



**SERVICIUL  
PREVENIREA ȘI COMBATEREA  
SPĂLĂRII BANILOR**



MD-2004, mun. Chișinău, bd. Ștefan cel Mare și Sfânt 198, www.spcsb.md, office@spcsb.gov.md Tel. (+373) 22-257-243

**ORDIN**

**23.08.2018**

**nr. 33**

***Cu privire la aprobarea Regulamentului  
privind măsurile de prevenire și combatere  
a spălării banilor și finanțării terorismului  
pentru entitățile raportoare prevăzute de art.4 alin.(1) lit.h)  
din Legea nr.308 din 22.12.2017 cu privire la  
prevenirea și combaterea spălării banilor și finanțării terorismului***

În temeiul art.15 din Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr.58-66, art.132),

**ORDON:**

**1.** Se aprobă Regulamentul privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului pe pentru entitățile raportoare prevăzute de art.4 alin.(1) lit.h) din Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, conform anexei.

**2.** Interacțiunea cu entitățile raportoare și controlul asupra executării prezentului ordin îl exercită Serviciul supraveghere și conformitate din cadrul Serviciului Prevenirea și Combaterea Spălării Banilor.

**3.** Prezentul Ordin intră în vigoare la 23 august 2018.

**Director**

**Vasile ȘARCO**

**REGULAMENT**  
**privind măsurile de prevenire și combatere a spălării banilor**  
**și finanțării terorismului pentru entitățile raportoare prevăzute de art.4 alin.(1) lit.h)**  
**din Legea nr.308 din 22.12.2017 cu privire la**  
**prevenirea și combaterea spălării banilor și finanțării terorismului**

**Capitolul I**  
**DISPOZIȚII GENERALE**

**1.** Presentul regulament privind măsurile de prevenire și combatere a spălării banilor (în continuare – Regulament) se aplică entităților raportoare prevăzute de art.4 alin.(1) lit.h) din Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. Regulamentul stabilește cerințele privind: identificarea și evaluarea riscurilor de spălarea banilor și finanțarea terorismului; elaborarea politicilor și procedurilor interne; aplicarea cerințelor de precauție privind clienții, inclusiv a măsurilor de precauție simplificată și sporită; păstrarea datelor; raportarea activităților și tranzacțiilor suspecte; implementarea sancțiunilor financiare aferente activităților teroriste și de proliferare a armelor de distrugere în masă; organizarea și realizarea elementelor aferente sistemului de control intern; precum și alte cerințe în vederea minimizării riscurilor aferente spălării banilor și finanțării terorismului.

**2.** Entitatea raportoare va întreprinde măsurile ce se impun, în conformitate cu legislația, în activitatea sa de prevenire și combatere a spălării banilor și finanțării terorismului.

**3.** Termenii și expresiile utilizate în prezentul Regulament au semnificațiile prevăzute în Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea nr. 59 din 28.04.2005 cu privire la leasing și actele normative ale Serviciului Prevenirea și Combaterea Spălării Banilor.

**Capitolul II**  
**RESPONSABILITĂȚI**

**4.** Entitatea raportoare va desemna persoana/persoanele învestite cu atribuții de executare a Legii nr. 308/2017 și, potrivit cerințelor legislației, va comunica Serviciului Prevenirea și Combaterea Spălării Banilor, numele acestora împreună cu natura și limitele responsabilităților.

**5.** Entitatea raportoare dispune de sistem de control intern adecvat pentru a identifica, evalua, monitoriza și înțelege riscurile de spălarea banilor și finanțarea terorismului. Entitatea raportoare întreprinde măsurile necesare, implicând resurse suficiente, pentru a minimiza riscurile identificate.

**6.** Administratorul entității raportoare este responsabil pentru elaborarea, aprobarea și asigurarea aplicării unui program propriu adecvat privind prevenirea și combaterea spălării banilor și finanțării terorismului, de care depinde prevenirea și depistarea la timp a operațiunilor suspecte. Dispunerea de un astfel de program constituie mijlocul cel mai eficient prin care o entitate raportoare poate să se protejeze contra implicării în tranzacții ce pot facilita activități ilicite, precum și să asigure respectarea normelor aplicabile de raportare a activităților suspecte.

**7.** Entitatea raportoare este responsabilă de conformarea activității acesteia prevederilor legislației în vigoare în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

**8.** Entitatea raportoare întreprinde măsuri de identificare, evaluare și minimizare a riscurilor în vederea prevenirii utilizării sau implicării entității raportoare în tranzacții de spălarea a banilor și finanțarea a terorismului.

### **Capitolul III**

## **CERINȚE FAȚĂ DE PROGRAMUL INTERN PRIVIND PREVENIREA ȘI COMBATerea SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI**

**9.** Programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului reprezintă politici, proceduri și alte reguli, inclusiv reguli de cunoaștere a clientului care previn utilizarea entității raportoare în scopul spălării banilor sau finanțării terorismului, în mod intenționat sau nu, de către elementele criminale. Acest program trebuie să asigure efectuarea operațiunilor într-un mod sigur și prudent.

**10.** Entitatea raportoare elaborează programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului în conformitate cu prevederile Legii nr. 308 din 22.12.2017, prezentului Regulament, altor acte normative ale Serviciului Prevenirea și Combaterea Spălării Banilor, precum și ale altor organe cu funcții de supraveghere, ținând cont de practica general acceptată în acest domeniu, inclusiv documentele Grupului de Acțiune Financiară Internațională (FATF).

**11.** La elaborarea programului intern se iau în considerație mărimea, complexitatea, natura și volumul activităților entității raportoare, tipurile (categoriile) de clienți, gradul (nivelul) de risc asociat cu diferiți clienți sau categoriile acestora și operațiunile desfășurate de aceștia.

**12.** Programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului va prevedea, fără a se limita la următoarele:

1) obligațiile administratorului responsabil al entității raportoare, care trebuie să includă cel puțin:

a) cunoașterea și identificarea criteriilor (indicilor) clienților cu grad de risc sporit;  
b) aprobarea operațiunilor semnificative ale clienților cu grad de risc sporit;  
c) determinarea domeniilor de activitate ale entității raportoare vulnerabile riscului spălării banilor și finanțării terorismului. Domeniile de activitate vulnerabile riscului spălării banilor și finanțării terorismului pot fi acelea care au tangență cu: produsele și serviciile acordate, operațiunile efectuate de către clienți etc.;

d) remedierea deficiențelor identificate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, inclusiv raportarea tranzacțiilor suspecte către Serviciul Prevenirea și Combaterea Spălării Banilor;

e) punerea în aplicare a programului intern privind prevenirea și combaterea spălării banilor și finanțării terorismului, inclusiv determinarea responsabilităților personalului la diferite nivele ierarhice;

f) desemnarea persoanelor investite cu atribuții de executare a Legii nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

g) determinarea responsabilităților personalului la diferite nivele ierarhice;

h) punerea în aplicare a procedurilor interne privind accesul într-un timp rezonabil al personalului responsabil la informația necesară exercitării obligațiilor de serviciu;

2) proceduri de acceptare a clienților care stabilesc cel puțin categoriile de clienți pe care entitatea raportoare își propune să-i atragă și nivelul ierarhic al personalului care aprobă începerea relației de afaceri cu aceștia, în funcție de gradul de risc asociat, tipurile de produse și servicii care le sînt furnizate;

3) măsuri de identificare, verificare și monitorizare a clienților și beneficiarilor efectivi în funcție de gradul de risc asociat (regulile de cunoaștere a clientului), criteriile și modul de trecere a clienților dintr-o categorie cu un grad de risc în alta;

4) proceduri privind măsurile de precauție privind clienții, inclusiv măsurile de precauție simplificate și sporite pentru fiecare dintre categoriile de clienți, produse, servicii sau operațiuni supuse acestor măsuri;

5) proceduri de monitorizare a operațiunilor efectuate de clienți în scopul depistării operațiunilor semnificative, complexe și neordinare, fără un scop legal sau economic clar, a activităților și operațiunilor suspecte;

6) măsuri de identificare și monitorizare a clienților și operațiunilor efectuate de clienți cu țările/zonile ce nu dispun de norme contra spălării banilor și finanțării terorismului ori dispun de norme inadecvate în acest sens, ori reprezintă un risc sporit datorită nivelului înalt de infraționalitate și de corupție și/sau sînt implicate în activități teroriste;

- 7) modul de întocmire și păstrare a informațiilor, precum și de stabilire a accesului la acestea;
  - 8) proceduri de raportare internă și către autoritățile competente privind activitățile și operațiunile suspecte;
  - 9) proceduri și măsuri de verificare a modului de conformare la normele elaborate și de evaluare a eficienței acestora;
  - 10) standarde pentru selectare, angajare a personalului și programe de instruire a acestuia în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;
  - 11) proceduri privind identificarea și analiza riscurilor de spălare a banilor și finanțare a terorismului, inclusiv măsurile de minimizare a acestora, legate de utilizarea tehnologiilor informaționale, inclusiv cele noi, procurate sau elaborate în cadrul produselor și serviciilor oferite de entitatea raportoare.
- 13.** Entitatea raportoare revizuieste (actualizează), ori de câte ori este necesar, programul intern privind prevenirea și combaterea spălării banilor și finanțării terorismului, dar cel puțin anual, ținând cont de prevederile legislației în vigoare.

#### **Capitolul IV**

### **EVALUAREA RISCURILOR DE SPĂLAREA BANILOR ȘI FINANȚAREA TERORISMULUI. ABORDAREA BAZATĂ PE RISC**

**14.** Entitatea raportoare este obligată să întreprindă acțiuni privind identificarea și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului în activitatea sa, ținând cont de evaluarea riscurilor de spălare a banilor și de finanțare a terorismului la nivel național, regional, precum și de criteriile și factorii stabiliți de Serviciul Prevenirea și Combaterea Spălării Banilor. Rezultatele evaluării în domeniul propriu de activitate a riscurilor de spălare a banilor și de finanțare a terorismului se aprobă și se actualizează periodic, responsabil de acest proces fiind administratorul responsabil al entității raportoare, iar la cerere se prezintă Serviciului Prevenirea și Combaterea Spălării Banilor.

**15.** Entitatea raportoare, în urma rezultatelor evaluării riscurilor de spălare a banilor și de finanțare a terorismului, utilizează abordarea bazată pe risc pentru ca acțiunile de prevenire și diminuare a spălării banilor și finanțării terorismului să fie proporționale cu riscurile de spălare a banilor și de finanțare a terorismului identificate în domeniul de activitate.

**16.** Entitatea raportoare, efectuează și actualizează, cel puțin o dată la 3 ani și la necesitate, atunci când se schimbă circumstanțele lor sau apar noi amenințări relevante, evaluarea riscurilor de spălare a banilor și finanțarea terorismului, proces care presupune cel puțin:

- a) elaborarea unui raport scris, aprobat de către conducerea entității raportoare prin care se determină țările sau zonele geografice, produsele, clienții și operațiunile cu grad de risc sporit, ponderea și impactul acestora asupra activității sale;
- b) întocmirea unui plan de acțiuni în scopul minimizării riscurilor de spălare a banilor și finanțarea terorismului identificate;

**17.** Entitatea raportoare identifică și evaluează riscurile de spălare a banilor și finanțarea terorismului pînă la:

- a) lansarea și dezvoltarea de produse și servicii noi;
- b) utilizarea tehnologiilor noi sau aflate în dezvoltare, atît pentru produsele și serviciile noi, cît și pentru cele existente.

**18.** În procesul de evaluare a riscurilor de spălare a banilor și de finanțare a terorismului, entitatea raportoare utilizează diverse surse de informații pentru a identifica, gestiona și diminua riscurile aferente domeniului său de activitate. Aceasta include luarea în considerare a tipologiilor, a indicatorilor de risc, a ghidurilor și/sau recomandărilor emise de autoritățile competente naționale și internaționale. În identificarea și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului la care poate fi expus, entitatea raportoare trebuie să ia în considerare o gamă de factori care pot include:

- natura, amploarea, diversitatea și complexitatea afacerii;
- proporția clienților deja identificați ca având un risc ridicat;
- jurisdicțiile cu care entitatea raportoare face operațiuni, în special, jurisdicțiile cu o vulnerabilitate mare datorată unor factori de risc contextuali și diferiți, precum predominarea criminalității, corupția, finanțarea terorismului, precum și nivelul general al aplicarea legii, controlul,

reglementarea și supravegherea domeniului de prevenire și combatere a spălării banilor și finanțării terorismului;

- auditul intern și reglementările interne;  
- volumul și mărimea tranzacțiilor entității raportoare, luând în considerare activitatea obișnuită a acestuia și profilul clienților săi.

19. Entitatea raportoare, atunci când este cazul, poate coopera la nivel sectorial sau național pentru realizarea evaluării de risc proprie.

## **Capitolul V MĂSURI DE PRECAUȚIE PRIVIND CLIENȚII**

### **Secțiunea a 1-a Proceduri de acceptare a clientului**

20. Procedura inițială de acceptare a clientului cuprinde identificarea și verificarea clientului și, dacă este cazul, a beneficiarului efectiv al clientului pe baza unor informații, date sau documente fiabile și independente. Aceasta include, de asemenea, înțelegerea scopului și naturii relației de afaceri (acolo unde este relevant) și, în situații de risc sporit, obținerea de informații suplimentare privind sursa banilor și a proprietăților.

21. Procedurile de acceptare a clientului vor include mai multe etape în funcție de gradul de risc al clienților, punând accentul pe clienții cu venituri înalte ale căror sursă este neclară. Deciziile de începere, continuare sau încetare a relațiilor de afaceri cu clienții cu un grad de risc sporit sunt luate de către administratorul entității raportoare responsabil de implementarea și conformarea cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.

22. Entitatea raportoare nu va intra în relații de afaceri și nu va continua relațiile existente cu clienții și/sau beneficiarii efectivi care sunt subiecți ale sancțiunilor sau altor măsuri restrictive de către organizațiile internaționale și alte autorități recunoscute la nivel internațional ce impun sancțiuni țintite asupra indivizilor implicați în acțiuni de spălarea banilor, finanțarea terorismului și proliferarea armelor de distrugere în masă (de exemplu, Organizația Națiunilor Unite, Uniunea Europeană, etc.).

23. Procedurile de acceptare a clientului nu trebuie să afecteze accesul publicului larg la serviciile entității raportoare.

### **Secțiunea a 2-a Măsuri de identificare a clientului și beneficiarului efectiv**

24. Entitatea raportoare aplică măsuri de identificare a clienților, precum și a beneficiarilor efectivi:

- a) până la stabilirea relațiilor de afaceri;
- b) la efectuarea tuturor tranzacțiilor ocazionale, inclusiv cu utilizarea mijloacelor electronice, în valoarea de peste 20 de mii de lei, precum și dacă tranzacțiile se efectuează prin una sau mai multe operațiuni care au legături între ele, în valoare de peste 300 mii lei;
- c) dacă există o suspiciune de spălare a banilor sau de finanțare a terorismului, indiferent de orice excepții, scutiri sau limite stabilite;
- d) dacă există îndoieli cu privire la veridicitatea și precizia datelor de identificare obținute.

25. Măsurile de identificare a clienților sunt următoarele:

- 1) pentru clienții - persoane fizice, entitatea raportoare obține cel puțin următoarele informații:
  - a) numele și prenumele;
  - b) data și locul nașterii;
  - c) cetățenia și datele documentului de identitate (IDNP, seria și numărul, data eliberării, codul organului care l-a eliberat (dacă există) sau alți indici unici dintr-un act de identitate ce conține fotografia titularului);
  - d) adresa de domiciliu și/sau reședință;
  - e) ocupația, funcția publică deținută și/sau denumirea/numele angajatorului;
  - f) scopul și natura relației de afaceri cu entitatea raportoare;
  - g) numărul de telefon, fax, adresa poștei electronice (e-mail) (dacă există);

h) statutul de rezident/nerezident.

2) pentru clienții - persoane juridice (inclusiv persoanele fizice întreprinzători individuali sau care practică alt tip de activitate și persoanele juridice care gestionează bunurile aflate sub administrare fiduciară), entitatea raportoare obține cel puțin următoarele informații:

a) denumirea, forma legală, statutul;

b) sediul/adresa de activitate;

c) numărul de identificare de stat (IDNO), conform certificatului de înregistrare și/sau extrasului din Registrul de stat eliberat de către organul abilitat cu dreptul de a efectua înregistrarea de stat;

d) adresa de corespondență, altă decât sediul (dacă există);

e) identitatea persoanei fizice împuternicită de a gestiona contul și care exercită control prin intermediul proprietății deținute sau prin alte căi (în cazul lipsei acestei informații, se indică administratorul persoanei juridice);

f) identitatea beneficiarului efectiv a persoanei juridice;

g) natura și scopul activității, legitimitatea acestora;

**26.** Entitatea raportoare identifică beneficiarul efectiv al clientului și aplică măsuri rezonabile și bazate pe risc pentru verificarea identității lui, astfel încât să aibă certitudinea că știe cine este beneficiarul efectiv pentru a înțelege structura proprietății și structura de control a clientului. Pentru identificarea beneficiarului efectiv entitatea raportoare aplică măsurile descrise la pct. 25 subpct.(1).

**27.** La identificarea beneficiarului efectiv al clientului - persoană juridică, inclusiv în cazul când acesta are o structură de proprietate complexă (persoană juridică a căror proprietari direcți nu sînt persoane fizice), entitatea raportoare determină beneficiarul efectiv în baza documentelor de înregistrare corespunzătoare.

**28.** Nu este necesară identificarea și verificarea identității beneficiarului efectiv în cazul în care clientul sau persoana juridică – proprietar al pachetului de control al clientului este o societate cotoată a căror valori mobiliare sunt acceptate spre tranzacționare pe o piață reglementată, cu obligația de dezvăluire publică a informației.

**29.** Entitatea raportoare determină dacă persoana care încheie contractul de leasing sau inițiază o relație de afaceri activează în numele său (declarația persoanei privind beneficiarul efectiv), iar în cazul în care încheierea contractului de leasing sau inițierea relației de afaceri este efectuată de către persoana împuternicită, entitatea raportoare solicită procura, legalizată în modul stabilit de legislație. Entitatea raportoare aplică măsuri de identificare a persoanei împuternicite în conformitate cu prevederile prezentului Regulament.

**30.** La identificarea clientului, entitatea raportoare verifică informația prezentată care se referă atât la client, cât și la beneficiarul efectiv.

**31.** Entitatea raportoare verifică identitatea clientului și a beneficiarului efectiv pînă la stabilirea relației de afaceri sau în momentul stabilirii relației de afaceri sau efectuării unei operații prevăzute la pct.24 lit.b).

**32.** În vederea verificării informației prezentate la identificarea clienților și a beneficiarilor efectivi, entitatea raportoare utilizează date și informații obținute din surse sigure și independente,. Verificarea informației trebuie să fie proporțională riscului pe care clientul și tipurile de documente prezentate le impun. În acest scop, entitatea raportoare utilizează proceduri documentare și nedocumentare de verificare:

1) pentru clienții - persoane fizice – entitatea raportoare verifică informația pe baza documentelor din categoria celor mai greu de falsificat sau de obținut pe cale ilicită sub un nume fals (de exemplu, actele de identitate emise de o autoritate oficială, care includ o fotografie a titularului). Verificarea informațiilor care nu se pot proba cu actele menționate mai sus se va realiza în funcție de gradul de risc prin orice altă metodă, cum ar fi:

a) pentru confirmarea datei și locului de naștere – certificatul de naștere;

b) pentru confirmarea validității documentelor de identitate – prin certificatele eliberate (de exemplu, în baza registrelor de stat sau private) de autoritățile publice sau de alte persoane competente (de exemplu, notari, ambasade etc.);

c) pentru confirmarea adresei de reședință în cazul în care nu corespunde cu domiciliul – prin solicitarea facturilor pentru serviciile comunale, a actelor privind plata impozitelor, a informației de la autoritățile publice sau de la alte persoane;

- d) verificarea referinței furnizate de alt persoană terță;
- 2) pentru clienții - persoane juridice (inclusiv persoanele fizice întreprinzători individuali sau care practică alt tip de activitate și persoanele juridice care gestionează bunurile aflate sub administrare fiduciară) – prin orice metodă corespunzătoare în funcție de gradul de risc, astfel încât entitatea raportoare să se asigure de veridicitatea informației, cum ar fi:
- a) verificarea existenței legale a persoanei juridice prin verificarea înscrisului în Registrul de stat al persoanelor juridice sau, după caz, într-un alt registru public sau privat sau alte surse sigure independente (ca exemplu: avocați, contabili, etc).
  - b) verificarea informației despre client în bazele de date privind relațiile de afaceri existente;
  - c) revizuirea ultimelor rapoarte financiare, dacă este cazul;
  - d) efectuarea unei analize, fie individuale sau prin intermediul altei persoane, privind existența procesului de insolvență sau lichidare, vânzare, a altor probleme financiare potențiale;
  - e) contactarea clientului prin telefon sau fax, prin intermediul serviciilor poștale sau e-mail, verificarea informației plasate pe pagina web a clientului, dacă există, sau efectuarea unei vizite pe teren la sediul sau la altă adresă indicată de persoana juridică și persoana fizică întreprinzător individual sau care practică alt tip de activitate;
- 3) pentru beneficiarul efectiv - măsurile prevăzute la subpt. 1).
- 4) în cazul în care o persoană este împuternicită în numele clientului să deschidă cont sau să efectueze tranzacții, entitatea raportoare verifică identitatea acesteia, precum și identitatea persoanei în numele căreia activează, utilizând aceleași proceduri descrise în prezentul Regulament.
- 33.** Documentele prezentate în vederea identificării clientului și a beneficiarului efectiv, precum și în vederea verificării identității acestora, trebuie să fie valabile la data prezentării lor, iar copiile acestora se stochează/arhivează de către entitatea raportoare corespunzător procedurilor interne stabilite.
- 34.** În cazul relațiilor de afaceri, entitatea raportoare revizuieste și actualizează informația cu privire la identificarea clienților și a beneficiarilor efectivi în funcție de riscul asociat. Entitatea raportoare poate actualiza informația ori de câte ori consideră necesar, dar cel puțin, pentru clienții cu grad de risc sporit - anual, iar pentru cei cu grad de risc scăzut - o dată la 3 ani. Clientul confirmă că datele și informațiile deținute de către entitatea raportoare sunt actuale și corespund scopului și naturii relației de afaceri declarat/înregistrat.

### **Secțiunea a 3-a**

#### **Măsuri de monitorizare a activităților și operațiunilor**

**35.** Entitatea raportoare trebuie să adapteze amploarea măsurilor de monitorizare a activităților și operațiunilor clienților în conformitate cu evaluarea instituțională a riscurilor și profilurilor de risc individuale ale clienților. Monitorizarea sporită este aplicată pentru situații cu risc înalt. Sistemele de monitorizare trebuie revizuite periodic, dar nu mai rar de o dată pe an.

**36.** Entitatea raportoare monitorizează continuu activitățile, operațiunile clientului sau relația de afaceri cu acesta. Acțiunile de monitorizare continuă cuprind:

- 1) determinarea operațiunilor ordinare (specifice) ale clientului de achitare a platilor de leasing;
- 2) examinarea minuțioasă a tranzacțiilor de leasing pe parcursul relației de afaceri pentru a avea siguranța că acestea sînt în corespundere cu informația disponibilă la entitatea raportoare, cu activitatea și riscul asociat clientului. Examinarea operațiunilor presupune cel puțin ca entitatea raportoare să dispună de mecanisme și soluții, inclusiv automatizate, pentru depistarea activităților, operațiunilor și persoanelor suspecte. Depistarea activităților, operațiunilor și persoanelor suspecte poate fi realizată prin stabilirea limitelor valorice ale tranzacțiilor pentru o grupă particulară sau categorie de operațiuni. O atenție deosebită se acordă operațiunilor care depășesc aceste limite valorice și operațiunilor ce nu au scop economic clar;
- 3) verificarea faptului dacă documentele și informațiile acumulate în procesul monitorizării clienților și tranzacțiilor sînt actualizate și relevante, inclusiv pentru categoriile clienților sau relațiile de afaceri cu grad de risc sporit;
- 4) identificarea activităților și operațiunilor suspecte, inclusiv a celor potențiale, precum și a surselor mijloacelor bănești utilizate în aceste activități și operații.

5) raportarea către persoana responsabilă a informației necesare pentru identificarea, analiza și monitorizarea eficientă a operațiunilor clienților, inclusiv pentru clienții cu grad de risc sporit;

6) monitorizarea în timp real a tuturor tranzacțiilor efectuate de clienți sau potențialii clienți pentru a depista persoanele, grupurile sau entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă, inclusiv în scopul identificării plăților pentru prevenirea efectuării acestora cu încălcarea sancțiunilor, interdicțiilor sau altor restricții aplicate.

37. Administratorul responsabil al entității raportoare are responsabilitatea pentru documentarea, păstrarea și comunicarea cu personalul relevant despre rezultatele monitorizării, precum și orice probleme care apar și soluționarea lor.

38. Entitatea raportoare se abține de la executarea activităților și operațiunilor cu mijloace financiare, pentru un termen de până la 5 zile lucrătoare, la stabilirea suspiciunilor pertinente care pot indica despre acțiuni de spălare a banilor, infracțiuni asociate acestora, acțiuni de finanțare a terorismului sau a proliferării armelor de distrugere în masă, în curs de pregătire, de tentativă, de realizare ori deja realizate.

39. Entitatea raportoare aplică cerințele pct.38 la solicitarea Serviciului Prevenirea și Combaterea Spălării Banilor sau din proprie inițiativă prin decizia (ordinul) administratorului responsabil al entității raportoare. La aplicarea cerințelor pct.38 din proprie inițiativă, entitatea raportoare informează imediat, dar nu mai târziu de 24 de ore, Serviciul Prevenirea și Combaterea Spălării Banilor despre decizia luată.

40. Entitatea raportoare în cazul aplicării cerințelor pct.38, poate solicita clientului furnizarea datelor și informației suplimentare, inclusiv a documentelor confirmative privind operațiunile efectuate, în scopul aplicării corespunzătoare a măsurilor de precauție, și în special, pentru înțelegerea scopului și a naturii relației de afaceri, precum și sursa bunurilor implicate.

41. Măsurile aplicate conform cerințelor pct.38 încetează din oficiu în baza permisiunii scrise și confirmate de Serviciul Prevenirea și Combaterea Spălării Banilor.

42. Entitatea raportoare este obligată:

a) să nu încheie contracte, să nu stabilească relații de afaceri, să nu efectueze operațiuni cu clientul, în cazul în care entitatea raportoare nu poate asigura respectarea cerințelor pct. 24,25, 31 și 32;

b) în cazul unei relații de afaceri existente, să întrerupă relația de afaceri în cazul în care entitatea raportoare nu poate asigura respectarea cerințelor pct.24, 25, 31 și 32;

c) raportează circumstanțele indicate la lit.a) și b) Serviciului Prevenire și Combaterea Spălării Banilor în conformitate cu Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

#### **Secțiunea a 4-a**

#### **Informația obținută de la persoanele terțe**

43. Entitatea raportoare, poate să recurgă la informația care aparține persoanelor terțe, pentru a realiza măsurile prevăzute la pct. 24, 25, 31 și 32, în următoarele condiții:

a) entitatea raportoare dispune de posibilitatea de a obține informațiile necesare aferente măsurilor prevăzute la pct. 24, 25, 31 și 32, deținute de către persoanele terțe;

b) entitatea raportoare adoptă și implementează proceduri eficiente privind accesul operativ la copiile datelor de identificare și la alte documente aferente măsurilor prevăzute la pct. 24, 25, 31 și 32, deținute de către persoanele terțe;

c) persoanele terțe sînt supravegheate adecvat și îndeplinesc cerințe similare celor prevăzute de Legea nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

d) persoanele terțe nu sînt rezidente în jurisdicțiile cu risc sporit.

44. Entitatea raportoare are responsabilitatea finală privind realizarea măsurilor prevăzute la pct. 24, 25, 31 și 32, în cazul în care apelează la persoane terțe.

### **Capitolul VI**

### **MĂSURI DE PRECAUȚIE SIMPLIFICATE PRIVIND CLIENȚII**



45. Entitatea raportoare aplică măsuri de precauție simplificată privind clienții atunci când, prin natura lor, pot prezenta un risc redus de spălare a banilor sau de finanțare a terorismului.

46. Măsurile de precauție simplificată privind clienții cuprind măsurile de precauție privind clienții prevăzute la pct. 24 și 25 în cadrul unei proceduri simplificate aferente riscului redus de spălare a banilor și de finanțare a terorismului, care include:

a) limitarea obținerii informațiilor cu privire la datele de identificare a clienților, prin aplicarea unei proceduri simplificate de verificare a identității clientului;

b) limitarea obținerii de informații specifice sau efectuarea de măsuri specifice privind scopul și natura relației de afaceri și deducerea scopului și naturii relației de afaceri din tipul tranzacțiilor sau a relației de afaceri stabilite;

c) verificarea identității clientului și a beneficiarului efectiv după stabilirea relației de afaceri (de exemplu, în cazul în care valorile tranzacției cresc deasupra pragul financiar definit);

d) reducerea frecvenței actualizărilor datelor de identificare a clienților în cazul unei relații de afaceri stabilite;

e) reducerea gradului și a amplitudinii monitorizării și controlului continuu a operațiunilor, bazate pe o limită a sumei rezonabilă.

47. Entitatea raportoare, în baza evaluării proprii, stabilește factorii care generează riscuri reduse de spălare a banilor și de finanțare a terorismului și care determină necesitatea aplicării măsurilor de precauție simplificată privind clienții. Următorii factori pot contribui la reducerea riscului:

a) relațiile de afaceri clienții și/sau produsele/serviciile acordate;

b) sume reduse și/sau regulate pentru plăți;

c) produsul sau serviciul poate fi folosit doar la nivel național;

d) produsul este disponibil numai pentru anumite categorii de clienți, de exemplu beneficiari de prestații sociale sau membri ai personalului unei companii care folosește produsul pentru a acoperi cheltuielile corporative;

e) alți factori identificați în cadrul evaluării riscurilor.

48. Entitatea raportoare nu va aplica măsuri de precauție simplificate în cazul existenței suspiciunii cu privire la spălarea banilor sau finanțarea terorismului.

## **Capitolul VII**

### **MĂSURI DE PRECAUȚIE SPORITE PRIVIND CLIENȚII**

49. În vederea aplicării legislației în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, entitatea raportoare stabilește categoriile clienților, activitățile și operațiunile ce prezintă un grad de risc sporit pe baza unor indicatori stabiliți în funcție de volumul operațiunilor efectuate, tipul serviciilor solicitate, tipul activității desfășurate, circumstanțele economice, reputația țării de origine a clientului, explicațiile oferite de client, limitele valorice prestabilite pe categorii de operațiuni.

50. În baza evaluării proprii, entitatea raportoare stabilește factorii care generează riscuri sporite și care determină necesitatea aplicării măsurilor de precauție sporită privind clienții. Factorii care generează riscuri sporite sînt:

a) bănueli rezonabile privind veridicitatea documentelor prezentate anterior referitor la starea financiară a locatarului;

b) transferuri ordonate de client plătite lui însuși din diferite țări;

c) tranzacții aranjate într-o manieră neordinară, în special dacă sunt dezavantajoase pentru client din punct de vedere economic sau financiar;

d) tranzacții efectuate de către terți în numele sau favoarea clientului fără a avea un motiv plauzibil;

e) alți factori identificați în cadrul evaluării riscurilor.

51. Entitatea raportoare aplică măsuri de precauție sporită privind clienții, suplimentar celor prevăzute în pct.25, în situațiile care, prin natura lor, pot prezenta un risc sporit de spălare a banilor sau de finanțare a terorismului, cel puțin prin:

a) obținerea informației suplimentare despre client (de exemplu genul de activitate, volumul activelor și/sau investițiilor preconizate, natura și scopul relației de afaceri preconizate, informația

disponibilă din alte surse publice, internet) și actualizarea frecventă a informației cu privire la identitatea clientului și a beneficiarului efectiv;

- b) obținerea informației suplimentare pentru stabilirea sau verificarea sursei mijloacelor bănești și a averii clientului;
- c) obținerea informației privind scopul activității;
- d) aprobarea la un nivel ierarhic superior a începerii sau continuării relației de afaceri cu astfel de clienți;
- e) monitorizarea sporită și permanentă a relației de afaceri, prin creșterea numărului și timpului verificărilor efectuate și selectarea activităților ce necesită examinare suplimentară;
- f) solicitarea ca prima plată să fie efectuată de client prin intermediul unui cont deschis în numele clientului la o instituție financiară care aplică cel puțin aceleași măsuri de precauție privind clientul;
- g) măsuri suplimentare prevăzute la pct. 52 – 53.

**52.** În cazul în care clientul nu se prezintă personal la identificare (de exemplu, în cazul relațiilor prin corespondență sau prin telefon, e-mail, internet sau alte mijloace electronice), entitatea raportoare aplică măsuri de precauție sporită prin utilizarea de mecanisme de tipul semnăturii digitale, a metodelor biometrice, cheilor de sesiune etc. Cu ocazia primei vizite a clientului la entitatea raportoare, se solicită documentele și informațiile conform cerințelor prezentului Regulament. Suplimentar, entitatea raportoare aplică una sau mai multe din următoarele măsuri:

- a) solicită documentele de identificare a clientului eliberate de către o autoritate sau un organ competent, inclusiv a specimenului de semnătură, alte documente, după caz, pentru completarea dosarului clientului;
- b) ia măsuri de protecție a autenticității documentelor în formă electronică transmise entității raportoare;
- c) acceptarea clientului utilizând procedurile care prevăd solicitarea informației de la o altă entitate raportoare;
- d) stabilirea și menținerea unei modalități de contact cu clientul, independentă de modalitatea prin care sunt realizate tranzacțiile cu clienții la distanță.

**53.** În tranzacțiile sau în relațiile de afaceri cu persoanele expuse politic, cu membrii familiilor persoanelor expuse politic și cu persoanele asociate persoanelor expuse politic, entitatea raportoare, suplimentar la măsurile de precauție prevăzute la pct.25, întreprind măsuri ce cuprind:

- a) elaborarea și implementarea sistemelor adecvate de gestionare a riscurilor, inclusiv a procedurilor bazate pe evaluarea riscurilor, pentru a stabili dacă un client, potențial client sau beneficiarul efectiv al unui client este persoană expusă politic;
- b) obținerea aprobării administratorului entității raportoare la stabilirea sau continuarea relațiilor de afaceri cu astfel de clienți;
- c) adoptarea măsurilor adecvate privind stabilirea sursei bunurilor și proprietăților implicate în relația de afaceri sau în operațiunile cu astfel de clienți;
- d) efectuarea monitorizării sporite și continue a relației de afaceri.

## **Capitolul X**

### **RAPORTAREA ACTIVITĂȚILOR ȘI A TRANZACȚIILOR**

**54.** Entitatea raportoare este obligat să informeze Serviciul Prevenirea și Combaterea Spălării Banilor despre:

- a) bunurile suspecte, activitățile sau tranzacțiile suspecte de spălare a banilor, de infracțiuni asociate acestora și de finanțare a terorismului, care sunt în curs de pregătire, de tentativă, de realizare sau sunt deja realizate - imediat, în cel mult 24 de ore de la identificarea actului sau circumstanțelor care generează suspiciuni;
- b) activitățile sau tranzacțiile clienților realizate în numerar, printr-o operațiune cu o valoare de cel puțin 100 mii de lei (sau echivalentul acesteia) sau prin mai multe operațiuni în numerar care par a avea o legătură între ele - în decurs de 10 zile calendaristice;

c) tranzacțiile clienților realizate prin virament, printr-o operațiune cu o valoare de cel puțin 500 mii de lei (sau echivalentul acesteia) - cel târziu la data de 15 a lunii următoare lunii de gestiune.

**55.** Entitatea raportoare va dispune de:

a) proceduri clare, reieșind din prevederile Legii nr. 308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, aduse la cunoștința întregului personal, care prevăd raportarea de către personal a tuturor activităților și tranzacțiilor suspecte;

b) sisteme de depistare a activităților și tranzacțiilor suspecte conform criteriilor stabilite, inclusiv de autoritățile competente;

c) proceduri de informare a administratorului responsabil privind problemele ce țin de prevenirea și combaterea spălării banilor și finanțării terorismului.

**56.** Entitatea raportoare informează, după caz, Serviciul Prevenirea și Combaterea Spălării Banilor sau alte organe cu funcții de supraveghere a entităților raportoare în conformitate cu Legea nr. 308 dn 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, despre activitățile și tranzacțiile suspecte, cazurile de fraudă ce afectează esențial siguranța, stabilitatea sau reputația entității raportoare.

**57.** Entitatea raportoare, persoanele cu funcții de răspundere, reprezentanții entității și angajații acesteia sunt obligați să nu comunice persoanelor fizice sau juridice care efectuează activitatea sau tranzacția ori terților despre transmiterea informației către Serviciul Prevenirea și Combaterea Spălării Banilor.

**58.** Entitățile raportoare trebuie să asigure protecția angajaților, persoanelor cu funcții de răspundere și reprezentanților acestora de orice acțiuni ostile care pot interveni ca urmare a aplicării măsurilor de precauție privind clienții, a terminării relațiilor de afaceri, a aplicării măsurilor asigurătorii, a transmiterii cu bună-credință a informației către Serviciul Prevenirea și Combaterea Spălării Banilor și organele cu funcții de supraveghere a entităților raportoare, precum și ca urmare a efectuării altor acțiuni în scopul executării prevederilor prezentei legi, cu excepția cazurilor când aceste acțiuni au fost săvârșite cu rea-credință, din neglijență și/sau prin abuz de serviciu.

## **Capitolul XI PĂSTRAREA DATELOR**

**59.** Entitatea raportoare păstrează toate documentele și informațiile despre clienți și beneficiarii efectivi, obținute în cadrul măsurilor de precauție privind clienții, inclusiv copiile documentelor de identificare, arhiva documentelor primare, corespondența de afaceri, rezultatele analizelor și cercetărilor efectuate privind identificarea operațiunilor complexe și neordinare, pe perioada activă a relației de afaceri și pe o perioadă de 5 ani după terminarea acesteia sau după data efectuării operațiunilor ocazionale și transferurilor de mijloace bănești. Datele păstrate trebuie să fie suficiente ca să permită reconstituirea fiecărei activități sau tranzacții în maniera în care să servească în caz de necesitate ca probă în cadrul procedurii penale, contravenționale și altor proceduri legale.

**60.** Procedurile de păstrare a documentelor și informației vor include cel puțin următoarele, după caz:

1) ținerea unui registru al clienților și al beneficiarului efectiv identificați, care va conține cel puțin: denumirea/numele și prenumele clientului; IDNO/IDNP; numărul contului de plată; data deschiderii; data închiderii);

2) păstrarea tuturor documentelor primare, inclusiv a corespondenței de afaceri;

3) păstrarea dosarelor privind identificarea și verificarea clienților, a beneficiarilor efectivi, privind monitorizarea operațiunilor clienților și păstrarea documentelor justificative aferente operațiunilor;

4) păstrarea informației privind operațiunile efectuate, inclusiv cele complexe și neordinare;

5) arhivarea informației privind operațiunile și corespondența de afaceri în sistemele tehnologiilor informaționale și păstrarea arhivei în condiții de siguranță și disponibilitate operativă.

**61.** Entitatea raportoare asigură că, în caz de solicitare, documentele și informația privind identificarea și verificarea clienților, a beneficiarilor efectivi, privind monitorizarea operațiunilor clienților, inclusiv documentele justificative aferente operațiunilor sînt accesibile și disponibile autorităților competente. La solicitarea autorităților competente termenul privind deținerea și păstrarea

informației aferentă clienților și operațiunilor acestora poate fi prelungit pentru o perioadă determinată în solicitare, dar nu mai mult de 5 ani.

## **Capitolul XII**

### **CERINȚE PRIVIND SISTEMUL DE CONTROL INTERN**

**62.** Entitatea raportoare va dispune de un sistem de control intern care va asigura conformarea continuă cu actele normative și programul intern în domeniu prevenirii și combaterii spălării banilor și finanțării terorismului ce va contribui la minimizarea riscurilor aferente.

**63.** Sistemul de control intern al entității raportoare depinde de o serie de factori, inclusiv natura, amploarea și complexitatea afacerii entității raportoare, diversitatea operațiunilor sale, inclusiv diversitatea geografică, baza de clienți, profilul de produs și activitate etc.

**64.** La deschiderea filialelor pe teritoriul altor state, precum și pe parcursul activității acestora, entitatea raportoare va aplica cerințele de prevenire și combatere a spălării banilor și finanțării terorismului în conformitate cu sistemul de control intern propriu, politicile și procedurile interne și actele normative ale Republicii Moldova, în măsura în care legislația țării gazde permite. În cazul în care, în țara gazdă cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt insuficiente, entitatea raportoare trebuie să asigure implementarea cerințelor actelor normative ale Republicii Moldova, în măsura în care legislația țării gazde permite. Dacă țara gazdă nu permite aplicarea corespunzătoare a cerințelor actelor normative ale Republicii Moldova, entitatea raportoare aplică măsuri suplimentare corespunzătoare în vederea micșorării riscului de spălare a banilor și finanțare a terorismului și informează Serviciul Prevenirea și Combaterea Spălării Banilor în decurs de 2 luni despre acest fapt. Serviciul Prevenirea și Combaterea Spălării Banilor poate efectua controale suplimentare pentru supravegherea respectării de către filialele deschise pe teritoriul altor state a actelor normative în vigoare aferente domeniului dat.

**65.** Sistemul de control intern trebuie să includă cel puțin următoarele elemente:

1) efectuarea de către personalul entității raportoare sau de către auditul independent în vederea verificării respectării programului intern privind prevenirea și combaterea spălării banilor și finanțării terorismului. Funcțiile auditului în acest scop sînt:

a) evaluarea independentă a programului privind prevenirea și combaterea spălării banilor și finanțării terorismului și a respectării cerințelor legislației în vigoare;

b) monitorizarea activității personalului prin testarea conformării;

c) testarea operațiunilor în caz de necesitate;

d) informarea administratorului responsabil privind rezultatele verificării;

2) desemnarea unei persoane, care este administrator/conducător, responsabil de asigurarea conformării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului cu cerințele legislației și aplicării acestuia adecvat (în continuare - administrator responsabil). În acest scop administratorul responsabil are următoarele atribuții:

a) acordă consultații angajaților entității raportoare în problemele ce apar în timpul realizării programului privind prevenirea și combaterea spălării banilor și finanțării terorismului, inclusiv în ce privește identificarea și examinarea clienților băncii și evaluarea riscului de spălare a banilor și finanțare a terorismului;

b) ia decizii în baza informației primite;

c) întreprinde măsuri privind raportarea autorității competente pentru prevenirea și combaterea spălării banilor și finanțării terorismului a informației în conformitate cu legislația;

d) organizează instruirea angajaților entității raportoare în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

e) colaborează, după caz, cu serviciul de audit în vederea verificării conformării activității entității raportoare la legislația în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

f) îndeplinește alte funcții în corespundere cu prezentul Regulament și documentele interne ale entității raportoare;

3) prevederi interne privind răspunderea angajaților care în mod intenționat nu raportează despre activitățile sau operațiunile suspecte administratorului sau direct autorității competente și/sau contribuie personal la efectuarea operațiunilor de spălare a banilor și finanțarea terorismului.

**66.** Persoana, care efectuează auditul entității raportoare, analizează realizarea programului privind prevenirea și combaterea spălării banilor și finanțării terorismului de către entitatea raportoare și prezintă în scris, administratorului responsabil al entității raportoare un raport privind rezultatele analizei efectuate;

**67.** Entitatea raportoare va dispune de programe de selectare și instruire continuă a personalului în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului. Entitatea raportoare asigură deținerea de către personalul său a cunoștințelor, calităților și abilităților corespunzătoare pentru îndeplinirea eficientă a responsabilităților de conformare la cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.

**68.** Programele de selectare și instruire indicate la pct. 67 vor cuprinde diverse aspecte ale procesului de prevenire și combatere a spălării banilor și finanțării terorismului și obligațiunile conform legislației în domeniu, inclusiv:

a) instruirea personalului nou angajat referitor la importanța și cerințele de bază ale programelor respective;

b) instruirea personalului de „prima linie” (angajații care nemijlocit intră în contact cu clienții) referitor la verificarea identității clienților noi, monitorizarea clienților existenți pe bază continuă, depistarea indicilor și raportarea activităților și tranzacțiilor suspecte și a celor supuse raportării;

c) actualizarea regulată a responsabilităților personalului;

d) noile tehnici, metode și tendințe de spălare a banilor și finanțarea terorismului;

e) nivelul implicării personalului în procesul de prevenire și combatere a spălării banilor și finanțării terorismului.

Conținutul și programul instruirii personalului trebuie să fie adaptat la necesitățile individuale ale entității raportoare.

### **Capitolul XIII**

#### **CERINȚE PRIVIND APLICAREA**

#### **MĂSURILOR RESTRICTIVE INTERNAȚIONALE**

**69.** Entitatea raportoare aplică imediat măsuri restrictive în privința bunurilor, inclusiv a celor obținute din sau generate de bunuri care aparțin sau sînt deținute ori controlate, direct sau indirect, de persoanele, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive, precum și de persoanele juridice care aparțin sau sînt controlate, direct sau indirect, de aceste persoane, grupuri și entități.

**70.** Pentru punerea în aplicare a măsurilor restrictive conform pct.69, entitatea raportoare elaborează proceduri și reguli interne care trebuie să includă cel puțin următoarele elemente:

a) proceduri de elaborare și actualizare a listei persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive internaționale (inclusiv prin utilizarea bazelor de date existente), conform cerințelor Legii nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului și Legii nr.25 din 04.03.2016 privind aplicarea măsurilor restrictive internaționale, folosind în acest scop inclusiv și Ordinul directorului Serviciului de Informații și Securitate privind listele persoanelor, grupurilor și entităților implicate în activități teroriste;

b) proceduri de verificare/depistare a persoanelor sau entităților desemnate și a operațiunilor/plăților în care sunt implicate bunuri, aplicabile potențialilor clienți, clienților existenți și solicitanților de operațiuni/plăți ocazionale și de transfer a mijloacelor bănești;

c) competențele persoanelor cu responsabilități în implementarea procedurilor și regulilor interne pentru punerea în aplicare a măsurilor restrictive internaționale de blocare a fondurilor;

d) procedurile de informare/raportare, intern și către autoritățile competente (Serviciul Prevenirea și Combaterea Spălării Banilor, Serviciul de Informații și Securitate, Ministerul Afacerilor Externe și Integrării Europene și Ministerul Finanțelor).

**71.** Entitatea raportoare, la identificarea bunurilor care aparțin sau sînt deținute ori controlate, direct sau indirect, de persoanele, grupurile și entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive, întreprinde succesiv următorii pași:

a) prin decizia (ordinul) administratorului responsabil al entității raportoare, se abține, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor în favoarea sau beneficiul, direct sau indirect, al persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive;

b) informează imediat, dar nu mai târziu de 24 ore, Serviciul Prevenirea și Combaterea Spălării Banilor și Serviciul de Informații și Securitate despre abținerea, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor în favoarea sau beneficiul, direct sau indirect, al persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive. Informația transmisă în adresa autorităților menționate va cuprinde cel puțin următoarele elemente:

i. date și informații (nume/denumire; IDNO/IDNP, dacă există; țara de origine/rezidență; lista autorității/organizației la care face referință măsura restrictivă aplicată, etc) despre persoana, grupul sau entitatea identificată;

ii. date și informații (volumul; moneda; destinatarul; destinația, etc) despre bunul identificat;

iii. informarea despre decizia administratorului responsabil al entității raportoare cu privire la abținerea, pentru un termen nedeterminat, de la executarea activităților și tranzacțiilor cu referire la bunul identificat;

iv. solicitarea de a furniza opinia scrisă în decurs de 5 zile, conform legislației în vigoare, despre necesitatea menținerii sau nu a măsurilor restrictive;

c) dacă este cazul, entitatea raportoare acceptă plăți suplimentare, efectuate de o parte terță, sau majorarea valorii bunurilor identificate și extinde aplicabilitatea măsurii de abținere asupra bunurilor, ținând cont de cerințele pct.71 lit.a), precum și informează despre acest fapt autoritățile menționate ținând cont de cerințele pct. 71 lit.b);

d) la primirea răspunsul în formă scrisă de la cel puțin una dintre autoritățile sesizate (în cazul opiniilor diferite ale autorităților sesizate, entitatea raportoare aplică măsura restrictive cea mai dură), entitatea raportoare întreprinde următoarele:

i. în cazul opiniei despre necesitatea neaplicării măsurilor restrictive - prin decizia (ordinul) administratorului responsabil al entității raportoare, măsura de abținere se anulează/abrogă;

ii. în cazul opiniei despre necesitatea de aplicare a măsurilor restrictive: prin decizia (ordinul) administratorului responsabil al entității raportoare, tranzacțiile/bunurile sunt blocate;

iii. dacă este cazul, entitatea raportoare acceptă plăți suplimentare, efectuate de o parte terță, sau majorarea valorii bunurilor identificate și extinde aplicabilitatea măsurii de blocare a acestora și informează despre acest fapt autoritățile menționate la pct. 71 lit.b);

iv. se informează suplimentar despre decizia luată Ministerul Afacerilor Externe și Integrării Europene și Ministerul Finanțelor, ținând cont de cerințele pct.71 lit.b) cifra (i) și (ii);

e) informează Serviciul Prevenirea și Combaterea Spălării Banilor despre măsura restrictivă aplicată, ținând cont de cerințele pct.71 lit.b) cifra (i) și (ii);

f) prin dispunerea încheierii/hotărârii instanței de judecată sau altei autorități competente, bunurilor blocate li se atribuie statutul indicat în încheiere/hotărâre.

**72.** Entitatea raportoare asigură monitorizarea permanentă a Monitorului Oficial, precum și a paginilor web oficiale ale Organizației Națiunilor Unite, Uniunii Europene și Serviciului de Informații și Securitate, pentru asigurarea aplicabilității corespunzătoare a măsurilor restrictive asupra persoanelor, grupurilor și entităților implicate în activități teroriste și de proliferare a armelor de distrugere în masă.

**73.** Entitatea raportoare nu stabilește și nu continuă relația de afaceri cu persoanele, grupurile sau entitățile implicate în activități teroriste și de proliferare a armelor de distrugere în masă. Despre refuzul de a stabili sau a continua relația de afaceri cu acestea, entitatea raportoare informează Serviciul Prevenirea și Combaterea Spălării Banilor ținând cont de prevederile legale în vigoare.

## **Capitolul XIV**

### **MĂSURI DE REMEDIERE ȘI SANCTIUNI**

74. În cazul în care se constată încălcarea prevederilor prezentului Regulament, a obligațiilor prevăzute de legislația privind prevenirea și combaterea spălării banilor și finanțării terorismului, Serviciul Prevenirea și Combaterea Spălării Banilor poate aplica măsuri de remediere și sancțiuni în conformitate cu art.35 alin.(2) din Legea nr.308 din 22.12.2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

75. În scopul lichidării încălcărilor și neajunsurilor constatate, precum și a condițiilor ce favorizează comiterea acestora, Serviciul Prevenirea și Combaterea Spălării Banilor, pe lângă măsurile de remediere și sancțiunile menționate la pct.74, poate dispune următoarele măsuri:

a) să prescrie modificarea programului privind prevenirea și combaterea spălării banilor și finanțării terorismului;

b) să prescrie efectuarea unei evaluări repetate a riscurilor de spălare a banilor și finanțare a terorismului;

c) să prescrie întocmirea unui nou plan de minimizare a riscurilor identificate de spălare a banilor și finanțare a terorismului;

d) să prescrie aplicarea măsurilor de precauție sporită de cunoaștere a clienților pentru produse, servicii, tranzacții (operațiuni) ori clienți, în cazul în care programul privind prevenirea și combaterea spălării banilor și finanțării terorismului stabilește aplicarea de măsuri standard sau simplificate de cunoaștere a clienților;

e) să prescrie înlocuirea administratorului responsabil al entității raportoare.