BANCA NAȚIONALĂ

HOTĂRÂRE Nr. 281
din 07-11-2024

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

Publicat : 14-11-2024 în Monitorul Oficial Nr. 467-469 art. 886

În temeiul art.5[1] alin. (3) 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, conform anexei.

2. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova. Entitățile raportoare, care au implementate soluții informatice pentru stabilirea relației de afaceri la distanță a clienților la data intrării în vigoare a prezentei hotărâri, se vor conforma noilor cerințe în decurs de 6 luni.

PREȘEDINTELE
COMITETULUI EXECUTIV **Anca-Dana DRAGU**

Nr. 281. Chișinău, 7 noiembrie 2024.

Anexă
la Hotărârea Comitetului executiv
al Băncii Naționale a Moldovei
nr. 281 din 7 noiembrie 2024

Regulament
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 entitățile raportoare specificate la pct. 3 la stabilirea relațiilor de afaceri cu clienții fără prezență fizică.

2. Cerințele și normele privind identificarea și verificarea identității clienților cu prezență fizică sunt aplicabile și clienților, identificarea cărora la distanţă este efectuată conform cerințelor 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 emise 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 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:

date biometrice - date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

identificarea și verificarea identității clienților prin intermediul mijloacelor electronice – reprezintă un proces de identificare și verificare a identității clientului la distanță în baza unei evaluări corespunzătoare a riscurilor și prin utilizarea, în funcție de risc, a uneia sau a mai multor metode concomitent prevăzute la art.5[1] alin.(2) din Legea nr.308/2017;

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

mijloace electronice - mijloace care utilizează tehnologii digitale inovatoare care folosesc, printre altele, inteligența artificială și/sau procese de învățare automată

(machine learning), cum ar fi aplicaţiile care realizează identificarea unei persoane şi/sau verificări ale actelor de identitate (de exemplu, prin capturi de imagini digitale, măsurători ale semnalmentelor biometrice faciale, comparare de imagini), tehnologia NFC (comunicare în câmp apropiat) încorporată în documentele electronice de identitate.

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

Secțiunea 1
Politici și proceduri

5. Entitatea raportoare va elabora politici și proceduri de identificare la distanță pentru a se conforma obligațiilor care îi revin în temeiul art.5 alin.(2) lit. a) 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 informatice pe care o utilizează pentru a colecta, stoca, contrapune, verifica, valida și actualiza informații pe tot parcursul procesului de stabilire a relațiilor de afaceri la distanță a clienților. Aceasta trebuie să includă o explicație a elementelor și a modului de funcționare a soluției informatice;

b) situațiile în care poate fi utilizată soluția informatică 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 care a fost identificat la distanță este executată numai după ce au fost aplicate toate măsurile de precauție privind clienții, prevăzute de Legea nr.308/2017;

e) descrierea programelor de inițiere și de formare periodică pentru a asigura sensibilizarea personalului, instruirea și informarea continuă și înțelegerea funcționării soluției informatice și a riscurilor asociate;

f) cerințele privind păstrarea datelor și informațiilor acumulate în procesul de identificare și verificare a identității persoanei prin mijloace electronice.

Secțiunea 2
Preimplementarea soluției informatice

6. Entitatea raportoare, atunci când analizează implementarea unei soluții informatice cu privire la identificare la distanță a clienților, va efectua o evaluare preimplementare a acestei soluții. Astfel, entitatea raportoare va stabili domeniul de aplicare, pașii și cerințele care urmează a fi respectate, inclusiv în materie de evidență a datelor, și care ar trebui să includă:

a) o evaluare a caracterului adecvat și sigur al soluției informatice în ceea ce privește: accesibilitatea, plenitudinea, acuratețea și nonrepudierea datelor și a documentelor care urmează a fi prelucrate, precum și a fiabilității și a veridicității și independenței surselor de informații utilizate;

b) o evaluare a impactului utilizării soluției informatice asupra riscurilor specifice ale entității, inclusiv de spălarea banilor și finanțarea terorismului, operaționale,

reputaționale și juridice, inclusiv evaluarea impactului asupra protecției datelor cu caracter personal în condițiile Legii nr. 133/2011 privind protecția datelor cu caracter personal;

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

d) identificarea capabilității soluției informatice de a reduce riscul de utilizare a rețelelor virtuale private (VPN-uri) sau proxy pentru ascunderea locației sau împiedicarea aplicării cerințelor de monitorizare;

e) evaluarea conformității soluției informatice cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace electronice stabilite pentru prestatorul de servicii de încredere calificat, stabilite în temeiul prevederilor Legii nr.124/2022 și actelor normative subordonate;

f) evaluarea conformității soluției informatice cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace electronice stabilite în standardele tehnice internaționale[1];

g) teste pentru a evalua riscurile de fraudă, inclusiv riscurile de fraudă prin furtul sau uzurparea identității;

h) o evaluare a riscurilor asociate tehnologiei informației și comunicațiilor (TIC) și securitatea informației;

i) o testare end-to-end a funcționării soluției informatice care vizează clienții, produsele și serviciile pentru care aceasta este aplicabilă.

7. Entitatea raportoare, în condițiile prevederilor pct. 49, va prezenta BNM actele/documentaţia justificativă aferentă evaluărilor și testelor menționate la pct. 6, rezultatul acestora, precum și modul în care aplicarea soluției informatice asigură atenuarea și remedierea riscurilor de spălare a banilor și finanțare a terorismului și alte riscuri identificate pentru tipurile de clienți, servicii și produse pentru care aceasta este aplicabilă. Evaluările și testele menționate la pct.6 pot fi efectuate/confirmate de către un audit independent sau prin certificări recunoscute internațional, dacă entitatea raportoare nu dispune de resurse necesare în acest sens.

Secțiunea 3
Monitorizarea continuă a soluției informatice

8. Entitatea raportoare va monitoriza soluția informatică în mod continuu pentru a se asigura că funcționează în conformitate cu scopul acesteia. În acest context, entitatea raportoare va include în politicile și procedurile de identificare la distanță, elaborate conform pct. 5, cel puțin următoarele:

a) pașii pe care entitatea raportoare îi va întreprinde pentru a asigura 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 revizuirilor periodice ale soluției informatice; și

c) temeiurile de inițiere și realizare a revizuirii ad-hoc ale soluției informatice, care ar trebui să includă cel puțin:

[1] *A se considera prevederile pct. 29 din Regulament.*

- modificări ale expunerii entității la riscul de spălare a banilor și finanțare a terorismului;

- deficiențe privind funcționarea soluției informatice detectate în cursul activităților de monitorizare, audit sau supraveghere;

- o creștere estimată a tentativelor de fraudă de identitate ale clienților, inclusiv prin furtul sau uzurparea identității, identificate de entitatea raportoare;

- modificări ale cadrului normativ relevant procesului de identificare la distanță a clienților.

9. Entitatea raportoare se asigură că are mecanisme de monitorizare bazate pe riscuri și care 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 stabilirea relației de afaceri la distanță;

c) indicatori privind compromiterea confidențialității, integrității sau autenticității sesiunii ca urmare a procedurii de identificare;

d) registrul de înregistrare a cazurilor de utilizare obișnuită sau contrară normelor stabilite a dispozitivului de acces sau a soluției informatice furnizată persoanei ce urmează a fi identificată de către entitatea raportoare;

e) poziția geografică (locația) anormală/neobișnuită a persoanei;

f) poziția geografică (jurisdicția) cu risc ridicat a persoanei;

g) cazurile de furt, uzurpare a identității sau prelucrare ilegală a datelor identificate.

10. Entitatea raportoare va stabili în politicile și procedurile de identificare la distanță, elaborate conform pct. 5, măsuri de remediere în cazul în care au fost identificate erori care au un impact asupra eficacității soluției informatice. Aceste măsuri vor include cel puțin:

a) o revizuire a tuturor relațiilor de afaceri afectate, pentru a evalua dacă entitatea raportoare a aplicat corespunzător măsurile de precauție față de clienți, prioritate fiind acordată clienților cu grad de risc sporit de spălare a banilor și finanțare a terorismului;

b) o evaluare bazată pe informațiile obținute în cadrul revizuirii de la lit. a) care să stabilească dacă o relație de afaceri afectată ar trebui să fie:

- reclasificată într-o altă categorie de risc și supusă măsurilor de precauție sporite;

- supusă stabilirii unor limite privind volumul tranzacțiilor;

- încetată;

- raportată către Serviciul Prevenirea și Combaterea Spălării Banilor la identificarea suspiciunilor de spălare a banilor și /sau finanțare a terorismului.

11. Entitatea raportoare va lua în considerare modalitatea cea mai eficientă de a monitoriza adecvarea și fiabilitatea continuă a soluției informatice. 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;

- testarea eșantionului;

- teste de penetrare;

- recenziile sau rapoartele de specialitate recunoscute ale experților din domeniu și/sau autorităților de supraveghere la nivel național sau internațional, inclusiv a celor din jurisdicții care implementează standarde similare de prevenire a spălării banilor și finanțării terorismului.

Capitolul III. Cerințe privind identificarea şi verificarea identităţii clienţilor prin intermediul mijloacelor electronice

12. Entitatea raportoare va efectua identificarea și verificarea identității clientului prin mijloace electronice, în privința potențialilor clienți noi cu care entitatea raportoare intenționează să inițieze relații de afaceri.

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

a) persoana fizică, cetățean al Republicii Moldova;

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

14. Entitatea raportoare se va asigura că soluția informatică are elemente care îi permit colectarea informației necesare pentru cunoașterea clienților în conformitate cu cerințele politicii și procedurilor de identificare la distanță elaborate de entitatea raportoare conform pct.5, în special poate colecta:

a) toate datele și documentele relevante pentru identificarea și verificarea identității 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) toate datele și documentele relevante pentru identificarea și verificarea identității beneficiarului efectiv;

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

15. Entitatea raportoare se va asigura că indiferent de metoda aplicată pentru identificarea și verificarea identității clienților la distanță, va fi asigurată colectarea și prezentarea de către client a informațiilor care de obicei se solicită clienților identificați cu prezență fizică. Modalitatea de colectare a informației va fi determinată de entitatea raportoare, dar urmează să stabilească care informație va fi colectată:

a) manual, introdusă de către client sau angajatul entității;

b) automat din documentele prezentate de către client;

c) din alte surse interne sau externe, colectate automat sau de angajatul entității.

16. Entitatea raportoare va pune în aplicare și va menține mecanisme pentru a se asigura că informațiile pe care le captează în format electronic sunt integre. Aceasta trebuie să aplice controale (cel puțin anuale) procesului de stabilire a relației de afaceri la distanță 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) sau proxy.

17. În cazul clientului persoană juridică, măsurile de identificare se vor aplica persoanei fizice cu mandat de reprezentare al acesteia și se vor obține documentele de înregistrare corespunzătoare ale persoanei juridice. În aceste condiții, pentru persoana fizică, reprezentant al persoanei juridice, entitatea raportoare va aplica procesul de

stabilire a relației de afaceri la distanță similar unui client - persoană fizică. 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.

18. Identificarea şi verificarea identităţii clienţilor prin mijloace electronice se realizează cu mijloace de verificare automatizate, fără operator uman, sau prin mijloace de verificare cu operator uman (angajatul entității). Entitatea raportoare poate utiliza și o soluție informatică de verificare combinată a identității persoanei la identificarea clientului la distanță.

19. Identificarea clientului utilizând mijloace electronice este precedată de exprimarea consimțământului pentru prelucrarea datelor cu caracter personal în conformitate cu legislația în vigoare.

20. La identificarea şi verificarea identităţii clienţilor prin mijloace electronice, entitatea raportoare va asigura aducerea la cunoștința clientului termenele și condițiile în care identificarea electronică este efectuată. Termenele și condițiile puse la dispoziția clientului, inclusiv până la accesarea de către client a soluției informatice, vor conține, fără a se limita:

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

b) „Nota de informare privind modul de prelucrare și protecție a datelor” – va conține informațiile ce se referă la dreptul de a fi informat a clientului în calitate de persoană fizică sau reprezentant al persoanei juridice și la general, măsurile organizatorice și tehnice asigurate, inclusiv informațiile care vor fi prelucrate conform cerințelor actelor normative aplicabile;

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

Capitolul IV. Metode de identificare şi verificare a identităţii clienţilor prin intermediul mijloacelor electronice

21. În cazul identificării şi verificării identităţii clienţilor prin mijloace electronice, entitatea raportoare, în funcție de amploarea riscului de spălare a banilor și finanțare a terorismului sau alte riscuri asociate, utilizează una sau mai multe dintre următoarele metode de identificare la distanță, prin:

a) mijloace de identificare electronică cu un nivel de securitate suficient şi conform standardelor stabilite în Legea nr.124/2022 (semnătură electronică calificată);

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

c) mijloace electronice care asigură cumulativ transmiterea în direct a fotografiei cu elementele de verificare a prezenței fizice și înregistrarea originalului actului de identitate;

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

22. La identificarea şi verificarea identităţii clienţilor utilizând mijloace de identificare video/foto a clientului, cu utilizarea mijloacelor de verificare cu operator uman, entitatea raportoare se asigură că procesul identificării este înregistrat și corespunde următoarelor:

a) este de o durată rezonabilă (stabilită conform reglementărilor entității) 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 domiciliu și/sau reședință), precum și ora/data/luna/anul în care se face înregistrarea și numărul de contact al telefonului mobil;

- momentul în care angajatul entității raportoare ia legătura cu persoana în timpul verificării video și/sau momentul în care clientul primește sau introduce codul unic sau accesează link-ul remis prin serviciul de mesaje scurte (SMS) la telefonul mobil sau e-mail;

- 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 se desfășoară în condiții de liniște, a unei bune iluminări și nicio persoană terță nu este implicată în proces, astfel încât să permită identificarea clară a persoanei, în caz contrar, procesul urmează a fi întrerupt;

- procesul de verificare video/foto se desfășoară 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;

- procesul identificării asigură o discuție liberă și clară între angajatul entității raportoare și client, precum și verificarea vizuală de către angajatul entității raportoare a documentelor prezentate de către client, inclusiv a elementelor de protecție aplicabile documentului respectiv;

- procesul identificării asigură că sunt utilizate actele de identitate în original și nu sunt prezentate pe baza unei reproduceri a documentului în original, cum ar fi fotografie, copie, scanare a documentului etc.;

- procesul identificării asigură că calitatea imaginii și a sunetului în timpul transmisiunii video este înaltă, cu o rezoluție de cel puțin 8 megapixeli sau cel puțin FullHD (1920x1080), în scopul identificării și recunoașterii necondiționate a persoanei;

- procesul identificării asigură că transmisiunea video în timp real se înregistrează în color și se desfășoară sincron cu sunetul;

- procesul identificării asigură captura automată a feței clientului și a documentului de identitate;

- procesul identificării asigură că soluția informatică nu permite încărcarea fotografiilor/videoclipurilor realizate anterior în timpul interviului sau identificării foto;

- procesul identificării asigură utilizarea tehnologiilor relevante pentru a asigura integritatea și securitatea înregistrărilor video/foto utilizate în cadrul verificărilor de identitate.

23. La identificarea şi verificarea identităţii clienţilor utilizând mijloace electronice de identificare video/foto a clientului cu utilizarea mijloacelor de verificare fără operator uman, în care clientul nu interacţionează cu un angajat, entitatea raportoare se asigură că procesul este înregistrat și corespunde următoarelor:

a) este de o durată rezonabilă (stabilită conform reglementărilor entității) 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 domiciliu și/sau reședință), precum și ora/data/luna/anul în care se face înregistrarea și numărul de contact al telefonului mobil;

- momentul în care clientul prezintă actul de identitate și acesta este înregistrat de cameră pe ambele părți;

b) este în concordanță cu următoarele condiții:

- fotografia (fotografiile) sau înregistrarea 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;

- soluția informatică utilizează 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;

- soluția informatică utilizează tehnologii care folosesc algoritmi de verificare a autenticității actului de identitate prezentat, precum verificarea design-ului și a elementelor de protecție a actelor de identitate, contrapunerea datelor înscrise în documentul prezentat cu datele conținute în zonele de citire optică (MRZ), evaluarea autenticității în baza profilului culorilor actelor prezentate, utilizarea algoritmilor biometrici pentru estimarea vârstei și sexului persoanei pentru a o valida cu informațiile prezentate în act etc.;

- soluția informatică utilizată la identificarea la distanță utilizează algoritmi care determină că actele de identitate utilizate sunt în original și nu sunt prezentate pe baza unei reproduceri a documentului în original, cum ar fi fotografie, copie, scanare a documentului etc.;

- calitatea imaginii și a sunetului în timpul transmisiunii video este de o calitate înaltă, cu o rezoluție de cel puțin 8 megapixeli sau cel puțin FullHD (1920x1080), în scopul identificării și recunoașterii necondiționate a persoanei;

- soluția informatică utilizează algoritmi fiabili capabili pentru a verifica dacă fotografia (fotografiile) sau înregistrarea video realizată (realizate) corespund fotografiei (fotografiilor) extrase din documentul (documentele) oficiale ale clientului sau fotografiile obținute din surse sigure și independente;

- soluția informatică nu permite încărcarea fotografiilor/videoclipurilor realizate anterior în timpul interviului sau identificării foto;

- soluția informatică utilizează tehnologii pentru a asigura integritatea și securitatea înregistrărilor video/foto utilizate în cadrul verificărilor de identitate;

c) utilizează mijloace electronice.

24. În cazul stabilirii relației de afaceri la distanță prin mijloace electronice, entitatea raportoare efectuează identificarea, verificarea și păstrarea datelor tehnice ale calculatorului/dispozitivului utilizat de către client (de exemplu, modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea), IP adresa, localizarea acestuia, precum și alte date disponibile și posibil a fi colectate.

25. Pe parcursul procesului de stabilire a relației de afaceri la distanță utilizând mijloace electronice, entitatea raportoare va verifica numărul de telefon și/sau adresa de e-mail ce va fi utilizată pentru comunicarea ulterioară cu clientul, prin transmiterea către persoana care parcurge procedura de identificare la distanță a unui cod de unică folosință (One Time Password - OTP) sau prin transmiterea unui link cu o durată limitată, special creat în acest scop, generat în mod individual (prin e-mail sau SMS).

26. Procedura de stabilire a relației de afaceri la distanță utilizând mijloace electronice poate fi încheiată numai dacă a fost finalizată transmiterea și validarea OTP sau numai dacă au fost finalizate transmiterea și accesarea linkului.

27. În cadrul stabilirii relației de afaceri la distanță prin mijloace electronice, 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) în cazul existenței suspiciunilor privind identitatea persoanei sau autenticitatea documentelor prezentate vor fi adresate întrebări adiționale în scopul verificării identității persoanei sau autenticității documentelor sau se va proceda la verificarea manuala a informației de către un angajat;

f) contrapunerea datelor din cadrul actelor de identitate prezentate cu datele din cadrul Registrului de stat al populației.

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;

b) obligată să solicite prezentarea fizică la oficiul său a persoanei în cazul existenței suspiciunilor și/sau dubiilor în privința viciului de consimțământ (presiuni sau influențe fizice sau psihologice) al clientului din partea terților persoane sau oricare alte suspiciuni în privința clientului;

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 reglementările din domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

29. Entitatea raportoare la stabilirea relațiilor de afaceri la distanță utilizând mijloace electronice va utiliza soluții informatice certificate conform standardelor internaționale aplicabile[2].

30. Entitatea raportoare poate utiliza soluția informatică pentru stabilirea relației de afaceri la distanță prin mijloace electronice pentru actualizarea informațiilor/datelor clienților existenți.

31. Entitatea raportoare nu va iniția relația de afaceri cu clientul prin mijloace electronice în cazul în care nu poate aplica măsurile standard de precauție privind clienții prevăzute de Legea nr.308/2017, precum și în situația când cerințele tehnice nu sunt întrunite sau entitatea nu poate verifica identitatea persoanei conform cerințelor prezentului regulament.

Capitolul V. Cerințe privind sistemul de control intern

32. În cazul stabilirii relației de afaceri la distanță utilizând mijloace electronice de identificare video/foto a clientului cu utilizarea mijloacelor de verificare cu operator uman, entitatea implementează, cel puțin, următoarele cerințe:

a) pentru angajatul entității raportoare responsabil de identificarea prin mijloace electronice a clienților:

- dispune de un nivel de calificare profesională suficientă în domeniul identificării clienților;
- dispune cel puțin de 1 an experiență la aplicarea măsurilor de precauție față de clienți;
- dispune de o instruire specială în scopul identificării prin mijloace electronice a clienților;

[2] 1. ISO/IEC 30107: Information technology - Biometric presentation attack detection;
2. ISO/IEC 24745: Information technology – Security techniques – Biometric information protection;
3. ISO/IEC 27034: Information technology – Security techniques – Application security;
4. ISO/IEC 15408: Information security, cybersecurity and privacy protection;
5. NIST SP 800-63: Digital Identity Guidelines;
6. NIST SP 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management.

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

- 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;

b) față de spațiul special amenajat în scop de identificare prin mijloace electronice a clienților:

- este sub control constant și supraveghere video în timpul procesului de stabilirea a relației la distanță utilizând mijloace electronice cu clienții;

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

33. Persoana cu funcție de conducere de rang superior trebuie să se asigure că politicile și procedurile de stabilire a relației de afaceri la distanță a clienților elaborate de entitate conform pct.5 sunt puse în aplicare în mod eficace, revizuite periodic și modificate, dacă este necesar.

34. 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 în situațiile cu risc sporit:

a) asigurarea efectuării de către client a unei tranzacții dintr-un cont de plăți deținut într-o altă entitate raportoare, inclusiv prin utilizarea unui instrument de plată;

b) asigurarea efectuării de către client a unei tranzacții dintr-un cont de plăți deținut într-o instituție financiară din străinătate dintr-o jurisdicție în care există cerințe de combatere a spălării banilor sau a finanțării terorismului cel puțin similare celor din Republica Moldova;

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

d) contactarea telefonică a clientului;

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

35. 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 și se asigură că se menține integritatea algoritmului utilizat pentru a genera numărul unic de identificare al documentului original.

36. Entitatea raportoare este obligată să informeze imediat, în conformitate cu cerințele Legii nr.308/2017, 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 protecție

37. 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 prevenirii și combaterii spălării banilor și finanțării terorismului;

c) actele normative emise de către Serviciul Prevenirea și Combaterea Spălării Banilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului;

d) prezentul Regulament;

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

38. La identificarea prin mijloace electronice, entitatea raportoare aplică măsuri de precauție sporită, suplimentar celor prevăzute la art.8 alin.(3) din Legea nr.308/2017, în următoarele cazuri:

a) persoana reprezintă fost client cu care a fost încetată relația de afaceri din cauza imposibilității aplicării măsurilor de precauție în conformitate cu art.5 alin.(3) din Legea nr.308/2017;

b) persoana 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.).

39. În funcție de risc, entitatea raportoare poate utiliza una sau mai multe din metodele prevăzute la pct. 21 pentru gestionarea și diminuarea riscurilor de spălare a banilor și finanțare a terorismului, inclusiv pentru obținerea de informații suplimentare de la client. În astfel de situații, metodele utilizate suplimentar nu se consideră metoda de identificare la distanță a clientului, dar drept o măsură aplicată de entitate pentru gestionarea eficientă a riscurilor de spălare a banilor sau finanțare a terorismului.

40. 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 apelează la persoane terțe sau în cazul în care procesul este internalizat.

41. Entitatea raportoare va utiliza canale de comunicare securizate pentru a interacționa cu clientul în timpul procesului de identificare la distanță și a schimbului de informație asociat. Soluția informatică 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 asigura confidențialitatea, autenticitatea, integritatea și disponibilitatea datelor care fac obiectul schimbului, după caz.

42. Entitatea raportoare va oferi clientului informație cu privire la măsurile de securitate aplicabile care trebuie luate pentru a garanta utilizarea securizată a soluției informatice.

43. Entitatea raportoare la stabilirea relațiilor de afaceri prin intermediul altor metode de identificare la distanță a persoanei utilizând mijloace digitale acceptate în condițiile Legii nr.124/2022, stabilite și reglementate de către Guvern, va evalua în ce măsură acestea respectă dispozițiile prezentului Regulament și va aplica măsurile necesare pentru a atenua riscurile relevante care decurg din utilizarea lor. Entitatea raportoare trebuie să ia în considerare, în special, dacă sunt abordate, cel puțin, următoarele riscuri:

a) riscul de fraudă prin uzurparea identității, inclusiv prin modificarea aspectului solicitantului prin mijloace fizice si/sau electronice;

b) riscul ca identitatea clientului să nu fie una pretinsă sau să nu corespundă cu cea din Registrul de evidență a populației;

c) riscul de contrafacere și falsificarea actelor de identitate prin mijloace fizice sau electronice;

d) 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;

e) riscul de scurgere de date cu caracter personal.

Capitolul VII. Prelucrarea și păstrarea datelor

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

45. 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 actelor normative cu privire la protecţia datelor cu caracter personal și prezentului Regulament.

46. Entitatea raportoare păstrează toate documentele şi informaţiile obținute de la clienţi, precum înregistrările video, audio, foto, capturile de ecran, inclusiv copiile documentelor de identificare, amprenta electronică aferentă computerului /dispozitivului utilizat, adresa IP, alte documente sau informații obținute, pe perioada activă a relaţiei de afaceri şi pe o perioadă de 5 ani după încetarea acesteia.

47. Entitatea raportoare 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 operaţiunilor sunt accesibile Băncii Naționale a Moldovei, Serviciului Prevenirea și Combaterea Spălării Banilor şi organelor de drept.

Capitolul VIII. Responsabilități

48. În aplicarea prezentului Regulament, entitatea raportoare informează Banca Naţională a Moldovei despre activitățile suspecte și incidentele de fraudă care prezintă riscuri pentru siguranţa, buna funcţionare sau reputația entității raportoare.

49. Entitatea raportoare, cel puțin cu 30 zile anterior demarării procedurii de identificare prin mijloace electronice a clienților, este obligată să notifice Banca Națională a Moldovei cu privire la corespunderea cu următoarele cerințe:

a) dovada că entitatea raportoare dispune de politici și proceduri de identificare la distanță corespunzătoare, care vor pune în aplicare cerințele din prezentul Regulament;

b) dovada că entitatea raportoare a efectuat evaluarea de pre implementare a soluției informatice în conformitate cu pct.6;

c) dovada că angajații entității raportoare responsabili de identificarea video cu utilizarea mijloacelor de verificare cu operator uman, sunt instruiți în conformitate cu pct. 32 lit. a);

d) dovada că entitatea raportoare dispune de spațiu corespunzător pentru efectuarea procedurii de identificare video cu utilizarea mijloacelor de verificare cu operator uman, în conformitate cu pct. 32 lit. b);

e) dovada că entitatea raportoare dispune de metode de identificare la distanță corespunzătoare, în conformitate cu cerințele cap. IV.

50. Notificarea stabilită la pct. 49 din prezentul Regulament este efectuată o singură dată, înainte ca entitatea raportoare să demareze procedura de identificare prin mijloace electronice a clienților și să pună în aplicare prevederile prezentului Regulament.

51. Externalizarea procesului de identificare și verificare a identității clienților prin mijloace electronice se efectuează de către entitatea raportoare conform dispozițiilor actelor normative aplicabile.

52. Entitatea raportoare va înceta imediat utilizarea soluției informatice de stabilire a relațiilor de afaceri la distanță utilizând mijloace electronice cu clienții la solicitarea Băncii Naționale a Moldovei, dacă se constată că aceasta prezintă riscuri semnificative pentru securitatea sau integritatea procesului de identificare și verificare a identității persoanelor.