proiect

BANCA NAȚIONALĂ A MOLDOVEI
COMITETUL EXECUTIV

HOTĂRÂREA nr.
din ___ _____ 2026

Pentru modificarea Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice

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

HOTĂRĂȘTE:

1. Regulamentul privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice, aprobat prin Hotărârea Comitetului executiv al Băncii Naționale a Moldovei nr.281/2024 (Monitorul Oficial al Republicii Moldova, 2024, nr. 467-469, art. 886), se modifică după cum urmează:

1.1. Pe tot parcursul textului, sintagmele „furtul sau uzurparea identității", „uzurparea identității" și „ furt, uzurpare a identității", la orice forma gramaticală, se substituie cu sintagma „falsul de identitate", la forma gramaticală corespunzătoare;

1.2. La pct. 6 lit. b) textul „în condițiile Legii nr. 133/2011" se substituie cu textul „în condițiile legislației";

1.3. La pct. 13:
lit. a) se completează cu textul „sau cetățean al statelor membre ale Uniunii Europene care deține un certificat calificat al cheii publice, eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene";

lit. b) se completează cu textul „sau cetățeni ai statelor membre ale Uniunii Europene, sau persoane care dețin un certificat calificat al cheii publice, eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene";

1.4. Pct. 14:
lit. a) va avea următorul cuprins:

„a) toate datele și documentele relevante pentru identificarea și verificarea identității persoanelor fizice cetățeni ai Republicii Moldova și/sau persoanelor juridice rezidente ai căror reprezentanți, fondatori, administratori şi beneficiari efectivi sunt cetățeni ai Republicii Moldova”;

1.5. se completează cu lit. a^1) cu următorul cuprins:
„a^1) toate datele și documentele relevante pentru identificarea și verificarea identității cetățenilor statelor membre ale Uniunii Europene care dețin un certificat calificat al cheii publice, eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene și/sau persoanelor juridice ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai statelor membre ale Uniunii Europene, sau persoane care dețin un certificat calificat al cheii publice, eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene;”;

1.6. La pct. 21:
lit. a) va avea următorul cuprins:
„a) mijloace de identificare electronică cu un nivel de securitate ridicat în sensul Legii nr.124/2022, inclusiv mijloace notificate conform cadrului UE eIDAS/eIDAS 2.0 sau prin portofel european pentru identitate digitală (EUDI Wallet), care furnizează atribute de identitate la un nivel de asigurare ale mijloacelor de identificare electronică ridicat”;

lit. d) se abrogă;

1.7. Regulamentul se completează cu pct. 21^1-21^5 cu următorul cuprins:
„21^1. Entitatea raportoare va utiliza, în procesul de identificare electronică a clientului, semnătura electronică calificată în următoarele condiții:
1) entitatea raportoare identifică clientul prin utilizarea unei semnături electronice calificate bazate pe un certificat calificat al cheii publice, emis de un prestator de servicii de încredere calificat înscris în lista sigură conform Legii nr.124/2022 sau de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene;
2) entitatea raportoare asigură cel puțin următoarele:
a) verificarea validității certificatului calificat (neexpirat și nerevocat), inclusiv a integrității lanțului de încredere;
b) validarea tehnică a semnăturii electronice și confirmarea faptului că semnătura este corect aplicată documentului relevant procesului de identificare;
c) confirmarea titularului certificatului calificat printr-o metodă separată de autentificare, de preferință verificare biometrică facială (compararea imaginii faciale din documentul de identitate cu imaginea captată în timp real);

3) semnătura electronică calificată este utilizată în cadrul unei sesiuni electronice securizate, care asigură autentificare strictă și legarea criptografică a sesiunii la identitatea clientului;
Utilizarea exclusivă a semnăturii electronice calificate fără verificarea cerințelor prevăzute la subpct. 2) și 3) nu se consideră suficientă pentru îndeplinirea cerințelor de identificare la distanță.

21[2]. Pentru metoda prevăzută la pct. 21 lit. a), atunci când identificarea se realizează printr-un mijloc de identificare electronică notificat conform cadrului eIDAS/eIDAS 2.0, aplicația guvernamentală integrată a serviciilor electronice EVO sau prin portofel european pentru identitate digitală (EUDI Wallet), la nivel de asigurare ridicat, entitatea raportoare poate să nu solicite o verificare biometrică suplimentară, cu respectarea cumulativă a următoarelor condiții:
a) mijlocul electronic să asigure verificarea biometrică a persoanei și dovada posesiei mijlocului electronic;
b) fluxul de identificare să fie legat criptografic de sesiunea electronică a clientului și să fie disponibilă dovada tehnică a autentificării;
c) entitatea să nu fi identificat indicatori de risc sporit care să justifice aplicarea unor măsuri suplimentare de precauție.
În situații de risc sporit, entitatea raportoare aplică măsuri de precauție care includ verificare biometrică suplimentară sau o altă metodă independentă de confirmare a identității.

21[3]. Pentru metodele prevăzute la pct. 21 lit. b) și c), entitatea raportoare aplică verificarea biometrică facială (compararea imaginii faciale din documentul de identitate cu imaginea captată în timp real), detecția prezenței clientului și caracterului viu al acestuia (liveness detection), precum și măsuri tehnice care să asigure legarea criptografică a sesiunii și prevenirea fraudei prin înregistrări prealabile.

21[4]. Entitatea raportoare înregistrează și păstrează într-o formă auditabilă toate dovezile aferente procesului de identificare electronică, inclusiv verificările biometrice, validările semnăturilor electronice și autentificările sesiunilor, pe o perioadă de minimum 5 ani de la încetarea relației de afaceri, astfel încât să poată demonstra ulterior conformarea cu cerințele prezentului regulament.

21[5]. În cazul documentelor de identitate emise de statele membre ale Uniunii Europene, în lipsa accesului la registrele oficiale ale statului emitent, autentificarea documentului în procedurile de identificare la distanță se realizează după cum urmează:
1) autentificarea se efectuează exclusiv prin una din următoarele metode:

a) utilizarea unui portofel european pentru identitate digitală (EUDI Wallet), la nivel de asigurare ridicat, cu autentificare strictă și legarea criptografică a sesiunii; sau
b) citirea electronică prin NFC a documentului (carte de identitate electronică/eMRTD), cu verificarea integrității și autenticității datelor electronice, inclusiv verificarea semnăturii electronice a fișierului de securitate SOD și după caz, a utilizării mecanismelor de Passive/Active/Chip Authentication, urmată de corelarea biometrică a imaginii faciale stocate pe cip DG2 cu imaginea captată și detecția prezenței clientului și caracterului viu al acestuia (liveness detection), în condițiile pct. 21^{3}.
2) utilizarea exclusivă a imaginilor documentului (fotografii/scanări) nu este admisă ca unică măsură pentru acceptarea documentelor de identitate emise de statele membre ale Uniunii Europene.
3) entitatea raportoare menține și actualizează certificatele și cheile publice ale autorităților emitente necesare validării și păstrează evidențele procesului de validare în condițiile de păstrare prevăzute de prezentul Regulament.
4) În cazul imposibilității de aplicare a metodelor prevăzute la subpct. 1), identificarea prin mijloace electronice nu se consideră realizată.";

1.8. La pct. 22 lit. b) alineatul 5 cu liniuță și pct. 23 lit. b) alineatul 5 cu liniuță, textul „de cel puțin 8 megapixeli sau" se exclude;

1.9. La pct. 25 textul „(prin e-mail sau SMS)" se exclude;

1.10. Pct. 29 va avea următorul cuprins:

„29. La stabilirea relațiilor de afaceri la distanță utilizând mijloace electronice, entitatea raportoare va utiliza soluții informatice care corespund cerințelor stabilite de standardele internaționale aplicabile, în funcție de componentele și tehnologiile utilizate. 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. 29^{3};
b) componenta de verificare a autenticității și prezenței fizice a documentului de identitate se conformează cerințelor pct. 29^{4};
c) soluția informatică în ansamblu, inclusiv infrastructura entității raportoare, se conformează cerințelor pct. 29^{5}.

1.11. Regulamentul se completează cu pct. 29^{1}-29^{17}, cu următorul cuprins:
„29^{1}. Standardele internaționale de referință aplicabile sunt:

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.

29[2]. Demonstrarea conformității cu standardele prevăzute la pct. 29[1] se realizează, după caz:
a) prin certificare emisă de un laborator acreditat pentru ISO/IEC 30107-3;
b) prin evaluare independentă, audit sau atestare documentată a furnizorului pentru standardele-cadru (ISO/IEC 24745, ISO/IEC 27034, NIST SP 800-63-3, NIST SP 800-63B, ISO/IEC 15408).
Lista standardelor prevăzute la 29[1] poate fi completată prin hotărâre a Comitetului executiv al Băncii Naționale a Moldovei, în funcție de evoluția cadrului internațional, inclusiv prin recunoașterea schemelor echivalente de testare și certificare.

29[3]. Cerințele de certificare prevăzute la pct. 29[4]- 29[6] constituie cerințe tehnice minime obligatorii. Abordarea bazată pe risc, prevăzută la pct. 37-43, se aplică în ceea ce privește alegerea metodei de identificare și măsurile suplimentare de precauție, nu în ceea ce privește securitatea tehnică a soluției informatice.

29[4]. Componenta biometrică utilizată pentru verificarea biometrică facială și detectarea prezenței prevăzute la pct. 21[1]-21[3] trebuie să demonstreze rezistență la atacuri de prezentare echivalentă cel puțin cu nivelul PAD Level 2 conform standardului ISO/IEC 30107-3, prin certificare de către un laborator de testare acreditat sau prin altă metodă de evaluare independentă acceptată de Banca Națională a Moldovei. Nivelul minim obligatoriu de certificare este PAD Level 2, care asigură rezistența componentei biometrice la atacuri sofisticate de prezentare, inclusiv măști parțiale și tehnici de manipulare digitală a imaginii (deepfake).

29[5]. Certificarea prevăzută la pct. 29[4] trebuie să îndeplinească cumulativ următoarele condiții:
a) să fie emisă de un laborator acreditat în domeniul testării conform ISO/IEC 30107-3, inclusiv laboratoare acreditate în cadrul programelor naționale de acreditare a laboratoarelor;

b) să nu fie mai veche de 3 ani de la data emiterii. Entitatea raportoare asigură efectuarea unei evaluări anuale intermediare, în scopul confirmării menținerii nivelului de rezistență la atacuri de prezentare, ținând cont de evoluția tehnicilor de atac;
c) să acopere toate platformele prin care entitatea raportoare oferă servicii de stabilire a relațiilor de afaceri la distanță prin mijloace electronice, inclusiv, după caz, sistemele de operare mobile (iOS, Android) și mediile web. În cazul în care certificarea nu acoperă toate platformele, entitatea raportoare este obligată:
- fie să obțină certificarea pentru celelalte platforme;
- fie să limiteze funcționalitatea de stabilire a relațiilor de afaceri la distanță la platforma certificată;
d) versiunea majoră a componentei biometrice (kit de dezvoltare software în continuare SDK) indicată în certificat să corespundă versiunii implementate în mediul de producție al entității raportoare. În cazul actualizării componentei biometrice:
- la o versiune majoră diferită de cea certificată entitatea raportoare asigură obținerea unei noi certificări;
- la o versiune minoră sau o actualizare de securitate (patch) entitatea raportoare obține o confirmare scrisă din partea producătorului privind menținerea conformității funcționalității de detectare a atacurilor de prezentare;
e) certificarea sau documentele conexe să indice explicit metoda de detectare a prezenței utilizată (activă, pasivă sau combinată) și ratele de eroare obținute la testare: rata de eroare la clasificarea atacurilor de prezentare (Attack Presentation Classification Error Rate — APCER) și rata de eroare la clasificarea prezentărilor bona fide (Bona Fide Presentation Classification Error Rate — BPCER).

29[6]. Certificarea componentei biometrice conform pct. 29[4]-29[5] nu substituie și nu înlocuiește obligația de testare a securității soluției informatice în ansamblu, prevăzută la pct. 29[10]-29[13]. Alte certificări deținute de furnizorul soluției (ISO/IEC 27001, SOC 2 sau similare) nu suplinesc cerința de certificare PAD conform ISO/IEC 30107-3 pentru componenta biometrică.

29[7]. Cerințele pct. 29[4]-29[6] nu se aplică verificărilor biometrice efectuate în cadrul portofelului european pentru identitate digitală (EUDI Wallet) sau al mijloacelor de identificare electronică notificate la nivel de asigurare a încrederii ridicat, atunci când entitatea raportoare nu operează propria componentă biometrică, ci se bazează pe asigurările furnizate de schema de identificare electronică notificată. În acest caz, entitatea raportoare documentează temeiul excluderii și nivelul de asigurare al schemei utilizate.

29[8]. Soluția informatică utilizată pentru stabilirea relațiilor de afaceri la distanță prin mijloace electronice trebuie să includă mecanisme de verificare a autenticității și prezenței fizice a documentului de identitate prezentat de client. Mecanismele trebuie să asigure, cel puțin:
a) detectarea documentelor fotografiate de pe ecranul unui dispozitiv electronic;
b) detectarea fotocopiilor sau documentelor tipărite;
c) verificarea elementelor de securitate ale documentului (holograme, elemente optice variabile), în măsura în care tehnologia disponibilă permite acest lucru;
d) detectarea manipulărilor digitale ale imaginii documentului.

29[9]. Entitatea raportoare documentează în cadrul dosarului prezentat Băncii Naționale a Moldovei capabilitățile de verificare a autenticității documentului, inclusiv limitările cunoscute ale soluției utilizate. Cerințele prevăzute la pct. 29[8] nu se aplică atunci când autenticitatea identității clientului este stabilită prin atestare criptografică în cadrul portofelului european pentru identitate digitală (EUDI Wallet) sau al unui mijloc de identificare electronică notificat la nivel de asigurare a încrederii ridicat. În acest caz, se aplică cerințele prevăzute la pct. 21[5].

29[10]. Anterior lansării în producție a soluției informatice pentru stabilirea relațiilor de afaceri la distanță prin mijloace electronice, entitatea raportoare asigură efectuarea unei testări independente de securitate (penetration test) care acoperă cel puțin:
a) componenta web (dacă există);
b) componenta mobilă (aplicația mobilă);
c) interfețele de programare a aplicațiilor (API);
d) scenarii de fraudă specifice procesului de identificare electronică (cel puțin tentative de impersonare, utilizare documente false, atacuri de prezentare, replay attacks, identitate sintetică, tentative de evaziune a sancțiunilor), inclusiv testarea legării criptografice a sesiunii prevăzute la pct. 21[1] și 21[3];
e) scenarii specifice integrării cu portofelul european pentru identitate digitală (EUDI Wallet), inclusiv tentative de falsificare a atestării portofelului, manipularea mecanismului de selective disclosure și atacuri relay asupra protocolului de prezentare, în cazul în care entitatea raportoare utilizează această metodă de identificare.

29[11]. Testarea de securitate prevăzută la pct. 29[10] trebuie:
a) să fie efectuată de o entitate independentă față de dezvoltatorul soluției;
b) să nu fie mai veche de 12 luni la momentul depunerii notificării;
c) să acopere infrastructura entității raportoare (inclusiv integrările, baza de date, rețeaua), nu exclusiv componenta furnizorului extern;

d) în cazul în care soluția informatică operează în model cloud sau ca serviciu extern (SaaS), scopul testării să includă punctele de integrare între entitate și mediul cloud al furnizorului, securitatea interfețelor de programare a aplicațiilor, protecția datelor în tranzit și în repaus, precum și evaluarea că infrastructura cloud a furnizorului îndeplinește standardele relevante de securitate.

29[12]. Vulnerabilitățile clasificate drept critice sau cu severitate înaltă, identificate în urma testării de securitate, trebuie remediate anterior lansării soluției în producție. Entitatea raportoare prezintă Băncii Naționale a Moldovei dovada remedierii acestor vulnerabilități.

29[13]. Testarea de securitate se efectuează periodic, cel puțin o dată pe an, precum și la fiecare modificare substanțială a soluției informatice.

29[14]. Entitatea raportoare menține un registru actualizat al certificărilor și testărilor de securitate aferente soluției informatice utilizate, care include cel puțin:
a) denumirea componentei certificate, versiunea și furnizorul;
b) standardul de referință și nivelul de certificare;
c) laboratorul sau entitatea care a efectuat certificarea/testarea;
d) data emiterii și data expirării certificării;
e) platformele acoperite;
f) ratele de eroare obținute (APCER și BPCER pentru certificarea PAD).

29[15]. Pentru metodele de identificare bazate pe portofelul european pentru identitate digitală (EUDI Wallet) sau pe scheme de identificare electronică notificate, registrul prevăzut la pct. 29[14] cuprinde cel puțin: identificatorul schemei sau portofelului, statul membru notificator, nivelul de asigurare a încrederii, data ultimei verificări a statutului de notificare și evaluarea riscurilor asociate schemei de către entitatea raportoare.

29[16]. Entitatea raportoare notifică Banca Națională a Moldovei, după cum urmează:
a) în termen de 72 de ore în cazul identificării unor vulnerabilități critice exploatate activ sau care prezintă risc imediat pentru securitatea procesului de identificare electronică;
b) în termen de 30 de zile calendaristice în cazul:
- expirării unei certificări prevăzute la pct. 29[4]- 29[7], fără obținerea unei certificări noi;
- modificării versiunii majore a componentei biometrice la o versiune diferită de cea certificată, care afectează starea certificării.

29^{17}. Banca Națională a Moldovei poate solicita entității raportoare, în orice moment, prezentarea certificărilor, rapoartelor de testare și a altor documente justificative privind conformitatea soluției informatice. ”.

1.12. Pct. 50 va avea următorul cuprins:
„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. Entitatea raportoare nu va demara procedura de identificare prin mijloace electronice a clienților până la expirarea termenului de 30 de zile prevăzut la pct. 49, cu excepția cazului în care Banca Națională a Moldovei comunică anterior expirării termenului confirmarea completitudinii notificării.”;

2. Prezenta Hotărâre intră în vigoare peste o lună de la data publicării în Monitorul Oficial al Republicii Moldova, cu excepția pct. 1 subpct. 1.3. și 1.5. din hotărâre, care vor intra în vigoare odată cu crearea condițiilor tehnice prevăzute la art. XVIII alin. (4) din Legea nr. 144/2025 pentru modificarea unor acte normative (susținerea economiei digitale și a serviciilor electronice).

Entitățile raportoare care, la data intrării în vigoare a prezentei Hotărâri, utilizează deja soluții informatice pentru stabilirea relațiilor de afaceri la distanță prin mijloace electronice dispun de un termen de 12 luni de la data intrării în vigoare a prezentei Hotărâri pentru a se conforma cerințelor art. 29^{4}-29^{17}. În acest termen, entitățile raportoare prezintă Băncii Naționale a Moldovei un plan de conformare aferent fiecărei cerințe.

PREȘEDINTELE
COMITETULUI EXECUTIV **Anca-Dana DRAGU**