BANCA NAŢIONALĂ A MOLDOVEI

H O T Ă R Â R E
cu privire la aprobarea Regulamentului cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea prestatorilor de servicii de plată nebancari

nr. 202 din 09.08.2018
(în vigoare 24.08.2018)

Monitorul Oficial al R. Moldova nr. 321-332 art. 1313 din 24.08.2018

* * *

ÎNREGISTRAT:
Ministerul Justiţiei
al Republicii Moldova
nr.1355 din 21.08.2018

În temeiul art.5 alin.(1) lit.m), art.11 alin.(1) şi art.27 alin.(1) lit.c) din Legea nr.548-XIII din 21 iulie 1995 cu privire la Banca Naţională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr.297-300, art.544), art.5 alin.(2), art.93 alin.(2) lit.b) şi art.94 din Legea cu privire la serviciile de plată şi moneda electronică nr.114 din 18 mai 2012 şi art.13 alin.(3) şi (14), art.15 alin.(2) din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr.58-66, art.133), Comitetul executiv al Băncii Naţionale a Moldovei

HOTĂRĂŞTE:

1. Se aprobă Regulamentul cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea prestatorilor de servicii de plată nebancari, conform anexei.

2. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

PREŞEDINTELE
COMITETULUI EXECUTIV
AL BĂNCII NAŢIONALE A MOLDOVEI **Sergiu CIOCLEA**

Nr.202. Chişinău, 9 august 2018.

Anexă
la Hotărîrea Comitetului executiv
al Băncii Naţionale a Moldovei
nr.202 din 9 august 2018

REGULAMENT
cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea prestatorilor de servicii de plată nebancari

Prezentul Regulament transpune parţial Regulamentul (UE) nr.2015/847 al Parlamentului European şi al Consiliului din 20 mai 2015 privind informaţiile care însoţesc transferurile de fonduri şi de abrogare a Regulamentului (CE) nr.1781/2006 (Text cu relevanţă pentru SEE), publicat în Jurnalul Oficial al Uniunii Europene L 141 din 5 iunie 2015.

Capitolul I
DISPOZIŢII GENERALE

1. Regulamentul cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea prestatorilor de servicii de plată nebancari (în continuare Regulament) stabileşte reguli privind: identificarea şi evaluarea de către prestatorii de servicii de plată nebancari a riscurilor de spălare a banilor şi finanţare a terorismului; elaborarea politicilor şi procedurilor interne; aplicarea cerinţelor de precauţie privind clienţii, inclusiv a măsurilor de precauţie simplificată şi sporită; păstrarea datelor; raportarea activităţilor şi tranzacţiilor suspecte; implementarea sancţiunilor financiare aferente activităţilor teroriste şi de proliferare a armelor de distrugere în masă; organizarea şi realizarea elementelor aferente sistemului de control intern; precum şi alte cerinţe în vederea minimizării riscurilor aferente spălării banilor şi finanţării terorismului.

2. Prestatorul de servicii de plată nebancar (în continuare - Prestatorul) aplică prezentul Regulament în relaţiile de afaceri cu clienţii şi agenţii săi şi la efectuarea tranzacţiilor (plăţilor) atît direct cît şi prin intermediul agenţilor.

3. Termenii şi expresiile utilizate în prezentul Regulament au semnificaţiile prevăzute în Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, Legea nr.114 din 18 mai 2012 cu privire la serviciile de plată şi moneda electronică, Legea nr.548 din 21 iulie 1995 cu privire la Banca Naţională Moldovei, precum şi în actele normative ale Băncii Naţionale a Moldovei şi ale Serviciului Prevenirea şi Combaterea Spălării Banilor aferente domeniului prevenirii şi combaterii spălării banilor şi finanţării terorismului.

De asemenea, în sensul prezentului Regulament se utilizează următorii termeni şi expresii:

identificatorul entităţii juridice (LEI) – un cod de referinţă alfanumeric unic de 20 de caractere, bazat pe standardul ISO 17442, atribuit unei persoane juridice.

[Pct.3 completat prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

Capitolul II
RESPONSABILITĂŢI

4. Prestatorul dispune şi pune în aplicare programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.

5. Prestatorul dispune de sistem de control intern adecvat pentru a identifica, evalua, monitoriza şi înţelege riscurile de spălare a banilor şi finanţare a terorismului. Prestatorul întreprinde măsurile necesare, implicând resurse suficiente, pentru a minimiza riscurile identificate.

6. Prestatorul este responsabil pentru elaborarea, aprobarea, asigurarea aplicării programului intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi conformarea activităţii prevederilor legislaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului.

7. Subdiviziunea de audit internă a prestatorului sau o entitate de audit/auditor extern efectuează, cel puţin anual, evaluarea caracterului adecvat şi a conformităţii activităţii prestatorului cu programul privind prevenirea şi combaterea spălării banilor

şi finanţării terorismului. Rezultatele evaluării se comunică administratorului responsabil al prestatorului, iar, la solicitare, şi Băncii Naţionale a Moldovei.

Capitolul III
CERINŢE FAŢĂ DE PROGRAMUL INTERN PRIVIND PREVENIREA ŞI COMBATEREA SPĂLĂRII BANILOR ŞI FINANŢĂRII TERORISMULUI

8. Programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului reprezintă politici, metode, practici, proceduri şi alte reguli, inclusiv reguli de cunoaştere a clientului, care promovează normele de etică şi profesionalism pe piaţa de prestare a serviciilor de plată şi care previn utilizarea prestatorilor în scopul spălării banilor sau finanţării terorismului de către grupuri criminale organizate sau de către asociaţii acestora. Acest program trebuie să asigure efectuarea operaţiunilor de plată într-un mod sigur şi prudent.
[Pct.8 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

9. Prestatorul elaborează programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în conformitate cu prevederile Legii nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, prezentului Regulament, actelor normative ale Serviciului Prevenirea şi Combaterea Spălării Banilor, emise întru executarea acestei legi ţinînd cont de practica general acceptată în acest domeniu, inclusiv documentele Grupului de Acţiune Financiară Internaţională (GAFI). Programul intern se aprobă de către administratorul prestatorului, responsabil de asigurarea conformităţii politicilor şi procedurilor prestatorului cu cerinţele legale privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.
[Pct.9 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

10. La elaborarea programului intern se iau în consideraţie mărimea, complexitatea, natura şi volumul activităţilor prestatorului, tipurile (categoriile) de clienţi, gradul (nivelul) de risc asociat cu diferiţi clienţi sau categoriile acestora şi operaţiunile desfăşurate de aceştia, agenţii şi filialele prin intermediul cărora îşi desfăşoară activitatea.

11. Programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului va prevedea, fără a se limita la următoarele:

1) obligaţiile administratorului responsabil al prestatorului, care trebuie să includă cel puţin:

a) cunoaşterea criteriilor (indicilor) clienţilor cu grad de risc sporit;

b) aprobarea operaţiunilor semnificative ale clienţilor cu grad de risc sporit;

c) determinarea domeniilor de activitate ale prestatorului vulnerabile riscului spălării banilor şi finanţării terorismului. Domeniile de activitate vulnerabile riscului spălării banilor şi finanţării terorismului pot fi acelea care au tangenţă cu: produsele şi serviciile acordate, operaţiunile efectuate atît direct cît şi prin intermediul agenţilor de plată, conturile de plăţi deschise etc.;

d) remedierea deficienţelor identificate în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, inclusiv raportarea tranzacţiilor suspecte către Serviciul Prevenirea şi Combaterea Spălării Banilor;

e) punerea în aplicare a programului intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, descrierea responsabilităţilor personalului la diferite nivele ierarhice, inclusiv ale celor cu funcţii de conducere de rang superior;

e[1]) determinarea mecanismului de protecţie a persoanelor responsabile de asigurarea conformităţii şi a angajaţilor care raportează încălcări ale legislaţiei privind prevenirea şi combaterea spălării banilor şi finanţării terorismului;

f) punerea în aplicare a procedurilor interne privind accesul într-un timp rezonabil al personalului responsabil la informaţia necesară exercitării obligaţiunilor de serviciu;

2) proceduri de acceptare a clienţilor care stabilesc cel puţin categoriile de clienţi pe care prestatorul îşi propune să-i atragă şi nivelul ierarhic al personalului care aprobă începerea relaţiei de afaceri cu aceştia, în funcţie de gradul de risc asociat, tipurile de produse şi servicii care le sunt furnizate;

3) măsuri de identificare, verificare şi monitorizare a clienţilor şi beneficiarilor efectivi în funcţie de gradul de risc asociat (regulile de cunoaştere a clientului), criteriile şi modul de trecere a clienţilor dintr-o categorie cu un grad de risc în alta;

4) proceduri privind măsurile de precauţie privind clienţii, inclusiv măsurile de precauţie simplificate şi sporite pentru fiecare dintre categoriile de clienţi, produse, servicii sau operaţiuni supuse acestor măsuri şi măsuri de administrare a riscurilor în cazul stabilirii relaţiei de afaceri până la verificarea identităţii clientului şi a beneficiarului efectiv;

5) proceduri de monitorizare a operaţiunilor efectuate de clienţi în scopul depistării operaţiunilor semnificative, complexe şi neordinare, fără un scop legal sau economic clar, a activităţilor şi operaţiunilor suspecte;

5^1) proceduri şi cerinţe privind aplicarea măsurilor de precauţie sporită la efectuarea tranzacţiilor clienţilor rezidenţi cu prestatorii de servicii privind activele virtuale autorizaţi în alte state;

6) măsuri de identificare şi monitorizare a clienţilor şi operaţiunilor efectuate de clienţi cu ţările/jurisdicţiile ce nu dispun de sisteme efective de prevenire şi combatere a spălării banilor şi finanţării terorismului, ori reprezintă un risc sporit datorită nivelului înalt de infracţionalitate şi de corupţie şi/sau sunt implicate în activităţi teroriste;

7) modul de întocmire şi păstrare a informaţiilor, precum şi de stabilire a accesului la acestea;

8) proceduri de raportare internă şi către autorităţile competente privind activităţile şi operaţiunile suspecte de spălare a banilor sau de finanţare a terorismului, ori de nerespectare a legislaţiei incidente în vigoare sau a procedurilor interne;

9) proceduri şi măsuri de verificare a modului de conformare la normele elaborate şi de evaluare a eficienţei acestora;

10) standarde pentru selectare, angajare a personalului şi programe de instruire a acestuia în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

11) proceduri privind identificarea şi analiza riscurilor de spălare a banilor şi finanţare a terorismului, inclusiv măsurile de minimizare a acestora, legate de utilizarea tehnologiilor informaţionale, inclusiv cele noi, procurate sau elaborate în cadrul produselor şi serviciilor oferite de prestator.

[Pct.11 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.11 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

12. Prestatorul revizuieşte (actualizează), ori de cîte ori este necesar, programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, dar cel puţin anual, ţinînd cont de prevederile legislaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului.

Capitolul IV
EVALUAREA RISCURILOR DE SPĂLARE A BANILOR ŞI FINANŢARE A TERORISMULUI. ABORDAREA BAZATĂ PE RISC

13. Prestatorul este obligat să întreprindă acţiuni privind identificarea şi evaluarea riscurilor de spălare a banilor şi de finanţare a terorismului în activitatea sa, ţinînd cont de evaluarea riscurilor de spălare a banilor şi de finanţare a terorismului la nivel naţional, precum şi de criteriile şi factorii stabiliţi de Banca Naţională a Moldovei şi

Serviciul Prevenirea şi Combaterea Spălării Banilor. Rezultatele evaluării în domeniul propriu de activitate a riscurilor de spălare a banilor şi de finanţare a terorismului sunt consemnate într-un raport de evaluare, care se se aprobă şi se actualizează periodic, responsabil de acest proces fiind administratorul responsabil al prestatorului, iar la cerere se prezintă Serviciului Prevenirea şi Combaterea Spălării Banilor şi/sau Băncii Naţionale a Moldovei.
[Pct.13 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

14. Prestatorul, în urma rezultatelor evaluării riscurilor de spălare a banilor şi de finanţare a terorismului, asigură implementarea abordării bazată pe risc pentru ca acţiunile de prevenire şi diminuare a spălării banilor şi finanţării terorismului să fie proporţionale cu riscurile de spălare a banilor şi de finanţare a terorismului identificate în domeniul de activitate.
[Pct.14 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

15. În scopul implementării pct.13, prestatorul efectuează şi actualizează evaluarea riscurilor în domeniul propriu de activitate, cel puţin anual şi după fiecare evaluare a riscurilor de spălare a banilor şi finanţare a terorismului la nivel naţional şi, după caz, la identificarea criteriilor şi factorilor de risc adiţionali de către Banca Naţională a Moldovei şi Serviciul Prevenirea şi Combaterea Spălării Banilor. Acest proces presupune cel puţin:

1) elaborarea unui raport scris prin care se determină ţările sau jurisdicţiile geografice, produsele, clienţii şi operaţiunile cu grad de risc sporit, ponderea şi impactul acestora asupra activităţii sale;

2) întocmirea unui plan de acţiuni în scopul minimizării riscurilor de spălare a banilor şi finanţare a terorismului identificate.
[Pct.15 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

16. Prestatorul identifică şi evaluează riscurile de spălare a banilor şi finanţarea terorismului pînă la:

1) lansarea şi dezvoltarea de produse şi servicii noi;

2) utilizarea tehnologiilor noi sau aflate în dezvoltare, atît pentru produsele şi serviciile noi, cît şi pentru cele existente.

17. În procesul de evaluare a riscurilor de spălare a banilor şi de finanţare a terorismului, prestatorul utilizează diverse surse de informaţii pentru a identifica, gestiona şi diminua riscurile aferente domeniului său de activitate. Aceasta include luarea în considerare a tipologiilor, a indicatorilor de risc, a ghidurilor şi/sau recomandărilor emise de autorităţile competente naţionale şi internaţionale. În identificarea şi evaluarea riscurilor de spălare a banilor şi de finanţare a terorismului la care poate fi expus, prestatorul trebuie să ia în considerare cel puţin următorii factori:

1) natura, amploarea, diversitatea şi complexitatea afacerii;

2) proporţia clienţilor deja identificaţi ca avînd un risc sporit;

3) jurisdicţiile cu care prestatorul face operaţiuni, în special, jurisdicţiile cu o vulnerabilitate sporită datorată unor factori de risc precum: criminalitate înaltă, corupţia, finanţarea terorismului, reglementare şi supraveghere limitată a domeniului de prevenire şi combatere a spălării banilor şi finanţării terorismului;

4) canalele de distribuţie, inclusiv măsura în care prestatorul face operaţiuni direct cu clientul sau prin intermediul agenţilor şi filialelor şi de măsura în care se bazează pe informaţia oferită de părţile terţe pentru a efectua măsurile de identificare a clientului, complexitatea lanţului de plată şi a sistemelor de decontare utilizate între operatori în lanţul de plată, utilizarea tehnologiei şi măsura în care reţelele agentului sunt utilizate;

5) auditul intern şi reglementările interne;

6) volumul şi mărimea tranzacţiilor prestatorului, luând în considerare activitatea obişnuită a acestuia şi profilul clienţilor săi.

Capitolul V
MĂSURI DE PRECAUŢIE PRIVIND CLIENŢII

Secţiunea 1
Proceduri de acceptare a clientului

18. Procedura de acceptare a clientului cuprinde identificarea şi verificarea clientului şi a beneficiarului efectiv al clientului pe baza unor informaţii, date sau documente fiabile şi independente. Aceasta include, de asemenea, înţelegerea scopului şi naturii relaţiei de afaceri şi, în situaţii de risc sporit, obţinerea de informaţii suplimentare.
[Pct.18 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

19. Procedurile de acceptare a clientului vor include mai multe etape în funcţie de gradul de risc al clienţilor. Deciziile de începere, continuare sau încetare a relaţiilor de afaceri cu clienţii cu un grad de risc sporit sunt luate de către administratorul prestatorului responsabil de implementarea şi conformarea cu cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului.

20. Prestatorul nu stabileşte relaţii de afaceri cu persoanele, grupurile sau entităţile implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masă, incluse în lista menţionată la art.34 alin.(11) din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului. Despre refuzul de a stabili relaţii de afaceri cu acestea, prestatorul informează neîntîrziat Serviciul Prevenirea şi Combaterea Spălării Banilor, în termen de cel mult 24 ore, prezentînd toate datele deţinute cu privire la acest caz.

21. Procedurile de acceptare a clientului vor ţine cont de riscurile de spălare a banilor şi finanţare a terorismului identificate de către prestator.

Secţiunea a 2-a
Măsuri de precauţie privind clienţii
[Denumirea secţiunii a 2-a în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

22. Prestatorul de servicii de plată aplică, în funcţie de risc, măsuri de precauţie privind clienţii:

1) la stabilirea relaţiilor de afaceri;

2) la efectuarea tuturor tranzacţiilor ocazionale, inclusiv cu utilizarea mijloacelor electronice, în valoarea de peste 20000 de lei dacă tranzacţia se efectuează printr-o singură operaţiune, precum şi dacă tranzacţiile se efectuează prin una sau mai multe operaţiuni care au legături între ele, în valoare de peste 200000 de lei;

3) dacă există o suspiciune de spălare a banilor sau de finanţare a terorismului, indiferent de orice excepţii, scutiri sau limite stabilite;

4) dacă există îndoieli cu privire la veridicitatea şi precizia datelor de identificare obţinute anterior.
[Pct.22 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

22[1]. În funcţie de gradul de risc implicat, inclusiv ţinând cont de tipul clientului, ţară (jurisdicţie), relaţia de afaceri, produsul/serviciul oferit sau tranzacţia efectuată, reţeaua de distribuţie etc., prestatorul aplică măsuri de precauţie standard, de precauţie simplificată sau sporită.
[Pct.22[1] *introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024*]

23. Prin derogare de la pct.22, pe baza unei evaluări corespunzătoare a riscurilor, care demonstrează existenţa unui risc scăzut de spălare a banilor şi de finanţare a terorismului, prestatorul, cu excepţia cazurilor de răscumpărare sau retragere a numerarului ce depăşeşte suma de 2000 de lei, poate omite aplicarea măsurilor de precauţie privind clienţii referitoare la moneda electronică sau instrumentul de plată preplătit în cazurile de respectare a următoarelor condiţii:

1) valoarea maximă depozitată electronic nu depăşeşte suma de 5000 de lei;

2) valoarea transferurilor lunare nu depăşeşte suma de 5000 de lei, iar pentru instrumentele de plată care pot fi utilizate doar pe teritoriul Republicii Moldova, aceasta poate fi majorată pînă la 10000 de lei;

3) instrumentul de plată este utilizat exclusiv pentru a achiziţiona bunuri şi servicii;

4) instrumentul de plată nu poate fi finanţat cu monedă electronică anonimă (care nu poate fi atribuită unei persoane identificate);

5) emitentul efectuează o monitorizare suficientă a tranzacţiilor sau a relaţiei de afaceri pentru a permite depistarea tranzacţiilor suspecte.

24. La aplicarea măsurilor standard de precauţie privind clienţii în cazurile prevăzute de pct.22, prestatorul obţine cel puţin următoarele informaţii:

1) pentru clienţii - persoane fizice:

a) numele şi prenumele;

b) data şi locul naşterii;

c) cetăţenia şi datele documentului de identitate (IDNP, seria şi numărul, data eliberării, codul organului care l-a eliberat (dacă există) sau alţi indici unici dintr-un act de identitate ce conţine fotografia titularului);

d) adresa de domiciliu şi/sau reşedinţă;

e) numărul de telefon, fax, adresa poştei electronice (e-mail) (dacă există);

f) statutul de rezident/nerezident;

g) ocupaţia, funcţia deţinută şi/sau denumirea/numele angajatorului;

h) sursa venitului;

i) identitatea beneficiarului efectiv;

j) scopul şi natura relaţiei de afaceri sau a tranzacţiei ocazionale (scopul iniţierii relaţiei de afaceri sau al efectuării tranzacţiei ocazionale, tipul produsului şi serviciului solicitat, tipul tranzacţiilor, volumul activelor preconizate pentru a fi depuse, volumul şi frecvenţa tranzacţiilor preconizate, potenţiala durată a relaţiei de afaceri;

2) pentru clienţii - persoane juridice, întreprinzători individuali şi fiducii sau construcţii juridice similare:

a) denumirea, forma juridică de organizare, actul de constituire, actul fiduciar şi actul privind înregistrarea de stat;

b) sediul/adresa de activitate;

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

d) adresa de corespondenţă, alta decît sediul (dacă există);

e) identitatea persoanei fizice împuternicită de a gestiona contul, legalitatea împuternicirilor (în cazul lipsei unei astfel de persoane, se indică administratorul persoanei juridice);

f) identitatea beneficiarului efectiv a persoanei juridice;

f^1) identitatea persoanelor care deţin poziţii de management superior, precum şi împuternicirile acestora de reprezentare;

g) drepturi si obligaţiunile organului de conducere de gestionare a companiei care reies din documentele primare de înregistrare sau actul de constituire;

g^1) pentru fiducii şi construcţiile juridice similare, identitatea fondatorului, administratorului, protectorului (dacă există), beneficiarilor sau clasele de beneficiari şi

a oricăror alte persoane care exercită în ultimă instanţă un control efectiv (în cazul altor tipuri de construcţii juridice similare fiduciilor – identitatea persoanelor care au poziţii echivalente);".

h) natura şi scopul activităţii, legitimitatea acestora;

i) scopul şi natura relaţiei de afaceri sau a tranzacţiei ocazionale (scopul iniţierii relaţiei de afaceri sau al efectuării tranzacţiei ocazionale, tipul produsului şi serviciului solicitat, tipul tranzacţiilor, volumul activelor preconizate pentru a fi depuse, volumul şi frecvenţa tranzacţiilor preconizate, potenţiala durată a relaţiei de afaceri).

[Pct.24 modificat *prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.24 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

25. Prestatorul identifică beneficiarul efectiv al clientului şi aplică măsuri rezonabile şi bazate pe risc pentru verificarea identităţii lui, utilizând documente, informaţii şi date obţinute din surse sigure, astfel încît să aibă certitudinea că ştie cine este beneficiarul efectiv şi înţelege structura proprietăţii şi structura de control a clientului. Pentru identificarea beneficiarului efectiv prestatorul aplică cel puţin cerinţele descrise la pct.24 subpct.(1).

[Pct.25 modificat prin Hot.BNM nr.38 din 11.*03.2021, în vigoare 02.07.2021]*

26. La identificarea beneficiarului efectiv al clientului - persoană juridică, inclusiv în cazul cînd acesta are o structură de proprietate complexă (persoană juridică a căror proprietari direcţi nu sunt persoane fizice), prestatorul determină beneficiarul efectiv în baza documentelor de înregistrare corespunzătoare. Dacă nu există motive de suspiciune privind tăinuirea informaţiei privind beneficiarul efectiv şi în cazul în care după epuizarea tuturor mijloacelor posibile stabilite conform pct.25, se constată că nici o persoană nu întruneşte condiţiile legale pentru a fi identificată în calitate de beneficiar efectiv (nici o persoană fizică nu este acţionar majoritar sau nu exercită controlul direct sau indirect prin alte modalităţi), cu titlu de excepţie, persoana fizică care ocupă funcţia de administrator al clientului este considerată beneficiar efectiv. Prestatorul păstrează toată informaţia şi documentele acumulate în procesul de determinare a calităţii de beneficiar efectiv al clientului persoană juridică, inclusiv cele care demonstrează epuizarea tuturor mijloacelor posibile de identificare, şi le prezintă, la cerere, Băncii Naţionale a Moldovei şi Serviciului Prevenirea şi Combaterea Spălării Banilor. La identificarea beneficiarului efectiv al persoanelor juridice cu scop lucrativ (comercial), organizaţiilor necomerciale, al fiduciilor sau construcţiilor juridice similare sau al altor tipuri de persoane juridice (inclusiv care administrează şi distribuie fonduri), prestatorul va ţine cont de criteriile de identificare stabilite la art.52 din Legea nr.308/2017 privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi de Ghidul Serviciului Prevenirea şi Combaterea Spălării Banilor privind identificarea beneficiarului efectiv.

[Pct.26 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.26 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

27. Atunci când clientul sau deţinătorul pachetului de control este o societate ale cărei valori mobiliare sunt tranzacţionate pe o piaţă reglementată/ sistem multilateral de tranzacţionare care impune cerinţe de divulgare a informaţiilor, fie prin norme bursiere, fie prin legislaţia aplicabilă, pentru a asigura transparenţa adecvată a beneficiarului efectiv, sau este o filială cu capital majoritar al unei astfel de societăţi nu este necesară identificarea şi verificarea identităţii oricărui dintre acţionari sau beneficiari efectivi ai acestor societăţi. Prestatorul obţine datele de identificare relevante din registre publice, de la client sau din alte surse sigure.

[Pct.27 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

28. Prestatorul determină dacă persoana care deschide contul de plăţi sau iniţiază o relaţie de afaceri activează în numele său (declaraţia persoanei privind beneficiarul efectiv), iar în cazul în care deschiderea contului de plăţi sau iniţierea relaţiei de afaceri este efectuată de către persoana împuternicită, prestatorul solicită procura, legalizată în modul stabilit de legislaţie. Prestatorul aplică măsuri de identificare a persoanei împuternicite, precum şi evaluează necesitatea aplicării măsurilor de precauţie sporită, în conformitate cu prevederile prezentului Regulament.

29. La identificarea clientului, prestatorul verifică informaţia prezentată care se referă atît la client, cît şi la beneficiarul efectiv.

30. Prestatorul verifică identitatea clientului şi a beneficiarului efectiv pînă la stabilirea relaţiei de afaceri sau efectuării unei operaţiuni prevăzute la pct.22 subpct.(2).

[Pct.30 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

31. În vederea verificării informaţiei prezentate la identificarea clienţilor şi a beneficiarilor efectivi, prestatorul utilizează documente, date şi informaţii obţinute din surse sigure şi independente. Măsurile aplicate trebuie să fie proporţionale riscului pe care clientul şi tipurile de documente prezentate le impun. În acest scop, prestatorul utilizează proceduri documentare şi nedocumentare de verificare:

1) pentru clienţii - persoane fizice:

a) confirmarea identităţii clientului sau beneficiarului efectiv dintr-un act oficial neexpirat, care includ o fotografie a titularului (de exemplu, buletin de identitate, paşaport, permis de şedere etc.);

b) confirmarea datei şi locului de naştere dintr-un document oficial – de exemplu, certificatul de naştere, buletin de identitate, paşaport, permis de şedere, etc;

c) confirmarea validităţii documentelor de identitate oficiale furnizate de către o persoană autorizată (de exemplu notari, ambasade etc.);

d) confirmarea adresei de reşedinţă– prin solicitarea facturilor pentru serviciile comunale, a actelor privind plata impozitelor, a informaţiei de la autorităţile publice sau de la alte persoane;

e) confirmarea informaţiei prezentate după deschiderea contului – prin contactarea clientului prin telefon sau remiterea unei scrisori pentru confirmarea informaţiei prezentate, fax sau e-mail (dacă există);

f) verificarea referinţei furnizate de alt prestator/bancă;

2) pentru clienţii - persoane juridice, întreprinzători individuali şi fiducii sau construcţii juridice similare – prin orice metodă corespunzătoare în funcţie de gradul de risc, astfel încît prestatorul să se asigure de veridicitatea informaţiei, cum ar fi:

a) verificarea existenţei 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: avocaţi, contabili, etc).

b) obţinerea unei copii a actului de constituire sau memorandumului de asociere, contractului de parteneriat, actului fiduciar;

c) verificarea informaţiei despre client în bazele de date privind relaţiile de afaceri existente;

d) analiza situaţiei financiare, dacă este cazul;

e) efectuarea unei verificări şi/sau investigaţii individuale sau prin intermediul altei persoane pentru determinarea, existenţei procesului de insolvabilitate sau lichidare, vînzare sau remedierea altor probleme financiare potenţiale;

f) obţinerea referinţei unui prestator/bancă cu care clientul a avut anterior relaţii de afaceri, dacă există;

g) contactarea clientului prin telefon sau fax, prin intermediul serviciilor poştale sau e-mail, verificarea informaţiei plasate pe pagina web a clientului, dacă există, sau

efectuarea unei vizite pe teren la sediul sau la altă adresa indicată de persoana juridică şi întreprinzătorul individual;

3) pentru beneficiarul efectiv - măsurile prevăzute la subpct.1);

4) în cazul în care o persoană este împuternicită în numele clientului să deschidă cont sau să efectueze tranzacţii, prestatorul verifică identitatea acesteia, precum şi identitatea persoanei în numele căreia activează, utilizînd aceleaşi proceduri descrise în prezentul Regulament.

[*Pct.31 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.31 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

32. Documentele prezentate în vederea identificării clientului şi a beneficiarului efectiv, precum şi în vederea verificării identităţii acestora, trebuie să fie valabile la data prezentării lor, iar copiile acestora se stochează/arhivează de către prestator corespunzător procedurilor interne stabilite. Documentele se prezintă de către client în original sau în copie (fotocopie) legalizate conform legislaţiei aplicabile. În cazul prezentării documentelor în copie (fotocopie) care nu sunt legalizate în modul corespunzător, prestatorul solicită prezentarea originalelor documentelor pentru coroborarea informaţiei şi datelor prezentate. În cazul identificării şi verificării identităţii clientului la distanţă, prestatorul solicită şi obţine informaţiile şi documentele necesare în conformitate cu reglementările Băncii Naţionale a Moldovei privind cerinţele pentru identificarea şi verificarea identităţii clienţilor prin intermediul mijloacelor electronice.
[Pct.32 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

33. Pe parcursul relaţiei de afaceri prestatorul revizuieşte şi actualizează informaţia cu privire la identificarea clienţilor şi a beneficiarilor efectivi în funcţie de riscul asociat. Acesta actualizează informaţia la necesitate, luând în considerare factorii relevanţi, dar cel puţin, pentru clienţii cu grad de risc sporit - anual, pentru clienţii cu grad de risc mediu – o dată la 2 ani, iar pentru cei cu grad de risc scăzut - o dată la 3 ani. Factorii relevanţi care pot determina necesitatea actualizării informaţiei includ neaplicarea anterioară a măsurilor de identificare, perioada aplicării acestora, gradul de adecvare a datelor obţinute, noi cerinţe normative privind măsurile de precauţie şi/sau schimbarea circumstanţelor relevante privind clientul.
[Pct.33 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

Secţiunea a 3-a
Măsuri de monitorizare a activităţilor şi operaţiunilor

34. Prestatorul trebuie să adapteze amploarea măsurilor de monitorizare a activităţilor şi operaţiunilor clienţilor în conformitate cu evaluarea instituţională a riscurilor şi profilurilor de risc individuale ale clienţilor. Monitorizarea sporită este aplicată pentru situaţii cu risc înalt. Sistemele de monitorizare trebuie revizuite periodic, dar nu mai rar de o dată pe an.

35. Operaţiunile iniţiate/efectuate de către agenţii prestatorului trebuie să fie monitorizate periodic în aceleaşi condiţii ca şi operaţiunile prestatorului. Monitorizarea trebuie efectuată de către prestator individual sau în colaborare cu agentul respectiv, pe baza unui acord încheiat şi sub controlul prestatorului.

36. Prestatorul care prestează servicii prin intermediul agenţilor de plată trebuie să îi includă în programul intern de prevenire şi combatere a spălării banilor şi finanţării terorismului şi să efectueze monitorizarea lor în vederea corespunderii cu programul prestatorului.

37. Prestatorul monitorizează continuu activităţile, operaţiunile clientului sau relaţia de afaceri cu acesta. Acţiunile de monitorizare continuă cuprind:

1) determinarea operaţiunilor ordinare (specifice) ale clientului;

2) examinarea minuţioasă a tranzacţiilor pe parcursul relaţiei de afaceri pentru a avea siguranţa că acestea sunt în corespundere cu informaţia disponibilă la prestator, cu activitatea şi riscul asociat clientului. Examinarea operaţiunilor presupune cel puţin ca prestatorul să dispună de mecanisme şi soluţii, inclusiv automatizate, pentru depistarea activităţilor, operaţiunilor şi persoanelor suspecte. Depistarea activităţilor, operaţiunilor şi persoanelor suspecte poate fi realizată prin stabilirea limitelor valorice ale tranzacţiilor pentru o grupă particulară sau categorie de operaţiuni. O atenţie deosebită se acordă operaţiunilor care depăşesc aceste limite valorice şi operaţiunilor ce nu au scop economic clar;

3) verificarea faptului dacă documentele şi informaţiile acumulate în procesul monitorizării clienţilor şi tranzacţiilor sunt actualizate şi relevante, inclusiv pentru categoriile clienţilor sau relaţiile de afaceri cu grad de risc sporit;

4) identificarea activităţilor şi operaţiunilor suspecte, inclusiv a celor potenţiale, precum şi a surselor mijloacelor băneşti utilizate în aceste activităţi şi operaţii.

5) raportarea către persoana responsabilă a informaţiei necesare pentru identificarea, analiza şi monitorizarea eficientă a conturilor de plăţi şi operaţiunilor clienţilor, inclusiv pentru clienţii cu grad de risc sporit;

6) monitorizarea în timp real a tuturor tranzacţiilor (plăţilor) efectuate de clienţi sau potenţialii clienţi pentru a depista persoanele, grupurile sau entităţile implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masă, inclusiv în scopul identificării plăţilor pentru prevenirea efectuării acestora cu încălcarea sancţiunilor, interdicţiilor sau altor restricţii aplicate.

38. Administratorul responsabil al prestatorului are responsabilitatea pentru documentarea, păstrarea şi comunicarea cu personalul relevant despre rezultatele monitorizării, precum şi orice probleme care apar şi soluţionarea lor.

39. Prestatorul se abţine de la executarea activităţilor şi operaţiunilor cu mijloace financiare, pentru un termen de pînă la 5 zile lucrătoare, la stabilirea suspiciunilor pertinente care pot indica despre acţiuni de spălare a banilor, infracţiuni asociate acestora, acţiuni de finanţare a terorismului sau a proliferării armelor de distrugere în masă, în curs de pregătire, de tentativă, de realizare ori deja realizate.

40. Prestatorul aplică cerinţele pct.39 la solicitarea Serviciului Prevenirea şi Combaterea Spălării Banilor sau din proprie iniţiativă. La aplicarea cerinţelor pct.39 din proprie iniţiativă, prestatorul informează imediat, dar nu mai tîrziu de 24 de ore, Serviciul Prevenirea şi Combaterea Spălării Banilor despre decizia luată.

41. Prestatorul în cazul aplicării cerinţelor pct.39, poate solicita clientului furnizarea datelor şi informaţiei suplimentare, inclusiv a documentelor confirmative privind operaţiunile efectuate, în scopul aplicării corespunzătoare a măsurilor de precauţie, şi în special, pentru înţelegerea scopului şi a naturii relaţiei de afaceri, precum şi sursa bunurilor implicate.

42. Măsurile aplicate conform cerinţelor pct.39 încetează din oficiu în baza permisiunii scrise şi confirmate de Serviciul Prevenirea şi Combaterea Spălării Banilor. Dispoziţiile prezentului punct nu exonerează prestatorul de la obligaţiile stabilite în art.5 alin.(3) din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului şi programul intern, elaborat conform pct.11.

43. Prestatorul este obligat:

1) să nu efectueze nicio activitate sau tranzacţie, inclusiv printr-un cont de plăţi şi să nu stabilească nicio relaţie de afaceri, în cazul în care nu poate asigura respectarea cerinţelor pct.24, 25, 30, 31 şi 37;

2) în cazul unei relaţii de afaceri existente, să înceteze relaţia de afaceri în cazul în care prestatorul nu poate asigura respectarea cerinţelor pct.24,25, 30, 31 şi 37;

2^1) atunci când există o suspiciune privind spălarea banilor sau finanţarea terorismului şi prestatorul consideră în mod rezonabil că respectarea cerinţelor pct.24,

25, 30, 31 şi 37 va determina încălcarea obligaţiei de nedivulgare, să nu finalizeze procesul de aplicare a măsurilor de precauţie în raport cu potenţialul client;

3) să transmită formularele speciale privind raportarea activităţilor şi tranzacţiilor suspecte, în circumstanţele indicate la sbp.(1), (2) şi (2^1) Serviciului Prevenirea şi Combaterea Spălării Banilor în conformitate cu art.11 din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului. În acest caz, prestatorul este în drept să nu explice clientului motivul refuzului.

[Pct.43 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

44. Prestatorul nu va deschide şi ţine conturi anonime sau conturi pe nume fictive, nu va emite şi accepta plăţi efectuate prin utilizarea de carduri preplătite anonime, nu va stabili sau nu va continua o relaţie de afaceri cu un partener fictiv (instituţie fictivă) sau cu un partener (instituţie) despre care se ştie că permite altui partener fictiv (instituţie fictivă) să utilizeze conturile sale sau care pune la dispoziţie pentru clienţii săi conturi anonime.

[Pct.44 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

44^1. Prestatorul nu va deschide şi ţine conturi pentru/ la prestatorii de servicii privind activele virtuale din alte state, precum şi conturi clienţilor nerezidenţi în scopul efectuării tranzacţiilor în/din adresa prestatorilor de servicii privind activele virtuale din alte state.

[Pct.44^1 *introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

Secţiunea a 4-a
Informaţia obţinută de la persoanele terţe

45. Prestatorul poate să recurgă la informaţia care o deţin persoanele terţe, pentru a realiza măsurile prevăzute la pct.24, 25, 30 şi 31 în următoarele condiţii:

1) persoanele terţe reprezintă entităţile raportoare prevăzute la art.4 alin.(1) din Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, rezidente sau cele similare situate într-o altă ţară (jurisdicţie), care sunt supravegheate adecvat şi îndeplinesc cerinţe similare celor prevăzute de Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, inclusiv privind măsurile de precauţie privind clienţii şi de păstrare a datelor,, şi;

2) persoanele terţe nu sunt rezidente în jurisdicţiile cu risc sporit.

[Pct.45 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.45 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

45^1. Prestatorii care apelează la persoane terţe dispun de proceduri eficiente pentru a se asigura că obţin de la acestea, imediat:

1) toate informaţiile necesare aferente măsurilor prevăzute la pct.24, 25, 30 şi 31;

2) la cerere, copiile datelor de identificare şi alte documente aferente măsurilor prevăzute la pct.24, 25, 30 şi 31, inclusiv datele obţinute prin intermediul mijloacelor electronice.

[Pct.45^1 *completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.45^1 *introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

46. Prestatorul are responsabilitatea finală privind realizarea măsurilor prevăzute la pct.24, 25, 30 şi 31 în cazul în care apelează la persoane terţe.

[Pct.46 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

Capitolul VI

MĂSURI DE PRECAUŢIE SIMPLIFICATE PRIVIND CLIENŢII

47. Prestatorul aplică măsuri de precauţie simplificată privind clienţii atunci cînd, prin natura lor, pot prezenta un risc redus de spălare a banilor sau de finanţare a terorismului.

48. Măsurile de precauţie simplificată privind clienţii cuprind măsurile de precauţie privind clienţii prevăzute la pct.22 şi 23 în cadrul unei proceduri simplificate aferente riscului redus de spălare a banilor şi de finanţare a terorismului, care include:

1) limitarea obţinerii informaţiilor cu privire la datelor de identificare a clienţilor, prin aplicarea unei proceduri simplificate de verificare a identităţii clientului;

2) limitarea obţinerii de informaţii specifice sau efectuarea de măsuri specifice privind scopul şi natura relaţiei de afaceri şi deducerea scopului şi naturii relaţiei de afaceri din tipul tranzacţiilor sau a relaţiei de afaceri stabilită;

3) verificarea identităţii clientului şi a beneficiarului efectiv după stabilirea relaţiei de afaceri, atunci când aceasta este necesar pentru a nu întrerupe practicile comerciale normale;

4) reducerea frecvenţei actualizărilor datelor de identificare a clienţilor în cazul unei relaţii de afaceri stabilite;

5) reducerea gradului şi a amplorii monitorizării şi controlului continuu a operaţiunilor, bazate pe o limită a sumei rezonabilă.

În cazul în care identitatea clientului şi beneficiarului efectiv nu a fost verificată până la stabilirea relaţiei de afaceri, prestatorul asigură realizarea acestei măsuri cât mai curând posibil după contactul iniţial, dar nu mai târziu de o lună. Până la finalizarea măsurilor de verificare, prestatorul nu permite efectuarea tranzacţiilor prin intermediului contului sau stabileşte condiţiile specifice de utilizare a acestuia (limite valorice, tipuri de servicii etc.), în conformitate cu politicile şi procedurile interne.

[Pct.48 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.48 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

49. Prestatorul, în baza evaluării proprii şi în corespundere cu rezultatele evaluării riscurilor la nivel naţional, stabileşte factorii care generează riscuri reduse de spălare a banilor şi de finanţare a terorismului şi care determină necesitatea aplicării măsurilor de precauţie simplificată privind clienţii. Aceştia includ cel puţin următorii factori:

1) relaţiile de afaceri/clienţii şi/sau produsele/serviciile stabilite în Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului;

2) sume reduse pentru plăţi, depunere sau retragere de numerar;

3) număr de plăţi limitate, de depunere sau răscumpărare, inclusiv retragerea numerarului într-o anumită perioadă de timp;

4) cont de plăţi care poate stoca doar valori limitate de fonduri;

5) produsul sau serviciul poate fi folosit doar la nivel naţional;

6) produsul sau serviciul este acceptat de un număr limitat de agenti, cu a căror activitate prestatorului este familiarizat;

7) mijloacele băneşti sunt acceptate ca mijloc de plată pentru tipuri limitate de servicii sau produse cu risc scăzut;

8) produsul este disponibil numai pentru anumite categorii de clienţi, de exemplu beneficiari de prestaţii sociale sau membri ai personalului unei companii care foloseşte produsul pentru a acoperi cheltuielile corporative.

Prestatorul, în baza evaluării riscurilor de spălare a banilor şi de finanţare a terorismului la nivel naţional, precum şi în baza criteriilor şi factorilor stabiliţi de către organul de supraveghere, acumulează informaţii suficiente pentru a identifica dacă clientul, tranzacţiile sau relaţiile de afaceri întrunesc condiţiile menţionate mai sus.

[Pct.49 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

49[1]. Pe baza unei evaluări corespunzătoare a riscurilor, care demonstrează existenta unui risc scăzut de spălare a banilor şi de finanţare a terorismului, pentru operaţiunile de achiziţionare a bunurilor sau serviciilor, prestatorul, cu excepţia cazurilor de răscumpărare sau retragere în numerar a valorii monetare a monedei electronice şi a cazurilor de operaţiuni de plată la distanţă care depăşesc 1000 lei pe operaţiune, poate aplica măsuri de precauţie simplificată referitoare la moneda electronică în cazurile de respectare a următoarelor condiţii:

a) valoarea maximă depozitată electronic nu depăşeşte suma de 3000 de lei;

b) valoarea transferurilor lunare nu depăşeşte suma de 3000 de lei;

c) emitentul (prestatorul) efectuează o monitorizare suficientă a tranzacţiilor sau a relaţiei de afaceri pentru a permite depistarea tranzacţiilor suspecte.

[Pct.49[1] introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

50. Prestatorul nu va aplica măsuri de precauţie simplificate în cazul existenţei suspiciunii cu privire la spălarea banilor sau finanţarea terorismului.

Capitolul VII
MĂSURI DE PRECAUŢIE SPORITE PRIVIND CLIENŢII

51. În vederea aplicării legislaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, prestatorul stabileşte categoriile clienţilor, activităţile şi operaţiunile ce prezintă un grad de risc sporit pe baza unor indicatori stabiliţi în funcţie de volumul operaţiunilor efectuate, tipul serviciilor solicitate, tipul activităţii desfăşurate, circumstanţele economice, reputaţia ţării de origine a clientului, plauzibilitatea explicaţiilor oferite de client, limitele valorice prestabilite pe categorii de operaţiuni.

52. În baza evaluării proprii, prestatorul stabileşte factorii care generează riscuri sporite şi care determină necesitatea aplicării măsurilor de precauţie sporită privind clienţii. Factorii care generează riscuri sporite sunt:

1) relaţiile de afaceri/clienţii şi/sau produsele/serviciile stabilite în Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului;

2) produsele sau serviciile care permit efectuarea de operaţiuni în valori mari sau nelimitate de mijloace băneşti;

3) operaţiunea este în numerar;

3[1]) clienţii şi tranzacţiile efectuate în/din adresa prestatorilor de servicii privind activele virtuale autorizaţi în alte state;

4) operaţiunile sunt efectuate de la unul sau mai mulţi plătitori din diferite ţări la un beneficiar local;

5) clientul efectuează operaţiuni pentru altcineva (în numele altei persoane);

6) tranzacţiile efectuate nu au niciun sens economic;

7) clientul efectuează întotdeauna tranzacţii sub limita stabilită de raportare;

8) utilizarea serviciului de către client este neobişnuită, de exemplu trimite sau primeşte bani către sau de la sine sau trimite fonduri imediat după primirea acestora;

9) clientul pare să ştie puţin sau este reticent să furnizeze informaţii despre beneficiar;

10) cîţiva dintre clienţii prestatorului transferă mijloace băneşti aceluiaşi beneficiar sau par să aibă aceleaşi informaţii de identificare, de exemplu adresa sau numărul de telefon;

11) operaţiunea nu este însoţită de informaţiile necesare despre plătitor sau beneficiar;

12) mijloacele băneşti trimise sau primite sunt în contradicţie cu venitul clientului (dacă este cunoscut);

13) partenerii de afaceri din jurisdicţii străine;

14) alţi factori identificaţi în cadrul evaluării riscurilor şi de către organele de supraveghere.

[Pct.52 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

53. Prestatorul aplică măsuri de precauţie sporită privind clienţii, suplimentar celor prevăzute în pct.24, în situaţiile care, prin natura lor, pot prezenta un risc sporit de spălare a banilor sau de finanţare a terorismului, cel puţin prin:

1) obţinerea informaţiei suplimentare despre client şi beneficiarul efectiv (genul de activitate, volumul activelor, cifra de afacere, altă informaţie disponibilă din surse publice, internet), precum şi actualizarea frecventă a datelor de identificare ale clientului şi beneficiarului efectiv;

2) obţinerea informaţiei suplimentare despre natura şi scopul relaţiei de afaceri;

3) obţinerea informaţiei despre sursa mijloacelor băneşti şi a averii clientului;

4) obţinerea informaţiei despre scopul activităţii sau operaţiunii în curs de pregătire, de realizare sau deja realizate;

5) obţinerea aprobării de către administrator a iniţierii sau continuării relaţiei de afaceri;

6) monitorizarea sporită şi permanentă a relaţiei de afaceri, prin creşterea frecvenţei controalelor aplicate şi selectarea tipurilor de tranzacţii ce necesită examinare suplimentară şi prin solicitarea de informaţii suplimentare ce confirmă legalitatea operaţiunilor şi corespunderea acestora genului de activitate declarat;

7) implementarea sistemelor informatice specializate în scopul asigurării eficienţei gestiunii informaţiei cu referire la identificarea, analizarea şi monitorizarea clienţilor şi tranzacţiilor acestora, precum şi raportarea către Serviciul Prevenirea şi Combaterea Spălării Banilor a tranzacţiilor suspecte de spălare a banilor şi finanţare a terorismului;

8) atenţionarea clienţilor ale căror activităţi sau operaţiuni impun un risc sporit de spălare a banilor şi finanţare a terorismului despre necesitatea sporirii măsurilor de cunoaştere a partenerilor de afaceri;

9) în cazul relaţiilor trasnfrontaliere, limitarea sau încetarea desfăşurării relaţiei de afaceri sau efectuării tranzacţiilor, în cazul constatării aplicării neadecvate şi nerespectării cerinţelor de prevenire şi combatere a spălării banilor şi finanţării terorismului de către instituţia parteneră/corespondentă;

10) măsuri suplimentare prevăzute la pct.53^1 - 56^2.

[Pct.53 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.53 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

53^1. În relaţiile de afaceri cu clienţii rezidenţi care efectuează tranzacţii în/din adresa prestatorilor de servicii privind activele virtuale autorizaţi în alte state, prestatorul:

1) deschide conturi speciale pentru clienţii rezidenţi pentru efectuarea acestor tipuri de tranzacţii;

2) nu admite efectuarea tranzacţiilor cu un volum ce depăşeşte cumulativ echivalentul a 50000 de lei pe parcursul unei luni pentru fiecare client rezident în parte;

3) nu admite efectuarea tranzacţiilor ocazionale de acest tip;

4) implementează soluţii IT specializate în scopul monitorizării sporite a acestor tipuri de tranzacţii, inclusiv pentru stabilirea sursei bunurilor implicate şi asigurarea trasabilităţii tranzacţiilor.

[Pct.53^1 introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

54. În cazul în care clientul nu se prezintă personal la identificare (de exemplu, în cazul relaţiilor prin corespondenţă sau prin telefon, e-mail, internet sau alte mijloace

electronice), prestatorul aplică măsuri de precauţie sporită prin utilizarea de mecanisme de tipul semnăturii electronice, a metodelor biometrice, cheilor de sesiune etc. Cu ocazia primei vizite a clientului la prestator, se solicită documentele şi informaţiile conform cerinţelor prezentului Regulament. Suplimentar, prestatorul aplică una sau mai multe din următoarele măsuri:

1) 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;

2) ia măsuri de protecţie a autenticităţii documentelor în formă electronică transmise prestatorului;

3) utilizează informaţia prezentată de un partener (prestator, agent, bancă) în care clientul are deschis un cont şi care aplică cel puţin aceleaşi măsuri de cunoaştere a clientului şi este supusă unei supravegheri efective;

4) solicită ca prima plată să fie efectuată în numele clientului printr-un cont deschis la alt prestator/bancă, care aplică cel puţin aceleaşi măsuri de cunoaştere a clientului şi este supusă unei supravegheri efective, la necesitate;

5) stabilirea şi menţinerea unei modalităţi de contact cu clientul, independentă de modalitatea prin care sunt realizate operaţiunile cu clientul la distanţă.

55. În relaţiile cu instituţiile corespondente, prestatorul acumulează informaţii suficiente despre partenerul său pentru a înţelege pe deplin sfera de activitate a acestuia. În acest scop prestatorul:

1) obţine cel puţin informaţiile privind:

a) organele de conducere ale instituţiei corespondente, activităţile cele mai importante, locul desfăşurării acestora şi măsurile aplicate de aceasta în vederea prevenirii şi combaterii spălării banilor şi finanţării terorismului;

b) scopul deschiderii contului de plăţi;

c) reputaţia instituţiei corespondente, inclusiv dacă aceasta a constituit subiectul unei investigări sau măsuri de remediere legate de spălare a banilor sau finanţare a terorismului, din sursele disponibile public;

2) evaluează cît de adecvate şi eficiente sunt politicile instituţiei corespondente privind prevenirea şi combaterea spălării banilor şi finanţării terorismului;

3) stabileşte relaţia corespondenţă după obţinerea aprobării de către administratorul responsabil al prestatorului;

4) stabileşte documentar responsabilităţile în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului în relaţie cu instituţia corespondentă, precum şi faptul că instituţia corespondentă verifică identitatea clienţilor săi, dispune de reguli eficiente de cunoaştere a clientului;

5) realizează acorduri prin care i se permite să verifice procedurile urmate de instituţia corespondentă în vederea cunoaşterii clienţilor şi să transmită/primească, la solicitare, documente şi informaţii aferente clienţilor, activităţii şi operaţiunilor acestora.

56. În tranzacţiile sau în relaţiile de afaceri cu persoanele expuse politic, cu membrii de familie ai persoanelor expuse politic şi cu persoanele cunoscute ca fiind asociaţi apropiaţi ai persoanelor expuse politic, prestatorul, suplimentar la măsurile de precauţie prevăzute la pct.24, întreprind măsuri ce cuprind:

1) elaborarea şi implementarea sistemelor adecvate de gestionare a riscurilor, inclusiv a procedurilor bazate pe evaluarea riscurilor, pentru a stabili dacă un client, potenţial client sau beneficiarul efectiv al unui client este persoană expusă politic;

2) obţinerea aprobării administratorului prestatorului la stabilirea sau continuarea relaţiilor de afaceri cu astfel de clienţi;

3) adoptarea măsurilor adecvate privind stabilirea sursei averii şi a bunurilor implicate în relaţia de afaceri sau în operaţiunile cu astfel de clienţi;

4) efectuarea monitorizării sporite şi continue a relaţiei de afaceri.

În relaţiile de afaceri sau în cazul tranzacţiilor cu persoanele expuse politic, cu membrii de familie ai persoanelor expuse politic şi cu persoanele cunoscute ca fiind asociaţi apropiaţi ai persoanelor expuse politic, prestatorul aplică măsurile de precauţie sporită prevăzute la subpunctele 1) – 4) pentru o perioadă de 12 luni de la încetarea exercitării funcţiei publice importante la nivel naţional sau internaţional. După expirarea acestei perioade, în baza unei evaluări a riscului care determină dacă persoana respectivă mai prezintă sau nu riscuri aferente persoanelor expuse politic, prestatorul aplică măsurile de precauţie în funcţie de riscul identificat.
[Pct.56 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.56 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

56[1]. În relaţiile de afaceri sau în cazul tranzacţiilor cu clienţii şi instituţiile financiare din ţările (jurisdicţiile) cu risc sporit desemnate/ monitorizate de GAFI, pe lângă măsurile de precauţie sporită prevăzute de prezentul capitol, prestatorul aplică suplimentar, în conformitate cu acţiunile solicitate de GAFI şi în dependenţă de risc, una sau mai multe din următoarele măsuri:

1) limitarea desfăşurării relaţiei de afaceri sau efectuării tranzacţiilor în/din ţara (jurisdicţia) cu risc sporit sau cu persoane din această ţară (jurisdicţie) ori, după caz, încetarea acesteia;

2) evaluarea, modificarea sau, după caz, încetarea relaţiei cu instituţia corespondentă din ţara (jurisdicţia) cu risc sporit;

3) efectuarea auditului extern pentru sucursalele prestatorului situate în ţările (jurisdicţiile) în cauză;

4) închiderea sucursalei prestatorului situate în ţările (jurisdicţiile) în cauză.

[Pct.56[1] *în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.56[1] *introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

56[2]. Măsurile prevăzute la pct.56[1], precum şi alte măsuri de precauţie sporită, urmează a fi aplicate şi în cazul în care acestea sunt solicitate de Serviciul Prevenirea şi Combaterea Spălării Banilor sau de autoritatea de supraveghere.
[Pct.56[2] *completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.56[2] *introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

Capitolul VIII
AGENŢII PRESTATORULUI

57. Prestatorul aplică măsurile de precauţie privind agenţii în vederea cunoaşterii formei juridice şi a structurii de proprietate şi control a agenţilor săi şi va crea relaţii de afaceri cu agenţi care vor implementa cerinţele legislaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului. Cerinţele descrise în prezentul capitol nu se vor aplica în cazul agenţilor care sunt entităţi raportoare licenţiate, reglementate şi supravegheate de Banca Naţională a Moldovei, şi anume, băncile licenţiate şi prestatorii de servicii de plată nebancari. Procedurile interne ale prestatorului privind agenţii de plată trebuie să includă aspecte precum:

1) la iniţierea relaţiei de afaceri, este necesar de identificat agentul şi de aplicat măsuri de precauţie privind activitatea anterioară, cum ar fi o schimbare recentă faţă de relaţia actuală cu alţi prestatori, indiferent dacă agentul furnizează servicii de plată în numele şi pe contul unuia sau mai multor prestatori, durata de activitate în domeniu, structura proprietăţii, soliditatea financiară, înregistrarea agentului în registrul societăţilor de plată/furnizorilor de servicii poştale şi registrul societăţilor emitente de monedă electronică a agentului;

2) obţinerea unor informaţii suplimentare adecvate pentru a înţelege activitatea agentului, cum ar fi oferirea de servicii altor prestatori, informaţii privind conformitatea

anterioară la prevederile legislaţiei, natura şi nivelul aşteptat al operaţiunilor, număr de clienţi şi expunerea geografică.

3) la aprobarea unui nou agent, este necesar de organizat pentru personalul agentului instruiri privind cerinţele legale aplicabile în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, programul, politicile şi procedurile interne de prevenire şi de conformitate combaterii spălării banilor şi finanţării terorismului cu ale prestatorului. Corespunzător, instruirile respective trebuie să fie organizate periodic;

4) furnizează îndrumări şi asistenţă agentului prestatorului pentru respectarea programului de prevenire şi combatere a spălării banilor şi finanţării terorismului a prestatorului;

5) asigurarea respectării prevederilor legislaţiei cum ar fi raportarea activităţilor suspecte, operaţiuni în valori mari, monitorizarea riscurilor aferente domeniului, raportarea şi păstrarea înregistrărilor, prin intermediul programului de verificare periodică;

6) asigurarea unei reacţii prompte şi remedierea situaţiilor de risc prin metoda verificării la distanţă şi pe teren la sediul agentului, şi, după caz, organizarea de instruiri suplimentare, suspendarea sau încetarea relaţiei de afaceri cu agentul.

58. Prestatorul monitorizează activitatea agentului în scopul asigurării implementării corespunzătoare de către acesta a cerinţelor de prevenire şi combatere a spălării banilor şi finanţării terorismului. Gradul şi natura monitorizării agenţilor de plată depinde de volumul operaţiunilor agentului, metoda de monitorizare utilizată (manuală, automată sau combinată), ţările în care sunt transferate mijloacele băneşti, rezultatele monitorizărilor anterioare (dacă este cazul) şi tipul de activitate. În aplicarea unei abordări bazate pe evaluarea riscului, gradul de monitorizare se va baza pe riscurile percepute, atât externe, cât şi interne, asociate cu agentul, cum ar fi produsele sau serviciile furnizate de agentul, locaţia agentului şi natura activităţii.

59. Prestatorul monitorizează activitatea agentului în cadrul unei abordări bazate pe risc şi identifică criterii specifice de risc pentru a determina care activităţi ale agenţilor de plată necesită a fi revizuite. Criteriile specifice definite în acest scop trebuie revizuite în mod periodic pentru a determina dacă sunt adecvate pentru nivelurile de risc stabilite.

60. Prestatorul, în scopul redresării şi minimizării riscurilor specifice care derivă din activitatea unui agent pune în aplicare cel puţin următoarele măsuri:

1) crearea şi ţinerea unui registru al agenţilor cu risc înalt;

2) necesitatea aplicării măsurilor de precauţie sporite în cazurile corespunzătoare;

3) aplicarea limitelor la tranzacţiile în numerar;

4) furnizarea de instruiri specifice pentru indicatorii de suspiciune specifici pentru agenţii de plată pentru a le îmbunătăţi cunoştinţele în domeniu şi privind standardele de raportare.

Capitolul IX
CERINŢE PRIVIND TRANSFERURILE DE FONDURI

61. Prezentul capitol se aplică transferurilor de fonduri, în orice monedă, care sunt transmise sau primite de către un prestator sau de un prestator intermediar.

62. Prezentul capitol nu se aplică transferurilor de fonduri efectuate prin utilizarea unui card de plată, a unui instrument de monedă electronică, a unui telefon mobil sau orice alt dispozitiv digital sau informatic preplătit sau plătit ulterior (de tip postpaid), cu caracteristici similare, în cazul în care sunt îndeplinite următoarele condiţii:

1) cardul, instrumentul sau dispozitivul respectiv este utilizat exclusiv pentru a plăti bunuri sau servicii; şi

2) numărul cardului, instrumentului sau dispozitivului respectiv însoţeşte toate transferurile care decurg din tranzacţie.

Cu toate acestea, prezentul capitol se aplică atunci când un card de plată, un instrument de monedă electronică, un telefon mobil sau orice alt dispozitiv digital sau informatic preplătit sau plătit ulterior (de tip postpaid), cu caracteristici similare, este folosit pentru a efectua un transfer de fonduri între persoane fizice care, în calitate de consumatori, acţionează în alte scopuri decât activitatea lor comercială, de afaceri sau profesională, inclusiv industrială şi artizanală.

[Pct.62 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

63. Prezentul capitol nu se aplică unui transfer de fonduri atunci când acesta:

1) implică retragerea de numerar de către plătitor din contul de plăţi propriu;

2) reprezintă un transfer de fonduri către o autoritate publică reprezentând plata impozitelor, a amenzilor sau a altor taxe;

3) este efectuat între prestatori de servicii de plată, în calitate de plătitor şi beneficiar al plăţii, care acţionează în nume propriu;

4) este efectuat prin schimburi de imagini ale cecurilor, inclusiv cecuri trunchiate.

[Pct.63 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

63[1]. Prezentul capitol nu se aplică:

1) serviciilor enumerate la art.2 alin.(2) subpct. 1)-13) şi 15) din Legea nr.114/2012 cu privire la serviciile de plată şi moneda electronică;

2) persoanelor care nu au nicio activitate în afară de cea de a transforma documentele pe suport de hârtie în date în format electronic şi care acţionează în temeiul unui contract încheiat cu un prestator de servicii de plată, şi nici persoanelor care nu au nicio altă activitate în afară de aceea de a furniza prestatorilor de servicii de plată sisteme de mesagerie ori alte sisteme de suport pentru transmiterea fondurilor sau sisteme de compensare şi decontare.

[Pct.63[1] introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

Secţiunea 1
Obligaţiile prestatorului plătitorului

64. Prestatorul plătitorului se asigură ca transferurile de fonduri sunt însoţite de următoarele informaţii cu privire la plătitor:

1) numele plătitorului (denumirea/numele şi prenumele);

2) numărul de cont de plăţi al plătitorului;

3) adresa plătitorului, inclusiv denumirea ţării, numărul actului de identitate şi numărul de identificare al clientului (de ex. IDNP/IDNO) sau, alternativ, data şi locul naşterii plătitorului;

4) LEI actual al plătitorului, sub rezerva existenţei câmpului necesar în formatul mesajului de pată relevant şi în cazul în care plătitorul furnizează această informaţie sau, în lipsa LEI, orice identificator oficial echivalent disponibil.

[Pct.64 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

65. Prestatorul plătitorului se asigură ca transferul de fonduri este însoţit de următoarele informaţii cu privire la beneficiarul plăţii:

1) numele (denumirea/numele şi prenumele) beneficiarului plăţii;

2) numărul de cont de plăţi al beneficiarului plăţii; şi

3) LEI actual al beneficiarului plăţii, sub rezerva existenţei câmpului necesar în formatul mesajului de plată relevant şi în cazul în care plătitorul furnizează această informaţie sau, în lipsa LEI, orice identificator oficial echivalent disponibil.

[Pct.65 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

66. Prin derogare de la pct.64 subpct.2) şi pct.65 subpct.2), în cazul transferurilor care nu se efectuează din sau către un cont de plăţi, prestatorul plătitorului se asigură că transferul de fonduri este însoţit de un cod unic de identificare a tranzacţiei în locul numărului (numerelor) de cont de plăţi.

67. Înainte de a transfera fondurile, prestatorul plătitorului verifică exactitatea informaţiilor menţionate la pct.64 şi, dacă este cazul, la pct.66, pe baza documentelor, a datelor sau a informaţiilor obţinute dintr-o sursă fiabilă şi independentă, ţinînd cont de prevederile prezentului Regulament.

[Pct.67 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

67[1]. Obligaţia de verificare a exactităţii informaţiilor cu privire la plătitor menţionată la pct.67 se consideră a fi îndeplinită dacă prestatorul plătitorului aplică măsuri de precauţie pentru verificare identităţii plătitorului, actualizează şi păstrează informaţia privind plătitorul în conformitate cu prevederile Cap. V-VII şi XI.

[Pct.67[1] introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

68. Prin derogare de la pct.64 şi, după caz, fără a aduce atingere informaţiilor cerute în conformitate cu Regulamentul cu privire la transferul de credit, debitare directă şi atribuirea codurilor IBAN, aprobat prin Hotărârea Comitetului Executiv al Băncii Naţionale a Moldovei nr.108/2023, în cazul în care prestatorul de servicii de plată al beneficiarului plăţii este stabilit în afara Republicii Moldova, prestatorul asigură că transferul de fonduri internaţional a cărui valoare nu depăşeşte 20000 lei şi care nu pare a fi legat de alte transferuri de fonduri care, împreună cu transferul în cauză, ar depăşi 20000 lei este însoţit, cel puţin, de informaţii privind numele plătitorului şi al beneficiarului plăţii, şi numărul de cont de plăţi al plătitorului şi al beneficiarului plăţii sau, în cazul aplicabilităţii pct.66, codul unic de identificare a operaţiunii.

[Pct.68 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

68[1]. Prin derogare de la pct.67, în situaţia prevăzută la pct.68, prestatorul plătitorului are obligaţia de a verifica informaţiile referitoare la plătitor doar când acesta:

1) a primit fondurile care fac obiectul transferului în numerar sau în monedă electronică anonimă; sau

2) are motive întemeiate să suspecteze o activitate de spălare a banilor sau finanţare a terorismului.

[Pct.68[1] introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

69. În cazul transferurilor de credit pe baza unui fişier de grup efectuate de un singur plătitor către mai mulţi beneficiari ai căror prestatori de servicii de plată activează în afara Republicii Moldova, pct.64 nu se aplică transferurilor individuale grupate, cu condiţia ca transferul procesat în baza unui fişier de grup să cuprindă informaţiile menţionate la pct.64, 65 şi 66, informaţiile respective să fi fost verificate în conformitate cu pct.67 şi 67[1], şi transferurile individuale să fie însoţite de numărul de cont de plăţi al plătitorului sau, acolo unde se aplică pct.66, de codul unic de identificare a tranzacţiei.

[Pct.69 completat prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

69[1]. Prin derogare de la pct.64 şi 65 şi, după caz, fără a aduce atingere informaţiilor cerute în conformitate cu Regulamentul cu privire la transferul de credit, debitare directă şi atribuirea codurilor IBAN, aprobat prin Hotărârea Comitetului Executiv al Băncii Naţionale a Moldovei nr.108/2023, atunci când toţi prestatorii de servicii de plată implicaţi în lanţul de plată sunt stabiliţi pe teritoriul Republicii Moldova, transferurile de fonduri sunt însoţite cel puţin de numărul de cont de plăţi al plătitorului şi al beneficiarului plăţii sau, în cazul aplicabilităţii pct.66, de codul unic de identificare

a tranzacţiei. În acest caz, în termen de cel mult trei zile lucrătoare de la primirea unei cereri de informaţii de la prestatorul de servicii de plată al beneficiarului plăţii sau a prestatorului intermediar, prestatorul plătitorului va pune la dispoziţie următoarele informaţii:

1) privind plătitorul sau beneficiarul plăţii în conformitate cu pct.64-66, în cazul transferului de fonduri care depăşeşte suma de 20000 lei, indiferent dacă transferul respectiv este efectuat printr-o singură tranzacţie sau mai multe tranzacţii care par să fie legate;

2) numele plătitorului şi al beneficiarului plăţii şi numărul de cont de plăţi al plătitorului şi al beneficiarului plăţii sau, la aplicabilitatea pct.66, codul unic de identificare a tranzacţiei, pentru transferurile de fonduri care nu depăşesc limita stabilită la subpct. 1). În acest caz, obligaţia de verificare a informaţiei privind plătitorul corespunde cu cea prevăzută la pct.68[1].

[Pct.69[1] *introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]*

70. Prestatorul nu va efectua transferul de fonduri dacă nu este asigurată respectarea deplină a cerinţelor pct.64-69[1].

[Pct.70 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

Secţiunea a 2-a
Obligaţiile prestatorului beneficiarului plăţii

71. Prestatorul beneficiarului plăţii instituie şi aplică proceduri eficace, inclusiv, acolo unde este cazul, controlul după efectuarea transferurilor sau controlul în cursul efectuării acestora, pentru a depista dacă câmpurile referitoare la informaţiile privind plătitorul şi beneficiarul plăţii din sistemul de mesagerie sau de plată şi decontare utilizat pentru efectuarea transferului de mijloace băneşti au fost completate folosind caractere sau elemente compatibile în conformitate cu convenţiile sistemului respectiv şi în corespundere cu cerinţele pct.64 subpct.1)-3), 65 subpct.1)-2), 66, 68, 69 şi 69[1] din prezentul Regulament.

[Pct.71 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

71[1]. În cazul transferurilor de fonduri în valoare ce depăşeşte 20000 lei, indiferent dacă transferurile respective sunt efectuate printr-o singură tranzacţie sau mai multe tranzacţii care par să fie legate între ele, prestatorul beneficiarului plăţii, înainte de înregistrarea transferului de fonduri în contul beneficiarului plăţii sau de a pune fondurile la dispoziţia acestuia, verifică exactitatea informaţiilor privind beneficiarul plăţii menţionate la pct.65 subpct. 1)-2). 66, 68, 69 şi 69[1] pe baza documentelor, a datelor sau informaţiilor obţinute dintr-o sursa credibilă şi independentă, ţinând cont de prevederile prezentului Regulament.

[Pct.71[1] *introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]*

72. În cazul transferurilor de fonduri care nu depăşesc limita stabilită la pct.71[1], prestatorul beneficiarului plăţii verifică plenitudinea şi exactitatea informaţiilor referitoare la beneficiarul plăţii menţionată la pct.71[1] doar în următoarele situaţii:

1) când plata este efectuată în numerar sau monedă electronică anonimă; sau

2) când există motive întemeiate pentru a suspecta că există o activitate de spălare a banilor sau de finanţare a terorismului.

[Pct.72 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]
[Pct.72 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

72[1]. Obligaţia de verificare a plenitudinii şi a exactităţii informaţiilor privind beneficiarul plăţii menţionată la pct.71[1] şi 72 se consideră a fi îndeplinită dacă prestatorul beneficiarului plăţii aplică măsuri de precauţie pentru verificarea

beneficiarului plăţii, actualizează şi păstrează informaţia privind beneficiarul plăţii în conformitate cu prevederile Cap. V-VII şi XI.
[Pct.72[1] *introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]*

73. Prestatorul beneficiarului plăţii pune în aplicare proceduri eficace bazate pe riscuri, inclusiv procedurile prevăzute la pct.11, în funcţie de riscul asociat privind măsurile de precauţie privind clienţii, pentru a determina dacă să execute, să respingă sau să suspende un transfer de fonduri în cazul în care informaţiile complete privind plătitorul şi beneficiarul plăţii lipsesc şi pentru a lua măsurile ulterioare adecvate.
[Pct.73 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

74. În cazul în care prestatorul beneficiarului plăţii constată, că la primirea transferului de fonduri, informaţiile menţionate la pct.64 subpct. 1)-3), 65 subpct. 1)-2), 66, 68, 69 şi 69[1] lipsesc sau sunt incomplete ori nu au fost completate folosind caractere sau elemente compatibile în conformitate cu convenţiile sistemului de mesagerie sau de plată şi decontare utilizat, astfel cum este menţionat la pct.71, prestatorul respinge transferul sau solicită informaţiile cerute privind plătitorul şi beneficiarul plăţii, înainte sau după creditarea contului de plăţi al beneficiarului plăţii sau punerea fondurilor la dispoziţia acestuia, în funcţie de riscul asociat.
[Pct.74 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

75. În cazul în care prestatorul de servicii de plată care efectuează transferul omite în mod repetat să furnizeze informaţiile cerute cu privire la plătitor sau beneficiarul plăţii, prestatorul beneficiarului plăţii ia măsuri care pot consta, mai întîi, în emiterea unor avertismente şi stabilirea unor termene-limită, înainte fie de a respinge orice transfer de mijloace băneşti care provine de la acesta, fie de a decide, dacă este cazul, să restrîngă sau să înceteze relaţia comercială cu respectivul prestator. Prestatorul beneficiarului plăţii informează Banca Naţională a Moldovei despre aceste omisiuni, precum şi despre măsurile întreprinse.
[Pct.75 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

75[1]. Prestatorul, atunci când acţionează în calitate de prestator al beneficiarului plăţii sau, după caz, concomitent a plătitorului şi al beneficiarului plăţii, ia în considerare toate informaţiile lipsă privind plătitorul şi beneficiarul plăţii pentru a evalua dacă transferul de fonduri sau orice tranzacţie conexă este suspectă şi dacă aceasta trebuie raportată Serviciului Prevenirea şi Combaterea Spălării Banilor conform legislaţiei.
[Pct.75[1] *în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]*
[Pct.75[1] *introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

Secţiunea a 3-a
Obligaţiile prestatorilor intermediari

76. Prestatorul intermediar instituie şi aplică proceduri eficace, inclusiv, acolo unde este cazul, controlul după efectuarea transferurilor sau controlul în cursul efectuării acestora, pentru a depista dacă câmpurile referitoare la informaţiile privind plătitorul şi beneficiarul plăţii din sistemul de mesagerie sau plată şi decontare, utilizat pentru efectuarea transferului de fonduri, au fost completate folosind caractere sau elemente compatibile în conformitate cu convenţiile sistemului respectiv şi în corespundere cu cerinţele pct.64 subpct. 1)-3), 65 subpct. 1)-2), 66 68, 69 şi 69[1] din prezentul Regulament şi se asigură că toate informaţiile primite privind plătitorul şi beneficiarul plăţii care însoţesc un transfer de fonduri sunt păstrate împreună cu acel transfer.
[Pct.76 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]
[Pct.76 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

[Pct.77 abrogat prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

78. Prestatorul intermediar pune în aplicare proceduri eficace bazate pe riscuri, pentru a determina dacă să execute, să respingă sau să suspende un transfer de fonduri în cazul în care informaţiile cerute privind plătitorul şi beneficiarul plăţii lipsesc şi pentru a lua măsurile ulterioare adecvate.
[Pct.78 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

79. Prestatorul intermediar, dacă constată că la primirea transferului de mijloace băneşti, informaţiile menţionate la pct.64 subpct. 1)-3), 65 subpct. 1)-2), 66, 68, 69 şi 69^1 lipsesc sau sunt incomplete, ori nu au fost completate folosind caractere şi elemente compatibile în conformitate cu convenţiile sistemului de mesagerie sau de plată şi decontare, astfel cum este prevăzut la pct.71 şi 76, fie respinge transferul sau solicită informaţiile cerute privind plătitorul şi beneficiarul plăţii înainte sau după transmiterea transferului de mijloace băneşti, în funcţie de riscul asociat.
[Pct.79 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

80. În cazul în care prestatorul de servici de plată care efectuează transferul omite în mod repetat să furnizeze informaţiile cerute cu privire la plătitor sau beneficiarul plăţii, prestatorul ia măsuri care pot consta, mai întîi, în emiterea unor avertismente şi stabilirea unor termene-limită, înainte de respingerea oricărui transfer de mijloace băneşti care provine de la acesta, fie în decizia de a restrînge sau de a înceta relaţia comercială cu respectivul prestator. Prestatorul intermediar informează Banca Naţională a Moldovei despre aceste omisiuni, precum şi despre măsurile întreprinse."
[Pct.80 în redacţia Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

80^1. Prestatorul intermediar ia în considerare informaţiile lipsă privind plătitorul sau beneficiarul plăţii atunci când evaluează dacă transferul de fonduri sau orice tranzacţie conexă este suspectă şi dacă aceasta trebuie raportată Serviciului Prevenirea şi Combaterea Spălării Banilor în conformitate cu art.11 din Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului.".
[Pct.801 introdus prin Hot.BNM nr.8 din 13.01.2025, în vigoare 16.01.2025]

Capitolul X
RAPORTAREA ACTIVITĂŢILOR ŞI A TRANZACŢIILOR

81. Prestatorul este obligat să raporteze Serviciului Prevenirea şi Combaterea Spălării Banilor, în conformitate cu art.11 din Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, despre:

1) bunurile suspecte, activităţile sau tranzacţiile suspecte de spălare a banilor, de infracţiuni predicat şi de finanţare 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 circumstanţelor care generează suspiciuni;

2) activităţile sau tranzacţiile clienţilor realizate în numerar în valoare de cel puţin 200000 de lei (sau echivalentul acesteia), realizate printr-o operaţiune sau prin mai multe operaţiuni care au legătură între ele, în decursul unei luni, începând cu prima zi şi terminând cu ultima zi a lunii - până la data de 5 a lunii următoare lunii în care au fost efectuate activităţile sau tranzacţiile;

3) tranzacţiile clienţilor realizate printr-o operaţiune cu o valoare de cel puţin 200000 de lei (sau echivalentul acesteia) şi care nu se încadrează în prevederile sbp.2) - până la data de 10 a lunii următoare lunii în care au fost efectuate tranzacţiile;

4) tranzacţiile realizate prin sistemele de remiteri de bani cu o valoare de cel puţin 40000 de lei (sau echivalentul acesteia) – în termen de 5 zile din momentul efectuării tranzacţiei.
[Pct.81 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.81 modificat prin Hot.BNM nr.324 din 20.12.2018, în vigoare 04.02.2019]

82. Prestatorul va dispune de:
1) proceduri clare, reieşind din prevederile Legii nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, aduse la cunoştinţa întregului personal, care prevăd raportarea de către personal a tuturor activităţilor şi tranzacţiilor suspecte;
2) sisteme de depistare a activităţilor şi tranzacţiilor suspecte conform criteriilor stabilite, inclusiv de autorităţile competente;
3) proceduri de informare a administratorului responsabil privind problemele ce ţin de prevenirea şi combaterea spălării banilor şi finanţării terorismului.
83. Prestatorul informează, după caz, Banca Naţională în conformitate cu Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, despre activităţile şi tranzacţiile suspecte, cazurile de fraudă ce afectează esenţial siguranţa, stabilitatea sau reputaţia prestatorului.

Capitolul XI
PĂSTRAREA DATELOR

84. Prestatorul păstrează toate documentele, datele şi informaţiile obţinute în temeiul prezentului regulament, inclusiv cele obţinute în cadrul măsurilor de precauţie privind clienţii şi beneficiarii efectivi, informaţiile obţinute prin intermediul mijloacelor electronice în cadrul procesului de identificare şi verificare a identităţii clientului la distanţă, cum ar fi copiile documentelor de identificare, arhiva conturilor şi documentelor primare, corespondenţa de afaceri, rezultatele analizelor şi cercetărilor efectuate, pe perioada activă a relaţiei de afaceri şi pe o perioadă de 5 ani de la încetarea acesteia sau de la data efectuării operaţiunilor ocazionale. Datele păstrate trebuie să fie suficiente ca să permită reconstituirea fiecărei activităţi sau tranzacţii în maniera în care să servească în caz de necesitate ca probă în cadrul procedurii penale, contravenţionale şi altor proceduri legale.
[Pct.84 modificat prin *Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*
[Pct.84 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

85. Procedurile de păstrare a documentelor şi informaţiei vor include cel puţin următoarele, după caz:
1) ţinerea unui registru al clienţilor şi al beneficiarului efectiv identificaţi, care va conţine cel puţin: denumirea/numele şi prenumele clientului; IDNO/IDNP; numărul contului de plată; data deschiderii; data închiderii);
2) păstrarea tuturor documentelor primare, inclusiv a corespondenţei de afaceri;
3) păstrarea dosarelor privind identificarea şi verificarea clienţilor, a beneficiarilor efectivi, privind monitorizarea operaţiunilor clienţilor şi păstrarea documentelor confirmative aferente operaţiunilor;
4) păstrarea informaţiei privind operaţiunile efectuate (tipul, volumul, moneda, destinaţia etc.), inclusiv cele complexe şi neordinare;
4^1) păstrarea informaţiei aferente transferurilor de fonduri, inclusiv în cazurile când limitările tehnice ale sistemului de plată nu permit transmiterea tuturor informaţiilor de către instituţia intermediară;
5) arhivarea informaţiei privind operaţiunile şi corespondenţa de afaceri în sistemele tehnologiilor informaţionale şi păstrarea arhivei în condiţii de siguranţă şi disponibilitate operativă.

[Pct.85 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

86. Prestatorul asigură că, în caz de solicitare, documentele şi informaţia privind identificarea şi verificarea clienţilor, a beneficiarilor efectivi, privind monitorizarea tranzacţiilor naţionale şi internaţionale clienţilor, inclusiv documentele confirmative aferente operaţiunilor sunt accesibile şi disponibile, în mod operativ, Băncii Naţionale a Moldovei şi Serviciului Prevenirea şi Combaterea Spălării Banilor. La solicitarea autorităţilor competente, conform art.9 alin.(2) din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, termenul privind deţinerea şi păstrarea informaţiei aferentă clienţilor şi operaţiunilor acestora poate fi prelungit pentru o perioadă determinată în solicitare, dar nu mai mult de 5 ani.
[Pct.86 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

Capitolul XII
CERINŢE PRIVIND SISTEMUL DE CONTROL INTERN

87. Prestatorul va dispune de un sistem de control intern care va asigura conformarea continuă cu actele normative şi programul intern în domeniu prevenirii şi combaterii spălării banilor şi finanţării terorismului ce va contribui la minimizarea riscurilor aferente.

88. Sistemul de control intern al prestatorului depinde de o serie de factori, inclusiv natura, amploarea şi complexitatea afacerii prestatorului de servicii de plată, diversitatea operaţiunilor sale, inclusiv diversitatea geografică, baza de clienţi, profilul de produs şi activitate, gradul de risc asociat fiecărei jurisdicţii a operaţiunilor şi canalelor sale de distribuţie, adică măsura în care prestatorul interacţionează direct cu clientul sau prin intermediul agenţilor de plată.

89. La deschiderea filialelor pe teritoriul altor state, precum şi pe parcursul activităţii acestora, prestatorul va aplica cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului în conformitate cu sistemul de control intern propriu, politicile şi procedurile interne şi actele normative ale Republicii Moldova, în măsura în care legislaţia ţării gazde permite. În cazul în care, în ţara gazdă cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului sunt insuficiente, prestatorul trebuie să asigure implementarea cerinţelor actelor normative ale Republicii Moldova, în măsura în care legislaţia ţării gazde permite. Dacă ţara gazdă nu permite aplicarea corespunzătoare a cerinţelor actelor normative ale Republicii Moldova, prestatorul aplică măsuri suplimentare corespunzătoare pentru a diminua riscul de spălare a banilor şi finanţare a terorismului şi informează Banca Naţională a Moldovei în decurs de 2 luni despre acest fapt. Banca Naţională poate aplica măsuri de supraveghere potrivit cadrului legal, pentru asigurarea respectării de către filialele deschise pe teritoriul altor state a actelor normative aferente domeniului dat, iar dacă se constată nerespectarea acestora, Banca Naţională a Moldovei poate limita activitatea sau retrage aprobarea emisă pentru deschiderea filialelor pe teritoriul altor state. În aplicarea prezentului punct, Banca Naţională a Moldovei emite standarde tehnice emise privind tipul de măsuri suplimentare, precum şi măsurile minime care trebuie realizate de prestator în cazul în care normele de drept ale altei ţări (jurisdicţii) nu permit punerea în aplicare a măsurilor prevăzute în prezentul punct.

89[1]. În cazul deschiderii filialelor pe teritoriul altor state, la nivelul grupului financiar, sistemul de control intern şi programul privind prevenirea şi combaterea spălării banilor şi finanţării terorismului va include, pe lângă elementele stabilite la pct.91-94, următoarele elemente adiţionale:

1) politici şi proceduri privind schimbul de informaţii în scopul aplicării măsurilor de precauţie privind clienţii şi de administrare a riscurilor de spălare a banilor şi finanţare a terorismului;

2) cerinţe privind furnizarea informaţiei în cadrul grupului privind clienţi, conturi şi tranzacţii, atunci când aceasta este necesar pentru aplicarea măsurilor de prevenire şi combatere a spălării banilor şi finanţării terorismului;

3) cerinţe adecvate privind păstrarea confidenţialităţii informaţiei supuse schimbului ce constituie secret profesional şi date cu caracter personal, precum şi modul de utilizare şi procesare a acestor informaţii.

[P ct.89[1] *introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

90. Prestatorul care efectuează operaţiuni prin intermediul agenţilor trebuie să îi includă pe aceştia în sistemele lor de control intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi să îi monitorizeze în vederea respectării prevederilor lor.

91. Sistemul de control intern trebuie să includă cel puţin următoarele elemente:

1) efectuarea auditului de către personalul prestatorului sau de către o entitate de audit/auditor extern în vederea verificării respectării programului intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului. Funcţiile auditului în acest scop sunt:

a) evaluarea independentă a programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi a respectării cerinţelor legislaţiei;

b) monitorizarea activităţii personalului prin testarea conformării;

c) testarea operaţiunilor în caz de necesitate;

d) informarea administratorului responsabil privind rezultatele verificării şi recomandarea asupra măsurilor necesare a fi întreprinse pentru minimizarea riscurilor şi neajunsurilor identificate;

2) desemnarea unei persoane, care este administrator, responsabil de asigurarea conformării programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului cu cerinţele legislaţiei şi aplicării acestuia adecvat (în continuare - administrator responsabil). În acest scop administratorul responsabil are următoarele atribuţii:

a) acordă consultaţii angajaţilor prestatorului în problemele ce apar în timpul realizării programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, inclusiv în ce priveşte identificarea şi examinarea clienţilor prestatorului şi evaluarea riscului de spălare a banilor şi finanţare a terorismului;

b) ia decizii în baza informaţiei primite;

c) întreprinde măsuri privind raportarea autorităţii competente pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului a informaţiei în conformitate cu legislaţia;

d) organizează instruirea angajaţilor prestatorului în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

e) colaborează cu serviciul de audit în vederea verificării conformării activităţii prestatorului la legislaţia în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

f) îndeplineşte alte funcţii în corespundere cu prezentul Regulament şi documentele interne ale prestatorului;

3) prevederi interne privind răspunderea şi sancţionarea angajaţilor care nu raportează despre activităţile sau operaţiunile suspecte administratorului sau direct autorităţii competente şi/sau contribuie personal la efectuarea operaţiunilor de spălare a banilor şi finanţare a terorismului.

[P ct.91 modificat prin *Hot.BNM nr.324 din 20.12.2018, în vigoare 04.02.2019]*

92. Persoana, care efectuează auditul prestatorului, analizează realizarea programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului

de către prestator şi prezintă în scris, administratorului responsabil al prestatorului un raport privind rezultatele analizei efectuate.

93. Prestatorul va dispune de programe de selectare şi instruire continuă a personalului în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului. Prestatorul asigură deţinerea de către personalul său a cunoştinţelor, calităţilor, inclusiv reputaţionale, şi abilităţilor corespunzătoare pentru îndeplinirea eficientă a responsabilităţilor de conformare la cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului.

[Pct.93 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]

94. Programele de selectare şi instruire indicate la pct.93 vor cuprinde diverse aspecte ale procesului de prevenire şi combatere a spălării banilor şi finanţării terorismului şi obligaţiunile conform legislaţiei în domeniu, inclusiv:

1) instruirea personalului nou angajat referitor la importanţa şi cerinţele de bază ale programelor respective;

2) instruirea personalului de "prima linie" (angajaţii care nemijlocit intră în contact cu clienţii) referitor la verificarea identităţii clienţilor noi, monitorizarea conturilor clienţilor existenţi pe bază continuă, depistarea indicilor şi raportarea activităţilor şi tranzacţiilor suspecte şi a celor supuse raportării;

3) actualizarea regulată a responsabilităţilor personalului;

4) noile tehnici, metode şi tendinţe de spălare a banilor şi finanţare a terorismului;

5) nivelul implicării personalului în procesul de prevenire şi combatere a spălării banilor şi finanţării terorismului.

Conţinutul şi programul instruirii personalului trebuie să fie adaptat la necesităţile individuale ale prestatorului.

95. Prestatorul realizează prelucrarea datelor cu caracter personal obţinute în procesul de implementare a cerinţelor prezentului regulament şi asigură confidenţialitatea acestora, ţinând cont de cerinţele actelor normative cu privire la protecţia datelor cu caracter personal.

Capitolul XIII
CERINŢE PRIVIND APLICAREA MĂSURILOR RESTRICTIVE INTERNAŢIONALE

96. Prestatorul aplică imediat măsuri restrictive aferente activităţilor teroriste şi de proliferare a armelor de distrugere în masă în privinţa bunurilor, inclusiv a celor obţinute din sau generate de bunuri care aparţin sau sunt deţinute ori controlate, direct sau indirect, integral sau în comun, de persoanele, grupurile şi entităţile implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive, precum şi de persoanele, grupurile şi entităţile care acţionează în numele, la indicaţia, care aparţin sau sunt controlate, direct sau indirect, de aceste persoane, grupuri şi entităţi.

[Pct.96 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]
[Pct.96 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]

97. Pentru punerea în aplicare a măsurilor restrictive conform pct.96, prestatorul elaborează proceduri şi reguli interne care trebuie să includă cel puţin următoarele elemente:

1) proceduri de colectare, păstrare şi actualizare a listei persoanelor, grupurilor şi entităţilor implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive internaţionale (inclusiv prin utilizarea bazelor de date existente), conform cerinţelor Legii nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului şi Legii nr.25 din 4 martie 2016 privind aplicarea măsurilor restrictive internaţionale, folosind în acest

scop inclusiv şi Ordinul directorului Serviciului de Informaţii şi Securitate privind listele persoanelor, grupurilor şi entităţilor implicate în activităţi teroriste;

2) proceduri de verificare/depistare a persoanelor sau entităţilor desemnate şi a operaţiunilor/plăţilor în care sunt implicate bunuri, aplicabile potenţialilor clienţi, clienţilor existenţi şi solicitanţilor de operaţiuni/plăţi ocazionale şi de transfer a mijloacelor băneşti;

3) competenţele persoanelor cu responsabilităţi în implementarea procedurilor şi regulilor interne pentru punerea în aplicare a măsurilor restrictive internaţionale de blocare a fondurilor;

4) procedurile de informare/raportare, intern şi către Serviciul Prevenirea şi Combaterea Spălării Banilor.

98. Prestatorul, la identificarea bunurilor, inclusiv a celor obţinute din sau generate de aceste bunuri, care aparţin sau sunt deţinute ori controlate, direct sau indirect, integral sau în comun, de persoanele, grupurile şi entităţile implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masă care fac obiectul măsurilor restrictive, întreprinde succesiv următorii paşi:

1) prin decizia (ordinul) administratorului responsabil al prestatorului, se abţine, pentru un termen nedeterminat, de la executarea activităţilor şi tranzacţiilor care sunt în curs de pregătire, tentativă, de realizare ori sunt deja realizate, în favoarea sau beneficiul, direct sau indirect, în mod integral sau parţial, al persoanelor, grupurilor şi entităţilor implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masa care fac obiectul măsurilor restrictive, al persoanelor juridice/ entităţilor care aparţin sau sunt controlate, direct sau indirect, de aceste persoane, grupuri şi entităţi, precum şi al persoanelor, grupurilor şi entităţilor care acţionează în numele, la indicaţia acestor persoane, grupuri şi entităţi;

2) informează imediat, dar nu mai târziu de 24 ore din momentul aplicării măsurii restrictive, Serviciul Prevenirea şi Combaterea Spălării Banilor despre abţinerea, pentru un termen nedeterminat, de la executarea activităţilor şi tranzacţiilor. Informaţia transmisă în adresa autorităţii menţionate va cuprinde cel puţin următoarele elemente:

a) date şi informaţii (nume/denumire; IDNO/IDNP, dacă există; ţara de origine/rezidenţă; lista autorităţii/organizaţiei la care face referinţă măsura restrictivă aplicată etc) despre persoana, grupul sau entitatea identificată;

b) date şi informaţii (volumul; moneda; destinatarul; destinaţia, etc) despre bunul identificat;

c) informarea despre decizia administratorului responsabil al prestatorului cu privire la abţinerea, pentru un termen nedeterminat, de la executarea activităţilor şi tranzacţiilor cu referire la bunul identificat;

3) dacă este cazul, prestatorul acceptă plăţi suplimentare, efectuate de o parte terţă, sau majorarea valorii bunurilor identificate şi extinde aplicabilitatea măsurii de abţinere asupra bunurilor, ţinând cont de cerinţele pct.98 subpct.1), precum şi informează despre acest fapt Serviciul Prevenirea şi Combaterea Spălării Banilor ţinând cont de cerinţele pct.98 subpct.2) lit.a) şi b);

4) informează Banca Naţională a Moldovei despre măsura restrictivă aplicată, ţinând cont de cerinţele pct.98 subpct.2) lit.a) şi b).

[Pct.98 *modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

99. În cazul unor îndoieli sau suspiciuni care nu permit stabilirea unei convingeri ferme privind identitatea persoanei, grupului sau entităţii incluse în lista menţionată la art.34 alin.(11) din Legea nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului, prestatorul informează neîntîrziat despre aceasta, în termen de cel mult 24 de ore, Serviciul Prevenirea şi Combaterea Spălării Banilor.

100. Prestatorul asigură monitorizarea permanentă a paginilor web oficiale ale Organizaţiei Naţiunilor Unite, Uniunii Europene şi Serviciului de Informaţii şi Securitate, pentru asigurarea aplicabilităţii corespunzătoare a măsurilor restrictive asupra persoanelor, grupurilor şi entităţilor implicate în activităţi teroriste şi de proliferare a armelor de distrugere în masă.

Capitolul XIV
ALTE DISPOZIŢII

101. În cazul în care se constată încălcarea prevederilor prezentului Regulament, a obligaţiilor prevăzute de legislaţia privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, Banca Naţională a Moldovei aplică sancţiuni în conformitate cu legislaţia în vigoare.

102. În aplicarea prezentului Regulament, prestatorul informează Banca Naţională a Moldovei despre activităţile suspecte şi incidentele de fraudă care prezintă riscuri pentru siguranţa, buna funcţionare sau reputaţia prestatorului.

[Pct.102 modificat prin Hot.BNM nr.324 din 20.12.2018, în vigoare 04.02.2019]

Anexă
la Regulamentul cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea prestatorilor de servicii de plată nebancari

RECOMANDĂRI
privind criteriile de identificare a beneficiarului efectiv

[Anexa abrogată prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]