A colorful emblem with a red and blue shield

Description automatically generated with medium confidence

**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 băncilor**

**nr. 200  din  09.08.2018**

*(în vigoare 24.08.2018)*

Monitorul Oficial al R. Moldova nr. 321-332 art. 1311 din 24.08.2018

\* \* \*

ÎNREGISTRAT:

Ministerul Justiţiei

al Republicii Moldova

nr.1354 din 21.08.2018

În temeiul art.11 alin.(1), art.27 alin.(1) lit.c) şi 44 lit.a) şi d) 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 ) şi art.95 din Legea privind activitatea băncilor nr.202 din 6 octombrie 2017 (Monitorul Oficial al Republicii Moldova, 2017 nr.434-439, art.727) 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 băncilor, 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.200. Chişinău, 9 august 2018.** | |

Anexă

la Hotărârea Comitetului executiv

al Băncii Naţionale a Moldovei

nr.200 din 9 august 2018

**REGULAMENT**

**cu privire la cerinţele privind prevenirea şi combaterea spălării**

**banilor şi finanţării terorismului în activitatea băncilor**

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 băncilor (în continuare - Regulament) stabileşte reguli privind: identificarea şi evaluarea de către bănci a riscurilor de spălare a banilor şi finanţare a terorismului; aplicarea cerinţelor de precauţie privind clienţii, inclusiv a măsurilor de precauţie simplificată şi sporită; raportarea activităţilor şi tranzacţiilor suspecte; păstrarea datelor; implementarea sancţiunilor financiare aferente spălării banilor, activităţilor teroriste şi de proliferare a armelor de distrugere în masă, precum şi organizarea şi realizarea elementelor aferente sistemului de control intern.

**2.** Banca şi sucursalele băncilor din alte state aplică cerinţele prezentului Regulament în relaţiile de afaceri cu clienţii săi şi la efectuarea tranzacţiilor şi operaţiunilor bancare.

**3.** Termenii şi expresiile utilizate în prezentul Regulament au semnificaţiile prevăzute în Legea nr.202 din 6 octombrie 2017 privind activitatea băncilor, 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, actele normative ale Băncii Naţionale a Moldovei şi ale Serviciului Prevenirea şi Combaterea Spălării Banilor emise întru executarea cerinţelor de prevenire şi combatere a spălării banilor şi finanţării terorismului. De asemenea, în sensul prezentului Regulament se utilizează următorii termeni şi expresii:

*tranzacţie semnificativă* – tranzacţia (operaţiunea) care depăşeşte limita valorică stabilită în politicile interne ale băncii luând în consideraţie riscurile asociate clienţilor şi tranzacţiilor efectuate;

*transferuri de fonduri* - orice tranzacţie efectuată, cel puţin parţial, prin mijloace electronice în numele unui plătitor prin intermediul unui prestator de servicii de plată, pentru a se pune fonduri la dispoziţia beneficiarului plăţii prin intermediul unui prestator de servicii de plată, indiferent dacă plătitorul şi beneficiarul plăţii sunt sau nu aceeaşi persoană şi indiferent dacă prestatorul de servicii de plată al plătitorului şi prestatorul de servicii de plată al beneficiarului plăţii sunt identici, inclusiv: transferuri de credit, debitări directe, remiteri de bani şi transferuri efectuate utilizând cardul de plată;

*identificatorul unic al companiei* (legal entity identifier) – un cod alfanumeric, alcătuit din 20 caractere, care identifică în mod unic o persoană juridică, stabilit în conformitate cu standardul ISO 17442;

*transfer de fonduri pe baza unui fişier de grup (batch file) -* mai multe transferuri ordonate de un singur plătitor către mai mulţi beneficiari, care sunt grupate în vederea transmiterii;

*fişier de grup (batch file) -* este un fişier text care conţine o secvenţă de comenzi pentru un sistem de operare al calculatorului;

*conturi corespondente de transfer (payable - through accounts)* - serviciu bancar, care permite clienţilor băncii corespondente străine utilizarea directă a conturilor corespondente deschise cu scopul efectuării tranzacţiilor directe în numele acestora;

*organizaţii internaţionale* – entităţi stabilite prin acorduri politice oficiale între statele membre care au statut de tratate internaţionale, iar existenţa lor este recunoscută prin lege în ţările membre şi nu sunt tratate ca unităţi instituţionale rezidente ale ţărilor în care se află (exemplu: Organizaţia Naţiunilor Unite, Consiliul Europei, OSCE, etc).

*[Pct.3 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**Capitolul II**

**RESPONSABILITĂŢI**

**4.** Banca elaborează şi pune în aplicare un program intern eficient privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.

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

**6.** Consiliul băncii este responsabil pentru aprobarea şi supravegherea aplicării programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului. Organul executiv al băncii este responsabil de implementarea eficientă a programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului.

**7.** Banca desemnează persoanele, inclusiv din rândul membrilor Consiliului băncii şi/sau organului executiv, învestite cu atribuţii de executare a cerinţelor acelor normative privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi de asigurare a conformităţii politicilor şi procedurilor cu aceste cerinţe.

**8.** Subdiviziunea de audit intern a băncii efectuează, cel puţin anual, evaluarea caracterului adecvat şi a conformităţii activităţii băncii cu programul privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, ţinând cont de pct.93 subpct.1). Banca, prin decizia Consiliul băncii sau la solicitarea organului de supraveghere, desemnează o entitate de audit/auditor extern, pentru efectuarea unei evaluări a caracterului adecvat şi a conformităţii activităţii băncii cu programul privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, ţinând cont cel puţin de prevederile pct.93 subpct.1) şi criteriile stabilite la solicitarea Băncii Naţionale a Moldovei. Rezultatele evaluării se comunică consiliului băncii şi organului executiv al băncii, iar banca informează despre rezultatele menţionate Banca Naţională a Moldovei în conformitate cu Instrucţiunea cu privire la modul de întocmire şi prezentare de către bănci a rapoartelor în scopuri prudenţiale, aprobat prin Hotărîrea Consiliul de administraţie al Băncii Naţionale a Moldovei nr.279 din 1 decembrie 2011 (Monitorul Oficial al Republicii Moldova, 2011, nr.216-221, art.2008), cu modificări şi completări ulterioare.

**Capitolul III**

**CERINŢE FAŢĂ DE PROGRAMUL INTERN PRIVIND PREVENIREA ŞI**

**COMBATEREA SPĂLĂRII BANILOR ŞI FINANŢĂRII TERORISMULUI**

**9.** Programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului reprezintă politici, metode, practici, proceduri şi controale interne, inclusiv reguli de cunoaştere a clientului, care promovează normele de etică şi profesionalism în sectorul bancar şi previne utilizarea băncii în scopul spălării banilor sau finanţării terorismului de către grupuri criminale organizate sau de către asociaţii acestora. Acest program trebuie să asigure efectuarea operaţiunilor bancare într-un mod sigur şi prudent.

*[Pct.9 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**10.** Banca 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, actele normative ale Serviciului Prevenirea şi Combaterea Spălării Banilor emise întru executarea acestei legi, ţinând cont de practica general acceptată în acest domeniu, inclusiv documentele Comitetului Basel şi ale Grupului de Acţiune Financiară Internaţională (GAFI).

*[Pct.10 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**11.** La elaborarea programului intern se iau în consideraţie mărimea, complexitatea, natura şi volumul activităţilor băncii, riscurile de spălare a banilor şi finanţare a terorismului identificate, tipurile (categoriile) clienţilor, produsele şi serviciile oferite, zona geografică implicată, gradul (nivelul) de risc asociat clienţilor şi/sau tranzacţiilor (operaţiunilor) desfăşurate de aceştia.

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

1) obligaţiile consiliului şi executivului băncii, care trebuie să includă cel puţin:

a) determinarea domeniilor de activitate ale băncii vulnerabile riscului spălării banilor şi finanţării terorismului, cu descrierea exactă a atribuţiilor fiecărei subdiviziuni pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului. Domeniile de activitate vulnerabile riscului spălării banilor şi finanţării terorismului pot fi acelea care au tangenţă cu: acceptarea depozitelor, operaţiunile de acordare/rambursare a creditelor, plăţile (transferurile) internaţionale, utilizarea instrumentelor de plată, operaţiunile bancare corespondente, serviciile bancare private, conturile deschise de intermediarii profesionişti în procesul exercitării de către aceştia a activităţilor de intermediere, sisteme automatizate de deservire la distanţă, sistemele de remitere de bani, operaţiuni alternative de finanţare a comerţului (acreditive, emitere de obligaţiuni etc), operaţiunile de brokeraj, de administrare fiduciară etc.;

b) determinarea mecanismului de identificare, evaluare şi întreprindere a acţiunilor de control şi minimizare a riscurilor de spălare a banilor şi finanţarea terorismului;

c) elaborarea măsurilor necesare pentru implementarea politicilor şi procedurilor de cunoaştere a clienţilor, inclusiv a celor cu grad de risc sporit;

d) alocarea resurselor suficiente pentru îndeplinirea eficientă a activităţilor de prevenire şi combatere a spălării banilor şi finanţării terorismului;

e) desemnarea persoanelor investite cu atribuţii de executare a Legii nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţarea terorismului, inclusiv cele cu funcţii de conducere de rang superior;

f) determinarea responsabilităţilor personalului băncii la diferite nivele ierarhice;

g) acordarea persoanelor responsabile, desemnate conform lit.e), a accesului într-un timp rezonabil la informaţia necesară executării Legii nr.308 din 22 decembrie 2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţarea terorismului şi prezentului regulament;

g1) 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;

h) remedierea deficienţelor identificate în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

2) proceduri de identificare, evaluare, control şi întreprinderea măsurilor de minimizare a riscurilor de spălare a banilor şi finanţare a terorismului;

3) proceduri de acceptare a clienţilor care stabilesc cel puţin categoriile de clienţi pe care banca 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;

4) 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;

5) măsurile de precauţie privind cunoaşterea clienţilor pentru fiecare dintre categoriile de clienţi, produse şi servicii ori tranzacţii (operaţiuni) efectuate;

6) proceduri de monitorizare a operaţiunilor efectuate de clienţi în scopul depistării tranzacţiilor semnificative, complexe şi neordinare, a activităţilor şi tranzacţiilor suspecte;

7) proceduri şi cerinţe privind aplicarea măsurilor de precauţie simplificate pentru clienţii şi tranzacţiile acestora atunci când, prin natura lor, pot prezenta un risc redus de spălare a banilor şi finanţarea terorismului, inclusiv măsuri de administrare a riscurilor în cazul stabilirii relaţiei de afaceri până la verificarea identităţii clientului şi a beneficiarului efectiv;

8) proceduri şi cerinţe privind aplicarea măsurilor de precauţie sporite la efectuarea tranzacţiilor complexe şi neordinare fără un scop legal sau economic clar, a tranzacţiilor semnificative şi a celor suspecte;

81) 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;

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

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

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

12) standarde pentru selectare, angajare a personalului şi programe de instruire a acestuia în domeniul cunoaşterii clienţilor;

13) 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 bancă.

*[Pct.12 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.12 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**13.** Banca revizuieşte (actualizează), ori de câte ori este necesar, programul intern privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, dar cel puţin anual, ţinând 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**

**14.** Banca este obligată să întreprindă acţiuni privind identificarea şi evaluarea riscurilor de spălare a banilor şi finanţare a terorismului, ţinând cont de ameninţările şi vulnerabilităţile identificate în rezultatul evaluării riscurilor la nivel naţional, precum şi de criteriile şi factorii de risc stabiliţi în acest sens de Banca Naţională a Moldovei şi Serviciul Prevenirea şi Combaterea Spălării Banilor. Rezultatele evaluării sunt consemnate într-un raport de evaluare, care se aprobă de către persoana cu funcţie de conducere de rang superior desemnată responsabilă în bancă de asigurarea conformităţii politicilor şi procedurilor cu cerinţele legale privind prevenirea şi combaterea spălării banilor şi finanţării terorismului şi se prezintă Consiliului băncii.

*[Pct.14 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**15.** În scopul implementării pct.14, banca efectuează anual evaluarea riscurilor de spălare a banilor şi finanţare a terorismului în domeniul propriu de activitate, proces care presupune cel puţin:

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

2) întocmirea unui plan de acţiuni în scopul minimizării riscurilor de spălare a banilor şi finanţarea terorismului identificate.

Banca actualizează evaluarea prevăzută la prezentul punct după fiecare evaluare a riscurilor de spălare a banilor şi finanţare a terorismului efectuată la nivel naţional de către Serviciul Prevenirea şi Combaterea Spălării Banilor şi la fiecare actualizare a criteriilor şi factorilor de risc stabiliţi în acest sens de Banca Naţională a Moldovei şi Serviciul Prevenirea şi Combaterea Spălării Banilor.

**16.** Banca identifică şi evaluează riscurile de spălare a banilor şi finanţare a terorismului până la:

1) lansarea şi dezvoltarea de produse şi servicii noi;

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

**17.** În procesul de evaluare a riscurilor de spălare a banilor şi finanţare a terorismului, banca utilizează diferite elemente şi caracteristici ale variabilelor implicate în analiză, cum sunt: destinaţia contului, scopul relaţiei de afaceri, volumul activelor implicate sau mărimea tranzacţiilor efectuate, frecvenţa şi durata relaţiei de afaceri etc.

**18.** Banca, ca urmare a rezultatelor evaluării riscurilor de spălare a banilor şi finanţare a terorismului, asigură implementarea abordării bazate pe risc prin stabilirea şi punerea în aplicare a procedurilor de identificare, evaluare, monitorizare, de gestionare şi minimizare a riscurilor identificate, inclusiv prin alocarea resurselor tehnologice, materiale şi umane corespunzătoare.

*[Pct.18 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**19.** Banca păstrează şi actualizează, conform programului intern, datele statistice din domeniul propriu de activitate necesare procesului de identificare şi evaluare a riscurilor de spălare a banilor şi finanţare a terorismului.

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

**Capitolul V**

**MĂSURI DE PRECAUŢIE PRIVIND CLIENŢII**

**Secţiunea 1**

**Proceduri de acceptare a clientului**

**21.** Procedurile de acceptare a clientului vor conţine prevederi despre clienţii care par să expună banca la un risc sporit de utilizare a ei în scopul spălării banilor şi finanţării terorismului. În vederea minimizării acestui risc, informaţia privind clienţii se va examina, cel puţin, în privinţa următoarelor aspecte: experienţa clienţilor în domeniul de activitate, ţara de origine, activităţile desfăşurate sau alţi indicatori de risc stabiliţi de bancă, ţinând cont de recomandările Băncii Naţionale a Moldovei privind implementarea abordării bazate pe risc.

*[Pct.21 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**22.** Procedurile de acceptare a clientului vor include mai multe etape în funcţie de gradul de risc al acestuia. Deciziile de începere, continuare sau încetare a relaţiei de afaceri cu clientul cu un grad de risc sporit se iau de către persoana responsabilă cu funcţie de conducere de rang superior în cadrul băncii sau de către conducătorul sucursalei, în cazul delegării atribuţiilor, prin coordonarea deciziei cu subdiviziunea internă a băncii responsabilă de implementarea şi conformarea cu cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului.

*[Pct.22 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**23.** Banca 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, banca informează neîntârziat Serviciul Prevenirea şi Combaterea Spălării Banilor, în termen de cel mult 24 ore, prezentând toate datele deţinute cu privire la acest caz.

**24.** Procedurile de acceptare a clientului nu trebuie să afecteze accesul publicului larg la serviciile bancare.

**Secţiunea a 2-a**

**Măsuri de precauţie privind clienţii**

*[Denumirea secţiunii a 2-a modificată prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**25.** Banca aplică, în funcţie de risc, măsuri de precauţie privind clienţii:

1) la iniţierea 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) atunci când există o suspiciune de spălare a banilor sau de finanţare a terorismului, independent de derogări, scutiri sau limite stabilite;

4) atunci când există suspiciuni privind veridicitatea, suficienţa şi precizia datelor de identificare obţinute anterior;

5) prin derogare de la subpct.2), operaţiunea de schimb valutar în numerar cu o valoare care depăşeşte 10000 de lei (conform cursului oficial al leului moldovenesc faţă de valutele străine valabil la data efectuării operaţiunii de schimb valutar) se efectuează cu prezentarea actelor de identitate, iar datele din acestea urmează a fi înregistrate de către bancă;

*[Pct.25 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**251.** 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., banca aplică măsuri de precauţie standard, de precauţie simplificată sau sporită.

*[Pct.251 introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**26.** La aplicarea măsurilor standard de precauţie privind clienţii în cazurile prevăzute la pct.25 banca 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) ocupaţia, funcţia deţinută;

f) sursa venitului;

g) identitatea beneficiarului efectiv;

h) 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 persoanele juridice şi întreprinzătorii individuali:

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

b) sediul/adresa principală de activitate;

c) numărul de identificare de stat (IDNO) şi codul fiscal, 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, altă decât 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;

f1) identitatea persoanelor care deţin poziţii de management superior, precum şi împuternicirile acestora de reprezentare;

g) drepturile şi obligaţiunile organului de conducere de a gestiona compania, care reies din documentele primare de înregistrare sau actul de constituire;

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);

3) pentru fiducii sau construcţii juridice similare:

a) denumirea şi dovada de încorporare/înregistrare, actul fiduciar;

b) sediul/adresa de activitate şi ţara de înregistrare;

c) natura, scopul şi obiectul activităţii (ca exemplu: discreţionar, testamentar, etc);

d) identitatea fondatorului, administratorului, protectorului (dacă există), beneficiarilor sau clasele de beneficiari şi a oricărei 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);

e) descrierea scopului/activităţii;

f) 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.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.** La identificarea unui grad de risc sporit, banca va aplica măsuri de precauţie sporită privind clienţii şi va obţine, suplimentar la datele indicate la pct.26, următoarele informaţii:

1) pentru clienţii - persoane fizice:

a) oricare alt nume utilizat (nume marital, nume deţinut anterior sau porecla);

b) adresa de serviciu, codul poştal, adresa de e-mail, numărul telefonului mobil;

c) statutul de rezident/nerezident;

d) genul (sexul);

e) numele angajatorului, dacă există;

f) sursa averii clientului;

g) sursa mijloacelor băneşti care tranzitează contul şi destinaţia acestora;

2) pentru persoanele juridice şi întreprinzătorii individuali:

a) identificatorul unic al companiei, dacă există;

b) numărul de telefon, adresa de email şi fax;

*[Lit.c) abrogată prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

d) situaţia financiară;

e) sursa mijloacelor băneşti parvenite în cont şi destinaţia mijloacelor băneşti care tranzitează contul;

3) pentru fiducii sau construcţii juridice similare:

a) numărul de telefon, adresa de e-mail şi fax;

*[Lit.b) abrogată prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

c) sursa mijloacelor băneşti;

d) destinaţia mijloacelor băneşti care tranzitează contul.

*[Pct.27 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.27 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**28.** În cazul efectuării operaţiunilor de schimb valutar în numerar cu persoane fizice prin intermediul birourilor sale de schimb valutar şi/sau aparatelor de schimb valutar, banca aplică măsuri de precauţie privind clienţii, inclusiv măsuri de precauţie sporite în conformitate cu prevederile cap. III şi IV din Regulamentul cu privire la cerinţele privind prevenirea şi combaterea spălării banilor şi finanţării terorismului în activitatea unităţilor de schimb valutar.

*[Pct.28 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**29.** Banca 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 încât să aibă certitudinea că ştie cine este beneficiarul efectiv şi înţelege structura proprietăţii şi structura de control a clientului. Pentru identificarea beneficiarului efectiv banca aplică, cel puţin, cerinţele descrise la pct.26 subpct.1) lit.a)-f) şi în funcţie de riscul identificat, suplimentar pct.27 subpct.1) lit.a)-f).

*[Pct.29 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**30.** La identificarea beneficiarului efectiv al clientului – persoană juridică, inclusiv în cazul celor cu structură de proprietate complexă (persoană juridică a căror proprietari direcţi nu sunt persoane fizice), banca 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.29, 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. Banca 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 a altor tipuri de persoane juridice (inclusiv care administrează şi distribuie fonduri), banca va ţine cont de criteriile de identificare stabilite la art.52 din Legea nr.308/2017 cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului şi de Ghidul Serviciului Prevenirea şi Combaterea Spălării Banilor privind identificarea beneficiarului efectiv.

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

*[Pct.30 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**31.** 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. Banca obţine datele de identificare relevante din registre publice, de la client sau din alte surse sigure.

*[Pct.31 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**32**. Banca determină dacă persoana fizică sau juridică 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 sau iniţierea relaţiei de afaceri este efectuată de către persoana împuternicită, banca solicită procura, legalizată în modul stabilit de legislaţie. Banca aplică măsuri de identificare a persoanei împuternicite, precum şi evaluează necesitatea aplicării măsurilor de precauţie sporită, în conformitate cu prevederile prezentului Regulament. Declaraţia persoanei privind beneficiarul efectiv este completată de către beneficiarul efectiv sau de către persoana împuternicită şi conţine informaţia conform pct.26 subpct.1), lit.a)-f) şi în funcţie de riscul identificat, suplimentar pct.27 subpct.1), lit.a)-f).

**33.** La identificarea clientului banca verifică informaţia prezentată care se referă atât la client, cât şi la beneficiarul efectiv.

**34.** Banca verifică identitatea clientului şi a beneficiarului efectiv până la stabilirea relaţiei de afaceri sau în momentul stabilirii relaţiei de afaceri sau efectuării unei tranzacţii prevăzute la pct.25 subpct.2), iar în situaţiile cu risc scăzut, conform pct.51 subpct.1) din prezentul Regulament.

**35.** În vederea verificării informaţiei prezentate la identificarea clienţilor şi a beneficiarilor efectivi, banca 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, banca 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 altă bancă/instituţie financiară;

g) verificarea informaţiei prin utilizarea bazelor de date publice, private sau alte surse sigure şi independente (de exemplu: referinţa birourilor/ agenţiilor istoriei de credit);

2) pentru clienţii - persoane juridice şi întreprinzătorii individuali – prin orice metodă corespunzătoare în funcţie de gradul de risc, astfel încât banca să se asigure de veridicitatea informaţiei, cum ar fi:

a) verificarea existenţei legale a persoanei juridice şi persoanei fizice întreprinzător individual sau care practică alt tip de activitate prin verificarea înscrisului în Registrul de stat al persoanelor juridice sau, după caz, într-un alt registru public sau privat, sau altă sursă sigură independentă (de exemplu: avocaţi, contabili etc.);

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

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

d) revizuirea ultimelor rapoarte financiare (cu excepţia cazului deschiderii contului persoanei juridice nou constituite şi persoanei fizice întreprinzător individual sau care practică alt tip de activitate) şi a conturilor supuse auditului extern, dacă este cazul;

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

f) obţinerea referinţei unei bănci 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 persoana fizică întreprinzător individual sau care practică alt tip de activitate;

h) verificarea identificatorului unic al companiei şi datele asociate în baza de acces publică;

3) pentru fiducii sau construcţii juridice similare, banca verifică informaţia cel puţin prin obţinerea copiei documentului care confirmă natura şi existenţa legală a deţinătorului de cont (ca exemplu: actul fiduciar, declaraţia de trust, registrul organizaţiilor de caritate etc.). Alte proceduri de verificare pot include:

a) confirmarea documentelor prezentate dintr-o sursă independentă, cu reputaţie bună şi cunoscută, aşa ca, companie de avocaţi, contabili;

b) obţinerea unei referinţe bancare până la stabilirea relaţiei de afaceri;

c) accesarea sau căutarea în bazele de date private şi publice sau alte surse independente şi sigure;

d) verificarea identităţii persoanelor autorizate şi beneficiarului efectiv;

4) pentru verificarea identităţii beneficiarului efectiv - măsurile prevăzute la subpct. 1);

5) în cazul în care o persoană este împuternicită în numele clientului să deschidă cont sau să efectueze tranzacţii, banca verifică identitatea acesteia, legalitatea împuternicirilor, precum şi identitatea persoanei în numele căreia activează, utilizând procedurile descrise în prezentul Regulament.

*[Pct.35 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.35 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**36.** Banca atrage atenţie specială la clienţii care sunt identificaţi cu grad de risc sporit. Surse de informaţie pentru aplicarea măsurilor suplimentare de verificare pot include:

1) confirmarea adresei permanente a clientului prin utilizarea documentelor oficiale, o referinţă a registrului/agenţiei de credit sau efectuarea unei vizite la domiciliu;

2) referinţa personală (de exemplu, de către un client existent al băncii);

3) obţinerea unei referinţe bancare sau grup bancar până la stabilirea relaţiei de afaceri prin contactarea directă cu bancă cu referire la client;

4) verificarea surselor de venit, a fondurilor şi a averii identificate;

5) verificarea angajării şi funcţiei deţinute.

*[Pct.36 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**37.** 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 bancă corespunzător procedurilor interne stabilite. Documentele se prezintă individual de către persoanele vizate (client, administrator, beneficiar etc.) sau de către persoana fizică împuternicită de aceştia.

**38.** 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, banca solicită prezentarea originalelor documentelor pentru coroborarea informaţiei şi datelor prezentate. În cazul identificării şi verificării identităţii clientului la distanţă, banca 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.38 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**39.** Pe parcursul relaţiei de afaceri banca revizuieşte şi actualizează informaţia cu privire la identificarea clienţilor şi a beneficiarilor efectivi în funcţie de riscul asociat. Aceasta 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.39 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 tranzacţiilor**

**40.** Banca monitorizează încontinuu activităţile, tranzacţiile (operaţiunile) clientului sau relaţia de afaceri cu acesta. Acţiunile de monitorizare continuă cuprind:

1) determinarea tranzacţiilor 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 bancă, cu activitatea şi riscul asociat clientului. Examinarea tranzacţiilor presupune cel puţin ca banca să dispună de mecanisme/soluţii informatice, inclusiv automatizate, pentru depistarea activităţilor, tranzacţiilor şi persoanelor suspecte. Depistarea activităţilor, tranzacţiilor şi persoanelor suspecte poate fi realizată prin stabilirea limitelor valorice ale tranzacţiilor pentru o grupă particulară sau categorie de operaţiuni, conturi bancare. O atenţie deosebită se acordă tranzacţiilor care depăşesc aceste limite valorice şi tranzacţiilor ce nu au scop economic clar (de exemplu, cele care par să nu aibă un sens economic sau care implică sume mari de bani ce nu corespund aşteptărilor băncii vizând clienţii respectivi sau nu sunt specifice tranzacţiilor obişnuite ale acestora);

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) întocmirea unei note de monitorizare în care sunt evidenţiate tranzacţiile efectuate (tipul, volumul, moneda, destinaţia etc.) şi documentele confirmative prezentate şi asociate acestora, ori de câte ori este necesar în funcţie de riscul asociat. Nota de monitorizare se păstrează în dosarul clientului, iar la solicitare, se prezintă Băncii Naţionale a Moldovei şi/sau Serviciului Prevenirea şi Combaterea Spălării Banilor;

5) identificarea activităţilor, tranzacţiilor suspecte, inclusiv a celor potenţiale, precum şi a surselor mijloacelor băneşti utilizate în aceste activităţi şi tranzacţii;

6) raportarea către persoana responsabilă a informaţiei cu privire la riscurile identificate cu referire la conturile şi tranzacţiile clienţilor, inclusiv pentru clienţii cu grad de risc sporit;

7) monitorizarea în timp real a tuturor tranzacţiilor 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.

**41.** Banca acordă atenţie sporită tuturor tranzacţiilor semnificative, complexe şi neordinare care aparent nu au un scop legal sau economic. Banca examinează natura şi scopul acestor tranzacţii, iar constatările le documentează în scris şi ia măsuri de precauţie sporită în conformitate cu cerinţele prezentului Regulament. În astfel de situaţii banca obţine documente confirmative la efectuarea tranzacţiilor şi determină sursa mijloacelor băneşti utilizate (contracte, facturi fiscale/facturi, documente de expediţie, declaraţii vamale, certificate despre salariu, dări de seamă fiscale, rapoarte de activitate, alte documente).

**42**. Banca se abţine de la executarea activităţilor şi tranzacţiilor cu bunuri, inclusiv mijloace financiare, pentru un termen de până 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.

**43.** Banca aplică cerinţele pct.42 la solicitarea Serviciului Prevenirea şi Combaterea Spălării Banilor sau din proprie iniţiativă. La aplicarea cerinţelor pct.42 din proprie iniţiativă, banca informează imediat, dar nu mai târziu de 24 de ore, Serviciul Prevenirea şi Combaterea Spălării Banilor despre decizia luată.

**44.** Banca în cazul aplicării cerinţelor pct.42, la necesitate, solicită clientului furnizarea datelor şi informaţiei suplimentare, inclusiv a documentelor confirmative privind tranzacţiile 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.

**45.** Măsurile aplicate conform cerinţelor pct.42 încetează din oficiu în baza permisiunii scrise şi confirmate de Serviciu Prevenirea şi Combaterea Spălării Banilor. Dispoziţiile prezentului punct nu exonerează banca 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.12.

**46.** Banca este obligată:

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 banca nu poate asigura respectarea cerinţelor pct.25-29, 34, 35, 40 şi 41;

2) în cazul unei relaţii de afaceri existente, să înceteze relaţia de afaceri, în cazul în care banca nu poate asigura respectarea cerinţelor pct.25-29, 34, 35, 40 şi 41;

21) atunci când există o suspiciune privind spălarea banilor sau finanţarea terorismului şi banca consideră în mod rezonabil că respectarea cerinţelor pct.25-29, 34, 35, 40 şi 41 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 21), 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, banca este în drept să nu explice clientului motivul refuzului.

*[Pct.46 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**47.** Banca nu va deschide şi ţine conturi anonime sau conturi pe nume fictive, casete de siguranţă anonime, carnete de economii anonime, 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 o bancă fictivă sau cu o bancă despre care se ştie că permite unei bănci fictive să utilizeze conturile sale sau care pune la dispoziţie pentru clienţii săi conturi anonime.

*[Pct.47 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**471.** Banca 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.471 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**

**48**. Banca poate să recurgă la informaţia care aparţine persoanelor terţe, pentru a realiza măsurile prevăzute la pct.25, 26, 27, 29, 34 şi 35, 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.48 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.48 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**481.** Băncile 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.25, 26, 27, 29, 34 şi 35;

2) la cerere, copiile datelor de identificare şi alte documente aferente măsurilor prevăzute la pct.25, 26, 27, 29, 34 şi 35, inclusiv datele obţinute prin intermediul mijloacelor electronice.

*[Pct.481 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.481 introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**49**. Banca are responsabilitatea finală privind realizarea măsurilor prevăzute la pct.25-27, 29, 34 şi 35, în cazul în care apelează la persoane terţe.

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

**Capitolul VI**

**MĂSURI DE PRECAUŢIE SIMPLIFICATE PRIVIND CLIENŢII**

**50.** Banca aplică măsuri de precauţie simplificată privind clienţii atunci când, prin natura lor, pot prezenta un risc scăzut de spălare a banilor sau de finanţare a terorismului.

**51.** Măsurile de precauţie simplificată privind clienţii cuprind măsurile de precauţie privind clienţii prevăzute la pct.25, în cadrul unei proceduri simplificate aferente riscului scăzut de spălare a banilor şi de finanţare a terorismului, care include:

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

2) reducerea frecvenţei actualizării datelor de identificare;

3) reducerea gradului de monitorizare continuă a tranzacţiei sau a relaţiei de afaceri;

4) limitarea obţinerii de informaţii privind scopul şi natura relaţiei de afaceri.

În cazul în care identitatea clientului şi beneficiarului efectiv nu a fost verificată până la stabilirea relaţiei de afaceri, banca asigură realizarea acestei măsuri cât mai curând posibil după contactul iniţial, dar nu mai târziu de o lună. Până la finalizarea măsurilor de verificare, banca 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.51 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**52.** Banca, în baza evaluării proprii şi în corespundere cu rezultatele evaluării naţionale a riscurilor, 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, inclusiv dacă:

1) clientul este o autoritate publică sau întreprindere de stat;

2) clientul 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;

3) clientul este rezident al jurisdicţiilor prevăzute la subpct.4) şi 5) care îndeplinesc cerinţele standardelor internaţionale de prevenire şi combatere a spălării banilor şi a finanţării terorismului;

4) ţara (jurisdicţia) dispune de un sistem eficient de prevenire şi combatere a spălării banilor şi a finanţării terorismului conform standardelor internaţionale şi este supusă regulat evaluării în acest sens de către organizaţiile internaţionale de profil;

5) ţara (jurisdicţia) are un nivel redus de corupţie şi de criminalitate conform evaluărilor oficiale;

6) produsele şi serviciile financiare sunt limitate şi bine definite pentru un cerc de clienţi, cu scopul de a spori incluziunea financiară;

Banca, 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.52 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**521.** Pe baza unei evaluări corespunzătoare a riscurilor, care demonstrează existenţa unui risc scăzut de spălare a banilor şi de finanţare a terorismului, pentru operaţiunile de achiziţionare a bunurilor sau serviciilor, banca în calitate de prestator de servicii de plată şi emitent de monedă electronică conform Legii nr.114/2012 cu privire la serviciile de plată şi moneda electronică, 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 (banca) efectuează o monitorizare suficientă a tranzacţiilor sau a relaţiei de afaceri pentru a permite depistarea tranzacţiilor suspecte.

*[Pct.521 introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**53.** Banca nu va aplica măsuri de precauţie simplificate în cazul existenţei suspiciunii cu privire la spălare a banilor sau finanţare a terorismului.

**Capitolul VII**

**MĂSURI DE PRECAUŢIE SPORITE PRIVIND CLIENŢII**

**54.** În vederea aplicării legislaţiei în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului, banca stabileşte categoriile clienţilor, activităţile şi tranzacţiile (operaţiunile) ce prezintă un grad de risc sporit pe baza unor indicatori stabiliţi în funcţie de volumul activelor sau al veniturilor, tipul serviciilor solicitate, tipul activităţii desfăşurate, circumstanţele economice, reputaţia ţării de origine, plauzibilitatea explicaţiilor oferite de client, limitele valorice prestabilite pe categorii de tranzacţii.

**55.** Banca, în baza evaluării proprii, stabileşte factorii care generează riscuri sporite de spălare a banilor sau de finanţare a terorismului şi care determină necesitatea aplicării măsurilor de precauţie sporită privind clienţii. Factorii care generează risc sporit sunt:

1) relaţia de afaceri este desfăşurată în circumstanţe neobişnuite (de exemplu distanţa geografică semnificativă dintre bancă şi client);

2) clienţii care îşi au reşedinţa în jurisdicţii cu risc sporit de spălare a banilor şi de finanţare a terorismului;

3) clienţii care nu se prezintă personal la identificare, cu excepţia clienţilor identificaţi prin aplicarea mijloacelor electronice;

4) persoane juridice cu rol de structuri de administrare a bunurilor personale;

5) societăţi care au acţionari mandataţi sau ale căror acţiuni sunt în custodie;

6) activităţile care implică frecvent numerar în proporţii considerabile;

7) situaţiile în care structura proprietăţii şi structura de control ale persoanei juridice sunt neobişnuite sau excesiv de complexe, având în vedere natura activităţii desfăşurate;

8) serviciile bancare acordate unei persoane fizice în baza unui portofoliu personalizat negociat cu clientul;

9) tranzacţiile sunt efectuate în/din ţările (jurisdicţiile) care, conform unor surse credibile (declaraţiile publice ale GAFI, evaluări reciproce, rapoarte detaliate de evaluare sau rapoarte de monitorizare publicate) nu dispun de sisteme efective de prevenire şi combatere a spălării banilor şi finanţării terorismului;

10) tranzacţiile sunt efectuate în/din ţările (jurisdicţiile) care sunt supuse unor sancţiuni, embargouri sau măsuri similare, instituite de către organizaţiile internaţionale de profil, conform angajamentelor asumate de către Republica Moldova;

11) tranzacţiile sunt efectuate în/din ţările (jurisdicţiile) care, conform unor surse credibile, au un nivel ridicat al corupţiei sau al altor activităţi infracţionale;

12) tranzacţiile sunt efectuate în/din ţările (jurisdicţiile) care acordă finanţare sau sprijin pentru activităţi teroriste sau pe teritoriul cărora activează organizaţii teroriste desemnate;

13) produsele sau tranzacţiile care ar putea favoriza anonimatul;

14) relaţiile de afaceri sau tranzacţiile la distanţă, fără anumite măsuri de protecţie, cum ar fi semnătura electronică;

15) plăţi primite de la terţi necunoscuţi clientului/băncii sau neasociaţi acestora;

16) relaţiile transfrontaliere de corespondenţă, inclusiv la efectuarea plăţilor prin intermediul acestor conturi (payable throuth accounts);

161) clienţii şi tranzacţiile efectuate în/din adresa prestatorilor de servicii privind activele virtuale autorizaţi în alte state;

17) tranzacţii sau relaţiile de afaceri cu persoanele expuse politic;

18) produsele noi şi practicile comerciale noi, inclusiv mecanismele noi de distribuţie şi de utilizare a unor tehnologii noi sau în curs de dezvoltare atât pentru produsele noi, cât şi pentru produsele preexistente;

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

*[Pct.55 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.55 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**56.** Banca, la evaluarea riscului de spălare a banilor şi finanţare a terorismului asociat clienţilor, ţărilor/jurisdicţiilor, a produselor/serviciilor oferite, tranzacţiilor şi canalului de distribuţie asociat, va lua în considerare şi variabilele de risc implicate. Aceste variabile includ cel puţin:

1) scopul deschiderii contului de plăţi sau iniţierii relaţiei de afaceri;

2) nivelul activelor/mijloacelor băneşti depozitate de un client sau volumul tranzacţiilor efectuate;

3) frecvenţa sau durata relaţiei de afaceri.

**57.** Măsurile de precauţie sporită aplicate de bancă presupun:

1) obţinerea informaţiei suplimentare despre client şi beneficiarul efectiv (genul de activitate, volumul activelor, cifra de afaceri, altă informaţie disponibilă în 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 bunurilor şi sursa averii clientului;

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

5) obţinerea aprobării de către persoana responsabilă cu funcţie de conducere de rang superior şi/sau conducătorul sucursalei, în cazul delegării atribuţiilor, a iniţierii sau continuării relaţiei de afaceri;

6) realizarea monitorizării sporite a relaţiei de afaceri prin creşterea frecvenţei şi duratei verificărilor efectuate şi prin selectarea activităţilor şi tranzacţiilor care necesită o examinare adiţională;

7) solicitarea ca prima plată a operaţiunilor să se efectueze printr-un cont deschis în numele clientului la o bancă care aplică măsuri similare de precauţie privind clienţii;

8) 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;

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

10) în cazul relaţiilor transfrontaliere, 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;

11) măsuri suplimentare prevăzute la pct.571- 622.

*[Pct.57 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.57 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**571.** În relaţiile de afaceri cu clienţii rezidenţi care efectuează tranzacţii în/din adresa prestatorilor de servicii privind activele virtuale autorizaţi în alte state, banca:

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.571 introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**58.** În cazul prevăzut la pct.55 subpct.14), banca aplică clientului care nu se prezintă personal la identificare (de exemplu, în cazul relaţiilor prin corespondenţă scrisă sau prin telefon, e-mail, internet sau alte mijloace electronice) 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 sediile băncii, banca solicită documentele şi informaţiile conform cerinţelor prezentului Regulament. Suplimentar, banca 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 băncii;

3) utilizează informaţia prezentată de o bancă în care clientul are deschis un cont şi care aplică cel puţin aceleaşi măsuri de cunoaştere a clientului;

4) solicită ca prima plată să fie efectuată în numele clientului printr-un cont de la o altă 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 tranzacţiile cu clientul la distanţă.

**59.** În relaţiile transfrontaliere banca acumulează informaţii suficiente despre banca (instituţia, organizaţia) corespondentă pentru a înţelege pe deplin sfera de activitate a acesteia. În acest scop banca:

1) obţine cel puţin informaţiile privind:

a) consiliul şi organul executiv al instituţiei corespondente, activităţile ei cele mai importante, locul desfăşurării acestora şi măsurile aplicate de aceasta în vederea prevenirii şi combaterii spălării banilor şi finanţării terorismului;

b) beneficiarii efectivi ai instituţiei corespondente;

c) scopul deschiderii contului;

d) reputaţia instituţiei corespondente şi calitatea supravegherii, 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 controalele efectuate de instituţia corespondentă în scopul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

3) stabileşte relaţia de corespondenţă după obţinerea aprobării persoanei responsabile în bancă;

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

5) în contextul tranzacţiilor prin intermediul "conturi corespondente de transfer", banca 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 tranzacţiilor acestora.

**60.** 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, banca aplică cel puţin următoarele măsuri:

1) dispune de un sistem de gestionare a riscului care:

a) permite determinarea dacă un client, un potenţial client şi/sau beneficiarul efectiv al acestuia este sau nu persoană expusă politic;

b) solicită informaţia relevantă de la client şi/ sau beneficiarul efectiv al acestuia, utilizează referinţa la o sursă de informaţie disponibilă public sau accesează o bază de date electronică comercială cu informaţii despre persoanele expuse politic;

2) obţine aprobarea persoanei responsabile cu funcţie de conducere de rang superior în bancă sau a conducătorului sucursalei, în cazul delegării atribuţiilor, pentru stabilirea sau continuarea relaţiei de afaceri, iar în cazul în care clientul sau beneficiarul efectiv al acestuia a devenit ulterior persoană expusă politic, pentru continuarea relaţiei de afaceri;

3) stabileşte şi verifică sursa averii şi a mijloacelor băneşti implicate în relaţia de afaceri sau în tranzacţie;

4) solicită informaţii privind membrii familiei şi persoanele cunoscute ca fiind asociaţi apropiaţi ai persoanei expuse politic.

5) monitorizează sporit relaţia de afaceri şi tranzacţiile efectuate de persoana expusă politic, inclusiv actualizează periodic informaţiile despre acesta.

*[Pct.60 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**601.** 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, banca aplică măsurile de precauţie sporită prevăzute la pct.60 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, banca aplică măsurile de precauţie în funcţie de riscul identificat.

*[Pct.601 introdus prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.61 abrogat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

*[Pct.62 abrogat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**621.** În relaţiile de afaceri sau în cazul tranzacţiilor cu clienţii şi instituţiile financiare din ţările (jurisdicţiile) cu risc sporit desemnate/monitorizare de GAFI, pe lângă măsurile de precauţie sporită prevăzute de prezentul capitol, banca aplică suplimentar, în conformitate cu acţiunile solicitate de GAFI şi în funcţie 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 acestora;

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

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

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

*[Pct.621 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.621 introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**622.** Măsurile prevăzute la pct.621, precum şi alte măsuri de precauţie sporită, urmează a fi aplicate şi în cazul în care acestea sunt solicitate de Banca Naţională a Moldovei sau Serviciul Prevenirea şi Combaterea Spălării Banilor.

*[Pct.622 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.622 introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**Capitolul VIII**

**CERINŢE PRIVIND INFORMAŢIILE CARE ÎNSOŢESC**

**TRANSFERURILE DE FONDURI**

**63.** Prezentul capitol se aplică transferurilor de fonduri, în orice monedă, care sunt transmise sau primite de către o bancă sau de o bancă intermediară.

**64.** Prezentul capitol nu se aplică transferurilor de fonduri efectuate utilizând un card de plată, un instrument de monedă electronică sau orice alt dispozitiv digital sau informatic preplătit, 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;

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 sau orice alt dispozitiv digital sau informatic preplătit, cu caracteristici similare, este folosit pentru a efectua un transfer de fonduri între persoane.

**65.** Prezentul capitol nu se aplică transferurilor de fonduri care implică retragerea de numerar de către plătitor din contul de plăţi propriu.

**Secţiunea 1**

**Obligaţiile băncii plătitorului**

**66.** Banca asigură că transferurile de fonduri sunt însoţite de următoarele informaţii cu privire la plătitor:

1) denumirea/numele şi prenumele plătitorului;

2) numărul de cont de plăţi al plătitorului;

3) adresa plătitorului, numărul actului de identitate, codul fiscal (IDNO/IDNP) sau data şi locul naşterii.

**67.** Banca asigură că transferul de fonduri este însoţit de următoarele informaţii cu privire la beneficiarul plăţii:

1) numele beneficiarului plăţii;

2) numărul de cont de plăţi al beneficiarului plăţii.

**68.** Prin derogare de la pct.66 subpct.2) şi pct.67 subpct.2), în cazul transferurilor care nu se efectuează din sau către un cont de plăţi (bancar), banca 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 (bancar).

**69**. Banca, înainte de a transfera fondurile, verifică plenitudinea şi exactitatea informaţiilor menţionate la pct.66 pe baza documentelor, a datelor sau a informaţiilor obţinute dintr-o sursă credibilă şi independentă, ţinând cont de prevederile prezentului Regulament.

**70.** Banca asigură că toate transferurile de fonduri transfrontaliere sunt însoţite cu informaţii privind numele plătitorului şi beneficiarului plăţii, şi numărul contului sau un cod unic de identificare a tranzacţiei/plăţii, precum şi completarea corespunzătoare a câmpului "destinaţii plăţii/transferului".

**71.** 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.66 nu se aplică transferurilor individuale grupate, cu condiţia ca transferul procesat în baza unui fişier de grup să cuprindă informaţiile menţionate la pct.66, 67 şi 68, informaţiile respective să fi fost verificate în conformitate cu pct.69, şi transferurile individuale să fie însoţite de numărul de cont de plăţi al plătitorului sau, acolo unde se aplică pct.68, de codul unic de identificare a tranzacţiei .

**72.** Banca nu va executa/efectua transferul de mijloace băneşti dacă nu este asigurată respectarea cerinţelor pct.66-71.

**Secţiunea a 2-a**

**Obligaţiile băncii beneficiarului plăţii**

**73.** Banca instituie proceduri eficace, inclusiv, acolo unde este cazul, control a posteriori sau control în timp real, pentru a depista dacă acele câmpuri referitoare la informaţiile privind plătitorul şi beneficiarul plăţii din sistemul de plată şi decontare, utilizat pentru efectuarea transferului de fonduri, au fost completate corespunzător cerinţelor pct.66 şi 67.

**74.** Banca, înainte de înregistrarea transferului de fonduri în contul beneficiarului plăţii sau de a pune mijloacele băneşti la dispoziţia acestuia, verifică plenitudinea şi exactitatea informaţiilor menţionate la pct.67 pe baza documentelor, a datelor sau a informaţiilor obţinute dintr-o sursă credibilă şi independentă, ţinând cont de prevederile prezentului Regulament.

**75.** Banca verifică plenitudinea şi exactitatea informaţiilor referitoare la beneficiarul plăţii, pe baza documentelor, a datelor sau a informaţiilor obţinute dintr-o sursă credibilă şi independentă, ţinând cont de prevederile prezentului Regulament, în cazul transferurilor de fonduri în cuantumul ce nu depăşeşte limita stabilită la pct.25 subpct.2) în următoarele situaţii:

1) când plata este efectuată în numerar, dacă tranzacţiile par a avea legătură între ele;

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

*[Pct.75 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**76.** Banca pune în aplicare proceduri eficace bazate pe evaluarea riscurilor, pentru a determina dacă să execute, să respingă sau să suspende un transfer de mijloace băneşti în cazul căruia informaţiile complete privind plătitorul şi beneficiarul plăţii lipsesc. Banca ia în considerare aplicarea acestor proceduri şi în cazul în care nu este completat câmpul "destinaţii plăţii/transferului".

**77.** Banca, dacă constată că la primirea transferului de fonduri, informaţiile menţionate la pct.66 şi 67 lipsesc sau sunt incomplete respinge transferul sau solicită informaţiile cerute privind plătitorul şi beneficiarul plăţii, înaintea înregistrării transferului de fonduri în contul beneficiarului plăţii sau de a pune mijloacele băneşti la dispoziţia acestuia, în funcţie de riscul asociat.

**78.** În cazul în care instituţia/banca care efectuează plata omite în mod regulat să furnizeze informaţiile obligatorii cu privire la plătitor sau beneficiarul plăţii, banca beneficiară ia măsuri care pot consta, mai întîi, în emiterea unor avertismente şi stabilirea unor termene-limită, înainte fie de a respinge orice transfer de fonduri care provine de la aceasta, fie de a decide, dacă este cazul, să restrângă sau să înceteze relaţia comercială cu respectiva instituţie/bancă. Banca informează despre astfel de situaţii Serviciul Prevenirea şi Combaterea Spălării Banilor conform actelor normative în vigoare.

**781.** Banca, atunci când acţionează în calitate de bancă a plătitorului şi a beneficiarului plăţii, ia în considerare toate informaţiile 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.781 introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**Secţiunea a 3-a**

**Obligaţiile băncii intermediare**

**79.** Banca instituie proceduri eficace, inclusiv, acolo unde este cazul, control a posteriori sau control în timp real, pentru a depista dacă acele câmpuri referitoare la informaţiile privind plătitorul şi beneficiarul plăţii din sistemul de plată şi decontare, utilizat pentru efectuarea transferului de fonduri, au fost completate corespunzător cerinţelor pct.66 şi 67 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.79 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**80.** Banca asigură că transferurile de fonduri pe baza unui fişier de grup conţine numărul contului de plată al plătitorului sau un cod unic de identificare a tranzacţiei/plăţii, iar fişierul de grup deţine informaţiile privind plătitorul şi beneficiarul plăţii, care are trasabilitate completă.

**81.** Banca pune în aplicare proceduri eficace bazate pe evaluarea riscurilor, pentru a determina dacă să execute, să respingă sau să suspende un transfer de mijloace băneşti în cazul căruia informaţiile cerute privind plătitorul şi beneficiarul plăţii lipsesc. Banca ia în considerare aplicarea acestor proceduri şi în cazul în care nu este completat câmpul "destinaţii plăţii/transferului".

**82.** Banca, dacă constată că la primirea transferului de fonduri, informaţiile menţionate la pct.66 şi 67 lipsesc sau sunt incomplete, fie respinge transferul sau solicită informaţiile cerute privind plătitorul şi beneficiarul plăţii înainte sau după transmiterea transferului de fonduri, în funcţie de riscul asociat.

**83.** În cazul în care instituţia/banca care efectuează transferul/plata omite în mod repetat să furnizeze informaţiile cerute cu privire la plătitor sau beneficiarul plăţii, banca intermediară ia măsuri care pot consta, mai întîi, în emiterea unor avertismente şi stabilirea unor termene-limită, înainte de respingerea oricărui transfer de fonduri care provine de la aceasta, fie de a decide, să restrîngă sau să înceteze relaţia comercială cu respectiva instituţie/bancă.

**84**. Banca informează despre situaţiile descrise la pct.83 Serviciul Prevenirea şi Combaterea Spălării Banilor conform actelor normative în vigoare.

**Capitolul IX**

**RAPORTAREA ACTIVITĂŢILOR ŞI A TRANZACŢIILOR**

**85.** Banca este obligată 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.85 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.85 modificat prin Hot.BNM nr.324 din 20.12.2018, în vigoare 04.02.2019]*

**86.** Banca 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 bunurilor suspecte, activităţilor sau tranzacţiilor suspecte de spălare a banilor, de infracţiuni asociate acestora şi de finanţare a terorismului;

2) sisteme de depistare a activităţilor şi tranzacţiilor suspecte conform criteriilor şi indicilor stabilite, inclusiv de autorităţile competente;

3) proceduri de informare a persoanei responsabile cu funcţii de conducere de rang superior în bancă şi la necesitate a serviciului de securitate internă privind problemele ce ţin de prevenirea şi combaterea spălării banilor şi finanţării terorismului.

*[Pct.86 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**Capitolul X**

**PĂSTRAREA DATELOR**

**87.** Banca 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 tranzacţiei ocazionale.

*[Pct.87 în redacţia Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.87 în redacţia Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**88.** 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 clientului; IDNO/IDNP, după caz; numărul contului; 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 tranzacţiile efectuate (tipul, volumul, moneda, destinaţia etc.) şi notele de monitorizare aferente, inclusiv pentru cele complexe şi neordinare;

41) 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 tranzacţiile şi corespondenţa de afaceri în sistemele tehnologiilor informaţionale (TI) şi păstrarea arhivei în condiţii de siguranţă şi disponibilitate operativă.

*[Pct.88 completat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

**89.** Banca asigură că, în caz de solicitare, documentele şi informaţia privind identificarea şi verificarea clienţilor, a beneficiarilor efectivi, privind monitorizarea operaţiunilor clienţilor, inclusiv documentele confirmative aferente tranzacţiilor naţionale şi internaţionale sunt accesibile, în mod operativ, Băncii Naţionale a Moldovei şi Serviciului Prevenirea şi Combaterea Spălării Banilor. Datele păstrate trebuie să fie suficiente ca să permită reconstituirea fiecărei tranzacţii şi să servească, la necesitate, în calitate de probe în cadrul procedurilor legale. La solicitarea autorităţilor competente, conform art.9 alin.(21) 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.89 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**Capitolul XI**

**CERINŢE PRIVIND SISTEMUL DE CONTROL INTERN**

**90.** Banca va dispune de sisteme de control intern care vor asigura conformarea continuă a băncii actelor normative şi programului intern în domeniu şi vor contribui la minimizarea riscurilor aferente.

**91.** La deschiderea de filiale şi sucursale pe teritoriul altor state, precum şi pe parcursul activităţii acestora, banca 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 (jurisdicţia) cerinţele de prevenire şi combatere a spălării banilor şi finanţării terorismului sunt insuficiente, banca trebuie să asigure implementarea cerinţelor actelor normative ale Republicii Moldova, în măsura în care legislaţia ţării (jurisdicţiei) permite. Dacă ţara (jurisdicţia) nu permite aplicarea corespunzătoare a cerinţelor actelor normative ale Republicii Moldova, banca 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 a Moldovei poate aplica măsuri de supraveghere potrivit cadrului legal, pentru asigurarea respectării de către filialele şi sucursalele deschise pe teritoriul altor state a actelor normative în vigoare aferente domeniului dat, iar dacă se constată nerespectarea acestora, Banca Naţională a Moldovei poate limita activitatea sau retrage aprobarea emisă pentru deschiderea filialelor şi sucursalelor deschise 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 bancă în cazul în care normele de drept ale altei ţări (jurisdicţii) nu permit punerea în aplicare a măsurilor prevăzute în prezentul punct.

**92.** Banca comunică şi implementează prevederile programului propriu pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului în cadrul sucursalelor, filialelor şi altor subdiviziuni deţinute, inclusiv al celor situate în alte ţări. În scopul prevenirii şi combaterii spălării banilor şi finanţării terorismului, banca efectuează schimb de date cu sucursalele, filialele şi alte subdiviziuni deţinute în condiţiile respectării cerinţelor actelor normative în vigoare.

**921.** În cazul deschiderii filialelor şi sucursalelor 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.93-95, 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 bancar şi date cu caracter personal, precum şi modul de utilizare şi procesare a acestor informaţii.

*[Pct.921 introdus prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

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

1) efectuarea de către subdiviziunea de audit intern a auditului independent în vederea verificării conformării băncii cerinţelor privind prevenirea şi combaterea spălării banilor şi finanţării terorismului. Funcţiile auditului în acest scop sunt:

a) evaluarea independentă a adecvării politicilor şi procedurilor aferente domeniului prevenirii şi combaterii spălării banilor şi finanţării terorismului riscurilor de spălare a banilor şi finanţare a terorismului identificate;

b) evaluarea independentă a eficienţei personalului băncii la implementarea politicilor şi procedurilor aprobate aferente domeniului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului;

c) evaluarea independentă a eficacităţii supravegherii conformităţii şi a controlului calităţii, inclusiv parametrii criteriilor pentru alertele automate;

d) evaluarea independentă a eficacităţii instruirii de către bancă a personalului relevant;

e) informarea organelor de conducere privind rezultatele verificării şi recomandarea asupra măsurilor necesare a fi întreprinse pentru minimizarea riscurilor şi neajunsurilor identificate;

2) desemnarea persoanelor responsabile de asigurarea conformării băncii cu actele normative în vigoare privind prevenirea şi combaterea spălării banilor şi finanţării terorismului. Persoana responsabilă cu funcţii de conducere de rang superior desemnată din rândul membrilor Consiliului băncii şi/sau organului executiv are următoarele atribuţii:

a) acordă consultaţii angajaţilor băncii 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 băncii şi evaluarea riscului de spălare a banilor şi finanţare a terorismului;

b) aprobă începerea, continuarea, încetarea relaţiilor de afaceri cu clienţii cu grad de risc sporit (sau deleagă atribuţia dată conducătorului sucursalei, după caz);

c) ia decizii în baza informaţiei primite;

d) întreprinde măsuri privind raportarea Serviciului Prevenirea şi Combaterea Spălării Banilor a informaţiei în conformitate cu legislaţia;

e) organizează instruirea angajaţilor băncii în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

f) prezintă în scris, cel puţin o dată pe an, consiliului băncii un raport privind rezultatele realizării programului privind prevenirea şi combaterea spălării banilor şi finanţării terorismului, inclusiv informează asupra riscurilor de spălare a banilor şi finanţare a terorismului identificate pe parcursul anului şi măsurile luate pentru minimizarea acestora;

g) colaborează cu serviciul de audit în vederea îndeplinirii scopului acestuia privind verificarea conformării activităţii băncii la legislaţia în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului;

h) îndeplineşte alte funcţii în corespundere cu prezentul Regulament şi documentele interne ale băncii;

3) prevederi interne privind răspunderea şi sancţionarea angajaţilor care nu informează/raportează despre activităţile sau tranzacţiile suspecte persoana responsabilă, serviciul securităţii sau direct autoritatea competentă şi/sau contribuie personal la efectuarea operaţiunilor de spălare a banilor şi finanţare a terorismului.

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

**94.** Banca va dispune de programe de selectare şi instruire continuă a personalului în domeniul prevenirii şi combaterii spălării banilor şi finanţării terorismului. Banca asigură deţinerea de către personalul şi persoana responsabilă cu funcţii de conducere de rang superior în bancă 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.94 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**95.** Programele de selectare şi instruire indicate la pct.94 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 identificarea clienţilor, verificarea identităţii acestora, monitorizarea conturilor/tranzacţiilor 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 băncii.

**96**. Banca 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 în vigoare cu privire la protecţia datelor cu caracter personal.

**Capitolul XII**

**CERINŢE PRIVIND APLICAREA MĂSURILOR**

**RESTRICTIVE INTERNAŢIONALE**

**97.** Banca 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.97 completat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

*[Pct.97 modificat prin Hot.BNM nr.38 din 11.03.2021, în vigoare 02.07.2021]*

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

1) proceduri de monitorizare, compilare, 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;

2) proceduri de verificare/depistare a persoanelor sau entităţilor desemnate şi a tranzacţiilor (operaţiunilor) în care sunt implicate bunuri, aplicabile potenţialilor clienţi, clienţilor existenţi şi solicitanţilor de tranzacţii 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.

**99.** Banca 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 masa care fac obiectul măsurilor restrictive, întreprinde succesiv următorii paşi:

1) prin decizia (ordinul) persoanei responsabile cu funcţii de conducere de rang superior în bancă, 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 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 restrictive aplicată etc) despre persoana, grupul sau entitatea identificată;

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

c) informarea despre decizia persoanei responsabile cu funcţii de conducere de rang superior în bancă cu privire la abţinerea, pentru un termen nedeterminat, de la executarea activităţilor şi tranzacţiilor cu referire la bunul identificat;

3) dacă este cazul, banca 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.99 subpct.1), precum şi informează despre acest fapt Serviciul Prevenirea şi Combaterea Spălării Banilor ţinând cont de cerinţele pct.99 subpct.2) lit.a) şi b);

4) informează Banca Naţională a Moldovei despre măsura restrictivă aplicată, ţinând cont de cerinţele pct.99 subpct.2) lit.a) şi b).

*[Pct.99 modificat prin Hot.BNM nr.20 din 24.01.2024, în vigoare 08.02.2024]*

**100.** 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, banca informează neîntîrziat despre aceasta, în termen de cel mult 24 de ore, Serviciul Prevenirea şi Combaterea Spălării Banilor.

**101.** Banca 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 XIII**

**ALTE DISPOZIŢII**

**102.** 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.

**103.** În aplicarea prezentului Regulament, banca informează Banca Naţională a Moldovei despre activităţile suspecte şi incidentele de fraudă care prezintă riscuri pentru siguranţa, buna funcţionare sau reputaţia băncii.

Anexă

la Regulamentul cu privire la cerinţele privind

prevenirea şi combaterea spălării banilor şi

finanţării terorismului în activitatea băncilor

**Recomandări**

**privind criteriile de identificare a beneficiarului efectiv**

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