



HOTĂRÎRE
cu privire la aprobarea Regulamentului privind măsurile de prevenire
și combatere a spălării banilor și finanțării terorismului
pe piața financiară nebancaară

nr. 49/14 din 21.10.2011

Monitorul Oficial nr.206-215/1820 din 02.12.2011

* * *

ÎNREGISTRAT:

Ministrul justiției

_____ Oleg EFRIM

nr.855 din 22 noiembrie 2011

În temeiul art.20 alin.(1), art.21 alin.(1), art.22 alin.(1) și alin.(2), art.25 alin.(2) din Legea nr.192-XIV din 12.11.1998 “Privind Comisia Națională a Pieței Financiare” (republicată în Monitorul Oficial al Republicii Moldova, 2007, nr.117-126 BIS) și art.10 alin.(2) din Legea nr.190-XVI din 26.07.2007 “Cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului” (Monitorul Oficial al Republicii Moldova, 2007, nr.141-145, art.597), Comisia Națională a Pieței Financiare

HOTĂRĂȘTE:

1. Se aprobă Regulamentul privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului pe piața financiară nebancaară (se anexează).

2. Entitățile raportoare, în termen de pînă la 3 luni de la data intrării în vigoare a prezentei hotărîri, vor elabora și aproba în conformitate cu legislația, programe proprii privind prevenirea și combaterea spălării banilor și finanțării terorismului, ținînd cont de prevederile prezentului Regulament.

3. Despre executarea pct.2, entitățile raportoare vor informa Comisia Națională a Pieței Financiare în termen de 30 zile.

4. Controlul asupra executării prevederilor pct.2 al prezentei hotărîri se pune în sarcina Direcției generale supraveghere valori mobiliare, Direcției generale supraveghere asigurări și Direcției generale plasamente colective și microfinanțare.

5. Se abrogă Hotărîrea Comisiei Naționale a Pieței Financiare nr.63/5 din 25.12.2007 “Cu privire la Recomandările privind aplicarea măsurilor de prevenire și combatere a spălării banilor și finanțării terorismului pe piața financiară nebancaară” (Monitorul Oficial al Republicii Moldova, 2008, nr.30-31, art.74).

**VICEPREȘEDINTELE COMISIEI
NAȚIONALE A PIEȚEI FINANCIARE**

Victor CAPTARI

Chișinău, 21 octombrie 2011.

Nr.49/14.

Anexă
la Hotărîrea Comisiei Naționale
a Pieței Financiare
nr.49/14 din 21 octombrie 2011

REGULAMENT

privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului pe piața financiară nebanară

I. DISPOZIȚII GENERALE

1. Regulamentul privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului pe piața financiară nebanară (în continuare Regulament) se aplică participanților profesioniști la piața financiară nebanară – entități raportoare determinate de art.4 din Legea nr.190-XVI din 26.07.2007 “Cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului” (în continuare – Legea nr.190 din 26.07.2007).

2. Prevenirea și combaterea spălării banilor și finanțării terorismului prezintă o atribuție majoră pentru economia națională și conduce la sporirea încrederii în sistemul financiar autohton.

3. Activitățile supuse riscului spălării banilor și finanțării terorismului sînt:

- 1) tranzacțiile complexe și neordinare;
- 2) operațiunile financiare internaționale;
- 3) operațiunile efectuate cu aplicarea tehnologiilor informaționale;
- 4) operațiunile de brokeraj;
- 5) operațiunile de administrare fiduciară;
- 6) acceptarea depunerilor de economii;
- 7) acordarea de împrumuturi.

4. Principalele elemente ale procesului de spălare a banilor și finanțare a terorismului sînt:

1) plasarea – circulația inițială a mijloacelor bănești sau a altor venituri provenite din activitatea infracțională cu scopul schimbării formei inițiale sau a locului acestora pentru a le face inaccesibile organelor de drept;

2) investirea – separarea de la sursa de proveniență a veniturilor obținute din activitatea criminală prin intermediul diferitelor tranzacții financiare;

3) integrarea – utilizarea unei tranzacții legitime pentru a ascunde veniturile ilicite, făcînd posibilă întoarcerea la infractor a mijloacelor bănești.

5. Entitatea raportoare va raporta Serviciului de Prevenirea și Combaterea Spălării Banilor din cadrul Centrului pentru Combaterea Crimelor Economice și Corupției (în continuare – SPCSB) și Comisiei Naționale a Pieței Financiare (în continuare – CNPF), în conformitate cu legislația, asupra activității sale de combatere și prevenire a spălării banilor și finanțării terorismului pe piața financiară nebanară.

6. La elaborarea programelor proprii contra spălării banilor și finanțării terorismului, entitățile raportoare trebuie să ia în considerație riscurile aferente spălării banilor și finanțării terorismului în scopul minimizării acestora. Aceste riscuri sînt:

1) Riscul legal – riscul că hotărîrile instanței de judecată sau contractele, de fapt, sînt irealizabile și pot afecta negativ operațiunile sau situația entităților raportoare. În scopul minimizării riscului legal entitățile raportoare trebuie să efectueze o monitorizare corectă la identificarea persoanelor fizice și juridice, precum și a beneficiarului efectiv.

2) Riscul imaginii – risc aferent spălării banilor și finanțării terorismului, care implică posibilitatea pierderii încrederii ca urmare a apariției publicității adverse privind practicile de afacere a entităților raportoare și a beneficiarului efectiv.

3) Riscul operațional – riscul pierderilor directe sau indirecte, care rezultă din procesele interne inadecvate sau eșuate, persoane sau evenimente externe.

4) Riscul tehnologiilor informaționale – riscul care poate apărea în urma lansării tehnologiilor informaționale noi și a dezvoltării celor existente, cînd acestea pot crea condiții favorabile pentru acțiuni de spălare a banilor și finanțare a terorismului.

II. RESPONSABILITATEA

7. Entitățile raportoare sînt responsabile 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. Disponerea 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.

8. Entitățile raportoare sînt responsabile de conformarea activității acesteia prevederilor legislației în vigoare în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

III. CERINȚE FAȚĂ DE PROGRAMELE PROPRII DE PREVENIRE ȘI COMBATERE A SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

9. Programele proprii de prevenire și combatere a spălării banilor și finanțării terorismului reprezintă politici și proceduri, inclusiv reguli cu privire la măsurile de identificare a clienților, care promovează normele de etică și profesionalism în sectorul financiar nebanca și previn implicarea entității raportoare în acțiuni ilicite, în mod intenționat sau nu, de către elementele criminale. Politicile și procedurile trebuie să asigure efectuarea operațiunilor financiare într-un mod sigur și prudent.

10. La elaborarea programelor privind prevenirea și combaterea spălării banilor și finanțării terorismului, entitățile raportoare trebuie să ia în considerație prezentul Regulament și să le adapteze la activitatea lor în dependență de mărimea, complexitatea, natura și volumul activităților entității raportoare, lista clienților, nivelul de risc asociat cu diferiți clienți și operațiunile desfășurate de aceștia, ținînd cont de prevederile legislației în vigoare și practica acceptată în acest domeniu.

11. Programul entității raportoare privind prevenirea și combaterea spălării banilor și finanțării terorismului trebuie să fie aprobat de entitățile raportoare și supus revizuirii ori de cîte ori este necesar, dar nu mai puțin de o dată pe an.

12. Structura programelor proprii de prevenire și combatere a spălării banilor și finanțării terorismului pe piața financiară nebanca trebuie să prevadă cel puțin următoarele componente:

1) obligațiile entităților raportoare, care trebuie să includă:

a) cunoașterea circumstanțelor clienților cu grad de risc sporit;

b) cunoașterea surselor de informare a părților terțe;

c) aprobarea tranzacțiilor semnificative ale clienților cu grad de risc sporit;

d) determinarea sectoarelor care pot fi supuse riscului spălării banilor și finanțării terorismului cu delimitarea exactă a atribuțiilor fiecărei subdiviziuni îndreptate spre prevenirea și combaterea spălării banilor și finanțării terorismului;

e) asigurarea înlăturării neconformărilor identificate în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului pe piața financiară nebanca;

f) punerea în acțiune a politicilor și procedurilor interne aferente prevenirii și combaterii spălării banilor și finanțării terorismului, inclusiv determinarea responsabilităților angajaților la diferite niveluri ierarhice;

2) definirea procesului posibil de spălare a banilor și finanțare a terorismului în dependență de particularitățile caracteristice ale entității raportoare;

3) măsuri de identificare a clientului (regulile “cunoaște-ți clientul”);

4) proceduri și măsuri de verificare a modului de conformare la normele elaborate și de evaluare a eficienței acestora;

5) proceduri de raportare internă și externă către autoritățile competente privind activitățile și operațiunile suspecte;

6) modalități de întocmire și păstrare a evidențelor corespunzătoare, precum și stabilirea accesului la acestea;

7) standarde pentru angajare și programe de pregătire a personalului în domeniul cunoașterii clienților, inclusiv proceduri privind selectarea angajaților noi.

IV. MĂSURI DE IDENTIFICARE A CLIENTULUI

13. Entitățile raportoare aplică măsurile de identificare a clienților:

1) la etapa stabilirii relațiilor de afaceri;

2) la efectuarea tranzacțiilor ocazionale în valoare de cel puțin 50 mii lei, precum și la efectuarea tranzacțiilor electronice în valoare de cel puțin 15 mii lei, indiferent de faptul că tranzacția se efectuează printr-o singură operațiune sau prin mai multe operațiuni;

3) la existența unor suspiciuni de spălare a banilor sau de finanțare a terorismului;

4) la existența unor îndoieli privind veridicitatea și precizia datelor de identificare obținute.

14. Entitățile raportoare identifică clientul și adoptă măsuri adecvate bazate pe risc pentru verificarea identității, astfel încât să posede informația și certitudinea despre client, structura proprietății și modalitățile de control ale acestuia.

15. Entitățile raportoare monitorizează continuu tranzacțiile sau relațiile de afaceri ale clientului, pentru a se asigura că acestea sînt conforme informațiilor furnizate și că sînt actualizate permanent.

16. Subiecții supuși identificării sînt:

1) persoana fizică sau juridică care deține un cont la entitatea raportoare sau acei în numele cărora este menținut contul;

2) proprietarii beneficiari ai tranzacțiilor efectuate de către intermediari-profesioniști;

3) orice persoană fizică sau juridică implicată într-o tranzacție care poate impune un risc semnificativ imaginii sau alt risc;

4) persoanele expuse politic.

17. Entitățile raportoare trebuie să obțină informații privind scopul și natura relației de afaceri, privind tranzacțiile complexe și neordinare.

18. Entitățile raportoare trebuie să elaboreze politici și proceduri clare de acceptare a clientului, inclusiv o descriere a tipurilor de clienți care par să impună un risc sporit instituției. La elaborarea acestor politici situația clienților cu un risc mai mare trebuie examinată sub un șir de aspecte cum ar fi experiența clienților, țara de origine, poziția socială, activitățile de afacere sau alți indicatori de risc. Procedurile de acceptare a clienților trebuie să includă mai multe etape în dependență de nivelul de risc al clienților, concomitent punînd accentul pe clienții cu un venit înalt a cărui sursă este neclară sau neidentificată. Deciziile de începere, continuare sau încetare a relațiilor de afaceri cu clienții cu un grad de risc sporit, trebuie să fie exclusiv luate la nivelul conducerii entității raportoare. Este important ca procesul de acceptare a clienților să nu restricționeze accesul publicului larg la serviciile financiare.

19. Entitățile raportoare vor dispune de o politică și o procedură sistematică de identificare a clienților (fie permanenți sau ocazionali, persoane fizice sau juridice sau alte aranjamente legale) și a beneficiarului efectiv, de instrumente adecvate de verificare din surse sigure și independente a informației despre clienți și despre tranzacțiile acestora și nu vor stabili o relație de afacere pînă cînd identitatea clientului nu este verificată. Informația cu privire la identificarea clienților și a beneficiarilor efectivi ai acestora urmează a fi actualizată ori de cîte ori este necesar.

20. La stabilirea unor relații de afaceri entitățile raportoare vor respecta normele legale și actele normative ale CNPF în scopul prevenirii și combaterii spălării banilor și finanțării terorismului prin obținerea cel puțin a următoarelor informații:

1) În cazul clientului – persoană fizică:

a) numele, prenumele și patronimicul, după caz;

b) data și locul nașterii;

c) numărul de identificare sau alți indici unici conținuți într-un act de identitate oficial neexpirat, care conține fotografia titularului (ca exemplu: pașaport, buletin de identitate, permisul de ședere eliberat de autoritățile împuternicite ale Republicii Moldova, alte acte de identitate);

d) adresa de domiciliu și/sau reședință;

e) numărul de telefon, fax, adresa de poștă electronică (în cazul în care există);

f) cetățenia;

g) ocupația și, după caz, numele angajatorului ori natura activității proprii;

h) funcția publică importantă deținută, după caz;

i) numele beneficiarului efectiv;

j) scopul și natura relației cu entitatea raportoare;

k) semnătura.

2) În cazul clientului – persoană juridică:

a) denumirea clientului;

b) sediul și/sau adresa unde sînt desfășurate operațiunile de afaceri ale persoanei juridice;

c) numărul de telefon, fax, adresa de poștă electronică, după caz;

d) numărul de identificare de stat (codul fiscal);

e) documentele de constituire în original sau copie autentificată, cu modificările și completările ulterioare;

f) informația privind identitatea persoanelor care, potrivit actelor constitutive și/sau hotărârii organelor statutare, sînt investite cu competența de a conduce și reprezenta entitatea, precum și împuternicirile acestora;

g) extrasul din Registrul de stat al persoanelor juridice;

h) natura și scopul afacerii și legitimitatea ei;

i) scopul și natura relației cu entitatea raportoare;

j) numele beneficiarului efectiv.

21. Entitățile raportoare vor identifica beneficiarul efectiv al clientului său și vor întreprinde măsuri rezonabile pentru a verifica identitatea beneficiarului efectiv pe bază de risc, utilizînd informația relevantă sau datele obținute din surse sigure, astfel încît să cunoască cine este beneficiarul efectiv. Pentru identificarea și verificarea beneficiarului efectiv se vor utiliza aceleași proceduri de identificare și verificare ca pentru persoane fizice.

22. La identificarea beneficiarilor efectivi ai clienților, entitățile raportoare vor întreprinde următoarele măsuri:

1) în cazul persoanelor fizice: dacă contul este deschis pe numele unei anumite persoane, entitățile raportoare vor determina dacă persoana respectivă activează în numele său (declarația persoanei privind beneficiarul efectiv).

2) în cazul persoanelor juridice: entitățile raportoare vor înțelege caracterul proprietății și mecanismul de control asupra persoanei juridice și vor utiliza măsuri rezonabile la verificarea identității beneficiarilor efectivi. Întru corespunderea acestor cerințe este necesară constatarea persoanelor fizice care dețin poziții de control, a persoanelor fizice care elaborează politica persoanei juridice și a persoanelor fizice care controlează această persoană (în baza documentelor de constituire, extrasului din Registrul de stat ș.a.).

23. Verificarea identității clientului se realizează pe baza documentelor oficiale din categoria celor mai greu de falsificat sau de obținut pe cale ilicită sub un nume fals, cum ar fi documentele de identitate, emise de o autoritate oficială, care să includă o fotografie a titularului. Verificarea informațiilor care nu se pot proba cu documentele menționate mai sus, se va realiza prin orice metodă corespunzătoare, cum ar fi: confirmarea datei de naștere, de exemplu, din certificatul de naștere, pașaport, buletin de identitate, permisul de ședere eliberat de autoritățile împuternicite ale Republicii Moldova etc.; confirmarea adresei de reședință în cazul în care nu corespunde cu domiciliul (de exemplu, informația de la autorități publice sau de la alte persoane abilitate etc.); contactarea clientului prin telefon, fax sau e-mail (în cazul în care există) pentru a confirma informația prezentată după deschiderea contului; confirmarea validității documentelor de identitate cu certificatele persoanelor autorizate, cu registrele de stat și private.

24. Entitățile raportoare au obligația de a verifica existența legală a persoanei juridice, respectiv dacă aceasta este înregistrată în Registrul de stat al persoanelor juridice sau, după caz, într-un alt registru public. Verificarea informațiilor furnizate de client se va realiza prin orice metodă corespunzătoare, astfel încît entitatea raportoare să se asigure de veridicitatea acestor informații. În acest sens entitățile raportoare vor utiliza cel puțin următoarele modalități: revizuirea ultimelor rapoarte financiare, utilizarea informației independente în procesul de verificare, așa ca prin accesul public (registrele de stat) sau baze de date private, efectuarea unei analize pentru a vedea dacă clientul nu a fost sau nu este în proces de insolvență sau lichidare, obținerea referinței unei entități raportoare cu care clientul a avut relații de afaceri, contactarea clientului prin telefon, prin intermediul serviciilor poștale sau e-mail, coroborarea cu informația prezentată pe pagina web a clientului, sau efectuarea unei vizite pe teren la adresa indicată de persoana juridică, și altele.

25. În cazul în care o persoană fizică este împuternicită în numele clientului să deschidă cont sau să efectueze tranzacții, entitatea raportoare va verifica împuternicirile acesteia, precum și va identifica și va verifica persoana în cauză utilizînd aceleași proceduri de identificare și verificare ca pentru persoanele fizice.

26. În cazul deschiderii contului de către un intermediar în numele unui singur client sau în numele mai multor clienți, entitățile raportoare vor solicita și vor obține informațiile și documentele corespunzătoare cu privire la identitatea intermediarului și a persoanelor beneficiare în contul cărora acesta acționează, precum și detalii privind natura împuternicirii lui. Entitățile raportoare vor accepta deschiderea a astfel de conturi numai cu condiția că sînt capabile să identifice atît intermediarii cît și

beneficiarii efectivi ai mijloacelor bănești. În cazul în care intermediarul nu are dreptul să acorde entităților raportoare informația necesară privind beneficiarii, acestea nu vor permite deschiderea contului.

27. Entitățile raportoare vor dispune de proceduri corespunzătoare pentru acumularea informației suficiente din partea unui client și a beneficiarului efectiv a acestuia și vor verifica informația disponibilă public, pentru a determina dacă clientul și beneficiarul efectiv a acestuia este sau nu persoană expusă politic, precum vor actualiza periodic informația obținută la deschiderea contului, avînd în vedere că clientul și beneficiarul efectiv a acestuia pot deveni ulterior persoană expusă politic. Este necesară asigurarea obținerii aprobării organului executiv pentru stabilirea sau, în cazul cînd a devenit ulterior, continuarea unor relații de afaceri cu persoane expuse politic, stabilirea sursei bunurilor și mijloacelor bănești ale acestora și efectuarea unei monitorizări sporite și permanente a relației de afaceri.

28. Entitățile raportoare la inițierea tranzacțiilor electronice autohtone sau internaționale, utilizînd în acest sens oricare din mijloacele disponibile, trebuie să obțină și să păstreze cel puțin următoarea informație despre inițiatorul tranzacției: numele; numărul contului (sau un număr unic de identificare); adresa (sau codul personal de identificare, sau data și locul nașterii). Entitățile raportoare participanți ca intermediari la efectuarea tranzacțiilor electronice sînt obligați să păstreze cel puțin aceeași informație.

29. Entitățile raportoare trebuie să adopte proceduri bazate pe risc efectiv pentru gestionarea situațiilor cînd informația necesară efectuării tranzacțiilor electronice nu este completă.

30. Entitățile raportoare sînt obligate să se abțină de la stabilirea unor relații de afaceri, să înceteze ori să refuze îndeplinirea tranzacțiilor în cazul în care nu au fost prezentate actele stabilite pentru identificarea persoanei fizice sau juridice ori datele și informațiile obținute sînt neautentice sau neveridice, sau există suspiciuni de spălare a banilor și/sau finanțare a terorismului. Entitățile raportoare în cazul apariției circumstanțelor descrise mai sus, după caz, trebuie să informeze organul abilitat în conformitate cu prevederile Legii nr.190 din 26.07.2007.

V. MĂSURI DE PRECAUȚIE SPORITĂ

31. În procesul de punere în aplicare a prevederilor Legii nr.190 din 26.07.2007, entitățile raportoare vor stabili categoria clienților și a tranzacțiilor ce prezintă un grad de risc potențial mai ridicat, pe baza unor indicatori de risc care pot avea în vedere, după caz, volumul activelor sau veniturilor, tipul serviciilor solicitate, tipul activității desfășurate de client, circumstanțele economice, reputația țării de origine, admisibilitatea explicațiilor oferite de client, niveluri valorice prestabilite pe categorii de tranzacții.

32. Entitatea raportoare trebuie să aplice măsuri de precauție sporită în cazul în care persoana fizică sau juridică implicată în operațiune nu este prezentă personal la identificare precum și la efectuarea (înregistrarea) tranzacțiilor cu participarea persoanei juridice rezidente a zonei off-shore și să întreprindă următoarele măsuri:

1) garantarea că identitatea persoanei este stabilită prin documente, date sau informații suplimentare;

2) verificarea și certificarea suplimentară a documentelor furnizate;

3) garantarea că prima plată a operațiunilor se efectuează printr-un cont deschis în numele persoanei.

33. În cazul în care persoana fizică sau juridică nu se prezintă personal la identificare, precum și în momentul efectuării tranzacțiilor (relații prin corespondență sau prin telefon, e-mail, Internet sau alte mijloace electronice), entitățile raportoare vor aplica clienților în cauză procedurile de identificare și standardele de monitorizare egale celor aplicabile clienților disponibili să se prezinte personal la entitatea raportoare (de ex., prin utilizarea semnăturii digitale, metode biometrice, chei de sesiune etc.).

34. În cazul unor astfel de relații, entitățile raportoare vor efectua următoarele măsuri:

1) certificarea documentației transmise entității raportoare, inclusiv a specimenului de semnătură;

2) solicitarea documentelor suplimentare pentru a completa dosarul conform procedurilor de identificare a clienților;

3) aplicarea măsurilor de protecție care să asigure autenticitatea documentației transmise entității raportoare, în cazul documentelor în formă electronică;

4) acceptarea clientului utilizând procedurile care prevăd solicitarea informației de la o altă entitate raportoare;

5) stabilirea și menținerea unei modalități de contact cu clientul, independentă de modalitatea prin care sînt realizate tranzacțiile cu clienții la distanță.

35. La efectuarea (înregistrarea) tranzacțiilor cu participarea persoanei juridice rezidente a zonei off-shore, persoana juridică în cauză va prezenta următoarele informații:

1) seria, numărul și data eliberării actului de identitate, adresa și alte date necesare pentru identificarea reprezentantului persoanei juridice;

2) actul de reprezentare (procura, ordin, extras din statutul societății etc.), autentificat în modul stabilit de legislație, care va conține numele și funcția reprezentantului persoanei juridice;

3) datele de identificare juridică (actul de înregistrare a persoanei juridice), adresa și alte date necesare pentru identificarea persoanei juridice;

4) documentele care confirmă identificarea fondatorilor persoanei juridice, pînă la nivelul stabilirii fondatorilor – persoane fizice.

36. O atenție deosebită trebuie acordată în cazul clienților nerezidenți, precum și clienților sau proprietarilor beneficiari care primesc fonduri din străinătate, concomitent ținînd cont de prevederile legislației în vigoare.

37. Pentru clienții și tranzacțiile cu un risc potențial sporit stabilite conform punctului 36 și concomitent ținînd cont de prevederile art.6 alin.(6) și art.14 din Legea nr.190 din 26.07.2007, entitățile raportoare vor stabili măsuri suplimentare de cunoaștere a clienților, care pot include următoarele dar nu se limitează la:

1) aprobarea la un nivel ierarhic superior a începerii sau continuării relației de afaceri cu astfel de clienți și/sau pentru realizarea acestor tranzacții, în special, ce depășesc un anumit nivel valoric prestabil ;

2) solicitarea ca prima tranzacție să se realizeze prin intermediul unui cont deschis la o entitate raportoare, supus unor cerințe de prevenire și combatere a spălării banilor și finanțării terorismului;

3) supravegherea sporită și permanentă a relațiilor de afaceri;

4) adoptarea de măsuri corespunzătoare pentru a stabili/verifica sursa mijloacelor bănești;

5) implementarea sistemelor informaționale adecvate de gestiune a informației, care să permită furnizarea în timp util a informațiilor necesare pentru identificarea, analiza și monitorizarea efectivă a acestor tranzacții, inclusiv luarea măsurilor privind informarea organului abilitat conform legislației. Sistemele informaționale implementate trebuie să evidențieze cel puțin lipsa sau insuficiența documentației corespunzătoare la începerea relației de afaceri, tranzacțiile neobișnuite derulate prin contul clientului și situația agregată a tuturor operațiunilor clientului cu entitatea raportoare;

6) necesitatea ca persoanele împuternicite cu coordonarea activității de prestare a serviciilor clienților respectivi cunosc și acordă o atenție sporită informațiilor provenite de la terțe părți în legătură cu aceste persoane;

7) în cazul persoanelor fizice, verificarea angajării, poziției publice deținute (după caz).

38. În cazurile în care există riscuri reduse, entitățile raportoare pot să aplice măsuri simplificate de cunoaștere a clienților care sînt stabilite astfel încît să le permită acestora respectarea tuturor prevederilor legislației în vigoare, prezentului Regulament și a altor acte normative.

39. Măsurile simplificate de cunoaștere a clienților trebuie să includă obținerea de suficiente informații despre clienți, care să asigure entității raportoare legitimitatea încadrării clienților în categoria de clienți cu grad scăzut de risc de spălare a banilor și finanțare a terorismului conform legislației, monitorizarea operațiunilor acestora pentru detectarea tranzacțiilor suspecte și stabilirea unei proceduri care să permită actualizarea și adecvarea informațiilor deținute despre clienți astfel încît entitatea raportoare să se asigure că aceștia se mențin în respectiva categorie de clienți.

VI. PROCEDURILE PRIVIND MONITORIZAREA CONTINUĂ A CONTURILOR ȘI A TRANZACȚIILOR

40. Procedurile privind monitorizarea continuă a conturilor și a tranzacțiilor includ:

1) determinarea operațiunilor ordinare (specifice) ale clientului;

2) monitorizarea operațiunilor clientului în scopul determinării corespunderii operațiunilor ordinare (specifice) pentru acel client sau pentru clienții din cadrul categoriilor similare;

3) dispunerea de sisteme informaționale manageriale adecvate în scopul prezentării persoanelor responsabile și a analizei centralizate a informației din cadrul tuturor sistemelor necesare pentru identificarea, analiza și monitorizarea eficientă a conturilor clienților cu grad de risc sporit;

4) identificarea de către entitatea raportoare a operațiunilor suspecte, inclusiv a celor ocazionale sau potențiale, precum și a surselor mijloacelor folosite de client în aceste operațiuni.

41. Entitățile raportoare pot controla eficient și pot minimiza riscul lor numai dacă înțeleg corect activitatea clienților lor, determinând operațiunile ordinare (specifice) ale clientului. Fără cunoașterea acestor activități, entitățile raportoare pot comite erori în raportarea tranzacțiilor suspecte către autoritățile de resort.

42. Pentru toate conturile, entitățile raportoare vor dispune de sisteme pentru detectarea activităților sau persoanelor suspecte. Acest lucru poate fi efectuat prin stabilirea limitelor pentru o grupă particulară sau categorie de conturi. O atenție deosebită se va acorda tranzacțiilor care depășesc aceste limite și tranzacțiilor care presupun că clientul efectuează activități neobișnuite sau suspecte. Acestea pot include tranzacții care nu par să aibă un sens economic sau comercial, sau care implică sume mari de bani care nu sînt specifice tranzacțiilor obișnuite sau așteptate ale clientului.

43. În vederea efectuării unei monitorizări adecvate a clienților și tranzacțiilor acestora este necesară solicitarea documentelor justificative care confirmă legalitatea uneia sau altei tranzacții (ca exemplu: contracte, facturi, documente de expediție, certificate de salarii, dări de seamă fiscale, rapoarte de activitate, etc., după caz).

44. Pentru categoria clienților cu un risc potențial sporit este necesar să se monitorizeze toate tranzacțiile derulate prin conturile acestora. Fiecare entitate raportoare va stabili persoanele care se încadrează în această categorie, luînd în considerație tipul clientului (persoană fizică sau juridică), istoria acestuia, țara de origine, poziția publică sau poziția importantă deținută, specificul activității desfășurate de către client, sursa fondurilor după caz, alți indicatori de risc.

45. Pentru clienții cu un risc potențial sporit, entitățile raportoare vor dispune de sisteme de control intern care vor evidenția în timp oportun lipsa sau insuficiența documentației corespunzătoare la deschiderea contului, tranzacțiile neobișnuite derulate prin contul clientului; vor acorda o atenție sporită informațiilor provenite de la terțe părți în legătură cu aceste persoane; vor pune la curent organul executiv cu situația monitorizării conturilor clienților cu risc sporit. Tranzacțiile de mare valoare a acestor clienți se vor aproba la nivelul organului executiv.

VII. PĂSTRAREA DATELOR DESPRE ACTIVITĂȚILE ȘI TRANZACȚIILE PERSOANELOR FIZICE SAU JURIDICE ȘI ALE BENEFICIARULUI EFECTIV

46. Entitățile raportoare vor dispune de proceduri privind deținerea și păstrarea informației, care vor include cel puțin următoarele:

1) menținerea unui registru al clienților identificați pentru o perioadă de cel puțin cinci ani (care va include cel puțin: denumirea sau numele clientului; codul fiscal; numărul contului; data deschiderii; data închiderii);

2) păstrarea tuturor înregistrărilor privind tranzacțiile timp de cel puțin cinci ani după ce a avut loc tranzacția;

3) păstrarea în formă arhivată a conturilor și a dosarelor privind identitatea clienților, inclusiv a documentelor primare și a corespondenței de afacere în decurs de cel puțin cinci ani după ce au fost închise conturile acestora.

47. Entitățile raportoare vor asigura accesul organelor abilitate la documentele și informația cu privire la identificarea și verificarea clienților, a beneficiarului efectiv, precum și privind monitorizarea operațiunilor clienților, inclusiv documentele justificative, în caz de solicitare.

VIII. SISTEMUL DE ASIGURARE A CONFORMĂRII PROGRAMELOR PROPRII DE PREVENIRE ȘI COMBATERE A SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI PE PIAȚA FINANCIARĂ NEBANCARĂ

48. În scopul asigurării respectării programelor proprii de prevenire și combatere a spălării banilor și finanțării terorismului, entitatea raportoare va dispune de:

1) Prevederi speciale ce țin de sistemul de control intern pentru a asigura conformarea continuă în vederea minimizării riscurilor aferente spălării banilor și finanțării terorismului. Acestea trebuie să includă, dar să nu fie limitate la următoarele:

a) procedurile de identificare a operațiunilor limitate și suspecte;

b) monitorizarea clienților care efectuează un volum mare de operațiuni nespecifice activității. În acest scop entitatea raportoare efectuează investigații privind apartenența clienților la grupul supus monitorizării;

c) monitorizarea activităților legate de conturile deschise la entitatea raportoare;

d) proceduri interne privind raportarea tranzacțiilor suspecte.

2) Un serviciu de audit al entității raportoare pentru verificarea conformării programului de prevenire și combatere a spălării banilor și finanțării terorismului, prestat de către personalul entității raportoare sau de o persoană independentă, ale cărui funcții includ cel puțin următoarele:

a) evaluarea independentă a politicilor interne și a procedurilor entității raportoare, inclusiv respectarea cerințelor legislației în vigoare;

b) monitorizarea activității personalului;

c) testarea tranzacțiilor în caz de necesitate;

d) atenționarea organului de conducere privind rezultatele verificării.

3) O persoană cu atribuții de luare a deciziilor, prin atribuirea responsabilității de a asigura că politica și procedurile entității raportoare sînt în conformitate cu cerințele și reglementările în domeniul spălării banilor și finanțării terorismului.

Persoana de răspundere contribuie la implementarea prevederilor programului intern de prevenire și combatere a spălării banilor și finanțării terorismului, în acest scop, fiind abilitată cel puțin cu următoarele atribuții:

a) acordă consultații personalului entității raportoare cu privire la întrebările apărute în timpul realizării programului de prevenire și combatere a spălării banilor și finanțării terorismului, inclusiv la identificarea și examinarea clienților entității raportoare și evaluarea riscului de spălare a banilor proveniți din acțiuni ilegale (criminale) și finanțare a terorismului;

b) ia decizii în baza informației primite;

c) organizează instruirea personalului entității raportoare în problemele contracarării spălării banilor proveniți din acțiuni ilegale (criminale) și finanțării terorismului;

d) întreprinde măsuri privind prezentarea SPCSB a informației în conformitate cu legislația în domeniu;

e) cel puțin o dată pe an prezintă, în scris, organului de conducere al entității raportoare un raport privind rezultatele implementării programului intern de prevenire și combatere a spălării banilor și finanțării terorismului;

f) colaborează cu serviciul de audit al entității raportoare în vederea verificării conformării activității entității raportoare legislației în vigoare în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

g) îndeplinește alte funcții în corespundere cu prezentul Regulament și documentele interne ale entității raportoare.

4) Proceduri adecvate de selectare ce conțin exigențele corespunzătoare la angajarea personalului.

5) Un program de instruire continuu a personalului privind conținutul și conformarea prevederilor programului de prevenire și combatere a spălării banilor și finanțării terorismului. Programul de instruire trebuie să cuprindă toate aspectele procesului de prevenire și combatere a spălării banilor și finanțării terorismului, personalul entității raportoare fiind adecvat instruit. Instruirea personalului trebuie să fie în dependență de nivelul implicării acestuia în procesul de prevenire și combatere a spălării banilor și finanțării terorismului. Cerințele de instruire trebuie să includă cel puțin:

a) instruirea personalului nou referitor la importanța programului intern de prevenire și combatere a spălării banilor și finanțării terorismului și cerințele de bază;

b) instruirea personalului de prima linie referitor la verificarea identității clienților noi, monitorizarea conturilor clienților deja existenți în bază continuă și detectarea indicilor de activitate suspectă;

c) instruiți regulate de actualizare a responsabilității personalului, inclusiv informarea privind noile dezvoltări de domeniu.

6) Normele interne ce prevăd tragerea la răspundere a angajaților care în mod intenționat nu își realizează atribuțiile de serviciu privind raportarea tranzacțiilor suspecte persoanei responsabile, serviciului securității sau direct autorităților de resort și/sau contribuie personal la derularea operațiunilor de spălare a banilor și finanțare a terorismului.

7) Soluții de tehnologii informaționale (IT) eficiente în scopul susținerii programului intern de combatere a spălării banilor și finanțării terorismului. Cerințele funcționale aferente soluțiilor IT vor avea la bază procedurile stabilite în cadrul programului intern.

IX. RAPORTAREA OPERAȚIUNILOR SUSPECTE

49. Entitățile raportoare trebuie să dispună de proceduri clare, aduse la cunoștința întregului personal, care prevăd raportarea de către personal a tuturor tranzacțiilor suspecte aferente unei persoane speciale din organul de conducere al entității raportoare, responsabile pentru acumularea informației și luarea măsurilor contra spălării banilor și finanțării terorismului. De asemenea, trebuie să fie stabilit un anumit lanț de comunicare, atât către conducere, cât și către serviciul de securitate intern pentru raportarea problemelor ce țin de spălarea banilor și finanțarea terorismului.

50. În cazul depistării operațiunilor suspecte, acestea se înregistrează de către entitatea raportoare prin completarea formularelor speciale și/sau prezentarea datelor, conform legislației în vigoare, cu raportarea ulterioară SPCSB în mod discret.

51. Entitatea raportoare informează, după caz, CNPF sau alte organe cu funcții de supraveghere a entităților raportoare în conformitate cu Legea 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.

52. Entitatea raportoare este obligată să informeze imediat SPCSB despre oricare activitate sau tranzacție suspectă, în decurs de pregătire, de realizare sau deja realizată. Datele privind tranzacția suspectă sînt reflectate într-un formular special, care se remite SPCSB în cel mult 24 de ore.

53. Entitatea raportoare completează un formular special pentru tranzacțiile realizate sau în proces de realizare printr-o operațiune în valoare de peste 500 mii lei, precum și cele realizate prin mai multe operațiuni, în decursul a 30 de zile calendaristice, în valoarea menționată. Formularul se remite SPCSB cel tîrziu la data de 15 a lunii imediat următoare lunii de gestiune.

54. Entitatea raportoare sistează la decizia SPCSB executarea operațiunilor suspecte pe un termen indicat în decizie, dar nu mai mare de 5 zile lucrătoare.

55. Entitatea raportoare și angajații acesteia sînt obligați să nu comunice persoanelor fizice sau juridice care efectuează activitatea sau tranzacția ori terților despre transmiterea informației către SPCSB.

X. MĂSURI DE SUPRAVEGHERE

56. În scopul înlăturării deficiențelor constatate la respectarea de către entitățile raportoare a legislației de prevenire și combatere a spălării banilor și finanțării terorismului, CNPF poate dispune următoarele măsuri:

1) solicitarea modificării programelor proprii de prevenire și combatere a spălării banilor și finanțării terorismului;

2) impunerea obligației de aplicare a măsurilor-standard de cunoaștere a clienților pentru produse, operațiuni și/sau clienți în cazul cărora normele interne ale entității raportoare stabilesc aplicarea de măsuri simplificate sau/și impunerea obligației de aplicare a măsurilor suplimentare pentru operațiuni ori clienți în cazul cărora normele interne stabilesc aplicarea de măsuri standard de cunoaștere a clienților;

3) informarea SPCSB și expedierea materialelor respective la identificarea semnelor de spălare a banilor sau de finanțare a terorismului cel tîrziu a doua zi lucrătoare din momentul constatării.

&