Proiect

BANCA NAȚIONALĂ A MOLDOVEI

HOTĂRÂRE

Nr. _____ din _____2023

cu privire la aprobarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice

În temeiul art.27 alin.(1) lit. c) din Legea nr.548/1995 cu privire la Banca Națională a Moldovei (republicată în Monitorul Oficial al Republicii Moldova, 2015, nr.297-300, art.544), cu modificările ulterioare, art. 5^1 alin. (3), art. 15 alin. (1) lit. a) și alin. (2) lit. a) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr. 58-66, art. 133), cu modificările ulterioare, Comitetul executiv al Băncii Naționale a Moldovei

HOTĂRĂŞTE:

1. Se aprobă Regulamentul privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (se anexează).

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

Președintele Comitetului executiv

Anexă
Aprobat prin Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr. ___ din _____ 2023

Regulamentul privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice

Capitolul I. Dispoziții generale

1. Prezentul Regulament privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (în continuare - Regulament) are drept scop stabilirea cerințelor privind politicile și procedurile necesare, sistemul de control intern, riscurile și măsurile de protecție, precum și cerințele tehnice minime în scop de identificare a clienților și verificarea identității acestora de către subiecții specificați la pct. 3 în cazul stabilirii și /sau desfășurării relațiilor de afaceri cu aceștia fără prezență fizică.

2. Cerințele, normele, regulile, procedurile, practicile, limitele și pragurile de raportare aplicabile pentru clienții identificați cu prezență fizică sunt aplicabile și prezentului Regulament, iar măsurile de prevenire și combatere a spălării banilor și finanțării terorismului se vor aplica în conformitate cu cerințele Legii nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (în continuare - Legea nr. 308/2017) și actele normative aprobate pentru implementarea acesteia.

3. Sub incidența prevederilor prezentului Regulament cad entitățile raportoare prevăzute la art. 4 alin. (1) lit. a), e), g) și i) din Legea nr. 308/2017.

4. Termenii, noțiunile și expresiile utilizate în prezentul Regulament au semnificațiile stabilite în Legea nr. 308/2017, Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere (în continuare - Legea nr. 124/2022) și actele normative emise pentru implementarea acestora. De asemenea, în sensul prezentului Regulament se utilizează următorii termeni și expresii:

soluție informatică pentru identificarea la distanță (soluție) – un ansamblul de elemente tehnologice implicate în procesul de identificare a persoanei la distanță prin mijloace digitale, prin care se transmit datele, imaginile capturate/încărcate și/sau informațiile comunicate de solicitant;

înregistrare la distanță a clientului – reprezintă identificarea și verificarea identității clientului prin intermediul mijloacelor electronice realizate prin utilizarea unei metode sau a mai multor metode concomitent, prevăzute la art.5[1] alin.(2) din Legea nr.308/2017.

Capitolul II. Politici și proceduri referitoare la identificarea și verificarea identității clienților prin mijloace electronice

A. Politici și proceduri interne

5. Entitatea va elabora, aproba și menține politici și proceduri pentru a se conforma obligațiilor care îi revin în temeiul art.5 alin.(2) lit. a) și lit. c) din Legea nr.308/2017, în situațiile în care clientul este identificat la distanță. Aceste politici și proceduri trebuie să fie stabilite în funcție de riscurile de spălare a banilor și finanțare a terorismului identificate și să cuprindă cel puțin următoarele:

a) o descriere generală a soluției pe care o utilizează pentru a colecta, verifica și înregistra informații pe tot parcursul procesului de înregistrare la distanță a clienților. Aceasta trebuie să includă o explicație a elementelor și funcționării soluției;

b) situațiile în care poate fi utilizată soluția de identificare la distanță a clienților, ținând cont de factorii de risc identificați și evaluați în conformitate cu art. 6 alin. (1) din Legea nr.308/2017, în cadrul evaluării riscurilor în domeniul propriu de activitate, inclusiv descrierea categoriei de clienți, produse și servicii eligibile pentru identificare la distanță;

c) etapele care sunt complet automatizate și etapele care necesită intervenție umană;

d) controalele instituite pentru a se asigura că prima tranzacție cu un client nou înregistrat este executată numai după ce au fost aplicate toate măsurile inițiale de precauție privind clienții;

e) descrierea programelor de inițiere și de formare periodică pentru a asigura sensibilizarea personalului și informarea continuă și înțelegerea funcționării soluției de identificare la distanță a clienților și a riscurilor asociate.

B. Evaluarea preimplementare a soluției

6. Entitatea raportoare, atunci când analizează dacă să fie implementată o nouă soluție de identificare la distanță a clienților, va efectua o evaluare preimplementare. Astfel, entitatea va stabili domeniul de aplicare, pașii și cerințele în materie de evidență a datelor, care ar trebui să includă cel puțin:

a) o evaluare a caracterului adecvat al soluției în ceea ce privește plenitudinea și acuratețea datelor și documentelor care urmează a fi colectate, precum și a fiabilității și independenței surselor de informații utilizate;

b) o evaluare a impactului utilizării soluției asupra riscurilor specifice ale entității, inclusiv de spălarea banilor și finanțarea terorismului, operaționale, reputaționale și juridice, în special, cel de neconformare cu cerințele aplicabile privind protecția datelor cu caracter personal;

c) identificarea posibilelor măsuri de atenuare și acțiuni de remediere pentru fiecare risc identificat;

d) evaluarea conformității soluției cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace digitale stabilite pentru

prestatorul de serviicii de încredere calificat, stabilite în temeiul prevederilor Legii nr. 124/2022;

e) teste pentru a evalua riscurile de fraudă, inclusiv riscurile de fraudă prin uzurparea identității;

f) o evaluare a riscurilor asociate tehnologiei informației și comunicațiilor (TIC) și de securitate;

g) o testare end-to-end a funcționării soluției care vizează clienții, produsele și serviciile oferite în conformitate cu politicile și procedurile de identificare la distanță aprobate.

7. Entitatea va prezenta și demonstra BNM realizarea evaluărilor și testelor menționate la pct. 6., rezultatul acestora, precum și modul în care aplicarea soluției asigură atenuarea și remedierea riscurilor de spălare a banilor și finanțare a terorismului și alte riscuri identificate pentru tipurile de clienți, servicii, produse, jurisdicții, pentru care aceasta este aplicabilă.

C. Monitorizarea continuă a soluției

8. Entitatea raportoare va monitoriza soluția de identificare la distanță a clienților în mod continuu pentru a se asigura că funcționează în conformitate cu scopul acesteia. În acest context, entitatea va dispune de politici și proceduri care vor cuprinde cel puțin:

a) pașii pe care entitatea îi va întreprinde pentru a fi satisfăcută de calitatea, plenitudinea, acuratețea, caracterul adecvat și securitatea datelor colectate în timpul procesului de identificare la distanță a clienților și care trebuie să fie proporțional cu riscurile de spălare a banilor și finanțare a terorismului la care aceasta este expusă;

b) scopul și frecvența unor astfel de revizuiri periodice; și

c) circumstanțele care vor declanșa revizuiri ad-hoc, care ar trebui să includă cel puțin:

- modificări ale expunerii la riscul de spălare a banilor și finanțare a terorismului entității;
- deficiențe privind funcționarea soluției detectate în cursul activităților de monitorizare, audit sau supraveghere;
- o creștere estimată a tentativelor de fraudă;
- modificări ale cadrului legal.

9. Entitatea raportoare se asigură că mecanismele de monitorizare sunt bazate pe riscuri și iau în considerare, ca o condiție minimă, cel puțin următorii factori:
   a) listele de elemente de identificare compromise sau furate;
   b) scenariile de fraudă cunoscute în ceea ce privește identificarea la distanță;
   c) indicatori privind compromiterea confidențialității, integrității sau autenticității sesiunii ca urmare a procedurii de identificare;
   d) registrul de utilizare normală și anormală a dispozitivului de acces sau a programului informatic furnizat persoanei ce urmează a fi identificată de către entitatea raportoare;

e) poziția geografică anormală/neobișnuită a persoanei;
f) poziția geografică cu risc ridicat a persoanei.

10. Entitatea raportoare va stabili în politicile și procedurile interne măsuri de remediere în cazul în care s-a materializat un risc sau în cazul în care au fost identificate erori care au un impact asupra eficacității soluției. Aceste măsuri vor include cel puțin:

a) o revizuire a tuturor relațiilor de afaceri afectate, pentru a evalua dacă entitatea a aplicat suficient măsurile de precauție față de cllienți; prioritatate fiind acordată relațiilor cu grad de risc sporit de spălare a banilor și finanțare a terorismului;

b) luând în considerare informațiile obținute în cadrul revizuirii menționate mai sus, o evaluare a faptului dacă o relație de afaceri afectată ar trebui să fie:

- supusă unor măsuri sporite de precauție;
- supusă unor stabiliri de limite privind volumul tranzacțiilor, până în momentul în care a avut loc o revizuire;
- încheiată;
- raportată către Serviciul Prevenirea și Combaterea Spălării Banilor;
- reclasificată într-o categorie de risc diferită.

11. Entitatea raportoare va lua în considerare modalitatea cea mai eficientă de a monitoriza adecvarea și fiabilitatea continuă a soluției de identificare la distanță a clienților. În acest scop, aceasta va lua în considerare unul sau mai multe dintre următoarele mijloace, dar fără a se limita la acestea:

- testarea asigurării calității;
- alerte critice automate și notificările;
- rapoartele automate regulate de calitate;
- testarea eșantionului;
- recenziile manuale ale experților din industrie și autorităților de supraveghere .

Capitolul III. Criteriile de eligibilitate și metode de identificare și verificare a identității clienților prin mijloace electronice

12. Entitatea raportoare va efectua identificarea și verificarea identității clientului prin mijloace electronice, în privința:

a) potențialilor clienți noi cu care entitatea intenționează să stabilească relații de afaceri;

b) clienților existenți, care fac obiectul procedurilor de revizuire și actualizare a informațiilor.

13. Entitatea raportoare va efectua identificarea și verificarea clienților prin mijloace electronice, în raport cu:

a) persoana fizică, cetățean al Republicii Moldova;

b) persoana juridică rezidentă, ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai Republicii Moldova.

14. Entitatea raportoare se va asigura că soluția de identificare la distanță a clienților are elemente pentru a colecta:

a) toate datele și documentele relevante pentru identificarea și verificarea persoanei fizice și/sau juridice;

b) toate datele și documentele relevante pentru a verifica dacă persoana fizică care acționează în numele persoanei juridice are dreptul legal de a acționa astfel;

c) informațiile privind beneficiarii reali;

d) toate datele și documentele relevante pentru determinarea naturii și scopului relației de afaceri.

15. Entitatea raportoare realizează identificarea și verificarea identității clienților, în baza unei evaluări corespunzătoare a riscurilor, și prin utilizarea uneia sau a mai multor metode, în funcție de risc:

a) prin mijloace de identificare electronică cu un nivel de securitate suficient și conform cu standardele stabilite în Legea nr.124/2022;

b) prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului;

c) prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022.

16. Indiferent de metoda aplicată, trebuie să fie asigurată colectarea și prezentarea de către client, cel puțin, a informațiilor care de obicei se solicită și sunt aplicabile clienților identificați cu prezență fizică. Modalitatea de colectare a informației va fi determinată de entitatea raportoare, dar urmează să definească care informație va fi colectată:

a) manual;

b) automat din documentele prezentate de către client;

c) din alte surse interne sau externe.

17. Entitatea raportoare va pune în aplicare și va menține mecanisme adecvate pentru a se asigura că informațiile pe care le captează automat, în conformitate cu punctul 14, sunt fiabile. Aceasta trebuie să aplice controale (cel puțin anuale) pentru a aborda riscurile asociate acestui proces, inclusiv de ascundere a locației adreselor de Protocol Internet (IP), utilizarea serviciilor de tipul rețelelor virtuale private (VPN-uri).

18. În cazul clientului persoană juridică, măsurile de identificare se vor aplica persoanei fizice cu mandat de reprezentat legal al acesteia, având în vedere documentele de înregistrare corespunzătoare a persoanei juridice. În aceste condiții, pentru persoana fizică,

entitatea raportoare va aplica procesul de identificare la distanță similar unei persoane fizice. În același context, vor fi aplicate măsuri pentru asigurarea verificării dacă persoana fizică care acționează în numele persoanei juridice are dreptul legal de a acționa astfel.

19. În scopul verificării și validării datelor obținute de la client, entitatea raportoare este în drept să acceseze resursele informaționale și bazele de date disponibile, cu respectarea prevederilor legale din domeniul protecției datelor cu caracter personal.

20. Identificarea clientului este precedată de exprimarea clară și neechivocă a consimțământului, inclusiv cu privire la înregistrarea video, audio, prelucrarea și păstrarea acestor date.

21. În cazul identificării clientului prin mijloace electronice, entitatea raportoare va asigura aducerea la cunoștință a clientului termenele și condițiile în care identificarea electronică a clientului este efectuată. Termenele și condițiile puse la dispoziția clientului, anterior sau concomitent cu primirea consimțământului pentru efectuarea identificării electronice a clientului, vor fi întocmite după cum urmează :

a) „Termenele de utilizare" (a paginii electronice, sistemului, platformei utilizate etc.) – urmează să conțină condițiile generale pentru accesarea sistemului utilizat în vederea identificării prin mijloace electronice a clientului;

b) „Politica de confidențialitate" – va conține informațiile pe care entitatea raportoare le primește de la client în procesul identificării (date cu caracter personal), obligațiile pe care le are conform legii în procesul de utilizare / prelucrare a datelor, precum și măsurile de control implementate pentru a asigura confidențialitatea datelor colectate;

c) „Politica privind fișierele cookie" – va conține descrierea fișierelor cookie pe care entitatea raportoare le folosește în scopul urmăririi acțiunilor clientului pe platformă sau pagina electronică (sub condiția utilizării);

d) „Dezvăluirea riscurilor" – în scopul respectării drepturilor consumatorului se explică natura aferentă comunicării electronice și riscurilor care derivă din aceasta;

e) „Politica prevenirii spălării banilor" – va conține versiunea succintă / desfășurată a politicii privind identificarea clientului, prevenirea spălării banilor, finanțarea terorismului și identificarea persoanelor expuse politic .

Capitolul IV. Metode de înregistrare la distanță a clienților

A. Identificarea prin mijloace de identificare electronică cu un nivel de securitate suficient și conform cu standardele stabilite în Legea nr.124/2022

22.Entitatea raportoare poate utiliza serviciile de încredere relevante și procesele de identificare electronică reglementate, recunoscute, aprobate sau acceptate la nivel național, pentru a se conforma prezentului Regulament. Atunci când utilizează astfel de soluții, entitatea trebuie să evalueze în ce măsură soluția respectă dispozițiile prezentului Regulament și să aplice măsurile necesare pentru a atenua riscurile relevante care decurg

din utilizarea soluțiilor respective. Aceasta trebuie să ia în considerare, în special, dacă sunt abordate următoarele riscuri:

a) riscurile pe care le implică autentificarea și care sunt prevăzute în politicile și procedurile sale specifice măsurilor de atenuare, în special în ceea ce privește riscurile de fraudă prin uzurparea identității;

b) riscul ca identitatea clientului să nu fie identitatea pretinsă;

c) riscul de pierdere, furt, suspendare, revocare sau expirare a dovezilor de identitate, inclusiv, după caz, a instrumentelor de detectare și prevenire a utilizării fraudelor de identitate.

B. Identificarea prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice cu înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului

23.Entitatea raportoare poate utiliza mijloacele electronice în scopul stabilirii/continuării relației de afaceri cu persoanele fizice și juridice, care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice (liveness), cu înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului.

24. La identificarea video, entitatea se asigură că procesul este înregistrat și corespunde următoarelor:

a) este de o durată rezonabilă (stabilită conform politicilor interne), și conține, cel puțin, următoarele informații/date relevante:

- ora, ziua, anul înregistrării;
- momentul exact în care persoana fizică supusă verificării video prezintă datele sale de identificare din documentul de identitate (numele și prenumele, IDNP, data/luna/anul nașterii, adresa de reședință, ora/data/luna/anul în care se face înregistrarea, precum și numărul de contact al telefonului mobil);
- momentul în care angajatul entității raportoare ia legătură cu persoana în timpul verificării video și/sau momentul în care clientul primește codul unic remis prin serviciul de mesaje scurte (SMS) la telefonul mobil;
- momentul în care clientul apropie actul de identitate de cameră și îl afișează pe ambele părți;

b) este în concordanță cu următoarele condiții:

- procesul identificării video se desfășoară în condiții de liniște și a unei bune iluminări în spațiul clientului, care permite identificarea clară a acestuia, în caz contrar, procesul urmează a fi întrerupt;
- în aceeași încăpere cu clientul nu trebuie să se regăsească persoane terțe;

- identificarea, verificarea și păstrarea datelor tehnice ale computerului / dispozitivului utilizat de către client (amprenta dispozitivului), IP adresa, localizarea acestuia, date despre calculatorul/dispozitivul utilizat (modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea), precum și alte date posibil a fi colectate;
- procesul de verificare video trebuie să se desfășoare în timp real și fără întreruperi prin flux continuu. Dacă procesul de verificare a fost întrerupt, indiferent de motivul întreruperii, acesta urmează a fi reluat de la început;
- calitatea informației audiovizuale (calitatea imaginii și a sunetului în timpul verificării video) trebuie să fie de o calitate înaltă, cu o rezoluție de cel puțin 8 mega pixeli sau mai mare FullHD (1920x1080), în scopul identificării și recunoașterii necondiționate a persoanei, asigurării unei discuții libere și clare între angajatul entității raportoare și client, precum și verificării vizuale de către angajatul entității raportoare a documentelor prezentate de către client, inclusiv a elementelor de protecție aplicabile documentului respectiv.

25. În cazul în care entitatea raportoare utilizează soluții de identificare la distanță neasistate, în care clientul nu interacționează cu un angajat pentru a efectua procesul de verificare, acestea trebuie pe lângă cerințele stipulate supra:

- să se asigure că orice fotografie (fotografii) sau înregistrare video este realizată (sunt realizate) în condiții de iluminare adecvate și că proprietățile necesare sunt captate cu claritatea necesară pentru a permite verificarea corespunzătoare a identității clientului;
- să se asigure că orice fotografie (fotografii) sau înregistrare video este realizată (sunt realizate) în momentul în care clientul efectuează procesul de verificare;
- să efectueze verificări de detectare a mișcării clientului, care pot include proceduri în cadrul cărora este necesară o acțiune specifică din partea clientului pentru a verifica dacă acesta este prezent la sesiunea de comunicare sau care se pot baza pe analiza datelor primite și nu necesită o acțiune specifică din partea clientului;
- să utilizeze algoritmi de verificare a corespunderii elementelor actului de identitate prezentat precum ortografia cifrelor, codului de autoritate și a altor înscrisuri existente;
- să utilizeze algoritmi puternici și fiabili pentru a verifica dacă fotografia (fotografiile) sau înregistrarea video realizată (realizate) corespund fotografiei (fotografiilor) extrase din documentul (documentele) oficiale ale clientului.

26.În cazul în care entitatea raportoare utilizează soluții de identificare la distanță neasistate, aceasta efectuează identificarea, verificarea și păstrarea datelor tehnice ale computerului / dispozitivului utilizat de către client, inclusiv a IP adresei, localizarea acestuia, precum și alte date posibil a fi colectate.

27. În cadrul identificării video entitatea raportoare verifică actele de identitate ale clientului sub următoarele aspecte:

a) identificarea deteriorării sau falsificării documentului, în special prin aplicarea (lipirea) fotografiei false deasupra originalului, corespunderea formei, elementelor de securitate (ex. holograme, elemente optic variabile, fonturi speciale etc.), caracterelor și a spațiilor între acestea cu standardele aplicabile tipului de document de identitate prezentat, înclinarea documentului pe orizontală și verticală;

b) verificarea corespunderii înfățișării clientului cu fotografia din actul de identitate;

c) verificarea valabilității actului de identitate;

d) confirmarea existenței și corespunderii elementelor de protecție care trebuie să fie prezente pe documentul de identitate prezentat de către client cu standardele aplicabile tipului respectiv de acte.

e) verificarea corespunderii a cel puțin trei elemente de securitate ale actului de identitate, selectate aleatoriu, cu elementele de securitate proprii tipului respectiv de acte;

f) în cazul existenței suspiciunilor privind identitatea persoanei sau autenticitatea documentelor prezentate vor fi adresate întrebări adiționale în scopul verificării identității persoanei și autenticității documentelor

28. În scopul verificării și validării datelor/ informațiilor obținute de la client în procesul verificării video, entitatea raportoare este:

a) obligată să verifice clientul sub aspectul:

- implicării în activități teroriste sau de proliferare a armelor de distrugere în masă;
- aplicării sancțiunilor internaționale;
- aplicării sancțiunilor financiare ale Uniunii Europene;
- deținerii calității de persoană expusă politic sau altor factori de risc sporit;
- existenței informațiilor care ar putea influența reputația clientului, prin accesarea surselor credibile informaționale și/sau baze de date disponibile, public accesibile și/sau internet, inclusiv deținute de alte instituții publice și entități;
- caracteristicilor comportamentale ale persoanei care pot indica un comportament suspect în timpul identificării video;

b) obligată să solicite informații despre natura și scopul relației de afacere și/sau operațiunii și poate solicita prezentarea fizică la oficiul său, în cazul existenței suspiciunilor și/sau dubiilor în privința viciului de voință/consimțământ (presiuni sau influențe fizice sau psihologice) al clientului din partea terților persoane;

c) în drept să solicite utilizarea semnăturii electronice pe copia actului de identitate, cu titlu de măsură suplimentară față de identificarea video, în cazul existenței dubiilor privind veridicitatea informației prezentate de către client;

d) obligată să verifice datele/informațiile primite prin intermediul comunicării electronice în conformitate cu prevederile reglementărilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

29. Entitatea raportoare este obligată să nu intre în relațiile de afaceri cu clientul urmare identificării video în următoarele cazuri:

a) procedura de verificare video nu corespunde cerințelor prezentului Regulament;

b) există suspiciuni în privința falsificării / nevalabilității semnăturii electronice/digitale, în situația cînd aceasta se utilizează;

c) există suspiciuni privind existența presiunii și/sau influenței fizice/psihologice (viciul de voință) din partea terțelor persoane asupra clientului;

d) actul de identitate prezentat este deteriorat;

e) există o suspiciune de spălare a banilor sau de finanțare a terorismului;

f) există suspiciuni privind veridicitatea, suficiența și precizia datelor de identificare obținute.

C. Identificarea prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022.

30. În cazul în care entitatea raportoare externalizează integral sau parțial procesul de identificare la distanță a clienților către un furnizor de servicii externalizate, aceasta va aplica, înaintea și în timpul relației de afaceri cu furnizorul de servicii externalizate, următoarele măsuri, a căror amploare trebuie ajustată în funcție de risc:

a) se asigură că furnizorul de servicii externalizate pune în aplicare în mod eficace și respectă politicile și procedurile de identificare la distanță a clienților entității în conformitate cu acordul de externalizare. Acest lucru trebuie realizat prin raportare periodice (cel puțin anuale), monitorizare continuă, vizite la fața locului sau teste prin eșantionare;

b) efectuează evaluări pentru a se asigura că furnizorul de servicii externalizate este suficient de echipat și capabil să efectueze procesul de identificare la distanță a clienților. Evaluările pot include, dar nu se limitează la evaluarea formării personalului, a adecvării tehnologice și a guvernanței datelor la furnizorul de servicii externalizate;

c) în caz de necesitate să solicite un audit complex, aferent procesului de identificare, conform standardelor internaționale în domeniu;

d) se asigură că furnizorul de servicii externalizate informează entitatea cu privire la orice propunere de modificare a procesului de identificare la distanță a clienților sau cu privire la orice modificare adusă soluției furnizate de furnizorul de servicii externalizate;

e) există mecanisme adecvate de confidențialitate în ceea ce privește datele și alte informații;

f) există o analiză aprofundată, bazată pe riscuri, a funcțiilor, a datelor și a sistemelor asociate care sunt avute în vedere pentru externalizare sau care au fost externalizate și să abordeze riscurile potențiale, în special riscurile operaționale, inclusiv riscurile de natură juridică, TIC, de conformitate și reputațional, precum și limitările de supraveghere aferente țărilor în care sunt sau pot fi furnizate serviciile externalizate și în care datele sunt stocate sau este posibil să fie stocate.

31. În cazul în care furnizorul de servicii externalizate stochează date ale clienților, inclusiv, dar fără a se limita la fotografii, materiale video și documente, în timpul procesului de identificare la distanță, entitatea raportoare trebuie să se asigure că:

a) numai datele necesare ale clientului sunt colectate și stocate în conformitate cu perioada de păstrare autorizată;

b) accesul la date este strict limitat și înregistrat;

c) sunt puse în aplicare măsuri de securitate adecvate pentru a asigura protecția datelor stocate.

Capitolul V. Cerințe privind sistemul de control intern

32. Angajatul entității raportoare responsabil de efectuarea identificării prin mijloace electronice a clientului trebuie să dispună de un nivel de calificare profesională suficientă în domeniul identificării clienților, în vederea prevenirii spălării banilor și combaterii finanțării terorismului, care include:

a) cel puțin 5 ani experiență;

b) dispune de o instruire specială în scopul identificării prin mijloace electronice a clienților;

c) dispune de cunoștințe suficiente despre reglementările aplicabile în materie de prevenirea și combaterea spălării banilor și a finanțării terorismului;

d) dispune de cunoștințe suficiente despre aspectele de securitate ale verificării la distanță și care este suficient de instruit pentru a anticipa și a preveni utilizarea intenționată sau deliberată a tehnicilor de înșelăciune legate de verificarea la distanță, precum și pentru a detecta și a reacționa în cazul apariției acestora.

33.Identificarea video a clientului este efectuată într-o încăpere, fizic separată de alte încăperi, în cadrul oficiului entității raportoare, care se află sub control constant și supraveghere video și are acces limitat doar pentru angajații autorizați, și care asigură cel puțin:

a) o calitate suficientă a informației audiovizuale, precum și confidențialitatea acesteia;

b) lipsa altor persoane și/sau obiecte în fața camerei video, precum și lipsa oricăror zgomote ce pot compromite calitatea informației.

34. Persoana cu funcție de conducere de rang superior trebuie să se asigure că politicile și procedurile de înregistrare la distanță a clienților sunt puse în aplicare în mod eficace, revizuite periodic și modificate, dacă este necesar.

35.În funcție de riscul de spălare a banilor sau de finanțare a terorismului asociat relației de afaceri sau a altor riscuri asociate, entitatea raportoare va utiliza unul sau mai multe dintre următoarele controale:

a) efectuarea primei plăți dintr-un cont de plăți deținut de către client într-o altă entitate raportoare dintr-o jurisdicție în care există cerințe de combatere a spălării banilor sau a finanțării terorismului nu mai puțin similare decât cele din Republica Moldova;

b) trimiterea către client a unui cod de acces generat aleatoriu pentru a confirma prezența acestuia în timpul procesului de verificare la distanță. Codul de acces trebuie să fie un cod de unică folosință și pentru o perioadă limitată de timp;

c) colectarea de date biometrice pentru a le compara cu datele colectate din alte surse independente și fiabile;

d) efectuarea unei tranzacții dintr-un cont de plăți al clientului deținut într-o altă entitate raportoare, inclusiv prin utilizarea unui instrument de plată;

e) contactarea telefonică a clientul;

f) corespondență directă (atât electronică, cât și poștală) către client.

36. În cazul în care entitatea raportoare acceptă reproduceri ale unui document original și nu examinează documentul original, aceasta va lua măsuri pentru a se asigura că reproducerea este fiabilă. Astfel, entitatea va stabili, cel puțin, următoarele:

a) dacă reproducerea include elemente de securitate încorporate în documentul original și dacă specificațiile documentului original care sunt reproduse sunt valabile și acceptabile, în special tipul, dimensiunea caracterelor și structura documentului, prin compararea acestora cu bazele de date oficiale;

b) dacă datele cu caracter personal au fost schimbate sau modificate în alt mod sau, după caz, dacă imaginea clientului inclusă în document nu a fost înlocuită;

c) dacă se menține integritatea algoritmului utilizat pentru a genera numărul unic de identificare al documentului original, în cazul în care documentul oficial a fost eliberat cu o zonă de citire optică (machine-readable zone – MRZ);

d) dacă reproducerea furnizată este de o calitate și o rezoluție suficiente pentru a se asigura că informațiile relevante sunt lipsite de ambiguitate;

e) că reproducerea furnizată nu a fost afișată pe un ecran pe baza unei fotografii sau a unei scanări a documentului de identitate original.

37.În cazul în care entitatea raportoare utilizează elemente pentru a citi automat informații din documente, cum ar fi algoritmii de recunoaștere optică a caracterelor (OCR) sau verificările zonei de citire optică (MRZ), aceasta va lua măsurile necesare pentru a se asigura că instrumentele respective captează informațiile într-un mod exact și consecvent.

38. Entitatea raportoare este obligată să informeze imediat, cel mai târziu în 24 de ore, de la identificarea actului sau circumstanțelor care generează suspiciuni, Serviciul Prevenirea și Combaterea Spălării Banilor despre clienții suspecți de implicare în operațiuni și activități sau tranzacții suspecte de spălare a banilor, de infracțiuni asociate acestora și/sau de finanțare a terorismului, care sunt în curs de pregătire, de tentativă, de realizare sau sunt deja realizate.

Capitolul VI. Riscuri și măsuri de precauție

39. În cazul identificării prin mijloace electronice a clientului se aplică abordarea bazată pe risc după cum este stabilit în:

a) Legea 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;

b) actele normative emise de către BNM în domeniul prevenirea și combaterea spălării banilor și finanțarea terorismului;

c) actele normative emise de către Serviciul Prevenirea și Combaterea Spălării Banilor în domeniul prevenirea și combaterea spălării banilor și finanțarea terorismului;

d) prezentul Regulament;

e) măsurile de precauție sporită suplimentare stabilite în actele interne ale entității raportoare.

40. Identificarea prin mijloace electronice nu poate fi efectuată în raport cu clientul dacă acesta:

a) a fost anterior clasificat ca fiind din categoria de risc sporit de spălare a banilor și/sau de finanțare a terorismului în baza analizei riscului entității raportoare;

b) este rezident, inclusiv temporar al unei jurisdicții cu risc sporit;

c) este o persoană care gestionează bunurile aflate sub administrare fiduciară (trust, fond de investiții etc.).

41. Entitatea raportoare va identifica și gestiona adecvat riscurile asociate tehnologiilor informației și de comunicații și de securitate legate de utilizarea procesului de identificare la distanță a clienților, inclusiv în cazul în care acestea se bazează pe terți sau în cazul în care serviciul este externalizat.

42. Entitatea raportoare va utiliza canale de comunicare securizate pentru a interacționa cu clientul în timpul procesului de identificare la distanță a clienților. Soluția de identificare la distanță a clienților trebuie să utilizeze protocoale securizate și algoritmi criptografici în conformitate cu cele mai bune practici din sector pentru a proteja confidențialitatea, autenticitatea și integritatea datelor care fac obiectul schimbului, după caz.

43. Entitatea raportoare va oferi un punct de acces securizat pentru începerea procesului de identificare la distanță a clienților pe baza certificatelor calificate pentru sigiliile electronice în conformitate cu Legea nr. 124/2022. De asemenea, clientul trebuie să fie

informat cu privire la măsurile de securitate aplicabile care trebuie luate pentru a garanta utilizarea securizată a sistemului.

44. Entitatea raportoare poate utiliza serviciile de încredere relevante și procesele de identificare electronică reglementate, recunoscute, aprobate sau acceptate în condițiile Legii nr. 124/2022. Atunci când utilizează astfel de soluții, aceasta va evalua în ce măsură soluția respectă dispozițiile prezentului Regulament și va aplica măsurile necesare pentru a atenua riscurile relevante care decurg din utilizarea soluțiilor respective. Entitatea raportoare trebuie să ia în considerare, în special, dacă sunt abordate următoarele riscuri:

a) riscurile pe care le implică autentificarea și care sunt prevăzute în politicile și procedurile lor specifice măsurilor de atenuare, în special în ceea ce privește riscurile de fraudă prin uzurparea identității;

b) riscul ca identitatea clientului să nu fie una pretinsă;

c) riscul de pierdere, furt, suspendare, revocare sau expirare a dovezilor de identitate, inclusiv, după caz, instrumentele de detectare și prevenire a utilizării fraudelor de identitate.

Capitolul VII. Prelucrarea și păstrarea datelor

45. La prelucrarea datelor cu caracter personal, entitatea raportoare este obligată să respecte regimul de confidențialitate a datelor, să întreprindă măsurile organizatorice şi tehnice necesare pentru protecția datelor cu caracter personal împotriva accesului ilicit sau întâmplător, împotriva distrugerii, modificării, blocării, copierii, răspândirii ilicite sau neautorizate, precum şi împotriva altor acțiuni ilicite.

46. În scopul identificării electronice a clientului, entitatea raportoare realizează prelucrarea datelor, dar și asigură protecția datelor cu caracter personal obținute în procesul de implementare a prevederilor și cerințelor prezentului Regulament, precum și confidențialitatea acestor date, în conformitate cu reglementările actelor normative naționale cu privire la protecția datelor cu caracter personal și prezentului Regulament.

47. Entitatea raportoare păstrează toate documentele şi informațiile despre clienți, inclusiv înregistrările video, audio, foto, capturile de ecran, obținute în cadrul identificării electronice, inclusiv copiile documentelor de identificare, arhiva, amprenta digitală aferentă computerului /dispozitivului utilizat, adresa IP, documentele, orice alte informații, pe perioada activă a relației de afaceri şi pe o perioadă de 5 ani după terminarea acesteia.

48. Entitatea raportoare asigură că, în caz de solicitare, documentele şi informația privind identificarea şi verificarea clienților, a beneficiarilor efectivi, privind monitorizarea operațiunilor clienților, inclusiv documentele confirmative aferente operațiunilor sunt accesibile Băncii Naționale a Moldovei, Serviciului Prevenirea și Combaterea Spălării Banilor și altor autorități competente.

Capitolul VIII. Responsabilități

49. În aplicarea prezentului Regulament, entitatea raportoare informează Banca Națională a Moldovei despre activitățile suspecte și incidentele de fraudă care prezintă riscuri pentru siguranța, buna funcționare sau reputația entității raportoare.

50. Entitatea raportoare, anterior demarării procedurii de identificare prin mijloace electronice a clienților, este obligată să informeze Banca Națională a Moldovei cu privire la corespunderea cu următoarele cerințe:

a) dovada că entitatea raportoare dispune de politici și proceduri interne corespunzătoare, care vor pune în aplicare cerințele din prezentul Regulament.

b) dovada că entitatea raportoare a efectuat evaluarea preimplementare a soluției de identificare la distanță a clienților în conformitate cu pct.6 din prezentul Regulament;

c) dovada că angajații entității raportoare responsabili de identificarea video sunt instruiți în conformitate cu pct. 32 din prezentul Regulament;

d) dovada că entitatea raportoare dispune de spațiu corespunzător pentru efectuarea procedurii de identificare video, în conformitate cu pct. 33 din prezentul Regulament;

e) dovada că entitatea raportoare dispune de mijloace tehnice corespunzătoare, în conformitate cu cerințele cap. IV din prezentul Regulament.

51. Procedura stabilită la pct. 50 din prezentul Regulament este efectuată o singură dată, înainte ca entitatea raportoare să pună în aplicare prevederile prezentului Regulament și se efectuează în scopul evidenței și verificării corespunderii criteriilor stabilite la lit. a) – e) din pct. 50.

52.Entitatea raportoare, anterior demarării procesului de externalizare integrală sau parțială a procesului de identificare la distanță a clienților, informează Banca Națională a Moldovei, cel puțin, asupra următoarelor :

a) numele furnizorului de servicii, numărul de înregistrare al companiei, codul de identificare (dacă este disponibil), adresa și alte date de contact relevante (dacă este cazul);

b) o descriere succintă a funcțiilor externalizate, inclusiv a datelor care sunt externalizate și dacă au fost transferate sau nu date cu caracter personal sau dacă prelucrarea lor este externalizată către un furnizor de servicii;

c) țara sau țările în care serviciul urmează să fie prestat, inclusiv locația datelor (și anume, țara sau regiunea);

d) dacă funcția externalizată este considerată sau nu critică sau importantă, inclusiv, dacă este cazul, un rezumat succint al motivelor pentru care funcția externalizată este considerată critică sau importantă;

e) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate.

f) data celei mai recente evaluări a riscurilor și un rezumat succint al principalelor rezultate;

g) în cazul externalizării către un furnizor de servicii de tip cloud, serviciile de tip cloud și modelele de implementare, și anume publice/private/hibride/comunitare, precum și natura specifică a datelor care urmează să fie deținute și locațiile (și anume, țări sau regiuni) unde datele respective sunt stocate;

53. În caz de necesitate, BNM poate solicita prezentarea informațiilor suplimentare pentru a verifica conformarea cu prezentul Regulament.

54. BNM poate solicita, după caz, un raport de audit, efectuat conform standardelor internaționale de audit în domeniul sistemelor informaționale.