



Către: Anca DRAGU
Guvernatoarea Băncii Naționale a Moldovei

Nr. 24 din 02.03.2026

Ref.: Dificultăți și impedimente în implementarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice, precum și propuneri aferent proiectului Hotărârii Comitetului Executiv al Băncii Naționale a Moldovei pentru modificarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice

Stimată doamnă Dragu,

Vă salutăm din numele Camerei de Comerț Americane din Moldova (în continuare „AmCham Moldova”).

AmCham Moldova susține pe deplin demersurile BNM de consolidare a cadrului privind identificarea și verificarea identității clienților prin mijloace electronice (eKYC), ca parte a procesului de modernizare a infrastructurii financiare și de aliniere la standardele internaționale AML/CFT. Considerăm această inițiativă una esențială pentru dezvoltarea serviciilor financiare digitale și pentru creșterea încrederii în ecosistemul financiar.

Totodată, în procesul de analiză și implementare practică a Regulamentului nr. 281/2024, membrii noștri au identificat anumite aspecte juridice, tehnice și operaționale care ar putea beneficia de clarificări sau ajustări, în vederea asigurării unei aplicări uniforme și eficiente. În lipsa unor precizări suplimentare, există riscul apariției unor dificultăți de conformare în termene rezonabile, a unor abordări neuniforme între entități sau a unor constrângeri operaționale pentru prestatorii care operează integral în regim digital.

Pentru entitățile raportoare, în special organizațiile nebankare reglementate și supravegheate de BNM, implementarea eKYC reprezintă un proces tehnic și operațional complex, care implică dependențe externe inevitabile (furnizori de soluții PAD/liveness, servicii de verificare, monitorizare, audit, certificări și testări independente). Aceste procese presupun timp de achiziție și integrare, costuri aferente și o capacitate limitată a furnizorilor specializați pe piața locală.

Observațiile formulate mai jos au drept scop susținerea unei implementări sustenabile a cadrului normativ, prin menținerea standardelor ridicate de securitate, concomitent cu asigurarea proporționalității și aplicabilității practice pentru toate entitățile vizate.

1. Necesitatea unei implementări etapizate și proporționale

Regulamentul impune un set complex de cerințe tehnice, procedurale și de securitate aplicabile uniform tuturor entităților, indiferent de dimensiune, model de business sau profil de risc, cumulativ cu cerințele ce urmează a fi introduse prin proiectul Hotărârii Comitetului Executiv al Băncii Naționale a Moldovei pentru modificarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice.

Intervenim respectuos cu solicitarea privind examinarea posibilității modificării cadrului normativ actual privind implementarea sistemului de identificare electronică a clienților (e-KYC).

Această inițiativă vizează scalarea progresivă a cerințelor de implementare a e-KYC pentru entitățile raportoare (bănci, instituții financiare non-bancare, furnizori de servicii de plată etc.), în scopul de a facilita tranziția către un sistem digital eficient, minimizând riscurile operaționale, tehnice și de conformitate, în special pentru entitățile mici și mijlocii.

Propunerea se bazează pe principiul proporționalității și pe abordarea bazată pe risc, prevăzute în art. 5 și art. 6 din Legea nr. 308/2017, precum și pe necesitatea de a asigura o implementare echitabilă, evitând blocaje în accesul cetățenilor la servicii financiare.

Această abordare nu ar diminua standardele propuse, ci le-ar da un caracter aplicabil pentru întregul sector și ar reduce riscul de distorsiuni concurențiale și blocaje de implementare.

Proporționalitatea este un principiu recunoscut în practica europeană de reglementare și este esențială pentru eKYC, astfel încât metoda să devină o capacitate funcțională a pieței, nu doar o cerință formală.

O implementare etapizată ar permite testarea graduală a sistemelor, reducerea costurilor inițiale și creșterea adopției eKYC, contribuind la digitalizarea economiei naționale, în conformitate cu obiectivele UE transpuse în legislația Republicii Moldova (Directiva (UE) 2015/849 și Directiva (UE) 2018/843).

La caz, conform proiectului Hotărârii Comitetului Executiv al Băncii Naționale a Moldovei pentru modificarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice, acesta ar urma să intre în vigoare parțial peste o lună din data publicării, iar anumite cerințe ar urma să fie implementate în termen de 12 luni de către entitățile care dispun deja de o soluție informatică, termen care considerăm oportun a fi extins pentru întregul proiect de modificare. Astfel, entitățile care, la data intrării în vigoare a Hotărârii, utilizează deja soluții informatice pentru stabilirea relațiilor de afaceri la distanță prin mijloace electronice să dispună de un termen de 12 luni pentru conformare cu toate cerințele noi introduse și nu doar cu unele dintre ele.

Etapa 1: Acte strict necesare

Certificările/Standardele Necesare pentru Soluția e-KYC

Conform Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (aprobat prin Hotărârea BNM nr. 281/2024), soluțiile informatice utilizate pentru e-KYC trebuie să fie certificate conform standardelor internaționale aplicabile (pct. 29). Lista detaliată din nota 2 a Regulamentului include:

1. **ISO/IEC 30107:** Information technology - Biometric presentation attack detection (detecție atacuri biometrice).
2. **ISO/IEC 24745:** Information technology – Security techniques – Biometric information protection (protecția informațiilor biometrice).
3. **ISO/IEC 27034:** Information technology – Security techniques – Application security (securitatea aplicațiilor).
4. **ISO/IEC 15408:** Information security, cybersecurity and privacy protection (securitate informațională și protecție a privacy).
5. **NIST SP 800-63:** Digital Identity Guidelines (ghiduri pentru identitate digitală).
6. **NIST SP 800-63B:** Digital Identity Guidelines - Authentication and Lifecycle Management (autentificare și management ciclul de viață).

Aceste certificări din partea prestatorului de servicii eKYC le considerăm strict necesare. Astfel, prestatorul soluției prezintă un raport detaliat de evaluare, inclusiv rezultatele testelor de securitate, anti-fraudă și conformitate cu standarde (ISO/IEC 30107, ISO/IEC 24745, NIST SP 800-63B).

Observăm că și prin proiectul de modificare s-a intervenit cu anumite concretizări aferente acestor certificări, fapt care va îngreuna și mai mult procesul.

Mai mult, unele dintre certificările conform standardelor internaționale (ex.: ISO/IEC 30107-3) implică procese de lungă durată. Or, obținerea acestor certificări depinde de laboratoare internaționale acreditate, ale căror calendare de testare pot depăși termenele de conformare impuse local.

Astfel, deși entitățile raportoare depun eforturi financiare și umane semnificative, finalizarea proceselor tehnice este adesea imposibilă într-un interval scurt, ceea ce face necesară o abordare graduală.

La prima etapă s-ar depune un pachet de acte de tipul:

1. Act de evaluare, pre-implementare a soluției informatice
2. Politică privind identificarea și verificarea identității clienților prin mijloace electronice
3. Regulament privind identificarea și verificarea clienților prin intermediul mijloacelor electronice.
4. Regulament privind măsurile de prevenire și combatere a spălării banilor și finanțării terorismului
5. Raport de audit cu privire la conformitatea sistemului de identificare video

Accentul este pus pe stabilirea unor cerințe robuste de securitate și conformitate pentru soluțiile eKYC, care să asigure alinierea deplină la cadrul legislativ aplicabil.

Totodată, este importantă crearea condițiilor pentru lansarea rapidă a serviciilor eKYC destinate operațiunilor cu risc redus (ex. deschiderea de conturi cu limite tranzacționale restrânse), în vederea diminuării barierelor de acces pentru utilizatori și stimulării incluziunii financiare.

În etapele 2 și 3, organizațiile ar urma să prezinte spre verificare, în termeni rezonabili stabiliți de către BNM (1-6 luni în dependență de complexitatea actelor solicitate) pachetul integral al actelor interne, inclusiv politici de securitate informațională aprofundată, teste de penetrare a sistemului/CRM-ului/spațiului de stocare a datelor, alte acte la solicitarea BNM, asumându-și, pe propria răspundere, perfectarea acestora în limitele termenului acordat.

În plus, considerăm oportun ca tranziția să fie încadrată într-un mecanism deja prevăzut de cadrul normativ BNM, în mod particular, regimul de proiect-pilot de până la 180 de zile, prevăzut pentru testarea instrumentelor de plată electronice. În mod similar, pentru eKYC ar putea fi acceptată o fază pilot de maximum 180 de zile, notificată prealabil către BNM, în baza cerințelor reduse, în care entitatea să opereze eKYC în condiții controlate, cu obligația transmiterii către BNM a concluziilor testării și a planului de dezvoltare.

2. Preimplementarea soluției informatice

Cu referire la pct. 6 din Regulament, propunem completarea capitolului cu o prevedere tranzitorie aplicabilă entităților raportoare care, la data aprobării Regulamentului BNM, aveau deja implementate soluții informatice conforme obiectului reglementării.

În acest sens, considerăm oportun ca aceste entități să nu fie obligate să efectueze evaluarea de preimplementare pentru soluțiile deja operaționale, cu condiția ca acestea să fie supuse în continuare

monitorizării, testării și evaluărilor periodice prevăzute la pct. 11 și alte dispoziții relevante ale Regulamentului.

Totodată, deși este prevăzută efectuarea unei evaluări complexe (analiză de risc, teste end-to-end, securitate IT), nu există o procedură prin care entitatea să poată obține o confirmare preliminară privind acceptabilitatea soluției înainte de lansare. Considerăm binevenită prevederea acestei proceduri.

3. Utilizarea VPN (pct. 6 lit. d) și pct. 16)

Regulamentul prevede necesitatea reducerii riscului asociat utilizării VPN sau proxy pentru ascunderea locației utilizatorului. Totuși, în practică, simpla utilizare a unui serviciu VPN nu constituie, în sine, un indicator suficient de risc, având în vedere că astfel de soluții sunt utilizate pe scară largă în scopuri legitime, inclusiv pentru protecția datelor și securizarea conexiunii.

Riscul relevant din perspectivă AML/CFT sau de securitate este mai degrabă asociat jurisdicțiilor cu risc sporit, inconsecvențelor geografice sau discrepanțelor între diferite surse de date privind localizarea utilizatorului. Aceste situații pot fi identificate prin mecanisme alternative și complementare, precum validarea prin GPS, corelarea adresei IP, analiza comportamentală sau alte instrumente de evaluare a riscului.

În acest context, considerăm oportună reformularea prevederii astfel încât utilizarea VPN sau proxy să fie tratată ca un posibil indicator suplimentar de risc, analizat în contextul unei abordări bazate pe risc și nu ca un element care trebuie prevenit, restricționat sau blocat automat.

4. Gestionarea situațiilor de fraudă în procesul e-KYC

Găsim necesară clarificarea noțiunii de „fraudă” utilizată în Regulament, întrucât nu este explicit dacă aceasta vizează exclusiv fraudele confirmate sau include și tentativele de fraudă detectate și respinse automat de sistemele informatice.

De asemenea, nu este precizat canalul oficial de comunicare pentru raportarea acestor situații și nici obligațiile entităților în cazurile în care există doar indicii tehnice de tentativă frauduloasă, fără posibilitatea identificării persoanei implicate.

În practică, pot exista situații în care entitatea deține fotografii, date biometrice sau înregistrări video aferente unei tentative de eKYC, însă fără a putea stabili identitatea persoanei. În acest context, nu este clar:

- dacă asemenea cazuri trebuie sesizate organelor de drept;
- dacă este posibilă instituirea unui mecanism centralizat de prevenire la nivel național (ex. o listă de alertă sau un sistem de schimb de informații între entități), cu respectarea cadrului privind protecția datelor.

Totodată, este necesară completarea secțiunii cu următoarele elemente:

- **stabilirea duratei de păstrare a datelor** colectate în cadrul procesului eKYC care au fost descalificate din cauza indicatorilor de suspiciune sau considerate frauduloase, inclusiv în situațiile în care nu s-a inițiat o relație contractuală, dar există necesitatea păstrării acestora în scop probatoriu sau pentru prevenirea riscurilor viitoare;
- **definirea criteriilor comportamentale și tehnice** în baza cărora, separat sau cumulativ, entitatea poate identifica o potențială fraudă (ex. inconsecvențe biometrice, utilizarea repetată a acelorași dispozitive, pattern-uri suspecte etc.).

În același context, se impune clarificarea:

- asupra aspectelor prioritare pe care BNM le va analiza în procesul de supraveghere a implementării la nivel național;
- tipului de date statistice care ar putea fi solicitate entităților pentru raportare (ex.: număr inițieri eKYC, cazuri respinse automat, cazuri analizate manual, suspiciuni confirmate, cazuri raportate organelor competente etc.).

5. Aferent pct. 9 din Regulament:

a) Potrivit literei a), entitatea raportoare trebuie să ia în considerare „listele de elemente de identificare compromise sau furate” în cadrul mecanismelor de monitorizare bazate pe riscuri. Nu este clar care este sursa oficială a acestor liste și ce entitate le furnizează.

Menționăm că lipsește o sursă oficială, fapt care condiționează imposibilitatea și ineficiența aplicării cerinței. În prezent, entitățile raportoare nu au acces la astfel de liste centralizate sau validate la nivel național.

În acest sens, propunem excluderea acestei cerințe din regulament sau clarificarea expresă a sursei acestor liste (de exemplu, autorități naționale, baze de date internaționale recunoscute sau furnizori specializați).

b) Potrivit literei g), entitatea raportoare trebuie să ia în considerare „cazurile de furt, uzurpare a identității sau prelucrare ilegală a datelor identificate”.

În legătură cu acest fapt, nu este clar cum ar trebui să fie accesate astfel de informații, deoarece nu există o bază de date centralizată, oficială, cu actele de identitate furate sau compromise.

Respectiv, găsim oportună clarificarea sursei informațiilor sau adaptarea cerinței astfel încât să fie fezabilă pentru entitățile raportoare.

6. Cu referire la pct. 11 din Regulament (alineatul privind testul de penetrare)

Se propune completarea prevederilor cu elemente suplimentare de clarificare, în vederea asigurării unei aplicări uniforme și previzibile.

În mod particular, considerăm necesară reglementarea următoarelor aspecte:

- tipul de testare acceptat sau preferat (ex. Black Box, Gray Box, White Box);
- frecvența minimă recomandată pentru efectuarea testelor;
- aria minimă de acoperire (aplicații, API-uri, infrastructură, componente critice, acces intern etc.);
- cerințe privind calificarea furnizorilor sau metodologia utilizată;
- formatul și conținutul minim al raportului de testare;
- posibilitatea entității raportoare de a contracta furnizori nerezidenți pentru prestarea acestor servicii.

Unele aspecte menționate supra se regăsesc parțial în proiectul de modificare al Regulamentului. Altele, însă, au rămas neelucidate.

Clarificarea acestor elemente ar contribui la creșterea nivelului de securitate cibernetică, asigurând totodată predictibilitate pentru entitățile vizate și o aplicare consecventă a cerințelor regulatorii.

7. Utilizarea semnăturii electronice ca metodă de identificare

Potrivit pct. 21¹ din proiect, în anumite condiții, entitatea raportoare va utiliza, în procesul de identificare electronică a clientului, semnătura electronică calificată.

Propunem excluderea subpct. 2, lit. c) (referitor la confirmarea biometrică facială suplimentară) și a ultimului paragraf (referitor la insuficiența utilizării exclusive a semnăturii calificate) din următoarele considerente:

- Semnătura electronică calificată (QES) confirmă deja identitatea clientului conform Legii nr. 124/2022 și reglementărilor europene. Biometria obligatorie la fiecare sesiune este redundantă.
- QES oferă cel mai înalt nivel de încredere, iar tratarea ei ca "insuficientă" contravine neutralității tehnologice și standardelor europene.
- Obligatorietatea biometriei pentru utilizatorii de semnătură electronică descurajează digitalizarea prin procese excesiv de greoaie și costisitoare.

Considerăm că verificarea biometrică trebuie să fie o măsură opțională, aplicată doar în situații de risc sporit, nu o cerință tehnică universală.

În practică, potrivit altor reglementări în domeniul AML/CFT și procedurilor interne ale entităților raportoare, este prevăzută obligația colectării și păstrării copiei actului de identitate. În acest context, nu este clar dacă, în cazul utilizării semnăturii electronice calificate, această cerință rămâne aplicabilă sau dacă semnătura poate substitui integral prezentarea și verificarea documentului de identitate.

În acest sens, propunem introducerea unei clarificări exprese în Regulament privind caracterul suficient al identificării prin semnătură electronică calificată.

8. Propunem excluderea punctelor 21², 21³, 21⁴, 21⁵ din următoarele considerente:

Legea nr. 308/2017 recunoaște utilizarea semnăturii electronice calificate (QES) ca instrument valid de identificare, fără a o condiționa de straturi tehnice suplimentare (biometrie, NFC, EUDI Wallet). Regulamentul introduce cerințe tehnice adiționale care pot depăși cadrul stabilit de lege și complica nejustificat procesul.

QES reprezintă nivelul maxim de încredere (eIDAS). Identitatea este deja garantată de emitent, iar reverificarea biometrică obligatorie la fiecare sesiune este inutilă și costisitoare.

Condiționarea identificării de tehnologii specifice (citire cip NFC, liveness detection PAD Level 2) generează bariere de acces pentru clienți și costuri excesive de implementare și poate limita aplicabilitatea practică în anumite scenarii, în special pentru entitățile cu resurse limitate.

Utilizarea QES trebuie să fie suficientă per se, fără a forța entitățile să mențină infrastructuri complexe de "live detection" pentru utilizatori deja certificați.

9. Cerința de rezoluție minimă

Potrivit pct. 22 lit. b) și pct. 23 lit. b), 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.

În practică, această cerință poate limita accesul unor clienți care utilizează dispozitive mai vechi sau conexiuni cu performanță redusă, fără ca acest fapt să afecteze în mod real capacitatea de identificare.

Nivelul de risc nu este determinat exclusiv de rezoluția tehnică a camerei, ci de capacitatea soluției informatice de a asigura identificarea clară și neechivocă a persoanei și verificarea autenticității documentului.

Prin proiectul de modificare a Regulamentului, cerința de cel puțin 8 megapixeli se exclude. Totuși, propunem reformularea prevederii astfel încât cerința să facă referire la „calitate suficientă pentru identificare neechivocă”, fără impunerea unui prag tehnic fix de rezoluție, similar regulamentelor din UE.

10. Verificarea clientului sub aspectul existenței informațiilor care ar putea influența reputația

Potrivit pct. 28 lit. a) din Regulament, în scopul verificării și validării datelor/ informațiilor obținute de la client în procesul verificării video, entitatea raportoare este 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.

În practică, procesul automat de screening prin liste adverse media („negative news”) generează un număr ridicat de alerte false pozitive, datorită probabilității mari de coincidență cu persoane neimplicate.

Confirmarea relevanței informațiilor obținute necesită intervenția manuală, ceea ce înseamnă că procesul nu poate fi realizat complet „fără operator uman”.

La fel, Regulamentul permite atât identificarea complet automatizată, cât și verificarea cu operator uman, însă nu sunt stabilite criteriile obiective pentru situațiile în care verificarea manuală devine obligatorie (cazuri neconcludente, scor biometric insuficient etc.).

În concluzie, menținerea prevederii în forma actuală ar limita aplicabilitatea identificării la distanță doar la scenarii cu operator uman, motiv din care propunem excluderea prevederii sau reformularea acesteia astfel încât să nu fie obligatorie.

11. La pct. 29 din proiect, propunem excluderea sintagmei „Certificarea sau confirmarea conformității se aplică diferențiat, în funcție de funcționalitatea specifică, indiferent de modul în care aceasta este integrată în cadrul soluției informatice în sensul prevăzut la pct. 4, după cum urmează:

- a) componenta biometrică — modulul responsabil de verificarea biometrică facială și detectarea atacurilor de prezentare (Presentation Attack Detection în continuare PAD) se conformează cerințelor pct. 29³;
- b) componenta de verificare a autenticității și prezenței fizice a documentului de identitate se conformează cerințelor pct. 29⁴;
- c) soluția informatică în ansamblu, inclusiv infrastructura entității raportoare, se conformează cerințelor pct. 29⁵, reieșind din propunerea de excludere a pct. 29³–29⁵, redată mai jos.

12. Propunem expunerea pct. 29¹ într-o nouă redacție, după cum urmează:

„Pct. 29¹: Standardele internaționale de referință aplicabile pot include, fără a se limita la, următoarele standarde sau cadre tehnice recunoscute la nivel internațional, în funcție de componentele și

tehnologiile utilizate: a) ISO/IEC 30107-3, Biometric presentation attack detection, Part 3: Testing and reporting, pentru componenta biometrică;
b) ISO/IEC 24745, Biometric information protection, pentru protecția datelor biometrice;
c) ISO/IEC 27034, Application security, pentru securitatea aplicației;
d) ISO/IEC 15408, Evaluation criteria for IT security (Common Criteria), pentru evaluarea securității produselor informatice;
e) NIST SP 800-63-3, Digital Identity Guidelines, pentru cadrul general de identitate digitală;
f) NIST SP 800-63B, Authentication and Lifecycle Management, pentru autentificare și gestionarea ciclului de viață al identității digitale.

Entitatea raportoare poate aplica și alte standarde, cadre tehnice ori scheme de certificare echivalente, care asigură un nivel comparabil de securitate și fiabilitate.”

Considerăm că enumerarea exhaustivă a standardelor internaționale la pct. 29¹ și condiționarea conformității de certificări specifice pot conduce la o abordare excesiv de prescriptivă din punct de vedere tehnologic. Cadrul european aplicabil în materia prevenirii spălării banilor și a identificării la distanță (Directiva (UE) 2015/849 și Orientările EBA/GL/2022/15 privind utilizarea soluțiilor de remote onboarding) este construit pe principiul abordării bazate pe risc și al neutralității tehnologice, fără a impune utilizarea unor standarde tehnice determinate în mod exclusiv.

În acest context, propunem reformularea pct. 29¹ în sensul utilizării unei liste orientative și recunoașterii posibilității demonstrării unui nivel echivalent de securitate prin alte standarde sau mecanisme de evaluare internațional recunoscute. O astfel de abordare ar asigura proporționalitate, flexibilitate tehnologică și acces nedistorsionat la piața furnizorilor de soluții de identificare electronică, menținând în același timp obiectivul de securitate urmărit de reglementare.

13. Propunem expunerea pct. 29² în următoarea redacție:

„Pct. 29²: Demonstrarea conformității cu standardele prevăzute la pct. 29¹ se realizează prin una dintre următoarele modalități:

a) prin certificare emisă de un laborator acreditat;

b) prin evaluare independentă, audit sau atestare documentată a furnizorului pentru standarde-cadru.”

Propunerea de reformulare a pct. 29² vine în contextul comentariului de mai sus și urmărește eliminarea legăturii rigide dintre anumite standarde și o modalitate prestabilită de demonstrare a conformității.

În varianta actuală, ISO/IEC 30107-3 este condiționat exclusiv de certificare emisă de un laborator acreditat, în timp ce alte standarde sunt asociate doar cu audit sau evaluare documentată, ceea ce poate restrânge nejustificat opțiunile tehnice disponibile pe piață.

Reformularea propusă permite demonstrarea conformității prin certificare, evaluare independentă sau audit, indiferent de standardul aplicabil, asigurând astfel flexibilitate, neutralitate tehnologică și proporționalitate, fără a diminua nivelul de securitate urmărit de reglementare.

14. Propunem excluderea pct. 29³ - 29⁷, reieșind din raționamentele expuse anterior privind necesitatea evitării unei reglementări excesiv de prescriptive din punct de vedere tehnologic. Stabilirea unor cerințe tehnice minime obligatorii, în afara unei abordări bazate pe risc, reduce flexibilitatea și

neutralitatea tehnologică și poate limita nejustificat opțiunile disponibile pe piață, fără a aduce un plus proporțional de securitate.

15. Potrivit pct. 29¹³ din proiect, testarea de securitate se efectuează periodic, cel puțin o dată pe an, precum și la fiecare modificare substanțială a soluției informatice.

Conform pct. 7 din Regulamentul actual, 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.

În acest context, solicităm respectuos revizuirea periodicității impuse pentru evaluarea soluției informatice și testarea de securitate, prin extinderea acesteia la cel puțin o dată la 3 ani sau ori de câte ori sunt introduse modificări semnificative în soluția eKYC. O astfel de abordare ar asigura menținerea standardelor de securitate, în același timp respectând principiul proporționalității și reducând riscul unor costuri excesive sau al unor blocaje operaționale generate de capacitatea limitată a furnizorilor de servicii de audit și evaluare.

16. Procedura de notificare

Conform pct. 49 din Regulament, 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

Se impune clarificarea expresă a naturii acestei notificări, respectiv dacă aceasta presupune o confirmare/acceptare formală din partea BNM sau dacă entitatea poate iniția procedura în lipsa unui răspuns oficial.

Observăm că proiectul urmărește să aducă claritate în acest sens. Totuși, considerăm necesară includerea unei prevederi explicite potrivit căreia, în cazul în care BNM nu formulează obiecții sau nu transmite un răspuns în termen de 30 de zile, soluția notificată să fie considerată conformă și să poată fi implementată.

17. Identificarea electronică și externalizarea

Aplicarea coroborată a cerințelor privind identificarea electronică și a celor privind externalizarea poate genera dificultăți semnificative de conformare în practică, neadaptat soluțiilor tehnologice actuale.

Principalele bariere identificate sunt:

- Soluțiile globale de top (e-KYC, biometrie, Cloud/SaaS) nu sunt configurate pentru a satisface cerințele specifice locale, forțând băncile către dezvoltări custom costisitoare și ineficiente.
- Rigiditatea regulamentului de externalizare (ex.: clauze de audit direct, control fizic, localizarea datelor, interdicția de externalizare în lanț etc.) este adesea respinsă de furnizorii internaționali de soluții digitale, blocând accesul la tehnologii sigure de validare a documentelor, recunoaștere facială și liveness detection.
- Acest cadru disproporționat poate crea diferențe de competitivitate față de alte jurisdicții din regiune și frânează digitalizarea serviciilor bancare prin costuri și complexitate prohibitivă.

Regulamentul permite externalizarea procesului de identificare la distanță, dar nu stabilește cerințe minime sau setul de documente pe care furnizorul tehnologic trebuie să le prezinte pentru a demonstra conformitatea soluției informatice. În practică, instituțiile investesc în integrare fără a avea certitudinea că soluția este acceptabilă.

18. Obținerea unei copii a actului de identitate (AI)

În contextul înăsprii cerințelor în domeniul protecției datelor cu caracter personal, digitalizării tuturor proceselor, inclusiv arhivelor, în situația identificării unui cetățean al Moldovei și accesului la MConnect, considerăm că obținerea unei copii a AI este excesivă: Un angajat al sucursalei vede și evaluează AI-ul, pe baza informațiilor din AI (o scanare a codului de bare de pe AI pentru a exclude simpla introducere a codului fiscal dintr-un alt document), primește și confirmă datele prin MConnect (inclusiv o fotografie), procesul este executat sub monitorizarea – în acest scenariu, obținerea unei copii nu are nici valoare.

Evident, în alte scenarii, obținerea unei copii va rămâne obligatorie.

Propunem prevederea posibilității de a atenua cerințele pentru participanții ale căror sisteme tehnice și procedurale permit acest lucru.

Subsidiar, în prezent, Regulamentul permite identificarea la distanță exclusiv în baza buletinului de identitate, în timp ce pașaportul este tratat ca document de călătorie și nu este acceptat în acest scop.

Considerăm oportună revizuirea acestei abordări, prin permiterea identificării cetățenilor Republicii Moldova în baza oricărui document oficial emis de autoritățile competente din Republica Moldova (ex. buletin de identitate, pașaport), cu condiția verificării autenticității și valabilității acestuia prin mecanismele disponibile (ex. interogarea bazelor de date ale ASP).

Complementar, susținem ca identificarea la distanță să fie permisă și pentru cetățenii străini care dețin documente de ședere emise de autoritățile Republicii Moldova, fără obligativitatea prezenței fizice, cu condiția verificării prin mecanismele oficiale disponibile.

19. Interpretarea extensivă a Regulamentului

Remarcăm că Regulamentul conține o serie de termeni și cerințe susceptibile de interpretări diferite în practică, în absența unor definiții explicite sau a unor praguri minime orientative.

Cu titlu de exemplu noțiunea de „încercări multiple” în procesul de identificare – nu este clar dacă aceasta se referă la un număr maxim de tentative per sesiune, per dispozitiv, per utilizator sau într-un anumit interval de timp;

- conținutul exact al procesului de „screening” – dacă acesta vizează exclusiv liste de sancțiuni sau include și verificări PEP, negative news, baze de date comerciale etc.;
- pragul acceptabil pentru mecanismele de liveness – scor minim, nivel de încredere sau toleranță la eroare;
- definiția noțiunii de „risc sporit” în anumite contexte tehnice.

În lipsa unor parametri minimi sau a unor exemple de aplicare, fiecare entitate este nevoită să își stabilească propriile criterii interne, ceea ce poate conduce la practici semnificativ diferite la nivel de piață, în funcție de interpretarea individuală a Regulamentului.

Totodată, nu este prevăzut un mecanism formal de comunicare sau schimb de practici între instituții, care să contribuie la o aplicare uniformă și coerentă a cadrului normativ. În consecință, implementarea poate deveni variabilă și neuniformă la nivel sectorial.

Propunem introducerea unor clarificări suplimentare sau exemple orientative privind parametrii minimi de aplicare (ex. încercări multiple, liveness, screening, definirea riscului sporit) și emiterea unor

ghiduri, instrucțiuni sau bune practici la nivel sectorial, care să asigure coerență și proporționalitate în implementare, menținând totodată flexibilitatea necesară unei abordări bazate pe risc.

La fel, remarcăm că Regulamentul nu conține o listă explicită și exhaustivă a documentelor acceptate pentru identificare, ci oferă descrieri generale, susceptibile de interpretări diferite în practică.

În acest sens, se impune introducerea în Regulament a unei liste clare și, pe cât posibil, exhaustive a documentelor acceptate pentru identificare, cu menționarea expresă a documentelor eligibile și, dacă este cazul, a celor excluse.

20. Spre deosebire de sectorul bancar, care poate recurge la rețeaua de sucursale pentru identificarea fizică, prestatorii nebancari (PSP) sunt dependenți structural de soluțiile digitale.

Suspendarea utilizării E-KYC fără o perioadă de tranziție rezonabilă îngreunează procesul de atragere de clienți noi, deoarece:

- PSP-urile nu dețin infrastructură fizică similară băncilor pentru a oferi o alternativă de identificare față în față.
- Blocarea soluției digitale duce la o incapacitate totală de operare pentru entitățile 100% online, generând un risc major de continuitate a afacerii.

Considerăm că, în absența unei soluții E-KYC funcționale, un prestator care nu dispune de o infrastructură fizică extinsă este exclus de facto din activitatea economică, fiindu-i afectată direct continuitatea afacerii. Deși se alocă resurse semnificative pentru aliniere la noile exigențe, conformarea „imediată” este obiectiv imposibilă din cauza unor factori externi independenți de voința noastră, cum ar fi termenele tehnice pentru obținerea certificărilor internaționale.

Obiectivul comun este implementarea unui eKYC sigur, funcțional și accesibil pentru întregul sector. Ajustările propuse nu diminuează nivelul de securitate, ci consolidează aplicabilitatea practică și sustenabilitatea cadrului normativ.

Cu respect,

Mila Malairău

Director Executiv

Camera de Comerț Americană din Moldova