în care profilul de risc al clientului indică un risc scăzut și în cazul în care, în conformitate cu evaluarea riscurilor realizată de societate, s-a identificat faptul că, în aceste circumstanțe, riscul de spălare a banilor sau de finanțare a terorismului este mai scăzut decât în mod obișnuit. În ceea ce privește serviciile prestate de Societate și evaluarea de risc a Societății, aceasta nu va aplica măsuri SDD clienților săi. Prin urmare, tuturor clienților li se vor aplica cel puțin măsuri standard de precauție, astfel cum se specifică mai jos.

5. **Aplicarea măsurilor standard de due diligence (nivelul 2)**

5.1. Măsurile standard de due diligence se aplică tuturor clienților în cazul în care măsurile de CDD trebuie aplicate în conformitate cu politica. Ar trebui aplicate următoarele măsuri standard de precauție:

- identificarea clientului și verificarea informațiilor furnizate pe baza informațiilor obținute dintr-o sursă credibilă și independentă, inclusiv prin utilizarea mijloacelor de identificare electronică și a serviciilor de încredere pentru tranzacțiile electronice;
- identificarea și verificarea unui reprezentant al clientului și a dreptului său de reprezentare;
- identificarea beneficiarului real și, în scopul verificării identității acestora, luarea de măsuri pentru ca societatea să se asigure că știe cine este beneficiarul real și că înțelege structura de proprietate și control a clientului;
- înțelegerea relațiilor de afaceri, a tranzacțiilor sau a operațiunilor și, dacă este cazul, colectarea de informații cu privire la acestea;
- colectarea de informații pentru a stabili dacă clientul este PEP, un membru al familiei acestuia sau o persoană cunoscută ca fiind un asociat apropiat;

-monitorizarea relației de afaceri.

5.2. Măsurile CDD specificate mai sus trebuie aplicate înainte de stabilirea relației de afaceri. Instrucțiunile exacte pentru aplicarea măsurilor standard de precauție sunt furnizate în politică.

6. **Aplicarea măsurilor sporite de due diligence (nivelul 3)**

6.1. În plus față de CDD, societatea aplică măsuri de precauție sporită (EDD) pentru a gestiona și a atenua un risc stabilit de spălare a banilor și finanțare a terorismului care este mai mare decât de obicei.

6.2. Compania aplică întotdeauna măsuri EDD, atunci când:

- profilul de risc al clientului indică un nivel de risc ridicat;
- după identificarea clientului sau verificarea informațiilor transmise, există îndoieli cu privire la veridicitatea datelor transmise, autenticitatea documentelor sau identificarea beneficiarului efectiv;
- clientul este un PEP;
- clientul provine dintr-o țară terță cu risc ridicat sau locul său de reședință sau sediul sau sediul prestatorului de servicii de plată al beneficiarului plății se află într-o țară terță cu risc ridicat;
- clientul provine dintr-o astfel de țară sau teritoriu sau locul său de reședință sau sediul sau sediul prestatorului de servicii de plată al beneficiarului plății se află într-o țară sau teritoriu care, în conformitate cu surse credibile, cum ar fi evaluările reciproce sau rapoartele de monitorizare publicate, nu a instituit sisteme eficiente de combatere a spălării banilor și a finanțării terorismului care sunt în conformitate cu recomandările Grupului de Acțiune Financiară Internațională sau care este considerat un teritoriu cu o rată scăzută de impozitare;
- activitatea economică sau profesională a clientului, domeniul sau factorii indică riscul de spălare a banilor sau de finanțare a terorismului, care este mai mare decât de obicei;
- suma totală a plăților primite sau efectuate de Client în cadrul relației de afaceri depășește limitele stabilite de Societate.

6.3. Înainte de a aplica măsurile EDD, angajatul societății se asigură că relația de afaceri sau tranzacția prezintă un risc ridicat și că o rată de risc ridicat poate fi atribuită acestei relații de afaceri sau tranzacții. Mai presus de toate, angajatul evaluează, înainte de aplicarea măsurilor EDD, dacă caracteristicile descrise mai sus sunt prezente și le aplică ca motive independente (adică fiecare dintre factorii identificați permite aplicarea măsurilor EDD cu privire la client).

6.4. Atunci când se aplică măsurile EDD, trebuie respectate următoarele măsuri suplimentare și relevante de due diligence:

- verificarea informațiilor transmise suplimentar la identificarea clientului, pe baza unor documente, date sau informații suplimentare provenind dintr-o sursă credibilă și independentă;

- colectarea de informații suplimentare privind scopul și natura relației de afaceri sau a tranzacției și verificarea informațiilor transmise pe baza unor documente, date sau informații suplimentare care provin dintr-o sursă veridică și independentă;[2]
- colectarea de informații și documente suplimentare cu privire la executarea efectivă a tranzacțiilor efectuate în cadrul relației de afaceri pentru a exclude sensibilitatea tranzacțiilor;
- colectarea de informații și documente suplimentare în scopul identificării sursei și originii fondurilor utilizate într-o tranzacție efectuată în cadrul relației de afaceri pentru a exclude sensibilitatea tranzacțiilor;
- efectuarea primei plăți legate de o tranzacție prin intermediul unui cont care a fost deschis pe numele clientului care participă la tranzacție într-o instituție de credit înregistrată sau cu sediul într-un stat contractant din Spațiul Economic European sau într-o țară în care sunt în vigoare cerințe egale cu cele ale Directivei (UE) 2015/849 a Parlamentului European și a Consiliului;
- aplicarea de măsuri de diligență privind clientul sau reprezentantul acestuia, în timp ce se află în același loc cu clientul sau reprezentantul acestuia;
- colectarea de informații suplimentare despre client și beneficiarul său real, inclusiv identificarea tuturor proprietarilor clientului, inclusiv a celor a căror participație este sub 25%;
- colectarea de informații cu privire la originea fondurilor și a averii clientului și a beneficiarului său real;
- îmbunătățirea monitorizării relației de afaceri prin creșterea numărului și frecvenței măsurilor de control aplicate și prin alegerea indicatorilor de tranzacție sau a modelelor de tranzacție care sunt verificate suplimentar;
- se face o analiză a impresiei digitale a clientului pe internet (Adverse Media Search);
- obținerea aprobării conducerii societății pentru tranzacțiile cu clienți noi și existenți;

6.5. Valoarea măsurilor EDD și domeniul de aplicare sunt stabilite de angajatul care aplică aceste măsuri. Angajatul notifică cu privire la măsurile EDD aplicate în termen de 2 zile lucrătoare de la începerea aplicării măsurilor EDD prin trimiterea notificării relevante persoanei responsabile.

[2] Această măsură se aplică întotdeauna atunci când societatea intră în contact cu țara terță cu risc ridicat prin intermediul clientului sau al tranzacției.

6.6. În cazul aplicării măsurilor EDD, societatea monitorizează relația de afaceri mai des decât de obicei și reevaluează profilul de risc al clientului nu mai târziu de o dată la șase luni.

V. MĂSURI DE CUNOAȘTERE A CLIENTELEI

1. Identificarea clientului - persoană fizică

1.1. Societatea identifică clientul care este o persoană fizică și, după caz, reprezentantul acestuia și păstrează următoarele date privind clientul:

- nume și prenume;
- codul personal de identificare;
- data nașterii;
- cetățenie;
- locul de reședință sau sediul;
- activitate economică sau profesională.

1.2. Următoarele documente de identitate valabile pot fi utilizate ca bază pentru identificarea unei persoane fizice:

- o carte de identitate;
- un permis de ședere;
- pașaportul unui străin;
- un permis de conducere eliberat într-o țară străină dacă documentul include numele utilizatorului, fotografia sau imaginea facială, semnătura sau imaginea unei semnături și data nașterii sau codul de identificare personală;
- un document de călătorie eliberat într-o țară străină (pașaport).

1.3. În timpul verificării datelor obținute în timpul identificării clientului și a reprezentantului de la o sursă credibilă și independentă, **prima sursă credibilă și independentă** este întotdeauna:

- un document de identitate menționat mai sus sau o copie/imagine colorată și lizibilă a acestui document.

1.4. Următoarele informații obținute pot fi a **doua sursă credibilă și independentă**:

- fotografia clientului (selfie) cu documentul de identitate;
- factura de utilități (de exemplu, factura emisă și plătită o dată pe lună de utilități, inclusiv electricitate, gaze naturale, apă, deșeuri etc.);

- informații pentru verificarea datelor[3] asociate direct cu persoana (de exemplu, locul de muncă, de reședință sau de studiu).

1.5. Clientul care este persoană fizică nu poate utiliza reprezentantul în cursul relației de afaceri sau al tranzacției ocazionale cu societatea.

2. **Identificarea clientului - persoană juridică**

2.1. Societatea identifică clientul, care este o persoană juridică, și reprezentantul acestuia și păstrează următoarele date privind clientul:

- denumirea comercială sau numele (cu forma juridică);
- codul de înregistrare sau numărul de înregistrare și data înregistrării;
- numele administratorului (administratorilor) sau numele membrului (membrilor) consiliului de administrație sau al membrului (membrilor) unui alt organism echivalent, precum și autoritățile acestora în reprezentarea clientului;
- locația clientului, de la care trebuie să se pornească teoria țării de stabilire;
- locul de desfășurare a activității;
- detaliile telecomunicațiilor.

2.2. Următoarele documente emise de o autoritate sau un organism competent cu cel puțin șase luni înainte de utilizarea lor pot fi utilizate pentru identificarea clientului:

- fișa de înregistrare în registrul relevant; sau
- certificatul de înregistrare din registrul relevant; sau
- un document echivalent cu documentele menționate anterior sau documentele relevante de stabilire ale clientului.

2.3. Societatea verifică corectitudinea datelor clientului specificate mai sus, utilizând în acest scop informații provenind dintr-o sursă credibilă și independentă. În cazul în care Societatea are acces la registrul comerțului, la registrul asociațiilor non-profit și al fundațiilor sau la datele din registrele relevante dintr-o țară străină, prezentarea documentelor specificate mai sus nu trebuie să fie cerută Clientului.

2.4. Identitatea persoanei juridice și dreptul de reprezentare al persoanei juridice pot fi verificate pe baza unui document specificat mai sus, care a fost autentificat de un notar sau certificat

[3] De exemplu, faptul că datele colectate în cursul identificării sunt adevărate și corecte poate fi dovedit printr-o confirmare într-un format care poate fi reprodus în scris, primită de la o sursă credibilă și independentă, care afirmă că persoana locuiește (de exemplu, consumă utilități acolo, adică dovedește că persoana locuiește în acel loc), studiază sau lucrează (profesie sau domeniu de activitate) în locul pe care l-a declarat etc.

de un notar sau în mod oficial, sau pe baza altor informații provenind dintr-o sursă credibilă și independentă, inclusiv mijloace de identificare electronică și servicii de încredere pentru tranzacții electronice, folosind astfel cel puțin două surse diferite pentru verificarea datelor într-un astfel de caz.

2.5. În timpul verificării datelor dintr-o sursă credibilă și independentă obținute în timpul identificării persoanei juridice, **sursa a fost considerată credibilă și independentă** atunci când societatea:

- vede originalul documentului menționat mai sus;
- vede o copie a documentului specificat mai sus care a fost autentificată de un notar, certificată de un notar sau certificată oficial; sau
- are acces la datele din registrul comerțului, registrul asociațiilor non-profit și al fundațiilor sau la registrele relevante din țări străine prin intermediul unei rețele informatice.

2.6. **Două surse diferite** în timpul identificării unei persoane juridice înseamnă că suportul de date, locul sau măsura de obținere a informațiilor trebuie să fie diferite (adică nu poate fi același suport de date).

2.7. Reprezentantul persoanei juridice va fi identificat ca fiind clientul, care este o persoană fizică în conformitate cu prezenta politică. De asemenea, Societatea trebuie să identifice și să verifice natura și domeniul de aplicare al dreptului de reprezentare. Numele, data emiterii și numele emitentului documentului care servește drept bază pentru dreptul de reprezentare trebuie să fie stabilite și păstrate, cu excepția cazului în care dreptul de reprezentare a fost verificat utilizând informații provenind din registrul relevant (de exemplu, registrul comerțului, registrul asociațiilor și fundațiilor non-profit sau registrul relevant al unei țări străine).

2.8. Societatea trebuie să respecte condițiile dreptului de reprezentare acordat reprezentanților persoanei juridice și să furnizeze servicii numai în cadrul dreptului de reprezentare.

3. Identificarea beneficiarului real al clientului

3.1. Societatea trebuie să identifice beneficiarul real al clientului și să ia măsuri pentru a verifica identitatea beneficiarului real în măsura în care îi permite societății să se asigure că știe cine este beneficiarul real.

3.2. Societatea solicită clientului informații cu privire la beneficiarul efectiv al clientului (de exemplu, oferind clientului posibilitatea de a-și specifica beneficiarul efectiv în chestionarul KYC).

3.3. Societatea nu stabilește relația de afaceri dacă clientul, care este o persoană fizică, are un beneficiar efectiv care nu este aceeași persoană cu clientul.

3.4. Beneficiarul efectiv al unei persoane juridice este identificat în etape în care entitatea obligată trece la fiecare etapă ulterioară dacă beneficiarul efectiv al persoanei juridice nu poate fi determinat în cazul etapei anterioare. Etapele sunt după cum urmează:

- este posibil să se identifice, în ceea ce privește clientul care este o entitate juridică sau o persoană care participă la tranzacție, persoana sau persoanele fizice care controlează efectiv în ultimă instanță entitatea juridică sau exercită influență sau control asupra acesteia în orice alt mod, indiferent de numărul acțiunilor, drepturile de vot sau drepturile de proprietate sau de natura lor directă sau indirectă;

- dacă clientul care este o persoană juridică sau persoana care participă la tranzacție are o persoană fizică sau persoane fizice care dețin sau controlează persoana juridică prin intermediul unei participații directe[4] sau indirecte[5] . Conexiunile familiale și contractuale trebuie, de asemenea, să fie luate în considerare aici;

- care este persoana fizică din conducerea superioară[6] , care trebuie să fie definită ca beneficiar real, ca urmare a executării celor două etape anterioare, nu au permis entității obligate să identifice beneficiarul real.

3.5. În cazul în care documentele utilizate pentru identificarea persoanei juridice sau alte documente prezentate nu indică în mod direct cine este beneficiarul real al persoanei juridice, datele relevante (inclusiv datele privind apartenența la un grup și structura de proprietate și de conducere a grupului) sunt înregistrate pe baza declarației reprezentantului persoanei juridice sau a documentului scris de mână de către reprezentantul persoanei juridice.

3.6. Societatea aplică măsuri rezonabile pentru a verifica exactitatea informațiilor stabilite pe baza declarațiilor sau a unui document scris de mână (de exemplu, prin efectuarea de investigații în registrele relevante), solicitând prezentarea raportului anual al persoanei juridice sau a altui document relevant. În cazul în care societatea are îndoieli cu privire la exactitatea sau caracterul complet al informațiilor relevante, aceasta verifică informațiile furnizate din surse disponibile publicului și, dacă este necesar, solicită informații suplimentare de la client.

[4] Deținerea directă este o modalitate de exercitare a controlului prin care persoana fizică deține o participație de 25 % plus o acțiune sau un drept de proprietate de peste 25 % în societate

[5] Proprietatea indirectă este o modalitate de exercitare a controlului prin care o participație de 25 % plus o acțiune sau un drept de proprietate de peste 25 % în societate este deținută de o societate controlată de o persoană fizică sau de mai multe societăți controlate de aceeași persoană fizică.

[6] Un membru al conducerii superioare este o persoană care ia deciziile strategice care afectează în mod fundamental activitățile și/sau practicile de afaceri și/sau tendințele generale (de afaceri) ale societății sau care, în absența acesteia, 15.8.2. îndeplinește funcții de conducere zilnice sau obișnuite ale societății în cadrul sferei puterii executive [de exemplu, director executiv (CEO), director financiar (CFO), director sau președinte etc.].

3.7. În cazul în care societatea stabilește relații de afaceri cu clientul ale cărui informații privind beneficiarii efectivi trebuie, în conformitate cu statutul unui stat membru al Uniunii Europene, să fie transmise statului sau să fie înregistrate acolo, societatea obține un certificat de înregistrare relevant sau un extras de registru după identificarea beneficiarului efectiv al clientului.

3.8. Beneficiarul real nu trebuie să fie identificat în cazul clientului cotat pe o piață reglementată care face obiectul unor cerințe de publicare conforme cu legislația Uniunii Europene sau care face obiectul unor standarde internaționale echivalente care asigură o transparență adecvată a informațiilor privind proprietatea.

VI. IDENTIFICAREA PERSOANEI EXPUSE POLITIC

1. Societatea ia măsuri pentru a stabili dacă clientul, beneficiarul real al clientului sau reprezentantul acestui client este o PEP, un membru al familiei sale[7] sau un asociat apropiat[8] , sau dacă clientul a devenit o astfel de persoană.

2. Societatea solicită clientului informații pentru a identifica dacă clientul este o PEP, un membru al familiei sale sau un asociat apropiat (de exemplu, oferind clientului posibilitatea de a specifica informațiile relevante în chestionarul KYC).

3. Societatea verifică datele primite de la client prin efectuarea de cercetări în bazele de date relevante sau în bazele de date publice sau prin efectuarea de cercetări sau verificarea datelor pe site-urile web ale autorităților sau instituțiilor de supraveghere relevante din țara în care clientul are reședința sau sediul. PEP trebuie verificat suplimentar utilizând Google și motorul de căutare local din țara de origine a clientului, dacă există, prin introducerea numelui clientului atât în alfabetul latin, cât și în alfabetul local, împreună cu data nașterii clientului.

4. Cel puțin următoarele persoane sunt considerate a fi PEP:

   - șef de stat sau șef de guvern;
   - ministru, ministru adjunct sau ministru adjunct;
   - membru al unui organism legislativ;
   - membru al unui organ de conducere al unui partid politic;
   - judecător al celei mai înalte instanțe a unei țări;
   - auditorul general sau un membru al consiliului de supraveghere sau al consiliului executiv al unei bănci centrale;
   - cancelarul justiției;
   - ambasador, trimis sau însărcinat cu afaceri;
   - ofițer de rang înalt în forțele armate;
   - membru al unui organ administrativ, de conducere sau de supraveghere al unei întreprinderi de stat;

[7] Membru al familiei înseamnă soțul/soția sau o persoană considerată a fi echivalentă soțului/soției unei PEP; un copil și soțul/soția sau o persoană considerată a fi echivalentă soțului/soției unei PEP; un părinte al unei PEP

[8] Asociat apropiat înseamnă o persoană fizică despre care se știe că este beneficiarul efectiv sau coproprietar efectiv al unei persoane juridice sau al unei construcții juridice, sau care are orice alte relații de afaceri strânse cu o persoană expusă politic; și o persoană fizică care este singurul beneficiar efectiv al unei entități juridice sau al unei construcții juridice despre care se știe că a fost înființată în beneficiul de facto al unei persoane expuse politic

- director, director adjunct și membru al unui organ de conducere al unei organizații internaționale;
- persoana din lista funcțiilor din România ai căror titulari sunt considerați persoane expuse politic se stabilește prin regulament al ministrului de resort;
- persoană în lista posturilor, care este stabilită de organizația internațională acreditată în România;
- o persoană care, conform listei publicate de Comisia Europeană, este considerată ca îndeplinind funcții publice importante de către un stat membru al Uniunii Europene, Comisia Europeană sau o organizație internațională acreditată pe teritoriul Uniunii Europene este considerată persoană expusă politic.

5. Funcționarii de rang mediu sau mai tineri nu sunt considerați PEP.

6. Societatea identifică asociații apropiați și membrii de familie ai PEP numai dacă legătura lor cu PEP este cunoscută publicului sau dacă societatea are motive să creadă că există o astfel de legătură.

7. În cazul în care clientul care este o PEP nu mai îndeplinește funcții publice importante care îi revin, societatea ia în considerare, cel puțin în termen de 12 luni, riscurile care rămân legate de client și aplică măsuri relevante și bazate pe sensibilitatea la risc, atât timp cât este sigur că riscurile caracteristice PEP nu mai există în cazul clientului.

8. **Identificarea scopului și a naturii relației de afaceri sau a unei tranzacții**

8.1. Societatea trebuie să înțeleagă scopul și natura stabilirii relației de afaceri sau a efectuării tranzacției. În ceea ce privește serviciile furnizate, Societatea solicită Clientului cel puțin următoarele informații pentru a înțelege scopul și natura relației de afaceri sau a tranzacției:

- cifra de afaceri estimată a tranzacțiilor cu societatea pe an calendaristic;
- sursa estimată a fondurilor utilizate în relația de afaceri sau în tranzacție;
- în cazul în care relația de afaceri sau tranzacția este legată de desfășurarea de către client a activităților economice sau profesionale.

8.2. Societatea aplică măsuri suplimentare și colectează informații suplimentare pentru a identifica scopul și natura relației de afaceri sau a unei tranzacții ocazionale în cazurile în care:

- există o situație care se referă la o valoare ridicată sau este neobișnuită; și/sau

- în cazul în care riscul și/sau profilul de risc asociat cu clientul și natura relației de afaceri justifică efectuarea unor acțiuni suplimentare pentru a putea monitoriza în mod corespunzător relația de afaceri ulterior.

8.3. În cazul în care clientul este o persoană juridică, în plus față de cele menționate mai sus, societatea va identifica clientul:

- **domeniul de activitate**, în care societatea trebuie să înțeleagă cu ce se ocupă și intenționează să se ocupe clientul în cursul relației de afaceri și în ce măsură acest lucru corespunde scopului și naturii relației de afaceri în general și dacă este rezonabil, inteligibil și plauzibil;

- **metodele de plată**, inclusiv țările din care sunt primite plățile și în care sunt efectuate plățile, durata preconizată a relației de afaceri, amploarea și canalele de numerar, canalele de plată (sucursală, bancă pe internet, plăți cu cardul) etc;

- **principalii parteneri de afaceri**, unde societatea trebuie să identifice care sunt principalii parteneri ai clientului cu care vor fi încheiate tranzacții în domeniul de activitate declarat și cu volumele de activitate declarate.

8.4. Domeniul de activitate, metodele de plată și principalii parteneri de afaceri trebuie să se încadreze în profilul de experiență al reprezentantului clientului (sau al persoanelor-cheie) și/sau al beneficiarului efectiv. Astfel, societatea trebuie să identifice de unde provin capacitatea, priceperea, abilitățile și cunoștințele (experiența în general) reprezentantului și/sau ale beneficiarului efectiv pentru a opera în acest domeniu de activitate, cu aceste volume de afaceri și cu acești parteneri de afaceri principali.

9. Monitorizarea relației de afaceri

9.1. Societatea monitorizează relațiile de afaceri stabilite în cazul în care sunt puse în aplicare următoarele măsuri continue de due diligence (ODD):

- asigurarea faptului că documentele, datele sau informațiile colectate în cursul aplicării măsurilor de due diligence sunt actualizate periodic și în cazul unor evenimente declanșatoare, și anume, în principal, datele privind clientul, reprezentantul acestuia (inclusiv dreptul de reprezentare) și beneficiarul efectiv, precum și scopul și natura relației de afaceri;

- monitorizarea continuă a relației de afaceri, care acoperă tranzacțiile efectuate în cadrul relației de afaceri pentru a se asigura că tranzacțiile corespund cunoștințelor societății despre client, activitățile și profilul de risc al acestuia;

- identificarea sursei și originii fondurilor utilizate în tranzacție (tranzacții).

9.2. Societatea verifică și actualizează în mod regulat documentele, datele și informațiile colectate în cursul punerii în aplicare a măsurilor CDD. Regularitatea verificărilor trebuie să se bazeze pe profilul de risc al clientului și verificările trebuie să aibă loc cel puțin:

- o dată pe semestru pentru clientul cu profil de risc ridicat;
- o dată pe an pentru clientul cu profil de risc mediu;
- o dată la doi ani pentru clientul cu profil de risc scăzut.

9.3. Documentele, datele și informațiile colectate trebuie, de asemenea, verificate dacă a avut loc un eveniment care indică necesitatea de a actualiza documentele, datele și informațiile colectate.

9.4. În cursul monitorizării continue a relației de afaceri, societatea monitorizează tranzacțiile încheiate în timpul relației de afaceri astfel încât aceasta din urmă să poată determina dacă tranzacțiile care urmează să fie încheiate corespund informațiilor cunoscute anterior despre client (și anume, ceea ce clientul a declarat la stabilirea relației de afaceri sau ceea ce a devenit cunoscut în cursul relației de afaceri).

9.5. Societatea monitorizează, de asemenea, relația de afaceri pentru a stabili activitățile sau faptele clientului care indică activități infracționale, spălare de bani sau finanțare a terorismului sau a căror legătură cu spălarea de bani sau finanțarea terorismului este probabilă, inclusiv tranzacții complicate, de mare valoare și neobișnuite și modele de tranzacții care nu au niciun scop economic sau legitim rezonabil sau evident sau care nu sunt caracteristice caracteristicilor specifice ale activității în cauză. Pe parcursul relației de afaceri, societatea evaluează în permanență modificările intervenite în activitățile clientului și stabilește dacă aceste modificări pot crește nivelul de risc asociat clientului și relației de afaceri, determinând necesitatea de a aplica măsuri EDD.

9.6. În cursul monitorizării continue a relației de afaceri, societatea aplică următoarele măsuri:

- screening, adică monitorizarea tranzacțiilor în timp real;
- monitorizarea, adică analizarea ulterioară a tranzacțiilor.

9.7. Obiectivul screeningului este de a identifica:

- tranzacții suspecte și neobișnuite și modele de tranzacții;
- tranzacțiile care depășesc pragurile prevăzute;
- persoanele expuse politic și circumstanțele privind sancțiunile internaționale.

9.8. Societatea identifică sursa[9] și originea[10] fondurilor utilizate în tranzacție (tranzacții), dacă este necesar. Necesitatea de a identifica sursa și originea fondurilor depinde de activitățile anterioare ale Clientului, precum și de alte informații cunoscute. Prin urmare, identificarea sursei și originii fondurilor utilizate în tranzacție se efectuează în următoarele cazuri:

- tranzacțiile depășesc limitele stabilite de Societate;
- în cazul în care tranzacțiile nu corespund informațiilor cunoscute anterior despre client;
- dacă societatea dorește sau ar trebui să considere în mod rezonabil că este necesar să evalueze dacă tranzacțiile corespund informațiilor cunoscute anterior despre client;
- în cazul în care societatea suspectează că tranzacțiile indică activități infracționale, spălare de bani sau finanțare a terorismului sau că legătura dintre tranzacții și spălare de bani sau finanțare a terorismului este probabilă, inclusiv tranzacții complicate, de mare valoare și neobișnuite și modele de tranzacții care nu au niciun scop economic sau legitim rezonabil sau evident sau care nu sunt caracteristice caracteristicilor specifice ale activității în cauză.

[9] Sursa fondurilor utilizate în tranzacție este motivul, explicația și baza (raportul juridic și conținutul acestuia) pentru care au fost transferate fondurile

[10] Originea fondurilor utilizate în tranzacție este activitatea prin care fondurile au fost câștigate sau primite

VII. PUNEREA ÎN APLICARE A SANCȚIUNILOR

1. La intrarea în vigoare, modificarea sau încetarea sancțiunilor, societatea verifică dacă clientul sau o persoană care intenționează să aibă o relație de afaceri sau o tranzacție cu acesta face obiectul sancțiunilor. În cazul în care societatea identifică o persoană care face obiectul sancțiunilor sau că tranzacția prevăzută sau efectuată de aceasta încalcă sancțiunile, societatea aplică sancțiunile și informează imediat DNA cu privire la aceasta.

2. **Procedura de identificare a subiectului sancțiunilor și a unei tranzacții care încalcă sancțiunile**

2.1. Societatea va utiliza cel puțin una dintre următoarele surse (baze de date) pentru a verifica relația clientului cu sancțiunile:

- Informații și căutare privind sancțiunile financiare;
- Alte baze de date interne sau baze de date gestionate de terți, care conțin cel puțin listele din bazele de date specificate mai sus.

2.2. În plus față de sursele menționate mai sus, societatea poate utiliza orice alte surse la decizia angajatului care aplică măsurile CDD.

2.3. Pentru a verifica dacă numele persoanelor rezultate în urma anchetei sunt aceleași cu persoanele enumerate într-o notificare care conține sancțiunea (sancțiunile), se utilizează datele personale ale acestora, ale căror caracteristici principale sunt, pentru o persoană juridică, denumirea sau marca sa, codul de înregistrare sau data înregistrării, iar pentru o persoană fizică, numele și datele de identificare personală sau data nașterii.

2.4. Pentru a stabili identitatea persoanelor specificate în actul juridic relevant sau în notificare ca fiind aceleași cu cele identificate ca urmare a interogării din bazele de date, societatea trebuie să analizeze numele persoanelor găsite ca urmare a interogării pe baza efectului posibil al factorilor de denaturare a datelor cu caracter personal (de exemplu, transcrierea numelor străine, ordinea diferită a cuvintelor, înlocuirea diacriticelor sau a literelor duble etc.).

2.5. Societatea efectuează verificările menționate anterior în mod continuu în cursul unei relații de afaceri stabilite. Frecvența verificărilor continue depinde de profilul de risc al clientului:

- o dată pe săptămână pentru clientul cu profil de risc ridicat;
- o dată pe lună pentru clientul cu profil de risc mediu;
- o dată pe trimestru pentru clientul cu profil de risc scăzut.

2.6. În cazul în care angajatul are îndoieli cu privire la faptul că o persoană face obiectul unor sancțiuni, acesta notifică imediat conducerea societății, care decide dacă solicită sau obține

date suplimentare de la persoana respectivă sau notifică imediat DNA cu privire la suspiciunea sa.

2.7. Societatea dobândește în primul rând informații suplimentare pe cont propriu cu privire la persoana care se află în relație de afaceri sau efectuează o tranzacție cu aceasta, precum și cu privire la persoana care intenționează să stabilească relația de afaceri, să efectueze o tranzacție sau un act cu aceasta, preferând informațiile dintr-o sursă credibilă și independentă. Dacă, din anumite motive, astfel de informații nu sunt disponibile, societatea întreabă persoana care se află în relație de afaceri sau care efectuează o tranzacție sau un act cu aceasta, precum și persoana care intenționează să stabilească o relație de afaceri, să efectueze o tranzacție sau un act cu aceasta, dacă informațiile provin dintr-o sursă credibilă și independentă și evaluează răspunsul.

3. Acțiuni la identificarea subiectului sancțiunilor sau a unei tranzacții care încalcă sancțiunile

3.1. În cazul în care angajatul societății constată că clientul care se află în relație de afaceri sau efectuează o tranzacție cu societatea, precum și o persoană care intenționează să stabilească relația de afaceri sau să efectueze o tranzacție cu societatea, face obiectul unor sancțiuni, angajatul notifică imediat conducerea societății cu privire la identificarea subiectului sancțiunilor, la îndoiala acestuia și la măsurile luate.

3.2. Conducerea societății refuză să încheie o tranzacție sau o procedură, ia măsurile prevăzute în actul privind impunerea sau punerea în aplicare a sancțiunilor și notifică imediat DNA cu privire la îndoielile sale și la măsurile luate.

3.3. La identificarea subiectului sancțiunilor, este necesar să se identifice măsurile care sunt luate pentru sancționarea acestei persoane. Aceste măsuri sunt descrise în actul juridic de punere în aplicare a sancțiunilor, prin urmare, este necesar să se identifice sancțiunea exactă care este pusă în aplicare împotriva persoanei pentru a asigura aplicarea legală și corectă a măsurilor.

VIII. REFUZUL TRANZACȚIEI SAU AL RELAȚIEI DE AFACERI ȘI ÎNCETAREA ACESTORA

1. Companiei îi este interzis să stabilească relații de afaceri, iar relația de afaceri sau tranzacția stabilită va fi reziliată în cazul în care:

   - societatea suspectează spălare de bani sau finanțare a terorismului;
   - este imposibil pentru societate să aplice măsurile CDD, deoarece clientul nu transmite datele relevante sau refuză să le transmită sau datele transmise nu oferă motive de asigurare că datele colectate sunt adecvate;
   - clientul al cărui capital constă în acțiuni la purtător sau alte titluri la purtător dorește să stabilească relația de afaceri;
   - clientul, care este o persoană fizică în spatele căreia se află o altă persoană care beneficiază efectiv de avantaje, dorește să stabilească o relație de afaceri (suspiciunea că este folosită o persoană care acționează ca paravan);
   - profilul de risc al clientului a devenit inadecvat cu nivelul de risc asumat de societate(adică nivelul profilului de risc al clientului este "interzis").

2. Cele de mai sus nu se aplică în cazul în care societatea a notificat DNA cu privire la stabilirea relației de afaceri, tranzacție sau tentativă de tranzacție în conformitate cu procedura prevăzută mai jos și a primit de la DNA o instrucțiune specifică de a continua relația de afaceri, stabilirea relației de afaceri sau tranzacția.

3. În cazul încetării relației de afaceri în conformitate cu prezentul capitol, societatea transferă activele clientului într-un termen rezonabil, dar preferabil nu mai târziu de o lună de la încetare.

IX. OBLIGAȚIA DE RAPORTARE

1. Conducerea Societății trebuie să raporteze DNA cu privire la activitatea sau circumstanțele pe care le identifică în cursul activităților economice și prin care:

   - caracteristicile indică utilizarea veniturilor provenite din infracțiuni sau săvârșirea de infracțiuni legate de acestea (este vorba în primul rând de un raport privind o tranzacție sau o activitate suspectă și neobișnuită, adică UTR sau UAR);

   - în cazul cărora suspectează sau cunosc sau ale căror caracteristici indică săvârșirea de infracțiuni de spălare a banilor sau infracțiuni conexe (este vorba, în primul rând, de un raport privind o tranzacție sau o activitate în cadrul căreia se suspectează spălarea banilor, și anume un STR sau SAR);

   - în cazul cărora suspectează sau cunosc sau ale căror caracteristici indică comiterea unei finanțări a terorismului sau a unor infracțiuni conexe (este vorba, în primul rând, de un raport privind o tranzacție sau o activitate în care se suspectează finanțarea terorismului, adică TFR);

   - în cazul în care este prezentă o tentativă de activitate sau circumstanțele specificate în clauzele anterioare.

2. Caracteristicile minime ale tranzacțiilor suspecte și neobișnuite sunt prevăzute în orientările elaborate de DNA (una dintre anexele la prezenta politică).

3. Conducerea societății trebuie să raporteze DNA:

   - cu privire la circumstanțele refuzului de stabilire a relației de afaceri și cu privire la încetarea relației de afaceri pe baza circumstanțelor prevăzute în capitolul anterior (în primul rând un raport privind tranzacțiile sau activitățile suspecte și neobișnuite, și anume UAR);

   - cu privire la fiecare tranzacție care a devenit cunoscută prin care o obligație pecuniară de peste 15 000 de euro sau o sumă egală în altă monedă este executată în numerar, indiferent dacă tranzacția este efectuată printr-o singură plată sau în mai multe plăți legate între ele pe o perioadă de până la un an (o raportare bazată pe sumă, CTR);

   - cu privire la identificarea subiectului sancțiunilor și la punerea în aplicare a sancțiunilor sau la suspiciunea acestora (raport internațional privind sancțiunile, ISR).

4. Rapoartele specificate mai sus trebuie întocmite înainte de încheierea tranzacției în cazul în care societatea suspectează sau știe că se comit infracțiuni de spălare de bani sau de finanțare a terorismului sau infracțiuni conexe și în cazul în care aceste circumstanțe sunt

identificate înainte de încheierea tranzacției. În cazul în care amânarea tranzacției poate cauza un prejudiciu considerabil, nu este posibilă omiterea tranzacției sau poate împiedica capturarea persoanei care a comis posibila spălare de bani sau finanțare a terorismului, tranzacția va fi încheiată și ulterior va fi înaintat un raport DNA. Societatea este în contact cu Serviciul Român de Investigare a Criminalității Financiare pentru a identifica astfel de circumstanțe.

5. În cazul în care apare necesitatea raportului menționat mai sus, angajatul căruia i s-a adus la cunoștință această necesitate trebuie să informeze imediat conducerea societății cu privire la aceasta.

6. În orice caz (și anume, și în situația în care o activitate sau o împrejurare este identificată după finalizarea tranzacției), obligația de raportare trebuie îndeplinită imediat, dar nu mai târziu de două zile lucrătoare de la identificarea activității sau a împrejurării sau de la apariția suspiciunii reale (și anume, situația în care suspiciunea nu poate fi înlăturată).

7. Raportul este trimis în conformitate cu regulamentele emise de DNA (una dintre anexele la prezenta politică).

8. Societății, unei unități structurale a Societății și angajatului îi este interzis să informeze o persoană, beneficiarul real al acesteia, reprezentantul sau un terț cu privire la un raport depus la DNA, la un plan de depunere a unui astfel de raport sau la apariția raportului, precum și cu privire la un precept emis de DNA sau la începerea procedurilor penale.

X. OBLIGAȚIA DE FORMARE

1. Societatea se asigură că angajații săi, contractanții săi și alte persoane care participă la activitate în mod similar și care îndeplinesc sarcini de lucru care sunt importante pentru prevenirea utilizării activității în scopul spălării banilor sau finanțării terorismului ("persoane relevante") au calificările relevante pentru aceste sarcini de lucru. Atunci când o persoană relevantă este recrutată sau angajată, calificările acesteia sunt verificate ca parte a procesului de recrutare/numire, prin efectuarea de verificări ale antecedentelor care cuprind extrase din cazierul judiciar, pe lângă obținerea obișnuită de referințe, care sunt documentate utilizând un formular standard special de evaluare a aptitudinilor angajaților.

2. În conformitate cu cerințele aplicabile societății cu privire la asigurarea adecvării persoanelor relevante, societatea se asigură că aceste persoane primesc în permanență o formare și informații adecvate pentru a putea îndeplini obligațiile societății în conformitate cu legislația aplicabilă. Prin intermediul formării, se asigură că aceste persoane au cunoștințe în domeniul AML/CFT într-o măsură adecvată, având în vedere sarcinile și funcția persoanei respective. Formarea trebuie să ofere, în primul rând, informații cu privire la cele mai actuale metode de spălare a banilor și de finanțare a terorismului și la riscurile care decurg din acestea.

3. Această formare se referă la părțile relevante din conținutul normelor și reglementărilor aplicabile, la evaluarea riscurilor societății, la politica și procedurile societății și la informațiile care ar trebui să faciliteze acestor persoane relevante detectarea suspiciunilor de spălare a banilor și finanțare a terorismului. Formarea este structurată pe baza riscurilor identificate prin intermediul politicii de evaluare a riscurilor.

4. Conținutul și frecvența formării sunt adaptate la sarcinile și funcția persoanei în ceea ce privește aspectele legate de măsurile de combatere a spălării banilor și a finanțării terorismului. În cazul în care politica este actualizată sau modificată în vreun fel, conținutul și frecvența formării sunt ajustate în mod corespunzător.

5. Pentru noii angajați, formarea cuprinde o revizuire a conținutului normelor și reglementărilor aplicabile, a politicii de evaluare a riscurilor a societății, a prezentei politici și a altor proceduri relevante.

6. Angajații și personalul de conducere al societății beneficiază de formare continuă în conformitate cu următorul plan de formare:

   - periodicitate: cel puțin o dată pe an;
   - domeniu de aplicare: revizuirea normelor și reglementărilor aplicabile, a politicii societății și a altor proceduri relevante. Informații specifice referitoare la caracteristicile noi/actualizate din normele și reglementările aplicabile. Raport și schimb de experiență cu privire la tranzacțiile revizuite de la formarea anterioară.

7. În plus față de cele de mai sus, persoanele relevante sunt informate permanent cu privire la noile tendințe, modele și metode și primesc alte informații relevante pentru prevenirea spălării banilor și a finanțării terorismului.

8. Formarea organizată trebuie documentată electronic și confirmată cu semnătura persoanei relevante. Această documentație trebuie să includă conținutul formării, numele participanților și data formării.

XI. COLECTAREA ȘI CONSERVAREA DATELOR

1. Societatea înregistrează și păstrează informațiile sau documentele relevante prin intermediul persoanei care le primește prima:

   - toate datele colectate în cadrul implementării măsurilor CDD;
   - informații cu privire la circumstanțele refuzului de stabilire a relației de afaceri de către societate;
   - circumstanțele refuzului de a stabili o relație de afaceri la inițiativa clientului, în cazul în care refuzul este legat de aplicarea măsurilor CDD de către societate;
   - informații privind toate operațiunile efectuate pentru a identifica persoana care participă la tranzacție sau beneficiarul efectiv al clientului;
   - informații în cazul în care este imposibil să se ia măsuri CDD utilizând mijloace informatice;
   - informații privind circumstanțele încetării relației de afaceri în legătură cu imposibilitatea aplicării măsurilor CDD
   - data sau perioada fiecărei tranzacții și o descriere a conținutului tranzacției;
   - informații care servesc drept bază pentru obligațiile de raportare specificate mai sus;
   - date privind tranzacții sau situații suspecte sau neobișnuite despre care Direcția Națională Anticorupție nu a fost informată.

2. În plus față de informațiile menționate anterior, societatea înregistrează următoarele date privind o tranzacție: suma tranzacției, moneda și numărul de cont.

3. Datele specificate mai sus trebuie păstrate timp de 5 ani după încetarea relației de afaceri sau a tranzacției de finalizare. Datele legate de îndeplinirea obligației de raportare trebuie păstrate timp de 5 ani după îndeplinirea obligației de raportare.

4. Documentele și datele trebuie păstrate într-un mod care să permită un răspuns exhaustiv și imediat la întrebările adresate de DNA sau, în conformitate cu legislația, de alte autorități de supraveghere, autorități de anchetă sau instanță.

5. Societatea pune în aplicare toate normele de protecție a datelor cu caracter personal prin aplicarea cerințelor care decurg din legislația aplicabilă. Societății i se permite să prelucreze datele cu caracter personal colectate la punerea în aplicare a CDD numai în scopul prevenirii spălării banilor și finanțării terorismului, iar datele nu trebuie prelucrate suplimentar într-un mod care nu corespunde scopului, de exemplu, în scopuri de marketing.

6. Societatea șterge datele păstrate după expirarea perioadei de timp, cu excepția cazului în care legislația care reglementează domeniul relevant stabilește o procedură diferită. Pe baza unui precept al autorității de supraveghere competente, datele importante pentru prevenirea, detectarea sau investigarea spălării banilor sau finanțării terorismului pot fi păstrate pentru o perioadă mai lungă, dar nu mai mult de cinci ani de la expirarea primei perioade de timp.

XII. EVITAREA CONFLICTULUI DE INTERESE

1. Angajații trebuie să evite conflictul de interese și, atunci când acest lucru se întâmplă, să informeze imediat conducerea companiei.

2. Conflictul de interese este înțeles ca fiind toate circumstanțele cunoscute de societate sau de angajații săi care pot afecta deciziile de efectuare a unei tranzacții sau de stabilire a unei relații de afaceri și care nu corespund intereselor societății sau ale clientului său.

3. Pentru a atinge obiectivul de evitare a conflictului de interese, societatea colectează și actualizează periodic datele angajaților săi pentru a identifica interesele acestora în contextul prevenirii spălării banilor și finanțării terorismului. Societatea colectează următoarele date cu privire la fiecare angajat:

   - locul de naștere și locul de reședință al angajatului;
   - alte poziții și contracte de muncă ale angajatului pe care acesta le are în contextul domeniului economic;
   - datele privind rudele apropiate ale angajatului (soț/soție, părinți, copii, frați/soții și copiii acestora): pentru fiecare persoană, locul de reședință și locul de muncă;
   - alte date cunoscute de angajat care pot indica interesele în contextul prevenirii spălării banilor și finanțării terorismului.

4. Omisiunea angajatului de a furniza datele specificate mai sus este considerată a fi o încălcare semnificativă a contractului de muncă și poate duce la încetarea contractului de muncă pentru motive imputabile angajatului.

5. Societatea identifică și analizează, printre altele, dacă persoanele care direcționează clienții către societate (de exemplu, agenți, revânzători etc.) au interese în ceea ce privește clientul (de exemplu, le furnizează servicii juridice, servicii de contabilitate, servicii de înființare de societăți și alte structuri juridice etc.) care cauzează conflictul de interese între persoana care direcționează clienții către societate și client.

6. În cazul identificării unui conflict de interese sau a unor circumstanțe care indică un conflict de interese, societatea aplică toate măsurile necesare pentru a-l preveni. În cazul în care este imposibil să se prevină conflictul de interese, societatea nu trebuie să încheie nicio tranzacție sau să stabilească relații de afaceri.

7. Conducerea societății este responsabilă pentru evitarea conflictelor de interese în cadrul societății.

XIII. CONTROLUL INTERN AL DE PUNERE ÎN APLICARE A POLITICII

1. Punerea în aplicare a prezentei politici este controlată intern de către conducerea societății.

2. Conducerea societății este responsabilă de exercitarea controlului asupra îndeplinirii corespunzătoare a cerințelor stabilite în prezenta politică, inclusiv de îndeplinirea funcției de control intern. Din acest motiv, conducerea societății trebuie:

   - analizează rezultatele controlului intern efectuat;
   - să pună în aplicare acțiuni pentru a elimina deficiențele apărute.