



Către: Anca Dragu
Guvernatoare a Băncii Naționale a Moldovei

Nr. 94 din 22 octombrie 2024

Ref.: Opinia AmCham Moldova cu referință la proiectul Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (e-KYC)

Stimată doamnă Guvernatoare,

Vă salutăm din numele Asociației Patronale „Camera de Comerț Americană din Moldova” (în continuare „AmCham Moldova”).

Urmare examinării Proiectului HCE al BNM cu referință la proiectul Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (e-KYC), intervine cu următoarele.

Analizând prevederile proiectului de Regulament, am observat că identificarea la distanță în cea mai mare parte se referă la utilizarea actelor de identitate, fără a ține cont de faptul că Legea 308/2017, la art. 5, alin. 2 lit. a) prevede identificarea în baza informațiilor obținute din surse sigure: ” (2) Măsurile standarde de precauție privind clienții cuprind: identificarea și verificarea identității clienților în baza actelor de identitate, precum și a documentelor, a **datelor sau a informațiilor obținute dintr-o sursă sigură și independentă, inclusiv, dacă sunt disponibile, a mijloacelor de identificare electronică, a serviciilor de încredere relevante sau a oricărui alt proces de identificare sigur, la distanță sau electronic, reglementat, recunoscut, aprobat sau acceptat de organele cu funcții de supraveghere** „

Astfel regulamentul limitează identificarea persoanei doar în baza actului de identitate fără a permite dezvoltarea noilor mecanisme de identificare, cum ar fi doar în baza datelor biometrice și a informației din Registrul Populației.

Nr	Proiectul Regulamentului BNM	Comentarii / Propuneri
1	Art. 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.	Conform Legii 308/2017 la art. 4 alin.1 lit. i) sunt indicare societățile de plată și emitenții de monedă electronică, cu excepția prestatorilor de servicii de informare cu privire la conturi și a prestatorilor de servicii de inițiere a plății – astfel nu este clar în ce condiții urmează să facă identificarea prestatorilor de servicii de informare cu privire la conturi și a prestatorilor de servicii de inițiere a plății. În cazul în care aceștia vor fi excluși de la aplicarea normelor de KYC la distanță se vor crea condiții ne loiale de activitate pe piața de plăți și va genera un risc sporit, neacoperit că prestatorii de informare și inițiere cont nu vor asigura



		identificarea persoanelor care obțin informații și gestionează conturile deschise la alți prestatori de plată.
2	Art. 7 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.	Nu este clar care audit se va considera corespunzător, dacă soluțiile pot fi prezentate către parteneri străini, iar accesul la codul sursă nu poate fi prezentat pentru audit.
3	<p>1. Art. 9 lit. a) și d) – în contextul „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:</p> <p>a) listele de elemente de identificare compromise sau furate;</p> <p>....</p> <p>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;”</p>	<p>Nu este clar de unde se poate utiliza o lista unica a actelor de identitate nevalabile sau furate, practic este o condiție neîndeplinibilă.</p> <p>De asemenea formarea unui registru de utilizare normală și anormală nu este rezonabil și costisitor de dezvoltat și menținut. În special nu este oportun în cazul utilizării aplicației dezvoltate de terți sau prestatori de servicii de încredere.</p>
4	Art. 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:	<p>Luând în considerație că la identificarea persoanei la distanță pot fi utilizate alte mecanisme digitale care nu pot fi utilizate la prezența fizică, nu este corect de limitat procesul în utilizarea aceluiași documente ca la prezența fizică.</p> <p>De asemenea la prezența fizică nu pot fi utilizate surse sigure de identificare, fiind necesar identificarea în baza unui act de identitate cu completarea anchetei clientului.</p> <p>Considerăm excesivă și limitatoare cerința de colectare a datelor ca la prezența fizică, ca urmare a faptului că Legea 308/2017 clar prevede ce se include în măsuri standard de precauție privind clienții (art. 5 alin. 2 al Legii 308/2017).</p>
5	Art. 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	<p>Este necesar de menționat că stabilirea relației de afaceri este un proces care prevede colectarea mai multor informații, inclusiv completerea chestionarului persoanei fizice cu privire la activitatea acestuia. În acest context considerăm excesivă solicitarea de aplicare față de reprezentantul companiei aceleași cerințe ca la client persoană fizică care deschide cont.</p> <p>De fapt se stabilește relație cu persoana juridică, și prin urmare pe reprezentant și beneficiar efectiv urmează a fi colectate</p>



	persoana fizică care acționează în numele persoanei juridice are dreptul legal de a acționa astfel	doar datele strict necesare pentru prestarea serviciilor persoanei juridice, în caz contrar procesarea excesivă a datelor personale ale administratorului sau beneficiarului efectiv poate contravine Legii 133/2011 privind protecția datelor cu caracter personal. Propunem să fie specificat : pentru persoana fizică, reprezentant al persoanei juridice, entitatea raportoare va aplica procesul de identificare a persoanei în similar unui client - persoană fizică.
6	Art. 19 Identificarea clientului utilizând mijloace electronice este precedată de exprimarea consimțământului pentru prelucrarea datelor cu caracter personal în conformitate cu legislația în vigoare.	În cazul în care se insistă pe procesul de consimțământ, atunci este necesar de specificat cum urmează să distrugă datele prestatorul de plată, dacă clientul retrage consimțământul (drept, asigurat de legea 133/2011) Se propune a exclude această clauză că contravine prevederilor art. 5 al Legii 133/2011, care prevede că consimțământul nu este necesar în cazul: a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înainte încheierii contractului, la cererea acestuia; b) îndeplinirea unei obligații care îi revine operatorului conform legii; Astfel prelucrarea datelor personale la identificare cade sub incidența lit. b) al art. 5 al Legii 133/2011 – fiind obligați prin Legea 308/2017 să efectueze identificarea clienților.
7	Art. 20 lit c) – în contextul La identificarea și verificarea identității clienților prin mijloace electronice, entitatea raportoare va asigura aducerea la cunoștință clientului termenele și condițiile	Luînd în considerație că regulamentul se referă la identificarea persoanelor și implică procesarea datelor cu caracter personal și nicidecum politicile de prevenire a spălării banilor, considerăm excesivă obligația prevăzută la lit. c).



	<p>în care identificarea electronică este efectuată. Termenele și condițiile puse la dispoziția clientului, inclusiv și pînă la accesarea de către client a soluției informatice, vor conține, fără a se limita:</p> <p>....</p> <p>„Politica prevenirii spălării banilor” – va conține versiunea succintă a politicii privind identificarea clientului, prevenirea spălării banilor, finanțarea terorismului și identificarea persoanelor expuse politic.</p>	<p>Conform practicelor europene, clientului i se aduce la cunoștință, Condițiile Generale și modul de prelucrare a datelor personale, iar restul actelor informative sunt prezentate în compartimente specializate.</p>
8	<p>Art. 23 lit. a) alin. 2 și 3</p> <ul style="list-style-type: none">- 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 legătură 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 email;	<p>Este necesar de menționat că procesul de inițiere de afaceri poate să difere la fiecare entitate și verificarea numărului de telefon și/sau email să fie efectuat anterior inițierii procedurii de identificare, astfel cerința de înregistrare a numărului de telefon sau de verificare a acestuia este excesivă.</p> <p>Se propune a include în formulare „după necesitate să facă înregistrarea” și respectiv „după necesitate momentul în care clientul primește sau introduce codul unic sau accesează link-ul remis prin serviciul de mesaje scurte (SMS) la telefonul mobil sau email”</p>
9	<p>Art. 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 email 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).</p>	<p>Prevederea este ambiguă și poate fi interpretată, ca fiind obligație de verificare în procesul de identificare, ceea ce nu este o cerință rezonabilă.</p> <p>Nr. telefon și email pot fi verificate anterior, iar includerea obligatorie unei astfel de etape la identificare, duce la faptul că la orice modificare a numărului de telefon sau email se prezumă parcurgerea procesului de identificare.</p> <p>Este necesar de reformulat în modul în care să fie specificat, că verificările la număr de telefon și email urmează a fi efectuate în procesul de stabilire a relației anterior etapei de identificare.</p>



10	<p>2. Art. 27 În cadrul stabilirii relației de afaceri la distanță prin mijloace electronice, entitatea raportoare verifică actele de identitate ale clientului sub următoarele aspecte:</p> <ul style="list-style-type: none">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 manuală a informației de către un angajat;f) contrapunerea datelor din cadrul actelor de identitate prezentate cu datele din cadrul Registrului de stat al populației	<p>Conform formulării art. 27 toate cerințele sunt obligatorii, ceea ce denotă elaborarea unui soft foarte costisitor.</p> <p>Nu este clară solicitarea din punctul d), dacă se contrapune datele din Registrul populației conform cerinței din punctul f).</p> <p>Se propune a reformula:</p> <p>„În cadrul stabilirii relației de afaceri la distanță prin mijloace electronice, entitatea raportoare verifică actele de identitate ale clientului sub cel puțin unul din următoarele aspecte:”</p> <p>De asemenea, se propune a clarifica mai exact care anume date urmează a fi contrapuse datele cu Registrul populației</p>
11	<p>Art. 28 În scopul verificării și validării datelor/informațiilor obținute de la client în procesul verificării video, entitatea raportoare este:</p>	<p>Luând în considerație că aceste cerințe sunt specificate în legea 308/2017 și Regulamentul BNM cu privire la combaterea spălării banilor, se propune a fi exclusă din acest regulament.</p>



12	Art. 28 lit. 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 terțelor persoane sau oricare alte suspiciuni în privința clientului;	Luând în considerație că conform art. 5, lit. b) al Legii 133/2011 nu este necesar consimțământul, se propune a exclude din formulare consimțământul. În cazul în care se referă al alt aspect în procesul de identificare decât consimțământul pentru prelucrarea datelor cu caracter personal (prevăzut art. 19 al Proiectului prezentului Regulamentului), corect ar fi de reformulat astfel încât să fie exclusă interpretarea ambiguă sau greșită.
13	Art. 29 Entitatea raportoare la stabilirea relațiilor de afaceri la distanță utilizând mijloace electronice va utiliza soluții informatice certificate conform standardelor internaționale aplicabile.	Conform formulării nu este clar ce prevede certificarea – deținerea tuturor certificatelor sau utilizarea unor soluții care respectă cel puțin unul din standarde ?
14	Art.30 Entitatea raportoare poate utiliza soluția informatică pentru stabilirea relației de afaceri la distanță prin mijloace electronice pentru actualizarea informațiilor/datelor clienților existenți	Se propune de a fi reformulate, după cum urmează: „Entitatea raportoare poate utiliza soluția informatică atât pentru stabilirea relației de afaceri la distanță prin mijloace electronice, cât și pentru actualizarea informațiilor/datelor clienților existenți
15	Art. 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:	Luând în considerație că personalul de identificare nu reprezintă o specialitate, dar prevede instruire se propune a reformula cerințele, pentru a asigura angajarea și continuitatea activității: „pentru angajatul entității raportoare responsabil de identificarea prin mijloace electronice a clienților: „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 una din următoarele cerințe.”
16	Art.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.	Clauza se referă la obligațiile prestatorilor de plată, de a raporta activitățile și operațiunile suspecte și nici decum nu poate fi atribuită la raportarea incidentelor de la identificare. Legea 308/2017 are cerințe stricte de raportare. Se propune a fi exclusă, duce în eroare și nu se referă la identificarea persoanei.



Suplimentar, menționăm că din conținutul Regulamentului așa și nu este clar cum rămâne cu aplicarea pct. 49, 50, dar și Secțiunea 2 „Preimplementarea soluției informatice” în raport cu entitățile care au deja o soluție implementată, urmează a se notifica BNM sau nu, în ce termen și despre ce urmează a se notifica, precum și cu anexarea căror informații exacte etc.

Vă rog să o considerați pe Veronica Sirețeanu, directoare adjunctă, în calitate de persoană de contact din partea AmCham Moldova (veronicasireteanu@amcham.md) pentru ulterioara interacțiune la acest subiect.

Cu această ocazie, AmCham Moldova apreciază deschiderea Băncii Naționale a Moldovei, exprimându-ne disponibilitatea pentru detalierea comentariilor și propunerilor adresate.

Cu respect,

Mila Malairău

Director Executiv

A.P. „Camera de Comerț Americană din Moldova”