

SINTEZA
 obiecțiilor și propunerilor/recomandărilor
 la proiectul Hotărârii Comitetului executiv al BNM cu privire la aprobarea
 Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice

Conținutul articolelor/ punctelor din proiectul prezentat spre avizare și coordonare	Participantul la avizare (expertizare)/consulta re publică	Nr. obiecției/ propunerii/ recomandă rii	Conținutul obiecției/propunerii/ recomandării	Argumentarea autorului proiectului
I. Obiecții și propuneri de ordin general				
	OCN Microinvest SRL	1	În vederea asigurării implementării treptate a Regulamentului și asigurarea unui termen rezonabil pentru entitățile raportare de a-și ajusta procesele în vederea conformării cu cerințele prevăzute în Regulament, în special în situația în care unele entități au deja setate procese ce țin de identificarea la distanță și/sau implementate soluții active de identificare la distanță propunem stabilirea intrării în vigoare și aplicării acestuia peste un termen de 6 luni din data publicării.	Se acceptă parțial. Regulamentul va intra în vigoare la data publicării în Monitorul Oficial. Entitățile raportoare care au implementate soluții informatice de identificare la distanță a clienților la data intrării în vigoare a Regulamentului se vor conforma noilor cerințe în decurs de 6 luni. În privința altor entități raportoare, termenul nu are relevanță, deoarece cerințele Regulamentului urmează a fi respectate până la implementarea soluției informatice de identificare la distanță a clienților.
	Banca de Finanțe și Comerț S.A.	2	Cum va fi respectata cerința de prezentare a copiei buletinului de identitate nemijlocit de client conform prevederilor p. 37 al Regulamentului BNM Nr. 200/2017	Prin prezentarea prin mijloace electronice a unei copii a BI semnate electronic sau obținerea capturii foto de pe BI în timpul sesiunii de video-audio/foto cu captarea imaginii și aplicarea altor elemente de verificare a informației/documentelor decât cele tradiționale.
		3	Cu ce tip de semnătură vor fi confirmate(semnate) datele chestionarului clientului? Din punctul de vedere al cerințelor Legii 124/2022 și art. 318 al	Prin semnătură electronică calificată sau avansată sau confirmarea informației prezentate prin utilizarea altor metode

	Codului civil reiese că se permite numai semnătura electronică avansată calificată sau semnătura electronică, ceea ce rezultă limitarea folosirii serviciului eKYC pentru populație și nu duce la promovarea utilizării serviciilor la distanță.	recunoscute (metode biometrice, chei de sesiune etc.)
4	Proiectul actual nu diferențiază amploarea măsurilor de precauție în funcție de modelul de eKYC selectat (full-automat, cu participarea angajatului entității) ceea ce poate rezulta la aplicarea incorectă a prevederilor prezentului Regulament. Propunem divizarea cerințelor în funcție de modelului eKYC selectat.	Se acceptă. Prevederile Regulamentului au fost ajustate pentru a stabili cerințe diferențiate.
5	În cazul externalizării parțiale/integrale, inclusiv cu importanța materială a serviciului eKYC nu este clar dacă se necesită obținerea aprobării din partea BNM conform prevederilor Regulamentului nr. 46/2020?	Cerințele de externalizare a unor activități/operațiuni ale băncii sunt reglementate de Regulamentul nr.46/2020 privind externalizarea activităților și operațiunilor băncii. Alte elemente specifice domeniului prevenirii și combaterii spălării banilor și finanțării terorismului sunt reglementate în actele normative aferente acestui domeniu (Legea nr.308/2017, Regulamentul 200/2018 etc.).
6	Din proiectul a Regulamentului nu este clar dacă se necesită aprobarea BNM pentru lansarea eKYC, dacă e posibil primirea unui refuz din partea BNM, care este termenul stabilit pentru analiza setului de analiza? În general acest proces nu este clar definit, ceea ce poate se aduce la interpretarea greșită și/sau tergiversarea prezentării concluziei și lansării serviciului.	Procedura de solicitare a aprobării BNM asupra inițierii procesului de identificare a clienților la distanță este prevăzută în punctele 50-53 din Regulament.

A.P. „Camera de Comerț Americană din Moldova”	7	În vederea asigurării implementării treptate a Regulamentului și asigurarea unui termen rezonabil pentru entitățile raportare de a-și ajusta procesele în vederea conformării cu cerințele prevăzute în Regulament, în special în situația în care unele entități au deja setate procese ce țin de identificarea la distanță și/sau implementate soluții active de identificare la distanță, se propune stabilirea intrării în vigoare și aplicării acestuia peste un termen de 6 luni din data publicării.	Se acceptă parțial. Regulamentul va intra în vigoare la data publicării în Monitorul Oficial. Entitățile raportoare care au implementat soluții informatice de identificare la distanță a clienților la data intrării în vigoare a Regulamentului se vor conforma noilor cerințe în decurs de 6 luni. În privința altor entități raportoare, termenul nu are relevanță, deoarece cerințele Regulamentului urmează a fi respectate până la implementarea soluției informatice de identificare la distanță a clienților.
Asociația Businessului European	8	În proiect sunt utilizate noțiunile de „mijloace digitale” și „mijloace electronice”; Pe tot parcursul textului, cuvântul „digital” se propune a fi substituit cu cuvântul „electronic”. Propunerea are scopul de a racorda limbajul utilizat cu cel regăsit în Legea 124/2022 privind identificarea electronică și serviciile de încredere.	Se acceptă
SPCSB	9	Reieșind din faptul că termenii, noțiunile și expresiile utilizate în proiectul Regulamentului au semnificațiile stabilite și de Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, se propune asigurarea pe întreg textul actului normativ a unei exprimări uniforme prin utilizarea instituției juridice definite de Legea nr. 308/2017, cea de „entitate raportoare”, or autorul de exemplu, la pct. 5-8 indică doar „entitatea”.	Se acceptă
B.C. MAIB S.A.	10	La pct.2 al proiectului Hotărârii, propunem completarea textului, înainte de sintagma „din data publicării în Monitorul Oficial al Republicii	Se acceptă parțial Regulamentul va intra în vigoare la data publicării în Monitorul Oficial.

		Moldova”, cu sintagma „la expirarea termenului de 6 luni”. Propunerea rezultă din faptul că Regulamentul stabilește anumite cerințe, inclusiv tehnice, existența cărora nu poate fi asigurată de către o bancă imediat. Mai mult, în prezent unele bănci utilizează deja anumite soluții informatice pentru identificarea și verificarea identității clienților la distanță, care au fost lansate în lipsa actelor normative ale BNM în acest domeniu. Adaptarea soluțiilor informatice existente la noile cerințe poate fi efectuată în timp, eventual – cu unele dezvoltări tehnice adiționale, fapt care necesită timpul suficient și investiții suplimentare. Astfel, considerăm imperios necesară oferirea unui termen rezonabil, de 6 minim luni de la data publicării hotărârii în Monitorul Oficial al Republicii Moldova, pentru asigurarea conformării entităților raportoare la cerințele Regulamentului nou. Este necesar de menționat un alt aspect important: În prezent, utilizarea de către entitățile raportoare, inclusiv băncile, a soluțiilor informatice pentru identificarea și verificarea identității clienților la distanță, nu este condiționată de faptul deținerii de către entitatea respectivă a statutului de prestator de servicii de încredere calificat, în sensul Legii nr.124/2022. Din pct.6 lit.d), pct.22, pct.44 din Regulament se poate deduce că o entitate raportoare trebuie să dețină calitatea de prestator al serviciilor de încredere calificat, conform Legii nr.124/2022, iar la pct.43 din Regulament este expres prevăzut că entitatea raportoare va oferi un punct de acces securizat pentru începerea procesului de identificare la distanță a clienților <u>pe baza certificatelor calificate pentru sigiliile electronice în conformitate cu Legea nr.124/2022.</u>	Entitățile raportoare care au implementate soluții informatice de identificare la distanță a clienților la data intrării în vigoare a Regulamentului se vor conforma noilor cerințe în decurs de 6 luni. În privința altor entități raportoare, termenul nu are relevanță, deoarece cerințele Regulamentului urmează a fi respectate până la implementarea soluției informatice de identificare la distanță a clienților. Cerințele Regulamentului nu stabilesc obligativitatea entității raportoare de a deține statutul de prestator de servicii de încredere calificat în condițiile Legii nr.124/2022 pentru implementarea politicilor de identificare a clienților la distanță. Regulile care se aplică unui prestator de serviciu calificat în conformitate cu Legea nr.124/2022 urmează a fi respectate dacă entitatea raportoare se bazează pe informația furnizată de către un terț la efectuarea identificării la distanță, utilizând serviciile/produsele acestuia din urmă (în acest caz, cerințele din Legea nr.124/2022 se aplică doar furnizorului terț, nu și entității raportoare).
--	--	--	---

		Totodată, deținerea de către entitatea raportoare a statutului de prestator de servicii de încredere calificat nu este indicată în textul Regulamentului, inclusiv la Capitolul II „Politici și proceduri referitoare la identificarea și verificarea identității clienților prin mijloace electronice”. Lipsa acestor prevederi creează incertitudini privind obligativitatea deținerii de către bancă a statutului respectiv. În conformitate cu prevederile Legii nr.124/2022, statutul de prestator de servicii de încredere calificat poate fi obținut în urma procedurii de acreditare, efectuate de către organul de supraveghere și control (SIS al RM). Această procedură presupune corespunderea entității anumitor cerințe, inclusiv tehnice, pregătirea unui set de documente etc., fapt care necesită timpul suficient și investiții suplimentare. Astfel, în cazul în care Banca Națională a Moldovei consideră că, pentru utilizarea de către o entitate raportoare a soluțiilor informatice pentru identificare la distanță, entitatea respectivă trebuie să dețină obligatoriu statutul de prestator de servicii de încredere calificat, solicităm respectuos să informați băncile despre acest fapt, pentru a asigura obținerea statutului respectiv în modul stabilit. Acest fapt va condiționa necesitatea oferirii unui termen suplimentar pentru asigurarea conformării entităților raportoare la cerințele Regulamentului nou.	
„Paymaster” SRL	11	La pct. 2 din Hotărâre, propunem excluderea textului „din data publicării în Monitorul Oficial al Republicii Moldova” și stabilirea unui termen rezonabil de intrare în vigoare a Regulamentului privind cerințele pentru identificarea și verificarea identității clienților prin intermediul mijloacelor electronice, astfel încât toate entitățile raportoare să	Se acceptă Punctul dat a fost redactat.

		dispună de timp suficient de a modifica și a ajuta procesele interne pentru conformarea la Regulamentul sus menționat.	
„QIWI-M” SRL	12	Ca urmare a modificării Legii 308/2017 prin transpunerea principiilor de identificare la distanță, se constată neconcordanță cu Regulamentul BNM nr. 202/2018 cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea prestatorilor de servicii de plată nebancari, după cum urmează: Conform pct. 54 al Regulamentului BNM nr. 202/2018 „În cazul în care clientul nu se prezintă personal la identificare (de exemplu, în cazul relațiilor prin corespondență sau prin telefon, e-mail, internet sau alte mijloace electronice), prestatorul aplică măsuri de precauție sporită prin utilizarea de mecanisme de tipul semnăturii electronice, a metodelor biometrice, cheilor de sesiune etc. Cu ocazia primei vizite a clientului la prestator, se solicită documentele și informațiile conform cerințelor prezentului Regulament. Suplimentar, prestatorul aplică una sau mai multe din următoarele măsuri:” Această prevedere presupune, ulterior identificării la distanță, prezentarea cu ocazia primei vizite a clientului în oficiu, și aplicarea măsurilor de precauție conform cerințelor Regulamentului BNM nr. 202/2018, ceea ce contravine lit. C) alin. 3 art. 8 al Legii 308/2017, precum și vine în contradicție cu prevederile proiectului Regulamentului BNM cu privire la e-KYC. De asemenea, conform proiectului Regulamentului BNM cu privire la e-KYC, deopotrivă și a Legii 308/2017, persoanele fizice rezidente ale RM care nu sunt cetățeni ai RM, nu sunt eligibili pentru identificarea la distanță, astfel se exclude posibilitatea de identificare a clienților în baza permiselor de ședere și altor acte de identitate	1. Prin modificările introduse la Regulamentul nr.202/2018, ca urmare a modificării Legii nr.308/2017, pct. 54 se exclude. 2. Legiuitorul a permis implementarea cerințelor de identificare la distanță a clienților doar cetățenilor R.Moldova, indiferent de reședința acestora. 3. Cerințele tehnice și tehnologice setate în Regulament au scop de a defini mecanismul pe care entitatea îl va implementa pentru asigurarea intrării în relații cu clienții utilizând metode electronice. La fel, acestea au ca scop protejarea sectorului financiar de eventuale riscuri de spălarea banilor și finanțarea terorismului sau oricare alte infracțiuni asociate crimelor cibernetice, în acest scop fiind utilizate cele mai bune practici internaționale și inclusiv Ghidul EBA/GL/2022/15. 4. Regulamentul setează cerințe pe care entitatea raportoare urmează să le respecte în procesul de identificare la distanță a clienților, însă procedurile individuale detaliate, urmează a fi aprobate de către entitate de sine stătător, dat fiind faptul că în funcție de soluția informatică adoptată, pașii pot fi diferiți. Respectiv, acestea (procedurile) vor conține pași concreți care urmează a fi respectați până la stabilirea relației cu un client (înregistrarea în sistem, completarea chestionarului, validarea datelor, transmiterea datelor, recepționarea,

		datele personale ale căror sunt păstrate în registrele populației RM. Proiectul Regulamentului BNM cu privire la e-KYC prevede cerințe tehnice și tehnologice cu parametri concreți, ceea ce îngreuează realizarea procesului de e-KYC, impune dezvoltări și costuri suplimentare, limitează prestatorii la utilizarea unor anumite soluții de identificare la distanță și nu permite dezvoltarea și utilizarea altor soluții inovatorii. Astfel de abordare contravine principiului PSD2 conform cărei actele legislative și secundare urmează să fie elaborate în modul în care să faciliteze dezvoltarea serviciilor de plată și inovarea acestora. Se propune ca proiectul Regulamentului BNM cu privire la e-KYC să mențină elementele fundamentale prevăzute de Ghidul EBA/GL/2022/15, oferind noțiuni și cerințe generale (cu ar fi: informațiile obținute prin intermediul soluției de înregistrare la distanță a clienților sunt actualizate și adecvate pentru a respecta standardele juridice; toate imaginile, înregistrările video, înregistrările audio și datele sunt captate într-un format lizibil și de o calitate suficientă, astfel încât clientul să poată fi recunoscut fără echivoc; procesul de identificare nu continuă dacă sunt detectate deficiențe tehnice sau întreruperi neașteptate ale conexiunii) oferind entității, în dependență de necesități, riscuri identificate și resurse, să utilizeze soluțiile optime de e-KYC. În proiectul Regulamentului BNM cu privire la e-KYC nu este bine definită noțiunea procesului de înregistrare la distanță. În proiectul Regulamentului BNM cu privire la e-KYC nu sunt delimitate etapele de înregistrare a clientului și identificarea acestuia, astfel se creează impresia că procesul de înregistrare trebuie să fie unul fără întreruperi, ceea ce nu corespunde practicilor internaționale și nu poate fi	verificarea, etc.). Procesele care nu pot fi întrerupte sunt descrise în Regulament și au ca scop, de obicei, validarea identității clientului prin metode video sau de alt gen. 5. Se acceptă, Regulamentul se completează cu cerințe pentru a reda claritate vis-a-vis de soluțiile tehnice care pot fi utilizate pentru identificarea clienților la distanță. Totuși, ținem să menționăm că cerințele Regulamentului nu îngreuează entitatea în dezvoltarea și/sau implementarea soluțiilor alternative de identificare la distanță a clienților, cu condiția că toate cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt respectate.
--	--	--	--

		asigurat în totalitate, deoarece procesul de înregistrare a clientului presupune câteva etape: a. Înregistrarea în sistem fără a iniția o relație de afaceri; b. Procesul de e-KYC: i. Completarea chestionarului financiar; ii. Completarea datelor de contact; iii. Completarea datelor personale; iv. Identificarea persoanei. Conform proceselor desfășurate la moment, completarea chestionarului financiar, a datelor de contact, precum și a datelor personale este o etapă separată pe care clientul o poate parcurge în orice moment, inclusiv în timp cu întreruperi, accentul fiind pus pe procesul de identificare video sau liveness care nu poate fi întrerup și urmează să fie reluat ori de câte ori este întrerupt sau dacă nu se încadrează în tipul indicat. Astfel este necesar de specificat care proces nu poate fi întrerupt și care etape în procesul de înregistrare a clientului în sistemul entității se reglementează de proiectul Regulamentului BNM cu privire la e-KYC propus spre consultare publică. În înțelegerea noastră în proiectul Regulamentului cu privire la e-KYC se pune accent, în mod special, pe procesele de identificare video, fără a se ține cont de existența unor soluții alternative care nu sunt bazate pe procesul video, cum ar fi: acceptarea de la client, în mod automatizat, a pozelor buletinului de identitate și a feței; contrapunerea biometriei feței (verificate liveness) cu datele biometrice din poza din buletinul de identitate ș.a., procese care funcționează fără verificarea datelor din buletinul de identitate și efectuarea proceselor de OCR sau verificarea deteriorării majore a buletinului de identitate, șrifturilor, hologramelor etc. și fără preluarea fișei de însoțire; preluarea datelor despre client (nume, prenume, datele buletinului de	
--	--	--	--

		identitate, locul de reședință, locul nașterii, etc.) direct din registrul populației (care este considerat o sursă sigură și poate fi utilizată pentru identificarea și verificarea identității conform lit. a) alin. 2 art. 5 al Legii 308/2017); cu compararea suplimentară a biometriei feței (verificate liveness) cu datele biometrice din poza din baza de date. Astfel, identificarea clienților se efectuează cu acuratețe maximă și preluare a informațiilor actualizate fără intervenția umană, fără stocarea înregistrării video și audio și fără verificarea calității buletinului (deoarece identificarea și verificarea identității nu se face în baza buletinului). În acest context propunem ajustarea proiectului Regulamentului cu privire la e-KYC în modul în care să fie prevăzute mai multe tipuri de identificare, inclusiv cu prelucrarea biometriei și utilizarea altor surse de identificare în afară de actul de identitate.	
„Credimatic Network” SRL	13	La nivel de UE a fost adoptat Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (“Regulamentul eIDAS”). Regulamentul eIDAS are aplicare directă în statele membre conform tratatelor UE. În baza Regulamentului eIDAS, statele membre au emis reglementări privind procedura legală cu privire la procesul de identificare electronică la distanță a persoanelor fizice. Astfel, cu titlu de exemplu, România prin Autoritatea pentru Digitalizarea României (“ADR”) a adoptat în 2021, Normele privind reglementarea, recunoașterea, aprobarea sau acceptarea procedurii de identificare a persoanei la distanță utilizând mijloace video (“Normele ADR”). Un al document important în raport de reglementarea propusă prin Proiect, este raportul publicat în martie 2021, de Agenția Uniunii	Cerințele Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă a UE și alte reglementări similare europene ce vizează cerință vis-a-vis de identificarea electronică și serviciile de încredere sunt transpuse în legislația națională prin Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere și actele normative subordonate acesteia, Hotărârea de Guvern privind procedura de identificare a persoanei la distanță utilizând mijloace digitale (la moment în consultație publică) și alte acte normative ale SIS emise în același context.

		Europene pentru Securitate Cibernetică (The European Union Agency for Cybersecurity – ENISA). Acest raport este intitulat Remote ID Proofing (“Raportul ENISA”) și care este disponibil aici: https://www.enisa.europa.eu/publications/enisa-reportremote-id-proofing . Raportul ENISA analizează metode de identificare de la distanță și analizează și cadrul legal la nivel european al reglementărilor în materie.	Regulamentul introduce cerințe de respectare a Legii nr.124/2022 și a actelor normative aprobate în contextul implementării legii date, doar la capitolul „evaluarea preimplementare a soluției” (cap.II, pct.B subpct.6 lit.d)). Scopul acestei prevederi este de a alinia cerințele tehnice specifice soluțiilor informatice de identificare electronică a clienților care sunt implementate la entitățile raportoare cu cerințele tehnice specifice domeniului IT care reies din legislația în vigoare, inclusiv cele care transpun standarde internaționale.
	14	Reglementare distinctă pentru (i) identificarea la distanță utilizând mijloace video utilizând mijloace de verificare automatizate, fără operator uman, și (ii) identificarea la distanță utilizând mijloace video care presupune implicarea operatorului uman. Proiectul nu reglementează clar aceste două metode, și anume, identificarea la distanță utilizând mijloace video utilizând mijloace de verificare automatizate, fără operator uman, respectiv identificarea la distanță utilizând mijloace video care presupune implicarea operatorului uman ba mai mult din formularea art. 23, 24, 25, 26, 27, 28 și 29 din Capitolul IV secțiunea B Identificarea prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice cu înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului, rezultă că entitatea raportoare trebuie să respecte în mod cumulativ toate criteriile și condițiile menționate în această secțiune. Or, cele două metode de identificare la distanță presupun acțiuni și formalități total diferite și imposibil de cumulat din punct de vedere tehnic. Spre exemplu, verificarea vizuală a actului de identitate extrasă din	Se acceptă Prevederile Regulamentului au fost ajustate pentru a stabili cerințe diferențiate. Astfel, pentru identificarea la distanță a clienților cu utilizarea mijloacelor de verificare automatizată sunt stabilite prevederi în punctele 24-29, iar pentru verificarea cu operator uman punctele 23, 25-29 și 34.

captura video nu poate fi realizată și de un operator uman și de o soluție software în mod automat. În mod similar, validarea datelor personale colectate ale solicitantului se realizează în mod diferit de un operator uman, respectiv de soluția software care realizează aceeași acțiune. Normele ADR prevăd și reglementează în mod expres această diferențiere între cele două metode. Astfel, art. 10 alineatul (1) din Normele ADR stipulează faptul că: Identificarea la distanță utilizând mijloace video poate fi realizată prin mijloace de verificare automatizate, fără operator uman, sau prin mijloace de verificare cu operator uman. În continuare, Normele ADR stipulează faptul că: Identificarea la distanță utilizând mijloace video realizată cu operator uman poate fi efectuată doar de personal instruit, și respectiv Identificarea la distanță utilizând mijloace video realizată prin mijloace de verificare automatizate, fără operator uman, va utiliza mijloace digitale în conformitate cu standardele în vigoare, dispozițiile din prezentele norme referitoare la personalul instruit sau operatorul uman neaplicându-se în acest caz. Observăm astfel o reglementare legală a celor două metode de identificare, în deplină conformitate cu legislația UE aplicabilă. Trebuie menționat faptul că, în comparație cu metoda de verificare electronică prin mijloace video care presupune un operator uman, metoda verificării automatizate de la distanță a identității prezintă unele avantaje, precum: nu presupune intervenție umană, care poate determina erori sau acțiuni de fraudă realizate în concurs cu persoana vizată și nu depinde de termenul de răspuns al personalului specializat și de disponibilitatea acestuia – prin verificarea automatizată de la distanță, timpul de răspuns este semnificativ mai scurt și nu depinde de disponibilitatea personalului, putând fi realizată 24/7. Reglementarea distinctă a celor două metode
--

	de identificare la distanță este consacrată și în alte state europene, precum Bulgaria, Estonia, Grecia și Norvegia. Prin urmare, vă solicităm în mod respectuos să modificați Proiectul, în sensul de a reglementa în mod distinct identificarea la distanță utilizând mijloace video utilizând mijloace de verificare automatizate, fără operator uman și respectiv (ii) identificarea la distanță utilizând mijloace video care presupune implicarea operatorului uman. În plus, această reglementare distinctă ar trebui să clarifice criteriile și condițiile pe care fiecare metodă trebuie să le îndeplinească în parte și pentru a evita formularea din prezent care conduce la concluzia că acestea trebuie cumulate.	
15	Introducerea standardelor internaționale pentru furnizorii care oferă servicii de identificare la distanță Având în vedere importanța și sensibilitatea chestiunilor reglementate de Proiect, este imperativ pentru operatorii economici care prestează servicii de identificare electronică la distanță ca aceștia să ofere soluții tehnice în deplină conformitate cu standardele internaționale de calitate. Cu toate că Proiectul face o referire marginală la standardele stabilite de Legea 124/2022 (în capitolul IV, secțiunea A din Proiect), dorim să menționăm ca Legea 124/2022 la rândul ei nu include referințe la standarde internaționale de calitate. Astfel, dorim să precizăm faptul ca Raportul ENISA are o secțiune dedicată doar aplicabilității standardelor internaționale în această materie a identificării video la distanță. În secțiunea 3.3 Standardizare la nivel internațional și la nivel de UE, se face mențiune despre standardele ISO aplicabile în domeniu , și respectiv standardele CEN/ETSI. De asemenea inclusiv Normele ADR fac referire la standardul ISO 27001 și regulamentul eIDAS (Regulamentul UE nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru	Se acceptă A fost introdusă cerință separată - pct.6 lit. e) din Regulament.

	tranzacțiile electronice pe piața internă), în Anexa 3 la Normele ADR. Prin urmare, pentru a se asigura un cadru normativ eficient și care să prezinte cele mai înalte garanții de securitate și calitate, este necesar ca Proiectul să conțină prevederi referitoare la necesitatea ca operatorii economici care prestează servicii de identificare electronică la distanță să dețină aceste acreditări și standarde, înainte de a le fi permisă desfășurarea activităților comerciale în conformitate cu Proiectul.	
16	Efectul juridic al verificării electronice a identității la distanță Proiectul nu conține vreo dispoziție cu privire la efectul juridic al parcurgerii cu succes al procesului de identificare electronică la distanță a identității. Pentru a asigura un climat juridic stabil și predictibil, Proiectul ar trebui să indice în mod expres faptul că din moment ce actele de identitate din registrul de evidență a populației au fost verificate în conformitate cu metodele reglementate de Proiect, acest aspect reprezintă o garanție pentru entitatea raportoare și pentru terți în sensul în care actul de identitate a fost validat.	Efectul juridic al verificării electronice a identității clientului constă în stabilirea relației de afaceri dintre entitate și client. Procesul de identificare și verificare a clienților prin mijloace electronice face parte din cerințele privind măsurile de precauție privind clienții stabilite în actele normative aferente domeniului PCSBFT ale BNM. În conformitate cu cerințele privind PCSBFT, în activitatea entităților supravegheate de BNM (cum ar fi, pct. 38 din Regulamentul 200/2018, pct. 32 din Regulamentul nr.202/2018, etc), prezentul proiect stabilește cerințele specifice pentru etapa de identificare și verificare atunci când aceasta se realizează prin intermediul mijloacelor electronice.
17	Distincția dintre verificarea identității la distanță și verificarea aspectelor legate de reglementările privind prevenirea spălării banilor și combaterii finanțării terorismului. Formularea prevederilor legale din Proiect par să conducă la ideea că verificarea aspectelor reglementate de legislația privind prevenirea spălării banilor și combaterii finanțării terorismului ("Componenta AML") este integrată în procesul de identificare și verificare a identității unui solicitant (spre exemplu, articolul 28	Se acceptă parțial Cerințele de verificare a identității persoanei în corespundere cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt diferențiate în Regulament. Totuși, stabilirea relației de afaceri cu clienții, indiferent de metoda de desfășurare a acestui proces (la ghișeu sau

din Proiect). Or, aceste două componente sunt total diferite și ar trebuie reglementate în mod distinct. Astfel, în România, Normele ADR reglementează exclusiv procedura verificării electronice a identității la distanță, iar alte norme adoptate de Banca Națională a României, Autoritatea pentru Supravegherea Financiară, precum și legea Legea 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, reglementează distinct conformarea entităților raportoare în ceea ce privește Componenta AML. Deși din perspectiva de tehnică legislativă, o reglementare distinctă a Componentei AML s-ar impune, pentru rațiuni de claritate și previzibilitate pentru actorii afectați de aceste reglementări, considerăm că această Componentă AML poate fi reglementată în Proiect, însă într-un mod total distinct de procedura de verificare electronice a identității la distanță (cu titlu de exemplu, reglementarea Componentei AML ar putea să se regăsească într-un capitol distinct). De asemenea, din punct de vedere cronologic și operațional, în primă fază este important ca procedura de identificare reglementată prin Proiect să fie finalizată. Odată identitatea persoanei fizice fiind stabilită (a se vedea și comentariul nostru din paragraful 5 de mai sus), entitatea raportoare poate să treacă la următorul pas și anume, parcurgerea Componentei AML. Astfel, trebuie precizat faptul că aceste două procese sunt total distincte și au efecte (inclusiv juridice) distincte de asemenea. Proiectul ar trebui să reglementeze în mod diferit aceste aspecte, comentariile noastre de mai sus fiind de asemenea relevante, cu titlu exemplificativ, realizarea Componentei AML ar putea fi de asemenea externalizată de entitatea raportoare unui terț care oferă astfel de servicii, dar care nu în mod necesar trebuie să ofere și servicii de verificare electronică a identității la distanță. Având în vedere	la distanță) nu poate fi desfășurată și finalizată fără parcurgerea etapei de verificare a identității persoanei.
--	--

		cele expuse în acest paragraf 6, considerăm că Proiectul ar trebui să fie modificat în sensul în care Componenta AML să fie clar disociată de procesul de verificare electronică a identității la distanță.	
„Nova Pay” SRL	18	În vederea asigurării implementării treptate a Regulamentului și asigurarea unui termen rezonabil pentru entitățile raportare de a-și ajusta procesele în vederea conformării cu cerințele prevăzute în Regulament, în special în situația în care sunt deja setate procese ce țin de identificarea la distanță și/sau implementate soluții active de identificare la distanță, se propune stabilirea intrării în vigoare și aplicării acestuia peste un termen de 6 luni din data publicării.	Se acceptă
Ministerul Justiției	19	De ordin redacțional, comunicăm că odată cu prezentarea proiectului spre înregistrare Ministerului Justiției urmează a fi inclusă parafa de înregistrare a acestuia.	Se acceptă
	20	La clauza de adoptare, subliniem asupra importanței respectării art. 16 alin. (2) și art. 44 alin. (1) din Legea nr. 100/2017 cu privire la actele normative. Astfel, se va indica doar temeiul juridic concret pentru emiterea actului normativ, referințe la alte prevederi care nu constituie temei juridic de adoptare a actului normativ elaborat, nu se vor indica în clauza de adoptare. În acest context, este oportună revizuirea temeiului juridic al proiectului, având în vedere că dispozițiile care se referă la competența generală a Băncii Naționale a Moldovei de a adopta acte normative în domeniul său de competență, nu constituie temei juridic de emitere. Prin urmare, în calitate de temei legal se va indica doar art. 5 ¹ alin. (3) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.	Se acceptă

		21	La proiectul Regulamentului, parafa de aprobare se va expune în următoare redacție: „Aprobat prin Hotărârea Comitetului executiv al Băncii Naționale a Moldovei nr. /2023”, cu excluderea cuvântului „Anexă”	Se acceptă
		22	Pe parcursul proiectului se va lua în considerare faptul că punctul se evidențiază printr-o ușoară retragere spre dreapta de la alinierea textului pe verticală.	Se accepta
		23	Capitolele II și IV urmează a fi revizuită în conformitate cu art. 53 din Legea nr. 100/2017 cu privire la actele normative potrivit căruia „(1) În funcție de complexitatea actului normativ, elementele structurale ale actului normativ pot fi grupate după cum urmează: a) articolele și punctele – în secțiuni, însemnate succesiv cu numere ordinare exprimate prin cifre arabe. În cazul unor acte normative complexe, articolele și punctele pot fi grupate mai întâi în paragrafe și/sau subsecțiuni. Observația se referă, în special, la însemnarea elementelor structurale cu literele A, B, C, care nu sunt caracteristice unui act normativ. Adițional, având în vedere art. 52 alin. (3) din Legea nr. 100/2017, pentru interpretare corectă și aplicare comodă, punctele pot fi divizate în subpuncte sau alineate. Subpunctele sunt însemnate cu numere ordinare, exprimate prin cifre arabe, urmate de o paranteză, și se evidențiază printr-o ușoară retragere spre dreapta de la alinierea textului pe verticală. Subpunctul poate conține diviziuni însemnate succesiv, de regulă, cu litere latine mici urmate de o paranteză. În acest sens, urmează a fi revizuit tot textul proiectului.	Se acceptă
II. Obiecții și propuneri la punctele din proiect				
Pct. 1: (v2 – pct.1) Prezentul Regulament privind cerințele pentru	BC MAIB S.A.	1	La pct. 1 al Regulamentului, propunem ca sintagma „stabilirii și/sau desfășurării relațiilor” să fie înlocuită cu sintagma „inițierii relației”.	Nu se acceptă

identificarea și verificarea identității clienților prin intermediul mijloacelor electronice (în continuare - Regulament) are drept scop stabilirea cerințelor privind politicile și procedurile necesare, sistemul de control intern, riscurile și măsurile de protecție, precum și cerințele tehnice minime în scop de identificare a clienților și verificarea identității acestora de către subiecții specificați la pct. 3 în cazul stabilirii și /sau desfășurării relațiilor de afaceri cu aceștia fără prezență fizică.			Propunerea se bazează pe terminologia utilizată în Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului nr.308 din 22.12.2017 (în continuare - „Legea nr.308/2017”) și anume - „inițierea relației de afaceri”. În ceea ce privește desfășurarea relației de afaceri cu clienții identificați la distanță, aceasta poate avea loc prin alte canale, de exemplu - prin sisteme automatizate de deservire la distanță, sau cu prezența fizică a clienților la oficiile băncii. În astfel de cazuri, sunt aplicabile alte acte normative ale Băncii Naționale a Moldovei din domeniile respective. Suplimentar menționez că domeniul de aplicare al Ghidului EBA privind utilizarea soluțiilor de înregistrare la distanță a clienților în temeiul articolului 13 alineatul (1) din Directiva (UE) 2015/849 (acest document este indicat ca unul dintre cele de bază pentru elaborarea proiectului Regulamentului), este doar înrolarea noilor clienți la distanță - a se vedea pct.5 din Ghidul menționat.	Ambii termeni sunt utilizați în Legea nr.308/2017 și actele normative subordonate acestora și au același sens. La pct. 12 din Regulament este exemplificat în privința cui sunt aplicabile cerințele de identificare și verificare a clienților, respectiv, la stabilirea relațiilor și în cazul actualizării informațiilor despre clienții existenți.
Pct. 2: (v2 – pct.2) Cerințele, normele, regulile, procedurile, practicile, limitele și pragurile de raportare aplicabile pentru clienții identificați cu prezență fizică sunt aplicabile și prezentului Regulament, iar măsurile de prevenire și combatere a spălării banilor și finanțării terorismului se vor aplica în conformitate cu cerințele Legii nr. 308/2017	B.C. MAIB S.A.	2	La pct. 2 din Regulament, propunem ca sintagma „prezentului Regulament” să fie înlocuită cu sintagma „clienților, identificarea cărora la distanță este efectuată conform prezentului Regulament”. Prin modificarea propusă, vor fi determinați clienții, în raport cu care sunt aplicabile normele Regulamentului.	Se acceptă

cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (în continuare - Legea nr. 308/2017) și actele normative aprobate pentru implementarea acesteia.				
Pct. 4 : (v2 – pct.4) Termenii, noțiunile și expresiile utilizate în prezentul Regulament au semnificațiile stabilite în Legea nr. 308/2017, Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere (în continuare - Legea nr. 124/2022) și actele normative emise pentru implementarea acestora. De asemenea, în sensul prezentului Regulament se utilizează următorii termeni și expresii: <i>soluție informatică pentru identificarea la distanță (soluție)</i> – un ansamblul de elemente tehnologice implicate în procesul de identificare a persoanei la distanță prin mijloace digitale, prin care se	A.P. „Camera de Comerț Americană din Moldova”	3	La pct. 4 din proiectul Regulamentului sunt utilizate noțiunile de <i>mijloace digitale</i> și <i>mijloace electronice</i> . În denumirea proiectului este utilizată noțiunea de <i>mijloace electronice</i> . Astfel, considerăm necesar de a utiliza aceleași noțiuni în tot textul Regulamentului, pentru evitarea confuziilor.	Se acceptă
	Banca Comercială Română Chișinău S.A.	4	La pct. 4 alineatul 2 „înregistrare la distanță a clientului” – propunem să fie revizuită sintagma deoarece noțiunea de înregistrare presupune/include mai multe procese, fără a se limita la procesul de identificare și verificare a identității clientului. Versiunea propusă “identificarea persoanei la distanță prin mijloace digitale”. Totodată se va asigura o uniformizare a noțiunilor, inclusiv o corelare cu noțiunile din proiectul hotărârii Guvernului cu privire la serviciul guvernamental de identificare a persoanei la distanță E-KYC.	Se acceptă parțial Noțiunea se expune conform cerințelor Legii nr.308/2017, respectiv – „stabilirea relației de afaceri la distanță a clientului”.

transmit datele, imaginile capturate/încărcate și/sau informațiile comunicate de solicitant; <i>înregistrare la distanță a clientului</i> – reprezintă identificarea și verificarea identității clientului prin intermediul mijloacelor electronice realizate prin utilizarea unei metode sau a mai multor metode concomitent, prevăzute la art.5¹ alin.(2) din Legea nr.308/2017.	Asociația Businessului European	5	La pct. 4, noțiunea soluție informatică pentru identificarea la distanță se propune a fi expusă în următoarea redacție: „soluție informatică pentru identificarea la distanță – ansamblu de elemente tehnologice în format electronic, care oferă posibilitatea sigură de a determina identitatea unei persoane fizice pe baza datelor biometrice (imaginea facială), voce, IDNP și după caz a altor date de identificare din actul de identitate și a datelor stocate în Registrul de stat al populației;” Comunicăm că definiția propusă vine în sine să înglobeze expres cerințele tehnice prin care să fie identificată o persoană, or, definiția din proiect, nu stabilește cerințe față de această soluție, ceea ce ar putea da o interpretare mai largă și imprevizibilă în cazul proiectului. A se evoca că pentru a exclude cazurile de atribuire a unor identități false, se necesită a condiționa faptul identificării cu coinciderea datelor prezentate cu cele din Registrul de stat al populației, or, în lipsa acestui element, simpla contrapunere a datelor din actul de identitate (imaginea din actul prezentat cu imaginea interlocutorului) nu va duce la stabilirea identității persoanei (identitatea persoanei este stabilită odată cu înregistrarea persoanei în Registrul de stat al populației). Suplimentar a se comunica că indicarea categoriilor de date utilizate și produsul final reprezintă un imperativ din punct de vedere al legislației privind protecția datelor, în special dreptul de a utiliza datele – art. 5 și art. 9 din Legea nr. 133/2011 privind protecția datelor cu caracter personal.	Nu se acceptă Definiția propusă îngustează aplicabilitatea și nu corespunde cu prevederile art.5¹ din Legea nr.308/2018. De asemenea, referința la Registrul de stat al Populației nu pare relevantă, având în vedere că actele normative în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului oferă posibilitatea utilizării și a altor metode de verificare a informației despre client. Cu referire la modificările propuse pentru o altă definiție, menționăm că Regulamentul înglobează cerințe de înregistrare și prelucrare a datelor cu caracter personal, nefiind necesară dublarea.
---	---------------------------------	---	---	---

			La pct. 4, noțiunea înregistrare la distanță a clientului se propune a fi expusă în următoarea redacție: 2 Noțiunea „înregistrare la distanță a clientului – reprezintă operațiune de prelucrare a datelor care permit identificarea și verificarea identității clientului prin intermediul mijloacelor electronice realizate prin utilizarea unei sau a mai multor metode realizate concomitent din cele prevăzute la art. 51 alin. (2) din Legea nr. 308/2017.” Propunerea este argumentată prin faptul că noțiunea din proiect nu reflectă expres activitatea la care se referă, inclusiv nu specifică activitățile care se includ ca măsuri tehnice.	
--	--	--	---	--

Asociația băncilor din Moldova	6	- noțiunea soluție informatică pentru identificarea la distanță se propune a fi expusă în următoarea redacție: „soluție informatică pentru identificarea la distanță – ansamblu de elemente tehnologice în format electronic, care oferă posibilitatea sigură de a determina identitatea unei persoane fizice pe baza datelor biometrice (imaginea facială), voce, IDNP și după caz a altor date de identificare din actul de identitate și a datelor stocate în Registrul de stat al populației;” Comunicăm că definiția propusă vine să înglobeze expres cerințele tehnice prin care să fie identificată o persoană, or, definiția din proiect, nu stabilește cerințe față de această soluție, ceea ce ar putea da o interpretare mai largă și imprevizibilă în cazul proiectului. A se evoca că pentru a exclude cazurile de atribuire a unor identități false, se necesită a condiționa faptul identificării cu coinciderea datelor prezentate cu cele din Registrul de stat al populației, or, în lipsa acestui element, simpla contrapunere a datelor din actul de identitate (imaginea din actul prezentat cu imaginea interlocutorului) nu va duce la stabilirea identității persoanei (identitatea persoanei este stabilită odată cu înregistrarea persoanei în Registrul de stat al populației). Suplimentar, menționăm că indicarea categoriilor de date utilizate și produsul final reprezintă un imperativ din punct de vedere al legislației privind protecția datelor, în special dreptul de a utiliza datele – art. 5 și art. 9 din Legea nr. 133/2011 privind protecția datelor cu caracter personal. - noțiunea înregistrare la distanță a clientului se propune a fi expusă în următoarea redacție: operațiune de prelucrare a datelor care permit identificarea și verificarea identității clientului prin intermediul mijloacelor electronice realizate prin utilizarea unei sau a mai multor metode realizate	Nu se acceptă Definiția propusă îngustează aplicabilitatea și nu corespunde cu prevederile art.5¹ din Legea nr.308/2018. De asemenea, referința la Registrul de stat al Populației nu pare relevantă având în vedere că actele normative în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului oferă posibilitatea utilizării și a altor metode de verificare a informației despre client. Cu referire la modificările propuse pentru o altă definiție, menționăm că Regulamentul înglobează cerințe de înregistrare și prelucrare a datelor cu caracter personal, nefiind necesară dublarea.
--------------------------------	---	---	--

		concomitent din cele prevăzute la art. 51 alin.(2) din Legea nr.308/2017.” Propunerea este argumentată prin faptul că noțiunea din proiect nu reflectă expres activitatea la care se referă, inclusiv nu specifică activitățile care se includ ca măsuri tehnice.	
--	--	---	--

B.C. MAIB S.A.	7	La pct.4 al Regulamentului este prevăzut că termenii și noțiunile utilizate au semnificațiile stabilite în Legea nr.308/2017, Legea nr.124/2022. Suplimentar, sunt definite două noțiuni (termeni). Necătând la acest fapt, prin textul Regulamentului se utilizează noțiunile (expresiile) care diferă de cele expuse în Legea nr.308/2017 și în pct.4 al Regulamentului, de exemplu: „identificarea la distanță a clienților” și nu „înregistrare la distanță a clienților”, „stabilirea relației de afaceri” și nu „inițierea relației de afaceri”, „terminarea relației de afaceri” sau „încheierea relației de afaceri” și nu „încetarea relației de afaceri”, „beneficiar real” și nu „beneficiar efectiv” ș.a.m.d. De asemenea, în diferite norme ale Regulamentului se utilizează diferite noțiuni (expresii), care după logica normei respective ar trebui să aibă conținut analogic, de exemplu: „identificare video” și „verificare video”, însă din motivul utilizării expresiilor diferite se poate înțelege că acestea sunt două procese diferite. Întru evitarea neclarităților /interpretărilor, considerăm necesară ajustarea terminologiei utilizate în Regulament, la cea din Legea nr.308/2017 și Legea nr.124/2022, iar în cazul noțiunilor, semnificația cărora este stabilită în pct.4 al Regulamentului – propunem utilizarea prin tot textul Regulamentului a acelorași noțiuni.	Se acceptă
Ministerul Justiției	8	Cu privire la pct. 4, propunem excluderea cuvântului „Termenii” având în vedere că este sinonim cu cuvântul „noțiunile”.	Se acceptă

Pct. 5: (v2 – pct.5) Entitatea va elabora, aproba și menține politici și proceduri pentru a se conforma obligațiilor care îi revin în temeiul art.5 alin.(2) lit. a) și lit. c) din Legea nr.308/2017, în situațiile în care clientul este identificat la distanță. Aceste politici și proceduri	Asociația Businessului European	9	La pct. 5 se propune a fi completată cu o nouă literă: „f) realizarea evaluării impactului asupra protecției datelor în corespundere cu legislația privind protecția datelor cu caracter personal”. Propunerea este argumentată de prevederile art. 23 din Legea nr. 133/2011 privind protecția datelor cu caracter personal dar și de prevederile art. 35 din proiectul de lege privind protecția datelor cu caracter personal care vine să transpună Regulamentul General privind Protecția Datelor (nr. 2016/679 GDPR).	Se acceptă
---	--	----------	---	-------------------

trebuie să fie stabilite în funcție de riscurile de spălare a banilor și finanțare a terorismului identificate și să cuprindă cel puțin următoarele: a) o descriere generală a soluției pe care o utilizează pentru a colecta, verifica și înregistra informații pe tot parcursul procesului de înregistrare la distanță a clienților. Aceasta trebuie să includă o explicație a elementelor și funcționării soluției; b) situațiile în care poate fi utilizată soluția de identificare la distanță a clienților, ținând cont de factorii de risc identificați și evaluați în conformitate cu art. 6 alin. (1) din Legea nr.308/2017, în cadrul evaluării riscurilor în domeniul propriu de activitate, inclusiv descrierea categoriei de clienți, produse și servicii eligibile pentru identificare la distanță; c) etapele care sunt complet automatizate și etapele care necesită intervenție umană; d) controalele instituite pentru a se	10	La pct. 5 lit. a), cuvintele „colecta, verifica și înregistra” se substituie cu cuvintele: „colecta, stoca, contrapune, verifica, valida actualiza”. Norma vizate se propune a fi completată cu noțiuni opozabile în ordinea procesului tehnologic de prelucrare a datelor, deoarece în versiunea proiectului, lipsește procesul de stocare, contrapunerea, validare și actualizare a datelor.	Se acceptă
--	----	---	------------

asigura că prima tranzacție cu un client nou înregistrat este executată numai după ce au fost aplicate toate măsurile inițiale de precauție privind clienții; e) descrierea programelor de inițiere și de formare periodică pentru a asigura sensibilizarea personalului și informarea continuă și înțelegerea funcționării soluției de identificare la distanță a clienților și a riscurilor asociate.	A.P. „Camera de Comerț Americană din Moldova”	11	Se propune excluderea cuvântului „inițiale” pentru a nu crea incertitudine, or Legea nr. 308/2017 nu operează cu astfel de calificative aferent măsurilor de precauție.	Se acceptă
	OCN Microinvest SRL	12	Se propune la pct. 5, lit. d) excluderea cuvântului „inițiale” pentru a nu crea incertitudine, ori Legea nr. 308/2017 nu operează cu astfel de calificative aferent măsurilor de precauție.	
	Banca Comercială Română Chișinău S.A.	13	La pct. 5, lit. d) solicităm să fie furnizate clarificări adiționale privitor la sintagma „inițiale” din textul „măsurile inițiale de precauție privind clienții”.	

Banca Comercială Română Chișinău S.A.	14	Solicităm să fie revizuită art. 5 lit. e) „descrierea programelor de inițiere și de formare periodică pentru a asigura sensibilizarea personalului și informarea continuă și înțelegerea funcționării soluției de identificare la distanță a clienților și a riscurilor asociate.” Propunem sa fie exclusă necesitatea descrierii programelor, ținând cont de existența elementelor din pct. 5 lit a)-d), astfel se va reda sensul ca entitățile raportoare, sa dispună de programe continue de instruire ale angajaților care realizează identificarea clienților la distanță prin utilizarea mijloacelor digitale, totodată asigurând o uniformizare cu prevederile art. 13 (3) lit. d) din Legea nr. 308/2017.	Nu se acceptă Formarea continuu a personalului în domeniul PCSBFT este un element-cheie în sistemul de control intern al entității și contribuie la îmbunătățirea abilităților și cunoștințelor angajaților de a gestiona procesele eficient.
„Qivi-M” SRL	15	Pct. 5 lit. d) : Nu este clar ce prevăd măsurile inițiale de precauție luând în considerație faptul că, în conformitate cu legislația națională aplicabilă, măsurile de precauție pot fi standarde, simplificate și sporite. Pentru o înțelegere mai bună a cerinței date, se propune reformularea textului de la lit. d).	Se acceptă

Asociația băncilor din Moldova	16	- la lit. a), cuvintele „colecta, verifica și înregistra” recomandăm a se substitui cu cuvintele: „colecta, stoca, contrapune, verifica, valida și actualiza”. Norma vizată se propune a fi completată cu noțiuni opozabile în ordinea procesului tehnologic de prelucrare a datelor, deoarece în versiunea proiectului, lipsește procesul de stocare, contrapunere, validare și actualizare a datelor.	Se acceptă
	17	- se propune a fi completat cu o nouă literă: „f) realizarea evaluării impactului asupra protecției datelor în corespundere cu legislația privind protecția datelor cu caracter personal”. Propunerea este argumentată de prevederile art. 23 din Legea nr. 133/2011 privind protecția datelor cu caracter personal dar și de prevederile art. 35 din proiectul de lege privind protecția datelor cu caracter personal care vine să transpună Regulamentul General privind Protecția Datelor (nr. 2016/679 GDPR).	Se acceptă
	18	- la lit. d) se propune excluderea cuvântului „inițiale”, or, Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului nr. 308 din 22.12.2017 (în continuare - Legea nr.308/ 2017) nu conține noțiunea „măsurile inițiale de precauție”.	Se acceptă

Pct. 6 : (v2 – pct.6) Entitatea raportoare, atunci când analizează dacă să fie implementată o nouă soluție de identificare la distanță a clienților, va efectua o evaluare preimplementare. Astfel, entitatea va stabili domeniul de aplicare, pașii și cerințele în materie de evidență a datelor, care ar trebui să includă cel puțin: a) o evaluare a caracterului adecvat al soluției în ceea ce privește plenitudinea și acuratețea datelor și documentelor care urmează a fi colectate, precum și a fiabilității și independenței surselor de informații utilizate; b) o evaluare a impactului utilizării soluției asupra riscurilor specifice ale entității, inclusiv de spălarea banilor și finanțarea terorismului, operaționale, reputaționale și juridice, în special, cel de neconformare cu cerințele aplicabile privind protecția datelor cu caracter personal; c) identificarea posibilelor măsuri de atenuare și acțiuni de	A.P. „Camera de Comerț Americană din Moldova”	19	Pct. 6 din proiectul Regulamentului propus include expresia „cel puțin” la pașii și cerințele în materie de evidență a datelor fiind urmat de 7 litere, iar la litera d) este prevăzută evaluarea conformității soluției din perspectiva Legii nr. 124/2022. Respectiv, urmează a fi clarificat dacă această literă este aplicabilă doar pentru cazul în care soluția include o identificare electronică folosind serviciile de încredere în conformitate cu Legea nr. 124/2022 sau pentru toate tipurile de soluții indicate în Legea nr. 308/2017, art. 51, alin (2) lit. a), b) și c), întrucât pentru lit. b) din Legea nr. 308/2017 art. 51, alin (2), nu este obligatorie integrarea soluției cu serviciile de încredere conform Legii nr. 124/2022. Prin urmare, pct. 6, lit. d) din prezentul Regulament ar trebui să includă o expresie suplimentară la redacția actuală, în care să prevadă că prezenta literă este obligatorie doar pentru soluțiile care conțin servicii de încredere care conform Legii nr. 308/2017 art. 51, alin (2) lit. a) și c)", lit. b) nu are nevoie de o asemenea evaluare a conformității. În temeiul celor menționate se propune următoarea redacție a pct. 6, lit. d): <i>„d) evaluarea conformității soluției cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace electronice stabilite pentru prestatorul de servicii de încredere calificat, Document semnat electronic. Pentru verificarea semnăturii a se accesa: https://msign.gov.md</i> <i>stabilite în temeiul prevederilor Legii nr. 124/2022, în cazul utilizării metodelor de identificare prin mijloacele electronice prevăzute la art. 51 alin. (2) lit. a) și c) din Legea 308/2017”.</i> Tot aici, la pct. 6, lit. b) este necesară includerea referinței la Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal deoarece aceasta explică în ce cazuri urmează a fi efectuată	Se acceptă parțial Evaluarea conformității soluției 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 urmează a fi efectuată pentru toate metodele de stabilire a relației de afaceri la distanță prevăzute de cerințele Legii nr.308/2017. În cazul lipsei acestei necesități, Raportul de evaluare preimplementare urmează să conțină această informație.
---	--	-----------	--	--

remediere pentru fiecare risc identificat; d) evaluarea conformității soluției cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace digitale stabilite pentru prestatorul de servicii de încredere calificat, stabilite în temeiul prevederilor Legii nr. 124/2022; e) teste pentru a evalua riscurile de fraudă, inclusiv riscurile de fraudă prin uzurparea identității; f) o evaluare a riscurilor asociate tehnologiei informației și comunicațiilor (TIC) și de securitate; g) o testare end-to-end a funcționării soluției care vizează clienții, produsele și serviciile oferite în conformitate cu politicile și procedurile de identificare la distanță aprobate.			evaluarea impactului (art. 23 și art. 24 din Legea vizată). De asemenea, sunt descrise criteriile în baza cărora entitatea raportoare/operatorul de date personale urmează să efectueze această evaluare. Prin urmare, referința dată va adăuga previzibilitate. În temeiul celor menționate se propune următoarea redacție a pct. 6 lit. b): <i>”b) o evaluare a impactului utilizării soluției asupra riscurilor specifice ale entității, inclusiv de spălare a banilor și finanțarea terorismului, operaționale, reputaționale și juridice, inclusiv evaluarea de impact în condițiile Legii nr. 133/2011 privind protecția datelor cu caracter personal”.</i>	
	BC Comerțbank S.A.	20	Pct. 6 din proiectul Regulamentului propus include expresia „cel puțin” la pașii și cerințele în materie de evidență a datelor fiind urmat de 7 litere, iar la litera d) este prevăzută evaluarea conformității soluției din perspectiva Legii nr. 124/2022. Respectiv, urmează a fi clarificat dacă această literă este aplicabilă doar pentru cazul în care soluția include o identificare electronică folosind serviciile de încredere în conformitate cu Legea nr. 124/2022 sau pentru toate tipurile de soluții indicate în Legea nr. 308/2017, art. 5¹, alin (2) lit. a), b) și c), întrucât pentru lit. b) din Legea nr. 308/2017 art. 5¹, alin (2), nu este obligatorie integrarea soluției cu serviciile de încredere conform Legii nr. 124/2022. Prin urmare, pct. 6, lit. d) din prezentul Regulament ar trebui să includă o expresie suplimentară la redacția actuală, în care să prevadă că prezenta literă este obligatorie doar pentru soluțiile care conțin servicii de încredere care	Se acceptă parțial Evaluarea conformității soluției 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 urmează a fi efectuată pentru toate metodele de stabilire a relației de afaceri la distanță prevăzute de cerințele Legii nr. 308/2017. În cazul lipsei acestei necesități, Raportul de evaluare preimplementare urmează să conțină această informație.

		conform Legii nr. 308/2017 art. 5¹, alin (2) lit. a) și c)", lit. b) nu are nevoie de o asemenea evaluare a conformității. În temeiul celor menționate se propune următoarea redacție a pct. 6, lit. d): <i>„d) evaluarea conformității soluției cu cerințele pentru realizarea procedurii de identificare a persoanei la distanță, utilizând mijloace digitale stabilite pentru prestatorul de servicii de încredere calificat, stabilite în temeiul prevederilor Legii nr. 124/2022. Prezenta literă este obligatorie doar pentru soluțiile de identificare electronică care îmbină serviciile de încredere”.</i> Tot aici, la pct. 6, lit. b) este necesară includerea referinței la Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal deoarece aceasta explică în ce cazuri urmează a fi efectuată evaluarea impactului (art. 23 și art. 24 din Legea vizată). De asemenea, sunt descrise criteriile în baza cărora entitatea raportoare/operatorul de date personale urmează să efectueze această evaluare. Prin urmare, referința dată va adăuga previzibilitate.	
B.C. „ProCredit Bank” S.A.	21	Așa cum este descris în punctele 6, 7 și 50, entitatea raportoare, anterior demarării procedurii de identificare prin mijloace electronice a clienților, este obligată să efectueze o evaluare preimplementare și să informeze BNM cu privire la corespunderea cu cerințele prezentului regulament și legislației în vigoare. În acest sens, Vă rugăm să specificați dacă va urma o aprobare/răspuns din	Se acceptă parțial Prevederile Regulamentului au fost modificate astfel încât entitatea raportoare să aibă obligația de a notifica BNM și nu de a informa cu 30 de zile înaintea demarării procedurii de stabilire a relației de afaceri la distanță. În cazul constatării anumitor deficiențe/necorespondere cu cerințele

Banca Comercială Română Chișinău S.A.		partea BNM și să indicați acest aspect în regulament. Adicional, în cazul în care va fi emisă decizia privind aprobarea/răspuns din partea BNM, Vă rugăm să specificați termenul examinării de către BNM. La pct. 6 lit. a) solicităm sa fie furnizate clarificări adiționale pentru a înțelege sensul aplicării sintagmei “...și independenței surselor de informații utilizate”. Privitor la pct. 6 lit. a), b), d), e), f) considerăm necesar să fie furnizate mai multe explicații din partea BNM, inclusiv un ghid privitor la riscurile evaluate și testele de fraudă solicitate. În special pentru lit. e) “teste pentru a evalua riscurile de fraudă, inclusiv riscurile de fraudă prin uzurparea identității”, solicităm să fie furnizate clarificări privitor la modul și conținutul acestor teste, cum necesită să arate/să fie efectuate testele, reperele testelor solicitate. Totodată solicităm BNM să revizuiască necesitatea și condițiile aplicării prevederilor pct. 6, în special lit. d) în cazul în care entitatea raportoare va utiliza soluții și servicii guvernamentale de identificare a persoanei la distanță, care se prezumă că sunt elaborate/dezvoltate asigurând o conformitate cu cadrul legal, totodată prezumându-se că până la punerea în folosință acestea sunt acumulate și obținute validările autorităților relevante la nivel național. La pct.6 lit. f) sintagma “și de securitate” solicităm sa fie înlocuit cu textul “securitatea informație”.	Regulamentului, BNM va informa entitatea asupra aspectelor necesar a fi îmbunătățite. Cerințele de prevenire și combatere a spălării banilor și finanțării terorismului stabilesc că identificarea și verificarea datelor/informației despre client urmează să fie efectuată din surse sigure și independente. Având în vedere cele menționate și ținând cont de faptul că unele soluții informatice care pot fi folosite de către entități pentru stabilirea relației de afaceri cu clienții la distanță utilizează anumite date/informații pentru verificarea identității persoanelor din surse terțe, cerința de la pct.6 lit.a), urmează să implementeze cerințele generale de PCSBFT. Teste de evaluare a altor riscuri pe care entitatea urmează să le aplice pentru asigurarea implementării unor soluții informatice fiabile de stabilire a relației la distanță trebuie să corespundă standardelor și bunelor practici specifice ariilor de riscuri țargetate (fraudă, securitatea informației, uzurparea identității). Respectiv, mecanismul de evaluare și raportare a rezultatelor urmează a fi stabilit de entitate de sine stătător.
--	--	---	---

Asociația Businessului European	22	1.La pct. 6 lit. a) va avea următorul cuprins: „a) o evaluare a caracterului adecvat și sigur al soluției de identificare la distanță 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”. Expunerea în redacția propusă urmărește scopul de a stabili suplimentar criteriile de eligibilitate a soluție, în special: accesibilitatea (ceea ce va asigura continuitatea și siguranța proceselor în cazul entităților raportoare), asigurarea criteriului tehnologic de nonrepudiare a informației (ceea ce va permite excluderea eventualelor intervenții de modificare/ștergere a datelor). 2.La pct. 6 lit. d) din proiect, acest punct trebuie sa fie aplicabil doar în cazul utilizării metodelor de identificare electronică prevăzute la art. 51 alin. (2) litera a) și litera c) din Legea nr. 308. Formularea acestui punct presupune ca evaluarea pre implementare trebuie să conțină toate măsurile indicate la literele a)-g), adică corespunderea cerințelor Legii nr. 124/2022 chiar și atunci când se face identificarea electronică în baza art. 51 alin. (2) litera b) din legea nr. 308 Urmează a fi utilizată denumirea de mijloace electronice în loc de mijloace digitale. 3.La pct. 6 lit. e) după cuvintele „de fraudă prin” se propune a fi completat cu cuvintele „furtul sau”. A se menționa că la moment furtul de identitate și uzurparea de identitate este prevăzut în proiectul de	1. Se acceptă 2. Evaluarea conformității soluției 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 urmează a fi efectuată pentru toate metodele de stabilire a relației de afaceri la distanță prevăzute de cerințele Legii nr.308/2017. În cazul lipsei aceste necesități, Raportul de evaluare preimplementare urmează să conțină această informație. 3. Se acceptă
---------------------------------	----	--	--

		lege prezentat spre consultări publice de Ministerul de Justiție https://justice.gov.md/ro/content/ministerul-justitiei-initiat-consultarile-publice-asupraproiectului-de-lege-care-prevede . 4.La pct. 6 se propune de a completa cu o literă nouă: „h) verificarea jurisdicției de operare și stocare a datelor prelucrate, în special din perspectiva țărilor care asigură un nivel adecvat de protecție a datelor cu caracter personal în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.” Propunerea are drept scop de a stabili criterii de evaluare în ceea ce privește jurisdicția unde vor fi prelucrate datele.	4. Nu se acceptă Prevederile art.32 din Legea privind protecția datelor cu caracter personal stabilește expres condițiile pentru transmiterea transfrontalieră a datelor cu caracter personal, iar entitățile au obligația de a respecta cerința dată. Astfel, considerăm că nu este necesar evidențierea suplimentară a acestei norme în Regulament. Suplimentar, cerințele Legii nr.308/2017 stabilesc obligativitatea entităților de a prelucra datele cu caracter personal în corespundere cu legislația cu privire la protecția datelor cu caracter personal.
„Qiw-M” SRL	23	Nu este clară cerința de evaluare a conformității soluției. Pe de o parte acesta ar putea fi interpretată ca o necesitate de obținere a certificatului de acreditare de la organul de supraveghere și control. Totodată, nu este clar care este acest organ de supraveghere și control? De asemenea, nu este clar care sunt cerințele pentru realizarea procedurii de identificare a persoanei la distanță stabilite în temeiul prevederilor Legii nr. 124/2022. În acest context considerăm oportun revizuirea acestui punct, inclusiv prin includerea unor referințe la prevederile din prezentul proiect de Regulament sau alt act normativ în care sunt	Comentariu. Scopul unei evaluări preimplementare a soluției informatice care va fi utilizată pentru stabilirea relațiilor de afaceri la distanță este corespunderea soluției criteriilor setate (de ex. plenitudinea/acuratețea datelor, fiabilitate, veridicitatea datelor obținute, stocarea etc.) și va asigura gestionarea adecvată a riscurilor (operaționale, securitate, juridice, de spălare a banilor și finanțare a terorismului etc.) în activitate.

		specificate cerințele de identificare a persoanei la distanță, utilizând mijloace digitale stabilite pentru prestatorul de servicii de încredere calificat.	
Asociația băncilor din Moldova	24	- lit. a) va avea următorul cuprins: „o evaluare a caracterului adecvat și sigur al soluției de identificare la distanță 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”. Expunerea în redacția propusă urmărește scopul de a stabili suplimentar criteriile de eligibilitate a soluției, în special: accesibilitatea (ceea ce va asigura continuitatea și siguranța proceselor în cazul entităților raportoare), asigurarea criteriului tehnologic de nonrepudiare a informației (ceea ce va permite excluderea eventualelor intervenții de modificare/ștergere a datelor).	Se acceptă
	25	- pe tot parcursul textului de proiect, cuvântul „digital” se propune a fi substituit cu cuvântul „electronic”. Propunerea are scopul de a racorda limbajul utilizat cu cel regăsit în Legea 124/2022 privind identificarea electronică și serviciile de încredere.	Se acceptă

26	- lit. d) se propune completarea textului indicat la lit.d), pct. 6 cu următorul text: "Această evaluare este obligatorie doar pentru soluțiile de identificare electronică care îmbină serviciile de încredere" Legea nr.308/2017, art. 51, alin (2) lit. b) prevede posibilitatea de identificare și verificare a identității clienților prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului. Norma respectivă nu conține careva referințe la Legea nr. 124/2022, similar cu norma din pct.15, lit.b) din proiectul Regulamentului.	Comentariu. Evaluarea conformității soluției 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 urmează a fi efectuată pentru toate metodele de stabilire a relației de afaceri la distanță prevăzute de cerințele Legii nr.308/2017. În cazul lipsei aceste necesități, Raportul de evaluare preimplementare urmează să conțină această informație.
27	- lit. e) după cuvintele „de fraudă prin” se propune a fi completat cu cuvintele „furtul sau”. A se menționa că la moment furtul de identitate și uzurparea de identitate este prevăzut în proiectul de lege prezentat spre consultări publice de Ministerul de Justiție https://justice.gov.md/ro/content/ministerul-justitiei-initiatconsultarile-publice-asupra-proiectului-de-lege-care-prevede	Se acceptă

		28	- se propune a complete pct. 6 cu o literă nouă: „h) verificarea jurisdicției de operare și stocare a datelor prelucrate, în special din perspectiva țărilor care asigură un nivel adecvat de protecție a datelor cu caracter personal în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.” Propunerea are drept scop de a stabili criterii de evaluare în ceea ce privește jurisdicția unde vor fi prelucrate datele.	Nu se acceptă Prevederile art.32 din Legea privind protecția datelor cu caracter personal stabilește expres condițiile pentru transmiterea transfrontalieră a datelor cu caracter personal, iar entitățile au obligația de a respecta cerința dată. Astfel, considerăm că nu este necesar evidențierea suplimentară a acestei norme în Regulament. Suplimentar, cerințele Legii nr.308/2017 stabilesc obligativitatea entităților de a prelucra datele cu caracter personal în corespundere cu legislația cu privire la protecția datelor cu caracter personal.
Pct. 7 : (v2 – pct.7) Entitatea va prezenta și demonstra BNM realizarea evaluărilor și testelor menționate la pct. 6., rezultatul acestora, precum și modul în care aplicarea soluției asigură atenuarea și remedierea riscurilor de spălare a banilor și finanțare a terorismului și alte riscuri identificate pentru tipurile de clienți, servicii, produse, jurisdicții, pentru care aceasta este aplicabilă.	A.P. „Camera de Comerț Americană din Moldova”	29	Se propune excluderea sintagmei „și demonstra”, deoarece art. 51 din Legea nr. 308/2017 nu prevede această obligație pentru entitățile raportoare.	Se acceptă parțial Textul prevederii a fost modificat.
	BC Comerțbank S.A.	30	Se propune excluderea sintagmei „și demonstra”, deoarece art. 5 ¹ din Legea nr. 308/2017 nu prevede această obligație pentru entitățile raportoare.	Se acceptă parțial Textul prevederii a fost modificat.
	Banca Comercială Română Chișinău S.A.	31	La pct. 7 sintagma „Entitatea va prezenta și demonstra BNM” solicităm să fie înlocuit cu textul”. Entitatea va prezenta la solicitarea BNM”.	Se acceptă parțial Textul prevederii a fost modificat.

SPCSB	32	La pct. 7, se propune înlocuirea sintagmei „va prezenta și demonstra BNM realizarea” cu sintagma „va prezenta BNM dovada realizării”.	Se acceptă parțial Textul prevederii a fost modificat.
Asociația Businessului European	33	Pct. 7, considerăm necesar excluderea sintagmei „și demonstra”, din motiv că art. 51 din Legea nr. 308 nu prevede această obligație pentru entitățile raportoare.	Se acceptă parțial Textul prevederii a fost modificat.
„Qiw-M” SRL	34	La ce etapa entitatea are obligația de a prezenta la BNM toate informațiile și documentele menționate la pct.6? Cum procedează entitatea care are deja înregistrat la BNM sistem care include și soluția pentru identificarea la distanță? Este necesar să prezinte suplimentar careva documente?	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.
Asociația băncilor din Moldova	35	se propune: a) Excluderea cuvântului ”jurisdicții”, în dependență de clarificările care vor fi oferite pentru pct.9, lit. e) și b) Substituirea sintagmei ”va prezenta și demonstra BNM realizarea” cu o altă sintagmă/expresie cum ar fi de exemplu: ”va prezenta BNM actele/informațiile justificative în măsură să demonstreze”. Legea nr.308/2017, art. 51, alin (1) Identificarea și verificarea identității clienților prin intermediul mijloacelor electronice în conformitate cu prevederile art.5 alin.(2) lit.a) se admit în cazul persoanelor fizice cetățeni ai Republicii Moldova, precum și în cazul persoanelor juridice rezidente ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai Republicii Moldova. Ținând cont de limitările indicate, se propune excluderea factorului ”jurisdicții” din obligația de evaluare a riscurilor. Utilizarea termenului ”demonstra” în obligația băncii la prezentarea rezultatelor testelor și evaluării de riscuri indicate la pct.6 creează confuzie privind modul în care acest lucru trebuie realizat. Respectiv, propunem utilizarea unei sintagme care pare mai	Se acceptă Se acceptă

			potrivită și clară, și anume ”cu prezentarea actelor/informațiilor confirmative”	
Pct. 8 : (v2 – pct.8) Entitatea raportoare va monitoriza soluția de identificare la distanță a clienților în mod continuu pentru a se asigura că funcționează în conformitate cu scopul acesteia. În acest context, entitatea va dispune de politici și proceduri care vor cuprinde cel puțin: a) pașii pe care entitatea îi va întreprinde pentru a fi satisfăcută de calitatea, plenitudinea, acuratețea, caracterul adecvat și securitatea datelor colectate în timpul procesului de identificare la distanță a clienților și care trebuie să fie proporțional cu riscurile de spălare a banilor și finanțare a terorismului la care aceasta este expusă; b) scopul și frecvența unor astfel de revizuri periodice; și c) circumstanțele care vor declanșa revizuri ad-hoc, care ar trebui să includă cel puțin: - modificări ale expunerii la riscul de	Banca Comercială Română Chișinău S.A.	36	La pct. 8 lit. c) liniuța 3, solicităm modificarea redacției textului în „o creștere estimată a tentativelor de fraude de identitate ale clienților, identificate de entitatea raportoare”.	Se acceptă
	SPCSB	37	La pct. 8 lit. a), se propune înlocuirea sintagmei „pentru a fi satisfăcută” cu sintagma „pentru a asigura”, la lit. b), se propune excluderea sintagmei „unor astfel de”, iar la lit. c) se propune înlocuirea sintagmei „circumstanțele care vor declanșa” cu sintagma „temeiurile de inițiere și realizare a”.	Se acceptă
	BC MAIB S.A.	38	La pct.8 lit.c) din Regulament, prima liniuță, sintagma „expunerii la riscul de spălare a banilor și finanțare a terorismului entității” propunem să fie înlocuită cu sintagma „expunerii entității la riscul de spălare a banilor și finanțare a terorismului”. La pct.8 lit.c) din Regulament, ultima liniuță, cuvântul „legal” propunem să fie înlocuit cu cuvântul „normativ”.	Se acceptă

spălare a banilor și finanțare a terorismului entității; - deficiențe privind funcționarea soluției detectate în cursul activităților de monitorizare, audit sau supraveghere; - o creștere estimată a tentativelor de fraudă; - modificări ale cadrului legal.				
Pct. 9: (v2 – pct.9) Entitatea raportoare se asigură că mecanismele de monitorizare sunt bazate pe riscuri și iau în considerare, ca o condiție minimă, cel puțin următorii factori: a) listele de elemente de identificare compromise sau furate; b) scenariile de fraudă cunoscute în ceea ce privește identificarea la distanță; c) indicatori privind compromiterea confidențialității, integrității sau	B.C. „ProCredit Bank” S.A.	39	Conform punctului 9 „Entitatea raportoare se asigură că mecanismele de monitorizare sunt bazate pe riscuri și ia în considerare, ca o condiție minimă, cel puțin următorii factori: [...] f) poziția geografică cu risc ridicat a persoanei”. Vă rugăm să specificați ce se are în vedere prin “poziția geografică cu risc ridicat”. De asemenea, considerăm necesar a se clarifica dacă trebuie luate în vedere jurisdicțiile cu risc sporit, sau/ și cele cu risc mediu, precum și lista jurisdicțiilor ce nu implementează standarde internaționale de transparență sau/și lista jurisdicțiilor cu risc sporit publicate pe site-ul SPCSB. Adițional, considerăm oportun a se face trimitere și la lista statelor care asigură un nivel adecvat de protecție a datelor, conform prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.	Comentariu: „Poziția geografică cu risc ridicat a persoanei” reprezintă un factor de risc care urmează a fi luat în calcul de către entitatea raportoare la stabilirea mecanismului și instrumentelor de monitorizare a clienților și tranzacțiilor acestuia. În interiorul unei jurisdicții există „locații” care pot prezenta un risc mai mare în comparație cu altele, dat fiind anumite circumstanțe sau elemente de risc (de ex. zone recunoscute pentru acordarea de facilități fiscale, zone portuare/tranzit, zonă recunoscută că facilitează contrabanda ori traficul de bunuri/persoane etc). Listele cu jurisdicții cu risc sporit este un factor suplimentar de risc (art.8 alin. (3) din legea nr.308/2017) pe care entitatea urmează să-l considere la stabilirea și pe parcursul relației de afaceri cu clienții săi.

autenticității sesiunii ca urmare a procedurii de identificare; d) registrul de utilizare normală și anormală a dispozitivului de acces sau a programului informatic furnizat persoanei ce urmează a fi identificată de către entitatea raportoare; e) poziția geografică anormală/neobișnuită a persoanei; f) poziția geografică cu risc ridicat a persoanei.	Banca Comercială Română Chișinău S.A.	40	Privitor la pct. 9 lit. a) pentru a asigura un astfel mecanism de monitorizare băncile trebuie să dispună de informații despre cazurile de date de identitate compromise sau furate. Rugăm să se țină cont că totuși este un proces de identificare la distanță, în care băncile în cazul aplicării unui astfel de proces pot presupune despre o eventuala compromitere/furt/falsificare. În lipsa unor investigații de către autoritățile naționale abilitate, băncile nu pot confirma cu certitudine un caz de compromitere/furt/falsificare. Aceste cazuri pot fi cunoscute doar în situațiile când acestea sunt cunoscute și finalizate cu investigații, pe parcursul utilizării aplicației pentru identificarea clienților la distanță. Astfel solicităm să fie efectuate clarificări cum astfel de factori pot fi aplicați în lipsa unor informații/investigații din partea autorităților naționale ca urmare cazurilor reale identificate.	Entitatea se bazează pe informații veridice furnizate de către autoritățile competente sau utilizând cele mai bune practici cunoscute și standarde internaționale, inclusiv din practica proprie, pentru identificarea elementelor compromise sau furate.
		41	Privitor la pct. 9 lit. c) și d) solicităm să fie furnizate clarificări adiționale, astfel încât nu sunt clare cerințele solicitate.	Comentariu: Indicatorii de risc sau elementele utilizate pentru compromiterea anumitor date/informații sau a aplicațiilor, vor fi folosite de către entitate pentru monitorizările ulterioare ale clienților și tranzacțiilor acestora. De asemenea, existența informației privind dispozitivele utilizate pentru stabilirea relației de afaceri și efectuarea tranzacțiilor, la fel, cu potențialele zone de risc în care se utilizează, pot contribui calitativ la capacitatea de monitorizare a clienților și tranzacțiilor acestora și determina o eventuală activitate suspectă

			din perspectiva spălării banilor și finanțării terorismului.
	42	Privitor la pct. 9 lit. e), f) solicităm respectuos să fie furnizate clarificări, după ce parametri se presupune că necesită să fie efectuate detectarea locației.	Comentariu: Dispozitivele moderne au incorporate modul de GPS și navigație care odată cunoscut entității, informația poate fi utilizată pentru monitorizarea clienților și tranzacțiilor acestora pentru determinarea eventualelor activități suspecte.
Asociația Businessului European	43	La pct. 9 se propune de a fi completat cu o literă nouă: „cazurile de furt, uzurpare a identității sau prelucrarea ilegală a datelor identificate”. Propunerea are scopul de a determina obiectivul de a urmări cazurile de prelucrare neconformă a datelor.	Se acceptă
SPCSB	44	La pct. 9 lit. d), se propune înlocuirea sintagmei „de utilizare normală și anormală” cu sintagma „de înregistrare a cazurilor de utilizare obișnuită, cât și a cazurilor de utilizare contrar normelor stabilite”, iar de la lit. e), se propune excluderea cuvântului „anormală”, or acest termen este unul uzual, dar nu este corespunzător limbajului juridic ce cuprinde noțiuni specifice domeniului său.	Se acceptă
A.P. „Camera de Comerț Americană din Moldova”	45	La pct. 9, lit. e) din proiect urmează a fi clarificat dacă se are în vedere poziția geografică ca țară / regiune (de tipul identificării în scurt timp din țări diferite) sau ca locație efectivă a clientului (de tipul încăperii /locației neobișnuite) care să genereze suspiciuni că clientul nu acționează din nume propriu fiind impus să facă anumite acțiuni.	Comentariu: Se are în vedere locația clientului în cadrul unei jurisdicții.

			Totodată, lit. f) specifică analizarea factorului cum ar fi poziția geografică cu risc ridicat a persoanei. În înțelegerea noastră, considerăm că mai degrabă se referă la lista acelor țări cu risc sporit. Astfel, solicităm precizări în acest sens.	Comentariu: Se are în vedere factorul de risc conform art.8 alin.(3) lit.m)-p) din Legea nr.308/2017.
B.C. MAIB S.A.	46		La pct.9 lit. d) din Regulament, propunem ca sintagma „programului informatic” să fie înlocuită cu sintagma „soluției informatice”.	Se acceptă
			La pct.9 lit. e) și lit. f) din Regulament, necesită a fi clarificate noțiunile utilizate, or ce poziție geografică a persoanei se va considera anormală /neobișnuită, sau cu risc ridicat – cea care diferă de domiciliul (țară, localitate), de reședință temporară sau o altă poziție geografică? Clarificarea este necesară și obligatorie reieșind din faptul că acești factori sunt indicați ca o condiție minimă pentru construirea de către bancă a mecanismelor de monitorizare. Astfel, propunem de a comasa lit.e) și lit.f) într-o normă având următorul conținut: „e) poziția geografică neobișnuită a persoanei, altă decât adresa de domiciliu indicată în actul de identitate sau adresa de reședință declarată de către client;”.	Se acceptă parțial Prevederile lit.e) și f) au fost ajustate pentru claritate.

„Paymaster” SRL	47	La pct. 9 lit. e) și lit. f) din proiect, propunem excluderea acestor condiții de stabilire a poziției geografice întrucât acestea pot fi relizate doar prin stabilirea adresei IP or, IP-adresa nu reprezintă o informație veridică privind poziția geografică a persoanei la momentul identificării.	Se acceptă parțial Prevederile lit.e) și f) au fost ajustate pentru claritate.
„Qivi-M” SRL	48	Nu este clar de unde și cum se vor obține listele de de elemente de identificare compromise sau furate? Aceste liste vor fi disponibile pentru accesare din surse externe sau entitatea va trebui să le întocmească individual? Scenariile de fraudă, sunt diverse și diferă în dependență de regiune și alți factori și nu sunt publicate sau deținute centralizat, prin urmare cum se va executa și ce indicatori se vor considera acceptabili și care nu ? Registrul de utilizare normală și anormală a dispozitivului de acces sau a programului informatic – ce presupune “normal” și „anormal”, mai ales dacă se utilizează în calitate de dispozitiv telefonul mobil? – sunt utilizați termeni și parametri care nu pot fi aplicabili. De asemenea, cum va fi posibil de monitorizat acești parametri dacă soluția va fi elaborată de companii străine cum ar fi Onfido, Regula, IDNow etc, care oferă servicii pentru societăți de plată din UE și respectă cerințele UE de e-KYC (care nu prevăd astfel de cerințe cum sunt specificate în pct. 9 din proiectul de Regulament). În ceea ce privește poziția geografică cu risc ridicată sau neobișnuită urmează să fie stabilită de către prestator ca criteriu de	Se acceptă parțial Textul prevederilor a fost modificat. Entitatea se bazează pe informații veridice furnizate de către autoritățile competente sau utilizând cele mai bune practici cunoscute și standarde internaționale, inclusiv din practica proprie, pentru identificarea elementelor compromise sau furate.

			combateră a fraudelor și spălării banilor și aplicată la monitorizarea tranzacțiilor și activității clientului și nu se poate referi exact la înregistrarea clientului. Se propune a exclude pct. 9 ca urmare a faptului că cerințele stipulate nu sunt argumentate și nu este clar modul în care entitatea le va putea respecta.	
	Asociația băncilor din Moldova	49	- se propune a fi completat cu o literă nouă: „cazurile de furt, uzurpare a identității sau prelucrarea ilegală a datelor identificate”. Propunerea are scopul de a determina obiectivul de a urmări cazurile de prelucrare neconformă a datelor.	Se acceptă

		50	- lit.e) și f), Nu este clar ce se are în vedere prin: - poziția geografică anormală/neobișnuită a persoanei; - poziția geografică cu risc ridicat a persoanei. Se impune claritate privind “poziția geografică cu risc ridicat”. De asemenea, considerăm necesar a se clarifica dacă trebuie luate în vedere jurisdicțiile cu risc sporit, sau/și cele cu risc mediu, precum și lista jurisdicțiilor ce nu implementează standarde internaționale de transparență sau/și lista jurisdicțiilor cu risc sporit publicate pe site-ul SPCSB. Adicional, considerăm oportun a se face trimitere și la lista statelor care asigură un nivel adecvat de protecție a datelor, conform prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal. Pentru o interpretare corectă a normelor, se propune detalierea acestora.	Se acceptă parțial Prevederile lit.e) și f) au fost ajustate pentru claritate.
--	--	----	--	--

Pct. 10 : (v2 – pct.10) Entitatea raportoare va stabili în politicile și procedurile interne măsuri de remediere în cazul în care s-a materializat un risc sau în cazul în care au fost identificate erori care au un impact asupra eficacității soluției. Aceste măsuri vor include cel puțin: a) o revizuire a tuturor relațiilor de afaceri afectate, pentru a evalua dacă entitatea a aplicat suficient măsurile de precauție față de clienți; prioritate fiind acordată relațiilor cu grad de risc sporit de spălare a banilor și finanțare a terorismului;	SPCSB	51	La pct. 10, reieșind din faptul că politicile și procedurile interne ale entității raportoare trebuie să prevadă măsuri de identificare, evaluare, gestionare și diminuare a potențialelor riscuri de spălare a banilor și de finanțare a terorismului, dar nu de remediere a riscurilor deja materializate, se propune excluderea sintagmei „în cazul în care s-a materializat un risc sau”, or în cazul „materializării riscului” măsurile descrise la pct. 10 din proiect sunt discordante obligațiilor impuse de art. 11 coroborat cu art. 33 din Legea nr. 308/2017.	Se acceptă
b) luând în considerare informațiile obținute în cadrul revizuirii menționate mai sus, o evaluare a faptului	„QIWI-M” SRL	52	Pct. 10 lit. b) :Reieșind din practica internațională, inclusiv conform Ghidului EBA/GL/2022/15, entitatea poate, dar nu este obligată, să aplice limite doar privind volumul tranzacțiilor, cum este prevăzut în proiectul de Regulament. Astfel se propune reformularea cerinței date în modul în care entitatea să aibă dreptul să stabilească diferite tipuri de restricții, inclusiv limite cu privire la volumul tranzacțiilor, accesul la serviciile de plată, etc. până la efectuarea unei revizuri.	Comentariu: Entitatea raportoare nu are obligația de a aplica elementele de menționate la lit.b) decât doar dacă constată această necesitate. Mai mult decât atât, entitatea raportoare are discreția de a determina care anume element din cele enumerate să-l aplice sau combinația acestora.

dacă o relație de afaceri afectată ar trebui să fie: - supusă unor măsuri sporite de precauție; - supusă unor stabiliri de limite privind volumul tranzacțiilor, până în momentul în care a avut loc o revizuire; - încheiată; - raportată către Serviciul Prevenirea și Combaterea Spălării Banilor; - reclassificată într-o categorie de risc diferită.	B.C. MAIB S.A.	53	La pct. 10 lit. a), se propune înlocuirea cuvântului „suficient” cu cuvântul „corespunzător”, iar cu referire la pct. b), observăm că, primul și ultimul subpunct reprezintă acțiuni interdependente reieșind din faptul că realizarea uneia determină și impune realizarea celeilalte, fiind oportună expunerea acestor prevederi la un singur subpunct. Cât privește penultimul subpunct, având în vedere că autorul indică evaluarea realizării unor acțiuni față de o relație de afaceri existentă și nu o activitate sau tranzacție, se propune excluderea respectivului subpunct.	Se acceptă parțial Textul prevederii a fost modificat. De asemenea, menționăm că cerința de identificare și raportare a activității/tranzacțiilor suspecte este corespunzătoare prevederilor Legii nr.308/2017.
		54	La pct.10 lit.a) din Regulament, propunem ca sintagma „relațiilor cu grad de risc sporit” să fie înlocuită cu sintagma „clienților cu grad de risc sporit”, deoarece anumit nivel sau grad de risc se atribuie clientului, nu relației de afaceri.	Se acceptă
		55	La pct.10 lit.b) din Regulament, a doua liniuță, propunem ca sintagma „unor stabiliri de limite” să fie înlocuită cu sintagma „stabilirii unor limite”.	Se acceptă
		56	Totodată, considerăm necesară excluderea din pct.10 lit.b), a doua liniuță, a sintagmei „, până în momentul în care a avut loc o revizuire”, deoarece stabilirea unor limite poate avea loc doar pentru viitor și nu retroactiv (până la revizuire). În caz dacă această sintagmă are o altă semnificație, pentru a oferi o claritate rugăm modificarea /concretizarea textului.	Se acceptă

		57	La pct.10 lit.b) din Regulament, a treia liniuță, cuvântul „încheiată” propunem să fie înlocuit cu cuvântul „încetată”.	Se acceptă.
		58	La pct.10 lit.b) din Regulament, ultima liniuță, propunem ca sintagma „categorie de risc diferită” să fie înlocuită cu sintagma „altă categorie de risc”.	Se acceptă
	Asociația băncilor din Moldova	59	Din redacția actuală, nu este clar dacă măsurile de remediere descrise ulterior trebuie aplicate oricărui risc identificat, fără a aplica abordarea bazată pe risc, sau în cazul în care riscul identificat are impact asupra funcționalității soluției. Se propune clarificarea dacă măsurile de remediere necesare de aplicat se referă la oricare risc identificat care are un impact asupra eficacității soluției.	Comentariu: Entitatea raportoare va stabili în politicile și procedurile interne măsuri de remediere în cazul în care au fost identificate erori care au un impact asupra eficacității soluției.

Pct. 11: (v2 – pct.11) Entitatea raportoare va lua în considerare modalitatea cea mai eficientă de a monitoriza adecvarea și fiabilitatea continuă a soluției de identificare la distanță a clienților. În acest scop, aceasta va lua în considerare unul sau mai multe dintre următoarele mijloace, dar fără a se limita la acestea: - testarea asigurării calității; - alerte critice automate și notificările; - rapoartele automate regulate de calitate; - testarea eșantionului; - recenziile manuale ale experților din industrie și autorităților de supraveghere .	A.P. „Camera de Comerț Americană din Moldova”	60	Urmează a fi clarificată periodicitatea solicitării recenziilor de către entitatea raportoare și dacă se poate prezuma că recenziile inițiale sunt actuale pentru toată perioada folosirii soluției în cazul în care nu sunt raportate probleme a soluției. În temeiul celor menționate se propune următoarea redacție: „ - recenziile manuale ale experților din industrie și autorităților de supraveghere, la nivel național sau internațional, cu excepția experților sau autorităților de supraveghere din țări/regiuni cu grad de risc sporit în domeniul combaterii spălării banilor și finanțării terorismului”.	Entitatea va determina individual periodicitatea solicitării recenziilor, astfel încât să se asigure despre fiabilitatea continuă a soluției. Se acceptă
---	--	-----------	--	--

Banca Comercială Română Chișinău S.A.	61	Privitor la pct. 11, liniuța 1-5, având în vedere că BNM a impus anumite cerințe exacte, solicităm să fie furnizate clarificări detaliate privitor la modul de aplicare, așteptările cum aceste cerințe sa fie aplicate de banca, prin exemplificare.	Comentariu: Entitatea raportoare își va stabili în politicile interne cerințe pentru monitoriza fiabilității soluției informatice utilizate pentru stabilirea relației de afaceri la distanță cu clienții săi. Apoi, cu o anumită regularitate, va efectua diferite teste pentru asigurarea fiabilității soluției și a capacității acesteia de a gestiona diferite riscuri asociate stabilirii relației de afaceri la distanță.
B.C. MAIB S.A.	62	La pct.11 lit.c) din Regulament, a doua liniuță, necesită a fi definită noțiunea „alerte critice”, utilizată în textul Regulamentului.	Nu se acceptă Fiecare soluție informatică se caracterizează prin configurarea parametrilor IT necesari unei bune funcționări, dar și monitorizări a eficienței de lucru a acesteia. Respectiv, pentru ca utilizatorii să poate utiliza rezultatele de eficiență a lucrului soluției sunt încorporate diferite mecanisme în acest scop (loguri, notificări, alerte etc). Astfel, pentru ca entitatea să se asigure despre lucrul eficient al soluției, urmează să stabilească elementele caracteristice pentru determinarea acestui fapt, iar

			alertele și notificările fiind parte a acestui proces.
„Paymaster” SRL	63	Pct. 11 din proiect propunem să fie exclus pentru că nu este clar sensul punctului dat mai ales în contextul în care pentru monitorizarea soluției sunt deja stabilite cerințe clare expuse la pc. 8-10.	Nu se acceptă Punctul dat are ca scop ca entitatea raportoare să monitorizeze adecvarea și fiabilitatea continuă a soluției informatice implementate.
„Qiw-M” SRL	64	Liniuța 4: Nu este clar care ar trebui să fie eșantionul supus testării. Propunem reformularea sintagmei în „testarea eșantioanelor” pentru corespunde scopului în sine a unei astfel de testări și a permite entității să stabilească criteriile de selectare a eșantioanelor pentru testare.	Comentariu: Entitatea raportoare va stabili individual eșantionul supus testării, în funcție de condițiile proprii în activitate și riscurile identificate sau potențiale care ar putea influența fiabilitatea soluției informatice.

		Este necesar de menționat că orice recenzie este subiectivă, nu se cunoaște care sunt experții din industrie (în mod special din RM) și nu este rezonabil de a fi aplicată în cazul utilizării soluțiilor dezvoltate și oferite de companii renumite specializate în domeniul de identificare la distanță, inclusiv care oferă soluții tehnice entităților din UE în conformitate cu cerințele UE. Luând în considerare că expunerea este una interpretabilă și nu aduce un cadru clar de acțiuni se propune a utiliza formularea din Ghidul EBA – „revizuire manuale”.	Textul prevederii este modificat, conform altor comentarii și propuneri.
Asociația băncilor din Moldova	65	Se identifică următoarele neclarități în aplicarea normei: a) conjuncția ”și” implică necesitatea obținerii ambelor tipuri de recenzii: atât a recenziilor din partea experților, cât și a recenziilor din partea autorităților de supraveghere. Solicităm clarificarea dacă existența recenziei doar din partea autorității de supraveghere ar fi suficientă, fără a fi necesară și o recenzie a experților din industrie;	Se acceptă
	66	b) dacă sunt acceptabile și recenziile autorităților de supraveghere din alte jurisdicții care implementează standarde similare de prevenire a spălării banilor și finanțării terorismului. Se propune detalierea normei, luând în considerare neclaritățile menționate.	Se acceptă

Pct. 12 : (v2 – pct.12) Entitatea raportoare va efectua identificarea și verificarea identității clientului prin mijloace electronice, în privința: a) potențialilor clienți noi cu care entitatea intenționează să stabilească relații de afaceri; b) clienților existenți, care fac obiectul procedurilor de revizuire și actualizare a informațiilor.	Asociația Businessului European	67	La pct. 12, lit. b) după cuvântul „revizuire” se propune a fi substituit cu cuvântul „identificare”. Ținem să precizăm că revizuirea și actualizarea datelor din punct de vedere a semnății etimologice au unul și același sens asupra datelor, pe când propunerea pe care o înaintăm de a indica în loc de cuvântul revizuirea cuvântul identificarea, are scopul de a putea utiliza identificarea la distanță în raport cu clienții deja existenți, atunci când se solicită modificarea unor servicii sau reclamarea unor eventuale neconformități în legătură cu serviciile financiar bancare, sau solicitarea de a dezvălui datele confidențiale (bancare). La pct. 12 lit. b) după cuvântul „persoana” se completează cu cuvintele: „fizică (administrator/reprezentant) în raport cu persoana”. A se menționa că procedura de identificare al distanță, așa cum prevede art. 51 alin. (1) din Legea nr. 308/2017, se referă exclusiv la persoana fizică. Deci, chiar și în cazul identificării persoanei juridice, în mod practic se va identifica administratorul sau reprezentantul mandatat al persoanei juridice.	Se acceptă Lit.b) de la pct. 12 nu conține cuvântul „persoana”.
---	--	-----------	---	---

B.C. „ProCredit Bank” S.A.	68	Cu referire la punctul 12 din capitolul III, propunem să faceți diferență între potențiali clienți noi și clienții existenți, și anume, pentru clienții existenți, entitatea raportoare să aibă posibilitatea să utilizeze canalele proprii de identificare clienți, fără a fi utilizată identificarea video sau captarea imaginii faciale a clientului. Băncile comerciale pot utiliza sistemele de auto deservire la distanță pentru actualizarea datelor clienților, unde clienții existenți au credențiale și sunt autentificați de către băncile comerciale, atât la accesarea acestor sisteme, cât și la confirmarea operațiunilor efectuate prin intermediul lor. Actualizarea datelor clienților existenți este un tip de operațiune efectuată de către clienți în sistemele de auto deservire la distanță.	Comentariu: Entitatea raportoare va stabili individual canalele electronice utilizate pentru actualizarea informațiilor/datelor despre clienții săi. Prevederile regulamentului acordă o posibilitate în plus (de actualizare a datelor) de utilizare a mijloacelor electronice implementate pentru un alt scop (stabilirea relației de afaceri la distanță).
B. C. MAIB S.A.	69	La pct.12 lit. a) din Regulament, propunem înlocuirea cuvântului „stabilească” cu cuvântul „inițieze”.	Se acceptă

Asociația băncilor din Moldova	70	Se impune o delimitare a metodelor electronice de identificare a potențialilor clienți de cele de identificare a clienților existenți, prin aplicarea măsurilor mai simplificate de identificare în contextul actualizării datelor, cu autentificare/confirmarea prin Token, conform procedurii standard utilizate la moment pentru efectuarea tranzacțiilor, prin intermediul sistemului de deservire la distanță. Pentru clienții existenți, se impune a specifica că entitatea raportoare să aibă posibilitatea să utilizeze canalele proprii de identificare clienți, fără a fi utilizată identificarea video sau captarea imaginii faciale a clientului. Băncile pot utiliza sistemele de auto deservire la distanță pentru actualizarea datelor clienților, unde clienții existenți au credențiale și sunt autentificați de către băncile comerciale, atât la accesarea acestor sisteme, cât și la confirmarea operațiunilor efectuate prin intermediul lor. Actualizarea datelor clienților existenți este un tip de operațiune efectuată de către clienți în sistemele de auto deservire la distanță. La lit. b) după cuvântul „revizuire” se propune a fi substituit cu cuvântul „identificare”. Precizăm că revizuirea și actualizarea datelor din punct de vedere a semnății etimologice au unul și același sens asupra datelor, pe când propunerea pe care o înaintăm de a indica în loc de cuvântul revizuirea cuvântul identificarea, are scopul de a putea utiliza identificarea la distanță în raport cu clienții deja existenți, atunci când se solicită modificarea unor servicii sau reclamarea unor eventuale neconformități în legătură cu serviciile financiar bancare, sau solicitarea de a dezvălui datele confidențiale (bancare). lit. b) , după cuvântul „persoana” se completează cu cuvintele: „fizică (administrator/reprezentant) în raport cu persoana”. A se menționa că procedura de identificare la distanță, așa cum prevede art. 51 alin.	Comentariu: Entitatea raportoare va stabili individual canalele electronice utilizate pentru actualizarea informațiilor/datelor despre clienții săi. Prevederile regulamentului acordă o posibilitate în plus (de actualizare a datelor) de utilizare a mijloacelor electronice implementate pentru un alt scop (stabilirea relației de afaceri la distanță). Se acceptă Lit.b) de la pct.12 nu conține cuvântul „persoana”.
--------------------------------	----	--	--

		(1) din Legea nr. 308/2017, se referă exclusiv la persoana fizică. Deci, chiar și în cazul identificării persoanei juridice, în mod practic se va identifica administratorul sau reprezentantul mandatat al persoanei juridice.	
--	--	--	--

Pct. 13: (v2 – pct.13) Entitatea raportoare va efectua identificarea și verificarea clienților prin mijloace electronice, în raport cu: a) persoana fizică, cetățean al Republicii Moldova; b) persoana juridică rezidentă, ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai Republicii Moldova.	„Nova Pay” SRL	71	La pct. 13, lit. a) se propune includerea sintagmei ”Rezidenți ai Republicii Moldova”, la lit. b) se propune excluderea sintagmei ”ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai Republicii Moldova”. În temeiul celor menționate se propune următoarea redacție a pct. 13: 13.Entitatea raportoare va efectua identificarea și verificarea clienților prin mijloace electronice, în raport cu: a) persoana fizică, cetățean al Republicii Moldova, rezident al Republicii Moldova; b) persoana juridică rezidentă.	Nu se acceptă Punctul dat transpune limbajul prevederilor Legii nr.308/2017 (art.5 ¹ alin.1)).
	„Paymaster” SRL	72	La pct. 13 din proiect, propunem includerea și a persoanelor rezidente cu cetățenie străină care să fie aplicabil atât pentru persoanele fizice cât și pentru reprezentanți, fondatori, administratori și beneficiari efectivi ai persoanelor juridice.	Nu se acceptă Punctul dat transpune limbajul prevederilor Legii nr.308/2017 (art.5 ¹ alin.1)).
	B.C. MAIB S.A.	73	La pct.13 din Regulament, propunem ca sintagma „identificarea și verificarea clienților” să fie înlocuită cu sintagma „identificarea și verificarea identității clienților”.	Se acceptă
		74	La pct.13 lit.a) din Regulament, propunem completarea cu regulile privind statutul de rezident fiscal și/sau rezident valutar al cetățeanului RM.	Nu se acceptă Punctul dat transpune limbajul prevederilor Legii nr.308/2017 (art.5 ¹ alin.1)), și respectiv nu poate fi modificat. Totuși, cu referire la tipul rezidenței, prevederile legii nu face distincție.

Pct. 14 : (v2 – pct.14) Entitatea raportoare se va asigura că soluția de identificare la distanță a clienților are elemente pentru a colecta: a) toate datele și documentele relevante pentru identificarea și verificarea persoanei fizice și/sau juridice; b) toate datele și documentele relevante pentru a verifica dacă persoana fizică care acționează în numele persoanei juridice are dreptul legal de a acționa astfel; c) informațiile privind beneficiarii reali; d) toate datele și documentele relevante pentru determinarea naturii și scopului relației de afaceri	SPCSB	75	La pct. 14, inclusiv pe textul proiectului (pct. 5, 11 etc.), se propune asigurarea unității de terminologie, or sunt utilizate diferite formulări „soluție informatică pentru identificare la distanță”; „soluție de identificare la distanță a clienților”, astfel că urmează a fi utilizată abrevierea de la pct. 4, unde autorul a explicat semnificația noțiunii de „soluție informatică pentru identificare la distanță”, iar între paranteze a indicat utilizarea ulterioară în textul actului normativ, a noțiunii corespondente de „soluție”.	Se acceptă
		76	Cu referire la același punct 14 lit. c), se propune aducerea în concordanță cu prevederile art. 5 alin. (2) lit. b) din Legea nr. 308/2017, inclusiv în vederea înlocuirii sintagmei „beneficiarii reali” cu noțiunea utilizată de legiuitor la art. 52 din Legea nr. 308/2017, cea de „beneficiar efectiv”, astfel că, prevederea să fie expusă în următoarea redacție „toate datele și documentele relevante pentru identificarea și verificarea identității beneficiarului efectiv”.	Se acceptă
	A.P. „Camera de Comerț Americană din Moldova”	77	La pct. 14 lit. c) din proiect se propune substituirea termenului „reali” cu „efectivi” în vederea uniformizării cu prevederile Legii nr. 308/2017.	Se acceptă
	OCN Microinvest SRL	78	Se propune la pct. 14 lit. c) din Regulament de substitui termenul “reali” cu noțiunea „efectivi” în vederea uniformizării cu prevederile Legii 308/2017.	Se acceptă.

BC Energbank S.A.	79	La pct. 14 lit c) "Entitatea raportoare se va asigura că soluția de identificare la distanță a clienților are elemente pentru a colecta informațiile privind beneficiarii reali", se utilizează expresia "beneficiarii reali", care nu este definită în Legea 308/2017 precum și în Regulamentul BNM 200/2018, astfel considerăm că trebuie să fie înlocuită expresia dată cu cea de "beneficiari efectivi" sau trebuie să fie clar definit în pct. 4 a Regulamentului.	Se acceptă
B.C. MAIB S.A.	80	La pct.14 lit.a) din Regulament, propunem ca sintagma „identificarea și verificarea persoanei fizice” să fie înlocuită cu sintagma „identificarea și verificarea identității persoanei fizice”. De asemenea, considerăm necesară completarea pct.14 lit.a) cu trimiterea la cerințele prevăzute la pct. 26, subpctele 1) și 2) din Regulamentul BNM nr.200/2018. La pct.14 lit.c) din Regulament, propunem ca sintagma „beneficiarii reali” să fie înlocuită cu sintagma „beneficiarii efectivi”. La pct.14 lit.d) din Regulament, propunem ca sintagma „naturii și scopului” să fie înlocuită cu sintagma „scopului și naturii dorite a”.	Se acceptă parțial Referința la prevederile Regulamentului nr.200/2018 se regăsește în pct.2.
Asociația Businessului European	81	Pct. 14 lit. d): Propunem a fi exclusă, deoarece depășește obiectul de reglementare a actului normativ, or, proiectul regulamentului se referă la cerințe față de identificarea și verificarea clienților prin intermediul mijloacelor electronice.	Nu se acceptă Soluția informatică implementată de către entitate în scopul stabilirii relației de afaceri cu clientul nu trebuie să periclitaze procesul de acumulare a informației și datelor de bază despre persoana fizică/juridică care sunt prevăzute de PCSBFT (art.2 alin.a)-d) din Legea nr.308/2017).

„Paymaster” SRL	82	La pct. 14 lit. c) din proiect, comunicăm că entitatea raportoare, în momentul identificării, nu poate să aplice și să stabilească norme suplimentare care să aibă drept scop stabilirea a beneficiarului efectiv prin alte metode decât prin declararea acestui fapt de către utilizator. Or, beneficiarul efectiv poate fi stabilit după monitorizarea activității pe cont și aplicarea măsurilor corespunzătoare stabilite de legislație.	Comentariu: Soluția informatică implementată de către entitate în scopul stabilirii relației de afaceri cu clientul nu trebuie să pericliteze procesul de acumulare a informației și datelor de bază despre persoana fizică/juridică care sunt prevăzute de cerințele de PCSBFT (art.2 alin. a)-d) din Legea nr.308/2017).
	83	La pct. 14 lit. d) din proiect, propunem excludere cuvântului „documente”. Documentele despre relația de afaceri există după ce are loc o activitate pe cont or, solicitarea de documente care pot fi prezentate la identificare fără ca însăși contul să fie deschis o considerăm excesivă.	
Asociația băncilor din Moldova	84	lit. c) se propune substituirea termenului „beneficiari reali” cu cuvântul „beneficiari efectivi”. În Legea nr.308/2017 se utilizează noțiunea de „beneficiar efectiv”.	Se acceptă
	85	lit. d) se propune a fi exclusă, deoarece depășește obiectul de reglementare a actului normativ, or, proiectul regulamentului se referă la cerințe față de identificarea și verificarea clienților prin intermediul mijloacelor electronice.	Nu se acceptă Soluția informatică implementată de către entitate în scopul stabilirii relației de afaceri cu clientul nu trebuie să pericliteze procesul de acumulare a informației și datelor de bază despre persoana fizică/juridică care sunt prevăzute de PCSBFT (art.2 alin. a)-d) din Legea nr.308/2017).

Pct. 15: (v2 – exclus) Entitatea raportoare realizează identificarea și verificarea identității clienților, în baza unei evaluări corespunzătoare a riscurilor, și prin utilizarea uneia sau a mai multor metode, în funcție de risc: a) prin mijloace de identificare electronică cu un nivel de securitate suficient și conform cu standardele stabilite în Legea nr.124/2022; b) prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului; c) prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022.	A.P. „Camera de Comerț Americană din Moldova”	86	Pct. 15, lit. b), urmează a fi clarificat dacă expresia „...în direct a înregistrării video și audio sau a fotografiei...” se interpretează în sensul asigurării transmiterii cumulative în direct a înregistrării și video și audio iar în cazul lipsei înregistrării audio, se asigură transmiterea cumulativă în direct a înregistrării video, a fotografiei cu elemente de verificare, etc. În sensul prezentului punct, înregistrarea originalului actului de identitate urmează a fi subînțeles inclusiv în sensul captării documentelor de identitate în color și la o calitate adecvată pentru a permite extragerea datelor.	Comentariu: Prevederea dată din Regulament transpune limbajul prevederilor Legii nr.308/2017 (art.5¹ alin.2)). În înțelegerea autorității de supraveghere, acest punct evidențiază două direcție de stabilire a relației de afaceri la distanță cu clienții: 1. prin utilizarea mijloacelor electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio, înregistrarea originalului actului de identitate în timpul transmiterii și captarea imaginii faciale a clientului și 2. prin utilizarea mijloacelor electronice care asigură cumulativ transmiterea în direct a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii și captarea imaginii faciale a clientului. Fiecare dintre metoda utilizată are în vedere 3 elemente constitutive: identificarea propriu-zisă utilizând mijloacele electronice, înregistrarea actului de identitate și captarea imaginii clientului. Ultimele două elemente având rol de verificare a identității clientului. Combinarea metodelor utilizată rămâne la discreția entității raportoare, cu condiția de asigurare obligatorie a
--	--	-----------	--	--

				elementelor: i) de identificare a clientului și ii) de verificare a identității clientului.
	BC Comerțbank S.A.	87	urmează a fi clarificat dacă expresia „...în direct a înregistrării video și audio sau a fotografiei...” se interpretează în sensul asigurării transmiterii cumulative în direct a înregistrării și video și audio iar în cazul lipsei înregistrării audio, se asigură transmiterea cumulativă în direct a înregistrării video, a fotografiei cu elemente de verificare, etc. În temeiul celor menționate se propune următoarea redacție a pct. 15, lit. b): „b) prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului. În sensul prezentei litere, mijloacele electronice de identificare vor asigura transmiterea cumulativă în direct <u>fie</u> a înregistrării video și audio cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului, <u>fie</u> transmiterea cumulativă în direct a înregistrării video și a fotografiei cu elementele de verificare a prezenței fizice, înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului”.	A se vedea comentariul de la pct. 86 din tabelul de sinteză.

			În sensul prezentului punct, înregistrarea originalului actului de identitate urmează a fi subînțeles inclusiv în sensul captării documentelor de identitate în color și la o calitate adecvată pentru a permite extragerea datelor utilizând tehnici OCR (Optical Character Recognition).	
	„Qivi-M” SRL	88	Considerăm că prevederea pct. 15 lit. b) limitează entitatea în utilizarea unor anumite soluții fără a oferi posibilitatea de a utiliza tehnologii noi, altele decât acele specificate în proiectul Regulamentului. Se propune a reda Lit. b) pct. 15 în următoarea redacție: „prin mijloace electronice care asigură unul sau mai multe funcționalități: a) transmiterea în direct a înregistrării video și audio și captarea imaginii faciale a clientului, sau b) efectuarea pozelor clientului cu elementele de verificare a prezenței fizice, sau c) înregistrarea originalului actului de identitate în timpul înregistrării video sau efectuării pozei, sau d) verificarea identității clientului din surse sigure și credibile”.	A se vedea comentariul de la pct. 86 din tabelul de sinteză.

Pct. 16: (v2 – pct.15) Indiferent de metoda aplicată, trebuie să fie asigurată colectarea și prezentarea de către client, cel puțin, a informațiilor care de obicei se solicită și sunt aplicabile clienților identificați cu prezență fizică. Modalitatea de colectare a informației va fi determinată de entitatea raportoare, dar urmează să definească care informație va fi colectată: a) manual; b) automat din documentele prezentate de către client; c) din alte surse interne sau externe.	SPCSB		La pct. 16, se propune excluderea sintagmei „și sunt aplicabile”, care nu se încadrează din punct de vedere semantic în construcția enunțului de expunere a normei juridice.	Se acceptă
	B.C. MAIB S.A.	89	La pct. 16 din Regulament, considerăm necesară completarea cu norme care să prevadă colectarea și prezentarea de către client, cel puțin, a informațiilor care de obicei se solicită și sunt aplicabile clienților identificați cu prezență fizică, prevăzute la pct.26 și pct.27 din Regulamentul BNM nr.200/2018. De asemenea, la pct.16 lit.a) din Regulament, considerăm necesară concretizarea termenului „manual” – dacă se are în vedere informația introdusă manual de către client în câmpurile destinate completării, sau informația introdusă manual de către un angajat al băncii în baza actelor clientului, sau o altă opțiune.	Referința la prevederile Regulamentului nr.200/2018 se regăsește în pct.2. Se acceptă

	„Qiwi-M” SRL	90	Pct. 16 lit. a): În înțelegerea noastră, prin „colectarea informației manual” se are în vedere introducerea manuală a informației de către client. Pentru a evita o interpretare eronată a prevederii și luând în considerare formularea din Ghidul EBA , propunem de substituit sintagma “manual” cu sintagma „introduse manual de către client”.	Se acceptă
	Asociația băncilor din Moldova	91	Nu este clar cum va fi aplicată cerința privind certificarea documentelor de către clienți conform art.5 alin.(5) din Legea nr.308/2017: „Corectitudinea și veridicitatea documentelor prezentate, inclusiv a documentelor prezentate prin mijloace electronice, sunt certificate de către clienți în mod obligatoriu.” Se propune de completat regulamentul cu prevederi/ concretizări privind modul de certificare a documentelor de către clienți.	Certificarea documentelor se face automat prin finalizarea procesului de identificare și verificare a identității persoanei.
Pct. 17: (v2 – pct.16) Entitatea raportoare va pune în aplicare și va menține mecanisme adecvate pentru a se asigura că informațiile pe care le captează automat, în conformitate cu punctul 14, sunt fiabile. Aceasta trebuie să aplice controale (cel puțin anuale) pentru a aborda riscurile asociate acestui proces, inclusiv de ascundere a locației	A.P. „Camera de Comerț Americană din Moldova”	92	Este necesar de a menționa acțiunile ce urmează a fi întreprinse aferent rapoartelor de locație a IP-urilor adresate.	Rapoartele de locație pot fi utilizate ca un factor suplimentar de risc, la stabilirea de către entitate a gradului de risc asociat clientului și, în consecință, a măsurilor de precauție sporită pe care urmează să le aplice.
	Asociația băncilor din Moldova	93	Cuvântul „automat” se propune a fi substituit cu cuvintele „în format electronic”. Menționăm că captarea nu se va realiza automat – declanșarea procesului nu se va realiza fără intervenția umană, astfel, esența valorilor reglementate se referă la procesul de prelucrare electronic al datelor. Totodată menționăm că sintagma „, inclusiv de ascundere a locației adreselor de Protocol Internet (IP), utilizarea serviciilor de tipul rețelelor virtuale	Se acceptă parțial Entitatea își va stabili mecanisme pentru a fi capabilă să determine locația adreselor IP utilizate , inclusiv a celor de tipul rețelelor virtuale, de client pentru a stabili relația de afaceri și, ulterior, pentru efectuarea operațiunilor/tranzacțiilor prin

adreselor de Protocol Internet (IP), utilizarea serviciilor de tipul rețelelor virtuale private (VPN-uri).			private (VPN-uri).” nu este clară, or, norma vizată nu determină acțiunea concretă pe care trebuie să o întreprindă entitatea raportoare în legătură cu serviciile VPN sau mascarea adresei IP – procese tehnologice care nu pot fi blocate/identificate de către entitatea raportoare. În cele din urmă, pentru a da o previzibilitate normei, fie vor fi descrise cerințe certe fie sintagma va fi exclusă din text.	intermediul entității astfel încât să poată determina adecvat riscul de SBFT asociat relației de afaceri.
	Asociația Businessului European	94	La pct. 17 cuvântul „automat” se propune a fi substituit cu cuvintele „în format electronic”. Menționăm că captarea nu se va realiza automat – declanșarea procesului nu se va realiza fără intervenția umană, astfel, esența valorilor reglementate se referă la procesul de prelucrare electronic al datelor. La pct. 17 sintagma „inclusiv de ascundere a locației adreselor de Protocol Internet (IP), utilizarea serviciilor de tipul rețelelor virtuale private (VPN-uri).”. Nu este clară, or, norma vizată nu determină acțiunea concretă pe care trebuie să o întreprindă entitatea raportoare în legătură cu serviciile VPN sau mascarea adresei IP – procese tehnologice care nu pot fi blocate/identificate de către entitatea raportoare. În cele din urmă, pentru a da o previzibilitate normei, fie vor fi descrise cerințe certe fie sintagma va fi exclusă din text.	Se acceptă parțial Entitatea își va stabili mecanisme pentru a fi capabilă să determine locația adreselor IP utilizate , inclusiv a celor de tipul rețelelor virtuale, de client pentru a stabili relația de afaceri și, ulterior, pentru efectuarea operațiunilor/tranzacțiilor prin intermediul entității astfel încât să poată determina adecvat riscul de SBFT asociat relației de afaceri.
	„Paymaster” SRL	95	La pct. 17 din proiect, propunem excluderea cerinței inclusiv de ascundere a locației adreselor de Protocol Internet (IP), utilizarea serviciilor de tipul rețelelor virtuale private (VPN-uri).	Nu se acceptă Entitatea își va stabili mecanisme pentru a fi capabilă să determine locația adreselor IP utilizate , inclusiv a celor de tipul rețelelor virtuale, de client pentru stabili relația de afaceri, și, ulterior, pentru efectuarea

				operațiunilor/tranzacțiilor prin intermediul entității astfel încât să poată determina adecvat riscul de SBFT asociat relației de afaceri.
	„QIWI-M” SRL	96	Reieșind din considerentul că prevederea din pct. 14 nu se referă la modalitatea de colectarea a informației, inclusiv captarea automată a informației, se propune a substitui sintagma „în conformitate cu punctul 14” cu sintagma „în conformitate cu punctul 16”	Nu se acceptă Pct. 14 descrie informația/datele pe care entitatea are obligația să le obțină în procesul de cunoaștere a clientului său.
	Ministerul Justiției	97	Cu referire la pct. 17, considerăm oportună excluderea cuvântului „adecvate”, deoarece asemenea formulă nu poate fi evaluată cantitativ și calitativ și nu oferă forță juridică sau o anumită conduită prestabilită pentru subiecții vizați (obiecție valabilă și pentru pct. 20, urmînd a fi excluse cuvintele „clară și neechivocă”).	Se acceptă
Pct. 18 : (v2 – pct.17) În cazul clientului persoană juridică, măsurile de identificare se vor aplica persoanei fizice cu mandat de reprezentat legal al acesteia, având în vedere documentele de înregistrare corespunzătoare a persoanei juridice. În aceste condiții, pentru persoana fizică, entitatea raportoare va aplica procesul de identificare la distanță similar unei	B.C. „ProCredit Bank” S.A.	98	Conform punctului 18 „În cazul clientului persoană juridică, măsurile de identificare se vor aplica persoanei fizice cu mandat de reprezentat legal al acesteia, [...]. În aceste condiții, pentru persoana fizică, entitatea raportoare va aplica procesul de identificare la distanță similar unei persoane fizice. [...]”. Totodată, în conformitate cu pct.26 din Regulamentul cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea băncilor, la identificarea persoanei fizice banca obține informații, printre care obligatoriu „ [...] f) sursa venitului; g) scopul preconizat de utilizare a contului (numărul și volumul tranzacțiilor, tipul tranzacțiilor, scopul	Comentariu: Prevederile pct.2 din Regulament stabilesc faptul că entitatea urmează să respecte cerințele Regulamentului BNM nr.200/2018, inclusiv a tuturor prevederilor ce țin de aplicarea măsurilor de precauție față de clienți. Procesul de stabilire a relației cu persoana juridică la ghișeul băncii presupune că persoana juridică este reprezentată de o persoană fizică care este împuternicită conform cerințelor legislației, iar aceasta din urmă prezintă toate informațiile/datele necesare pentru identificarea persoanei juridice. Respectiv, aplicarea măsurilor de

persoane fizice. În același context, vor fi aplicate măsuri pentru asigurarea verificării dacă persoana fizică care acționează în numele persoanei juridice are dreptul legal de a acționa astfel.			și frecvența tranzacțiilor preconizate);[...] h) produsul și serviciul financiar solicitat;”. Având în vedere că aceste informații se referă la relația dintre bancă și client, iar reprezentantul persoanei juridice nu este clientul băncii în sensul că nu deține conturi și nu efectuează tranzacții în nume propriu, rugăm să fie specificat în regulament dacă este obligatorie colectarea acestor date în procesul de identificare de la persoanele fizice care reprezintă entitatea juridică.	precauție față de clientul persoană juridică nu poate fi diferit în cazul procesului de stabilire a relației de afaceri la distanță prin metode electronice.
	B.C. MAIB S.A.	99	La pct.18 din Regulament, a doua propoziție, nu este clară sintagma „pentru persoană <u>fizică</u> , entitate raportoare va aplica procedura de identificare la distanță similar unei persoane <u>fizice</u> ”. Rugăm corectarea erorii prin concretizarea normei respective – dacă în primul caz se are în vedere persoana fizică care reprezintă o persoană juridică. Tot la pct.18 din Regulament, ultima propoziție repetă norma pct.14 lit.b) din Regulament. Propunem excluderea ultimei propoziții din pct.18.	Se acceptă parțial A fost precizată referința la reprezentantul persoanei juridice. Referitor la ultima propoziție, este de menționat că prevederea dată are ca scop stabilirea obligației ca entitatea să se asigure că persoana fizică care acționează în numele persoanei juridice care stabilește relații de afaceri la distanță are dreptul legal de a acționa astfel și nu are ca scop de a dubla prevederile din diferite acte normative referitor la verificarea împuternicirilor persoanei fizice.

	Asociația băncilor din Moldova		Conform punctului 18 „În cazul clientului persoană juridică, măsurile de identificare se vor aplica persoanei fizice cu mandat de reprezentat legal al acesteia, [...]. În aceste condiții, pentru persoana fizică, entitatea raportoare va aplica procesul de identificare la distanță similar unei persoane fizice. [...]”. Totodată, în conformitate cu pct.26 din Regulamentul cu privire la cerințele privind prevenirea și combaterea spălării banilor și finanțării terorismului în activitatea băncilor, la identificarea persoanei fizice banca obține informații, printre care obligatoriu „ [...] f) sursa venitului; g) scopul preconizat de utilizare a contului (numărul și volumul tranzacțiilor, tipul tranzacțiilor, scopul și frecvența tranzacțiilor preconizate);[...] h) produsul și serviciul financiar solicitat;”. Având în vedere că aceste informații se referă la relația dintre bancă și client, iar reprezentantul persoanei juridice nu este clientul băncii în sensul că nu deține conturi și nu efectuează tranzacții în nume propriu, rugăm să fie specificat în regulament dacă este obligatorie colectarea acestor date în procesul de identificare de la persoanele fizice care reprezintă entitatea juridică.	Comentariu: Prevederile pct.2 din Regulament stabilesc faptul că entitatea urmează să respecte cerințele Regulamentului BNM nr.200/2018, inclusiv a tuturor prevederilor ce țin de aplicarea măsurilor de precauție față de clienți. Procesul de stabilire a relației cu persoana juridică la ghișeul băncii presupune că persoana juridică este reprezentată de o persoană fizică care este împuternicită conform cerințelor legislației, iar aceasta din urmă prezintă toate informațiile/datele necesare pentru identificarea persoanei juridice. Respectiv, aplicarea măsurilor de precauție față de clientul persoană juridică nu poate fi diferit în cazul procesului de stabilire a relației de afaceri la distanță prin metode electronice.
Pct. 19: (v2 – exclus) În scopul verificării și validării datelor obținute de la client, entitatea raportoare este în drept să acceseze resursele informaționale și bazele de date disponibile, cu respectarea prevederilor legale din domeniul protecției datelor cu caracter personal.	Asociația Businessului European	100	Pct. 19 propunem a fi exclus, deoarece norma de referință generează un înțeles incert, în special „dreptul” de a accesa bazele de date cu respectarea cerințelor legale din domeniul protecției datelor cu caracter personal. A se menționa că conform Legii nr. 308, accesarea/verificarea datelor din surse veridice nu este un drept dar o obligație. Mai mult, norma de referință din proiect mai mult duce în eroare decât reglementează eventuala coroborare cu înțelesul cerințelor din domeniul protecției datelor cu caracter personal.	Se acceptă

	Asociația băncilor din Moldova	101	Propunem a fi exclus, deoarece norma de referință generează un înțeles incert, în special „dreptul” de a accesa bazele de date cu respectarea cerințelor legale din domeniul protecției datelor cu caracter personal. A se menționa că conform Legii nr. 308, accesarea/verificarea datelor din surse veridice nu este un drept dar o obligație. Mai mult, norma de referință din proiect mai mult duce în eroare decât reglementează eventuala coroborare cu înțelesul cerințelor din domeniul protecției datelor cu caracter personal. 5 Complementar, prevederea menționată în proiect creează confuzii în privința acțiunilor care trebuie întreprinse de bancă pentru ”validarea datelor obținute”, având în vedere că clientul certifică veridicitatea datelor și informațiilor prezentate, iar banca are obligația de a le verifica.	Se acceptă
Pct. 20 : (v2 – pct.19) Identificarea clientului este precedată de exprimarea clară și neechivocă a consimțământului, inclusiv cu privire la înregistrarea video, audio, prelucrarea și păstrarea acestor date.	A.P. „Camera de Comerț Americană din Moldova”	102	se propune substituirea frazei „ <i>inclusiv cu privire la înregistrarea video, audio, prelucrarea și păstrarea acestor date</i> ” cu următoarea frază: „ <i>pentru prelucrarea datelor cu caracter personal în conformitate cu legislația în vigoare</i> ”, ceea ce ar permite includerea tuturor acțiunilor de prelucrare a datelor cu caracter personal în procesul reglementat de prevederile Regulamentului, corelarea noțiunii de consimțământ cu Legea nr. 133/2011 specială în acest domeniu și ar exclude segmentarea consimțământului pe categorii de date și necesitatea obținerii acestuia pe fiecare categorie aparte.	Se acceptă

OCN Microinvest SRL	103	Se propune substituirea frazei “inclusiv cu privire la înregistrarea video, audio, prelucrarea și păstrarea acestor date” din pct. 20 din Regulament cu următoarea fraza: “pentru prelucrarea datelor cu caracter personal în conformitate cu legislația în vigoare”, ceea ce ar permite includerea tuturor acțiunilor de prelucrare a datelor cu caracter personal în procesul reglementat de prevederile Regulamentului, corelarea noțiunii de consimțământ cu Legea nr. 133/2011 specială în acest domeniu și ar exclude segmentarea consimțământului pe categorii de date și necesitatea obținerii acestuia pe fiecare categorie aparte.	Se acceptă
B.C. MAIB S.A.	104	La pct.20 din Regulament, propunem ca sintagma „, inclusiv cu privire la înregistrarea video, audio, prelucrarea și păstrarea acestor date” să fie înlocuită cu sintagma „pentru prelucrarea datelor cu caracter personal în conformitate cu legislația în vigoare aplicabilă”. Propunerea se bazează pe faptul că art.5/1 al Legii nr.308/2017 prevede posibilitatea utilizării altor metode de identificare și verificare a identității clienților prin mijloace electronice, decât prin utilizarea înregistrării video și audio. Totodată, păstrarea datelor cu caracter personal este una dintre modalitățile de prelucrare a acestora. Formularea propusă este una universală, care ar acoperi orice modalitate de prelucrare a datelor cu caracter personal, urmare a aplicării oricărei metode din cele specificate la art.5/1 din Legea nr.308/2017.	Se acceptă

	„Qiwi-M” SRL	105	În conformitate cu prevederile Legii 133/2011 privind protecția datelor cu caracter personal, entitățile colectează datele cu caracter personal ale clienților, inclusiv la efectuarea e-KYC. Entitatea are dreptul de a colecta datele personale ale clientului în scopul respectării Legislației aplicabile în domeniul prevenirii și combaterii spălării banilor fără consimțământul clientului (art. 5 Legea 133/2011), cu obligația de a indica în Politica sa de confidențialitate scopul și categoriile de date colectate. Astfel se propune a exclude pct. 20 fiind în contradicție cu prevederile Legii 133/2011.	Nu se acceptă Cerința de exprimare a consimțământului persoanei pentru prelucrarea datelor cu caracter personal are ca scop implementarea cerințelor Legii 133/2011.
	Asociația băncilor din Moldova	106	Nu este clar dacă în pct.20 și 21 se face referință la unul și același consimțământ sau la două diferite. Suplimentar, nu considerăm oportună includerea obligației de prezentare a Politicii prevenirii spălării banilor – versiunea desfășurată, ținând cont de faptul că atunci când clientul prezintă un interes sporit asupra politicii de control al entității raportoare, reprezintă un criteriu de determinare/identificare a suspiciunilor. În cazul în care este unul și același consimțământ, se propune de utilizat aceeași denumire. De exclus calificativul ”desfășurat” din textul lit.e), pct.21	Se acceptă
Pct. 21: (v2 – pct.20) În cazul identificării clientului prin mijloace electronice, entitatea raportoare va asigura aducerea la cunoștință a clientului termenelor și condițiile în care identificarea electronică a clientului este efectuată.	Banca de Finanțe și Comerț S.A.	107	Politicele descrise în punctul dat sunt publicate de către entitățile raportoare pe paginile oficiale. Nu este clar dacă vizualizarea acestor politici trebuie să fie disponibilă nemijlocit în procesul de identificare sau în mod general să fie disponibilă clientului într-un compartiment de pe pagina oficială a entității raportoare. În cazul dacă includem descrierea politicilor, chiar și succintă, nemijlocit în proces de Ekyc –	Nu se acceptă Volumul extrasului din politicile băncii care se aduc la cunoștință clientului sunt determinate de entitate în mod individual. Dreptul clientului de a fi informat despre entitate, produs, riscuri, etc. înainte de stabilirea relației de afaceri cu entitatea este o parte esențială din programul băncii de interacțiune și informare a clienților.

Termenele și condițiile puse la dispoziția clientului, anterior sau concomitent cu primirea consimțământului pentru efectuarea identificării electronice a clientului, vor fi întocmite după cum urmează:			această v-a îngreuna procesul și chiar poate să influențeze clientul să refuză efectuarea eKYC.	
a) „Termenele de utilizare” (a paginii electronice, sistemului, platformei utilizate etc.) – urmează să conțină condițiile generale pentru accesarea sistemului utilizat în vederea identificării prin mijloace electronice a clientului;	A.P. „Camera de Comerț Americană din Moldova”	108	La pct. 21 este menționat faptul că entitatea raportoare aduce la cunoștința clientului termenele și condițiile în care este efectuată identificarea electronică. Considerăm necesar de a clarifica dacă este posibilă aducerea la cunoștință a acestor informații și până la accesarea soluției tehnice de identificare, spre exemplu într-o altă aplicație IT, anterioară accesării soluției tehnice de identificare electronică.	Se acceptă parțial
b) „Politica de confidențialitate” – va conține informațiile pe care entitatea raportoare le primește de la client în procesul identificării (date cu caracter personal), obligațiile pe care le are conform legii în procesul de utilizare / prelucrare a datelor, precum și măsurile de control implementate pentru a asigura confidențialitatea datelor colectate;			În temeiul celor menționate se propune următoarea redacție a pct. 21: „În cazul identificării clientului prin mijloace electronice, entitatea raportoare va asigura aducerea la cunoștință a clientului termenele și condițiile în care identificarea electronică a clientului este efectuată. Termenele și condițiile puse la dispoziția clientului, inclusiv și până la accesarea de către client a soluției de identificare electronică anterior sau concomitent cu primirea consimțământului pentru efectuarea identificării electronice a clientului, vor fi întocmite după cum urmează:”.	Se acceptă clarificarea privind perioada de accesare a informației referitor la procesul de identificare electronică.
c) „Politica privind fișierele cookie” – va conține descrierea fișierelor cookie pe care entitatea raportoare le			Tot aici, se propune excluderea de la pct. 21 a literei d) și e) întrucât nici Legea nr. 157/2014 privind încheierea și executarea contractelor la distanță privind serviciile financiare de consum și nici Codul civil nu prevede anumite cerințe specifice aferent dezvăluirii riscurilor și nu impune o obligație de punere la dispoziție a informației cu privire la „politica prevenirii spălării banilor” care în esență se bazează inclusiv și pe riscurile care pot să apară.	De asemenea, în scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice și riscurilor care derivă din aceasta, inclusiv cele de spălare a banilor și finanțare a terorismului.

folosește în scopul urmăririi acțiunilor clientului pe platformă sau pagina electronică (sub condiția utilizării); d) „Dezvăluirea riscurilor” – în scopul respectării drepturilor consumatorului se explică natura aferentă comunicării electronice și riscurilor care derivă din aceasta; e) „Politica prevenirii spălării banilor” – va conține versiunea succintă / desfășurată a politicii privind identificarea clientului, prevenirea spălării banilor, finanțarea terorismului și identificarea persoanelor expuse politic .			Totodată, conform legislației AML, atunci când clientul prezintă un interes sporit asupra politicii de control al entității raportoare, acest criteriu se tratează ca fiind în sine un factor de determinare/identificare a tranzacțiilor suspecte. Prin urmare, punerea la dispoziția clientului a acestor informații care în esență fac parte din programul intern al entității elaborat cu scopul de a preveni și combate spălarea banilor și finanțarea terorismului sensibilizează în sine procesul. La caz, prin prezentarea informațiilor enumerate supra în punct considerăm că clientul totuși obține informațiile necesare și de interes suficiente pentru acesta.	
	Banca Comercială Română Chișinău S.A.	109	Privitor la pct. 21 solicităm să fie furnizate clarificări privitor la momentul și forma de preluare a consimțământului.	Consimțământul se preia până la stabilirea relației de afaceri cu clientul sau în timpul procesului de stabilire a relației. De altfel, procesul urmează să fie similar cazului de stabilire a relației de afaceri fizic cu clientul.
	Asociația Businessului European	110	La pct. 21, cuvintele „, anterior sau concomitent cu primirea consimțământului pentru efectuarea identificării electronice a clientului” se vor exclude. A se menționa că pentru identificarea clientului la distanță nu este necesar consimțământul deoarece identificarea face parte din procedura obligatorie de stabilire a identității persoanei, or, prin analogie dacă clientul vine la ghișeu atunci el nu depune consimțământ în scris pentru a fi identificat. Mai mult ca atât, conform art. 3 și 5 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, consimțământul nu poate fi obținut în mod obligatoriu dar trebuie să fie acordat liber și nesilit, însă fără ca să ducă la imposibilitatea accesării acestui serviciu, inclusiv, conform normelor de	Se acceptă

		referință (alin. (2) din art. 5) consimțământul poate fi retras la orice etapă ceea ce va duce la necesitatea radierii datelor. La pct. 21, lit. b) va avea următorul conținut: „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 informații privind cookie dacă vor fi prelucrate.”	
Banca de Finanțe și Comerț S.A.	111	Legislația în vigoare, inclusiv Lege privind protecția datelor cu caracter personal nr. 133 din 08.07.2011 nu prevăd cerințe de elaborarea Politicilor privind fișierele cookie. <u>Propunerea:</u> Întocmirea Politicii privind fișierele cookie ca un document opțional la discreția entității și/sau cerințe interne ale entității.	Nu se acceptă În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice, precum și datele păstrate în relația cu clientul.
Asociația Businessului European	112	Lit. c) se va exclude. A se menționa că normele din proiect, în calitate de act normativ subordonat legii, nu pot diminua/modifica cerințele prevăzute la art. 12 din Legea nr. 133/2011 privind protecția datelor cu caracter personal dar și nici nu pot institui cerințe suplimentare deoarece lipsește temeiul legal din care rezultă expres reglementarea. Mai mult ca atât, termenul de Politică de confidențialitate este impropriu valorilor reglementate, or, Legea nr. 133/2011, impune obligația de a implementa măsuri organizatorice și tehnice adecvate (conformitate și securitate), nu doar confidențialitatea.	Nu se acceptă În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice, precum și datele păstrate în relația cu clientul. Remarcăm că aceste prevederi sunt în favoarea clienților și corespund scopului Legii 133/2011 de a proteja datele cu caracter personal.

OCN Microinvest SRL	113	Se propune excluderea de la pct. 21 a literei d) și e) din Regulament, întrucât nici Legea 157/2014 privind încheierea și executarea contractelor la distanță privind serviciile financiare de consum și nici Codul civil nu prevede careva cerință specifică aferent dezvăluirii a careva riscuri și nu impune o obligație de punere la dispoziție a informației cu privire la “politica de prevenirii spălării banilor” care în esență se bazează inclusiv și pe riscurile care pot să apară. Totodată, conform legislației AML, atunci când clientul prezintă un interes sporit asupra politicii de control al entității raportoare, acest criteriu se tratează ca fiind în sine un factor de determinare/identificare a tranzacțiilor suspecte. Prin urmare, punerea la dispoziția clientului a acestor informații care în esență fac parte din programul intern al entității elaborat cu scopul de a preveni și combate spălarea banilor și finanțării terorismului sensibilizează în sine procesul. La caz, prin prezentarea informațiilor enumerate supra în punct considerăm că clientul totuși obține informațiile necesare și de interes suficiente pentru acesta.	Nu se acceptă În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice și riscurilor care derivă din aceasta, inclusiv cele de spălare a banilor și finanțare a terorismului.
„Paymaster” SRL	114	La pct. 21 lit. e) din proiect, propunem excluderea obligativității de a expune normele AML în mod obligatoriu într-un document separat („Politicii prevenirii spălării banilor”) și examinarea oportunității de a include normele corespunzătoare inclusiv în alt document cum ar fi Contractul - cadru	Nu se acceptă. În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice și riscurilor care derivă din aceasta, inclusiv cele de spălare a banilor și finanțare a terorismului.

„Qiwi-M” SRL	115	În conformitate cu prevederile Legii 133/2011 privind protecția datelor cu caracter personal, entitățile colectează datele cu caracter personal ale clienților, inclusiv la efectuarea e-KYC. Entitatea are dreptul de a colecta datele personale ale clientului în scopul respectării Legislației aplicabile în domeniul prevenirii și combaterii spălării banilor fără consimțământul clientului (art. 5 Legea 133/2011), cu obligația de a indica în Politica sa de confidențialitate scopul și categoriile de date colectate. Astfel se propune a exclude art. 21 fiind contrar prevederilor Legii 133/2011. De asemenea, o astfel de practică este depășită și nu se utilizează de prestatorii de servicii de plată din UE (Revolut, Klarna, Monzo, Paysera etc.). În ceea ce privește Termenii și condițiile de utilizare, Politica de Confidențialitate și Politica AML se aduc la cunoștința clientului la înregistrarea în sistem și nu se practică a fi incluse în procesul de identificare. Menținerea unor astfel de prevederi va pune în dificultate implementarea și aplicarea acestora în practică, astfel stopând dezvoltarea în domeniul tehnologiilor a prestatorilor de servicii de plată.	Nu se acceptă În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice și riscurilor care derivă din aceasta, inclusiv cele de spălare a banilor și finanțare a terorismului. Remarcăm că prevederile punctului dat sunt în favoarea clienților și corespund scopului Legii 133/2011 de a proteja datele cu caracter personal.
Asociația băncilor din Moldova	116	- cuvintele „anterior sau concomitent cu primirea consimțământului pentru efectuarea identificării electronice a clientului” se propune a fi excluse. Menționăm că pentru identificarea clientului la distanță nu este necesar consimțământul, deoarece identificarea face parte din procedura obligatorie de stabilire a identității persoanei, or, prin analogie dacă clientul vine la ghișeu atunci el nu depune consimțământ în scris pentru a fi identificat. Mai mult ca atât, conform art. 3 și 5 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, consimțământul nu poate fi obținut în mod obligatoriu dar trebuie să fie acordat liber și nesilit, însă fără ca să ducă la imposibilitatea accesării acestui serviciu, inclusiv, conform normelor de referință (alin. (2) din art. 5) consimțământul poate	Se acceptă

			fi retras la orice etapă ceea ce va duce la necesitatea radierii datelor. - lit. b) va avea următorul conținut: „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 informații privind cookie dacă vor fi prelucrate.” Iar lit. c) se va exclude. A se menționa că normele din proiect, în calitate de act normativ subordonat legii, nu pot diminua/modifica cerințele prevăzute la art. 12 din Legea nr. 133/2011 privind protecția datelor cu caracter personal dar și nici nu pot institui cerințe suplimentare deoarece lipsește temeiul legal din care rezultă expres reglementarea. Mai mult ca atât, termenul de Politică de confidențialitate este impropriu valorilor reglementate, or, Legea nr. 133/2011, impune obligația de a implementa măsuri organizatorice și tehnice adecvate (conformitate și securitate), nu doar confidențialitatea.	Se acceptă Nu se acceptă În scopul respectării drepturilor consumatorului, entitatea urmează să explice natura aferentă comunicării electronice, precum și datele păstrate în relația cu clientul. Remarcăm că aceste prevederi sunt în favoarea clienților și corespund scopului Legii 133/2011 de a proteja datele cu caracter personal.
Capitolul IV (v2 – cap.IV)	Asociația băncilor din Moldova	117	Conținutul capitolului IV impune unele clarificări la: A. Identificarea prin mijloace de identificare electronică cu un nivel de Securitate suficient și conform cu standardele stabilite în Legea nr.124/2022 – Se are în vedere identificarea clienților/potențialilor clienți cu utilizarea semnăturii electronice calificate, fără aplicarea altor măsuri electronice de identificare? B. Identificarea prin mijloace electronice care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu	Comentariu: Au fost introduse ajustări pe textul prevederii pentru a reda claritate. Se acceptă

			elementele de verificare a prezenței fizice cu înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului – Se solicită delimitarea măsurilor de identificare pentru inițierea relații cu potențiali clienți și actualizarea datelor pentru clienții existenți care au fost identificați anterior în cadrul Băncii. C. Identificarea prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022 – se are în vedere identificarea clienților/potențialilor clienți utilizând serviciul de stat eKYC?	Alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022 pot fi considerate oricare alte soluții tehnologice furnizate în scopul stabilirii relației de afaceri la distanță, care nu sunt cunoscute la moment, dar în virtutea dezvoltărilor tehnologice pot apărea în viitor.
--	--	--	--	--

Capitolul IV lit. B (v2 – cap.IV secțiunea 1)	B.C. MAIB S.A.	118	Normele Capitolului IV lit.B (punctele 23-29) din Regulament, propunem a fi divizate în două sub-compartimente, care să descrie regulile aplicabile fiecărui proces în parte: (1) identificarea prin mijloace electronice care asigură transmiterea în direct a înregistrării video și audio și (2) identificarea prin mijloace electronice care asigură transmiterea fotografiei clientului și nu presupun transmiterea în direct a înregistrării video și audio. Mai mult, normele aplicabile primului proces propunem a diviza în două secțiuni: (1.1) normele aferente utilizării soluției asistate de un angajat al băncii și (1.2) normele aferente utilizării soluției neasistate. În Regulamentul propus spre examinare, punctele 23-29 reprezintă normele aplicabile diferitor procese, în unele cazuri lipsind o claritate fără echivoc, ce proces din cele menționate mai sus se are în vedere. Respectiv, se creează o incertitudine privind aplicabilitatea normelor și cerințelor stabilite pentru anumit proces (metodă) de identificare la distanță.	Se acceptă parțial Prevederile Regulamentului au fost ajustate pentru a stabili cerințe diferențiate. Astfel, pentru identificarea la distanță a clienților cu utilizarea mijloacelor de verificare automatizată sunt stabilite prevederi în punctele 24-29, iar pentru verificarea cu operator uman punctele 23, 25-29 și 34. Diferențierea granulară solicitată poate fi efectuată de către entitatea raportoare de sine stătător în actele sale normative interne.
	„Qiw-M” SRL	119	Textul nu corespunde proceselor care pot fi utilizate pentru identificarea clienților la distanță. Se propune a reformula după cum urmează: „Identificarea prin mijloace electronice care asigură înregistrarea video și audio sau fotografia.”	Se acceptă Prevederile cap. IV au fost ajustate.
Capitolul IV secțiunea C (v2 – cap.IV secțiunea 1)	„Credimatic Network” SRL	120	Capitolul IV secțiunea C din Proiect, face mențiune la situația în care entitatea raportoare externalizează integral sau parțial procesul de identificare la distanță către un furnizor de servicii externalizate. Cu toate acestea, Proiectul nu reglementează în mod distinct acest furnizor de	Se acceptă parțial Prevederile Regulamentului au fost ajustate, inclusiv prin stabilirea termenului de „furnizor de servicii externalizat”.

		servicii externalizate, în special prin reglementarea unor condiții și obligații pe care acest furnizor trebuie să le respecte pentru a putea fi contractat de către entitatea raportoare. Articolele 30 și 31 se limitează la a muta întreaga responsabilitate către entitățile raportoare, lăsând nereglementați acești furnizori. Normele ADR reglementează în mod distinct acești furnizori de servicii externalizate prin conceptul de terț de verificare a identității persoanei prin mijloace video. Acesta este definit ca fiind un emitent al mijloacelor de identificare electronică ce utilizează mijloace video sau o persoană juridică aflată într-o relație contractuală cu o entitate publică sau privată, în scopul furnizării serviciilor de identificare la distanță a persoanei utilizând mijloace video. Mai mult se poate observa faptul că Normele ADR la art. 9 precizează faptul că procesul de verificare a identității persoanei la distanță utilizând mijloace video se pot utiliza serviciile furnizate de către terți în baza unui contract, iar Terțul care efectuează identificarea persoanei la distanță utilizând mijloace video în numele unei alte entități este obligat să respecte prevederile prezentelor norme. Prin urmare, deși Normele ADR au avut ca scop reglementarea situației din art. 30 și 31 din Proiect (și anume externalizarea serviciului), reglementarea din România a impus acestui furnizor extern să respecte pe deplin prevederile normelor cu privire la identificarea electronică la distanță. Este evident faptul că s-a dorit asigurarea calității și a nivelelor de securitate necesare cu privire la aceste servicii prestate de terți, având în vedere importanța domeniului reglementat. Mai mult după cum am văzut, la nivel UE, o preocupare semnificativă o reprezintă conformarea acestor furnizori cu standardele internaționale și la nivel de UE. Or, în lipsa reglementării exprese a acestor furnizori de servicii externalizate, se creează un risc semnificativ în industria bancară, a asigurărilor și a	Cerințele pe care furnizorul urmează să le respecte sunt condiții stabilite între entitatea raportoare și acesta prin acordul dintre părți, iar entitatea raportoare se va asigura că acesta le respectă, altfel fiind în situația în care se încalcă prevederile Regulamentului (pct.32) și ale cerințelor privitor la externalizarea serviciilor de cunoaștere a clienților în contextul actelor normative cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. Suplimentar, este de menționat că Legea 124/2022 stabilește cerințe cu privire la prestatorii de servicii de încredere, inclusiv acreditarea acestora, dacă e cazul.
--	--	--	---

		procesatorilor de plată care sunt reglementate de Proiect, în ipoteza în care entitățile raportoare vor externaliza aceste servicii. Considerăm că nu este suficient ca Proiectul să impună anumite obligații exclusiv în sarcina entităților raportoare. Prin urmare, având în vedere cele de mai sus, propunem în mod respectuos introducerea conceptului de terț de verificare a identității persoanei prin mijloace video în Proiect, prin reglementarea acestuia în mod similar cu reglementarea din Normele ADR pentru ca BNM să asigure securitatea și stabilitatea industriilor cheie afectate de Proiect. De asemenea, considerăm necesar ca acești terți să parcurgă o procedură prealabilă de autorizare care să fie realizată de BNM, înainte ca aceștia să presteze servicii. În plus, având în vedere faptul că economia Republicii Moldova nu este izolată și în perioada recentă a cunoscut o integrare cu economiile internaționale, și având în vedere faptul că libertatea de circulație este un pilon critic al UE (sistem în care Republica Moldova va adera în curând), considerăm oportună reglementarea în Proiect a posibilității furnizorilor de servicii de identificare electronică la distanță care deja sunt autorizați în alte jurisdicții să presteze acest tip de servicii (ex., sunt autorizați în România conform Normele ADR) să își recunoască pe teritoriul Republicii Moldova aceasta autorizare. În acest sens, pentru a permite dezvoltarea serviciilor și pentru a asigura o competiție eficientă pe piața din Republica Moldova, operatorii economici străini care dețin deja o autorizare într-un stat membru al UE ar trebui să parcurgă o procedură simplificată de autorizare.	
--	--	--	--

Pct. 22 : (v2 – pct.44) Entitatea raportoare poate utiliza serviciile de încredere relevante și procesele de identificare electronică reglementate, recunoscute, aprobate sau acceptate la nivel național, pentru a se conforma prezentului Regulament. Atunci când utilizează astfel de soluții, entitatea trebuie să evalueze în ce măsură soluția respectă dispozițiile prezentului Regulament și să aplice măsurile necesare pentru a atenua riscurile relevante care decurg din utilizarea soluțiilor respective. Aceasta trebuie să ia în considerare, în special, dacă sunt abordate următoarele riscuri: a) riscurile pe care le implică autentificarea și care sunt prevăzute în politicile și procedurile sale specifice măsurilor de atenuare, în special în ceea ce privește riscurile de fraudă prin uzurparea identității; b) riscul ca identitatea clientului să nu fie identitatea pretinsă; c) riscul de pierdere, furt, suspendare, revocare sau expirare a dovezilor de	Asociația Businessului European	121	La pct. 22, lit. b) va avea următorul cuprins: „b) riscul ca identitatea pretinsă să lipsească sau să nu corespundă cu cea din Registrul de stat al populației”. Norma din proiect este redundantă și generează un înțeles inexact, or, conceptul de identitate dacă ne referim de cetățenii RM, trebuie de raportat doar la identitatea oficială constatată de organele abilitate prin emiterea actului de identitate.	Se acceptă
	B.C. MAIB S.A.	122	Pct.22 este reprodus integral în pct.44 al Regulamentului. Propunem excluderea din Regulament a pct.22, cu menținerea pct.44, deoarece norma respectivă se referă la administrarea riscurilor, prin urmare, ar trebui să fie în Capitolul VI „Riscuri și măsuri de precauție”. În orice caz (dacă se acceptă sau nu excluderea pct.22), considerăm necesară completarea Capitolului IV lit.A cu norme aplicabile procesului respectiv în activitatea entității raportoare (Identificarea prin mijloace de identificare electronică cu un nivel de securitate suficient și conform cu standardele stabilite în Legea nr.124/2022).	Se acceptă.
	„Paymaster” SRL	123	La pct. 22 din proiect, nu este clar în ce mod trebuie stabilită și executată norma privind reglementarea, recunoașterea, aprobarea sau acceptarea la nivel național a soluțiilor de identificare la distanță.	Comentariu: Cerințele de reglementare, recunoaștere, aprobare sau acceptare la nivel național a soluțiilor de identificare la distanță sunt prevăzute în Legea nr.124/2022.
	Asociația băncilor din Moldova	124	La pct. 22: lit. b) se propune următorul text: „riscul ca identitatea pretinsă să lipsească sau să nu corespundă cu cea din Registrul de stat al populației”. Norma din proiect este redundantă și generează un înțeles inexact, or, conceptul de identitate dacă ne referim la cetățenii Republicii	Se acceptă

identitate, inclusiv, după caz, a instrumentelor de detectare și prevenire a utilizării fraudelor de identitate.			Moldova, trebuie de raportat doar la identitatea oficială constatată de organele abilitate prin emiterea actului de identitate.	
	„QIWI-M” SRL	125	Conform Legii 124/2022 noțiunea de autentificare nu se referă la procesul de identificare e-KYC și prevede „proces electronic care permite confirmarea identificării electronice a persoanelor fizice și/sau juridice sau a originii și integrității anumitor date în formă electronică” Prin urmare se propune a modifica sintagma de „autentificare” cu „identificare”.	Se acceptă
Pct. 23 : (v2 – exclus) Entitatea raportoare poate utiliza mijloacele electronice în scopul stabilirii/continuării relației de afaceri cu persoanele fizice și juridice, care asigură cumulativ transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice (liveness), cu înregistrarea originalului actului de identitate în timpul transmiterii în direct și captarea imaginii faciale a clientului.	B.C. MAIB S.A.	126	La pct.23 din Regulament, propunem înlocuirea cuvântului „stabilirii” cu cuvântul „inițierii”.	Nu se acceptă În Legea 308/2017 sunt folosite ambele cuvinte deopotrivă. Respectiv, nu considerăm a fi cuvinte cu sens diferit.
	„QIWI-M” SRL	127	Expunerea pct. 23 din proiectul Regulamentului nu prevede metode de identificare existente care sunt bazate pe tehnologii AI și de verificare liveness. Se propune a reformula și reda pct. 23 în următoarea redacție: „Entitatea raportoare poate utiliza mijloacele electronice în scopul stabilirii/continuării relației de afaceri cu persoanele fizice și juridice, care asigură una sau mai multe funcționalități: a) transmiterea în direct a înregistrării video și audio și captarea imaginii faciale a clientului, sau b) efectuarea pozelor a clientului cu elementele de verificare a prezenței fizice (liveness), sau c) înregistrarea originalului actului de identitate în timpul înregistrării video sau efectuării pozei, d) Verificarea identității din surse sigure și credibile cum ar fi baze de date”	Comentariu: În contextul ajustării prevederilor Regulamentului, conform altor comentarii/propuneri parvenite, punctul dat a fost exclus.

Pct. 24 : (v2 – pct.22-23) La identificarea video, entitatea se asigură că procesul este înregistrat și corespunde următoarelor: a) este de o durată rezonabilă (stabilită conform politicilor interne), și conține, cel puțin, următoarele informații/date relevante: - ora, ziua, anul înregistrării; - momentul exact în care persoana fizică supusă verificării video prezintă datele sale de identificare din documentul de identitate (numele și prenumele, IDNP, data/luna/anul nașterii, adresa de reședință, ora/data/luna/anul în care se face înregistrarea, precum și numărul de contact al telefonului mobil); - momentul în care angajatul entității raportoare ia legătură cu persoana în timpul verificării video și/sau momentul în care clientul primește codul unic remis prin serviciul de mesaje	OCN Microinvest SRL	128	Se propune la pct. 24 lit. b) din Regulament de a se include după fraza “la procesul identificării video se desfășoară în condiții” cuvântul „suficiente”, deoarece sunt stipulate condiții care se pot deosebi de la caz la caz în dependență de locația clientului, fiind riscul ca procesul să fie afectat din motive neobiective. Iar cuvintele ”aceeași încăpere” din al doilea alineat din pct. 24 lit. b) să fie substituit cu cuvântul „cadru”, or entitatea raportoare nu poate stabili cu exactitate acest factor. Totodată, ca și esență, identificarea la distanță în cele mai dese cazuri survine în legătură cu necesitățile clientului de a fi creditat la anumit moment, într-un anumit loc, când acesta se poate afla în spații publice, comerciale, de vânzări bunuri sau prestării servicii, și anume, în situațiile când pentru acesta prezintă interes anume creditarea la distanță în raport cu cea ordinară. Situația când elementar clientul nu are unde se retrage pentru a fi singur și în liniște totală.	Comentariu: Prevederile Regulamentului au fost ajustate pentru a stabili cerințe diferențiate pentru circumstanțele când clienții stabilesc relații de afaceri la distanță prin diferite metode și, respectiv, cerințele sunt diferențiate. Astfel, pentru identificarea la distanță a clienților cu utilizarea mijloacelor de verificare automatizată sunt stabilite prevederi în punctele 24-29, iar pentru verificarea cu operator uman punctele 23, 25-29 și 34.
	Banca de Finanțe și Comerț S.A.	129	<i>Pct. 24 subp.3, lit. b)</i> - identificarea, verificarea și păstrarea <i>datelor tehnice ale computerului / dispozitivului utilizat de către client (amprenta dispozitivului), IP adresa, localizarea acestuia, date despre calculatorul/dispozitivul utilizat (modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea), precum și alte date posibil a fi colectate;</i> Din proiectul nu este clar dacă lista datelor este una obligatorie sau unele date sunt opționale. Acest moment este important din motivul că în dependență de producătorul dispozitivului unele date pot fi indisponibile . De exemplu compania	Comentariu: Entitatea va obține datele/informațiile despre dispozitiv pe cele disponibile și posibil a fi obținute.

scurte (SMS) la telefonul mobil; - momentul în care clientul apropie actul de identitate de cameră și îl afișează pe ambele părți; b) este în concordanță cu următoarele condiții: - procesul identificării video se desfășoară în condiții de liniște și a unei bune iluminări în spațiul clientului, care permite identificarea clară a acestuia, în caz contrar, procesul urmează a fi întrerupt; - în aceeași încăpere cu clientul nu trebuie să se regăsească persoane terțe; - identificarea, verificarea și păstrarea		Apple nu prezintă datele aferent ID dispozitivului, IP private. Suplimentar scopul obținerii a unor parametre nu este clar definit din punct de vedere al prevederilor protecției datelor cu caracter personal conform prevederilor al Legii 133/2011: modelul dispozitivului, setări de limba, dimensiunea ecranului, etc.	
	130	subp.5, p. b) P. 24 : În dependența de producătorul dispozitivului calitatea imaginii se diferă chiar și în cazul declarării unei rezoluții mare. De exemplu 8 megapixeli de pe Apple se diferă de la 8 megapixeli de pe OPPO. <u>Propunerea :</u> De indicat cerințe clare asupra calității imaginii în funcția de posibilitatea evaluării corespunzătoare a feței clientului.	Comentariu: Prevederile Regulamentului setează cerințe minime tehnice pentru dispozitivul care urmează a fi utilizat în scopul obținerii unei imagini clare a persoanei care dorește să stabilească relații de afaceri la distanță. Entitatea raportoare are obligația să nu stabilească relația de afaceri la distanță, în cazul în care nu este posibil obținerea informațiilor/datelor corespunzătoare cerințelor stabilite.

datelor tehnice ale computerului / dispozitivului utilizat de către client (amprenta dispozitivului), IP adresa, localizarea acestuia, date despre calculatorul/dispozitivul utilizat (modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea), precum și alte date posibil a fi colectate; - procesul de verificare video trebuie să se desfășoare în timp real și fără întreruperi prin flux continuu. Dacă procesul de verificare a fost întrerupt, indiferent de motivul întreruperii, acesta urmează a fi reluat de la început; - calitatea informației audiovizuale (calitatea imaginii și a sunetului în timpul verificării video) trebuie să fie de o calitate înaltă, cu o rezoluție de cel puțin 8	Banca Comercială Română Chișinău S.A.	131	La pct. 24 lit. a) liniuță 2, după sintagma “adresa de reședință” necesită să fie închisă paranteza, astfel încât doar datele din paranteza sunt cele se regăsesc în documentul de identitate. În continuare pentru sintagma “ora/data/luna/anul în care se face înregistrarea, precum și numărul de contact al telefonului mobil” necesită să revizuiască și să vină cu clarificări privitor la contextul aplicării (cum ar fi dacă ora/data/luna/anul în care se face înregistrarea se referă la înregistrarea video, se referă la comunicarea verbală via video a numărului de contact?).	Cât privește alte cerințe, menționăm că prevederile Regulamentului a fost ajustat pentru a reda claritate asupra măsurilor pe care entitatea să le aplice în funcție de metoda utilizată de identificare la distanță.
		132	La pct. 24 lit. a) liniuță 3, solicităm să fie furnizate mai multe clarificări privitor la aplicarea în practica a sintagmei „și/sau momentul în care clientul primește codul unic remis prin serviciul de mesaje scurte (SMS) la telefonul mobil”, pe textul reglementării nu se regăsesc clauze privitor la factorul de identificare prin One Time Password, și în ce scopuri/situații banca urmează să asigure această clauză. În cazul în care se prezumă a fi prevederea conexă cu pct. 35 lit. b), atunci solicităm sa fie revizuite ambele clauze ca sa fie o claritate despre legătura între cele 2 prevederi.	Comentariu: Textul Regulamentului a fost ajustat pentru a reda claritate la folosirea diferitelor elemente de securitate la stabilirea relației de afacere cu clienții.

mega pixeli sau mai mare FullHD (1920x1080), în scopul identificării și recunoașterii necondiționate a persoanei, asigurării unei discuții libere și clare între angajatul entității raportoare și client, precum și verificării vizuale de către angajatul entității raportoare a documentelor prezentate de către client, inclusiv a elementelor de protecție aplicabile documentului respectiv.	133	Privitor la pct. 24 lit. a), liniuța 4, având în vedere că este o parte a procesului prevăzut la pct. 24 lit. a) liniuța 2, propunem ca acestea sa fie comasate într-o singur punct. Totodată menționam că la pct. 24 lit. a) liniuța 2 se conține sintagma „momentul exact” pe când 24 a) liniuța 4 se menționează textul „momentul”. Privitor la pct. 24 lit. b), liniuța 3, si pct. 26, solicităm să fie furnizate clarificări privitor la toate datele necesare, fără a lasă spațiu de acțiuni individuale, precum și scopurile pentru care entitățile urmează să asigure păstrarea datelor. Totodată solicităm să fie furnizate clarificări privitor sintagma „...verificarea ...datelor tehnice ale computerului/dispozitivului utilizat de	
	134	Privitor la pct. 24 lit. b), liniuța 5, solicităm să fie furnizate precizări privind cerințele aferente calității sunetului în timpul verificării video.	Comentariu: Calitatea informației audiovizuale trebuie să fie de o calitate înaltă astfel încât entitatea să aibă certitudinea că persoana supusă procesului de identificare și verificare a identității este cea reală declarată.

Asociația Businessului European	135	La pct. 24: - lit. a) liniuța 2, propunem a fi exclusă sintagma „data/luna/anul nașterii” – ca fiind excesivă scopului dar și prevederilor art. 4 alin. (1) din Legea nr. 133/2011. Astfel, nu este clară necesitatea colectării acestor categorii de date atât timp cât interacțiunea cu Mconnect sau oricare alt serviciu de consum de date din bazele de date de stat sau private este IDNP. Astfel aceste date nu sunt necesare și împovărează procesul de identificare nejustificat. Aceeași situație se referă și la numărul de telefon mobil. Nu este clară necesitatea de a colecta numărul de telefon mobil a telefonului dar și expedierea SMS prin GSM în situația în care tehnologia utilizată este alta – Internetul. Așadar, datele (actul de identitate și imaginile foto/video/audio vor fi colectate prin intermediul internetului și nu prin GSM. - lit. b) va avea următorul cuprins: „iluminarea este suficientă pentru a capta imaginile foto/video și a declanșa procesul de identificare”. A se menționa că formularea textului din proiect este incertă, ori, nu este clar cum de estimat dacă în încăpere este liniște (nivelul de zgomot redat în decibeli – norme cuantificabile, spre exemplu dacă s-a mai auzit o voce decât cea a clientului procesul trebuie de încetat, sau dacă clientul este în ascensor, automobil, la locul de muncă etc.). Mai mult, în ceea ce privește necesitatea iluminării spațiului clientului la fel nu este clară cerința, or, spațiul în care se află persoana fizică cade sub incidența inviolabilității domiciliului, respectiv este lipsită de necesitate iluminarea spațiului (a întregii camere, sau dacă clientul este afară etc.). Comunicăm că în caz de menținere a textului proiectului fără operarea	Nu se acceptă Prevederile punctului este în corespundere cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului. Nu se acceptă Cerință față de entitate este ca această să asigure că la stabilirea relației de afaceri cu clientul prin mijloace electronice procesul de identificare și verificare a identității corespunde unor norme minime pentru care să aibă certitudinea că persoana cu care stabilește relația este cea pretinsă, iar informația/datele colectate să fie sigure. Calitatea habitatului în care se află potențialul client este unul primordial în acest sens, iar entitatea va stabili în politicile interne care trebuie să fie condițiile acceptabile care determină acest fapt (calitatea iluminatului, zgomotul etc.) Stabilirea relației de afaceri este un acord între două părți, în care ambele cad de
---------------------------------	-----	--	--

	ajustărilor, procedura de identificare în marea majoritate a cazurilor va fi încetată. - Lit. b) liniuța 2 propunem a fi exclusă. Nu este argumentată această interdicție, or, ar rezulta că entitatea raportoare va trebui să determine dacă nu sunt și alte persoane în cameră prin solicitarea de a arăta împrejurările. - Lit. b) cuvintele „(amprenta dispozitivului)” urmează a fi exclusă deoarece duce la înțelesul amprentelor digitale și nu la datele tehnice despre dispozitiv. Mai mult, propunem a fi exclus și textul „(modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea)” deoarece se creează un înțeles impropriu prin care aceste date devin a fi obligatorii spre colectare, însă din punct de vedere tehnic, clientul ar putea refuza furnizarea acestor date. - Lit. b) liniuța 5, sintagma „cu o rezoluție de cel puțin 8 mega pixeli sau mai mare FullHD (1920x1080),” urmează a fi modificată deoarece este contradictorie. A se menționa că rezoluția Full HD cu 1920x1080 poate fi asigurată de un senzor nu mai mic de 2 MPx	acord cu anumite condiții fie de stabilire sau de desfășurare a acestei relații, iar entitatea raportoare având obligații de gestionare a anumitor riscuri, urmează să se asigure că are capacitatea de a o face, pe când potențialul client, dacă nu cade de acord cu procesul stabilit, poate să se apropie la ghișeu la bancii pentru a avea o mai bună interacțiune cu entitatea. Se acceptă Se acceptă parțial A fost exclusă prevederea din acest subpunct, fiind expusă separat (pct.24). Totuși, cerința de colectare a informației despre dispozitivul utilizat nu poate fi exclus, iar entitatea va acumula informații posibile a fi colectate din cele enumerate. Comentariu: Nu este clar de ce sintagma este contradictorie. Considerăm că aceasta stabilește cerința minimă pentru informația audiovizuală care urmează a fi colectată de entitate în anumite condiții de calitate.
--	---	---

		pe când norma vizată determină obligația să fie de cel puțin 8MPx.	
BC Energbank SA	136	În conformitate cu prevederile pct. 24 lit. b) care stabilește că " La identificarea video, entitatea se asigură că procesul este înregistrat și corespunde următoarelor condiții: în aceeași încăpere cu clientul nu trebuie să se regăsească persoane terțe,, considerăm relevant indicarea faptului dacă copii fac excepție sau nu din categoria persoanelor terțe enunțată în norma dată.	Se acceptă S-a exclus prevederea dată.
B.C. MAIB S.A.	137	La pct.24 lit.a) din Regulament, propunem ca sintagma „politicilor interne” să fie înlocuită cu sintagma „reglementărilor interne”. La pct.24 lit.a) din Regulament, a doua liniuță, propunem ca sintagma „adresa de reședință” să fie înlocuită cu sintagma „adresa de domiciliu și/sau reședință”.	Se acceptă

„Paymaster” SRL	138	La pct. 24 lit.a) pct.2 din proiect, propunem excluderea numărului de contact (care nu se regăsește în documentul de identitate) precum și datele de reședință- deoarece aceste date nu sunt eligibile pentru colectare într-un proces autoamtizat de identificare. La fel propunem ca ora/data/luna momentului de identificare să nu fie obligatorie pe video dar să fie acceptate și în alt format de înregistrare, cum ar fi în sistemul intern al prestatorului.	Comentariu: Prevederile menționate au fost ajustate pentru a diferenția cerințele la stabilirea relației de afaceri prin mijloace electronice cu și fără operator uman.
	139	Pct. 24 lit.b) pct.3 din proiect, propunem să fie exclus deoarece aceste date le considerăm excesive și lipsite de informație utilă procesului de identificare.	Se acceptă parțial A fost exclusă prevederea din acest subpunct, fiind expusă într-o separat (pct.24). Totuși, cerința de colectare a informației despre dispozitivul utilizat nu poate fi exclus, iar entitatea va acumula informații posibile a fi colectate din cele enumerate.
	140	Pct. 24 lit.b) pct.5 din proiect,, propunem excluderea “cu o rezoluție de cel puțin 8 mega pixeli sau mai mare FullHD (1920x1080)” pentru că astfel de video vor ocupa foarte mult spațiu de stocare da și nu toți utilizatorii au dispozitive performante care ar permite rezoluția nominalizată.	Comentariu: Calitatea informației audiovizuale trebuie să fie de o calitate înaltă astfel încât entitatea să aibă certitudinea că persoana supusă procesului de identificare și verificare a identității este cea reală declarată.

141	Lit. b) liniuta 2: Luând în considerație că actualmente majoritatea persoanelor utilizează un smartphone pentru identificare și convorbirea video poate fi efectuată inclusiv din mașină sau locuri publice sau de serviciu, nu este corect să limităm identificarea în încăpere izolată și fără prezența altor persoane. Limitările de acest gen vor duce la dificultăți de dezvoltare a procesului de identificare. De asemenea, nu este clar cum entitatea poate asigura ca în aceeași încăpere cu clientul nu se regăsesc persoane terțe. Se propune a exclude această condiție.	Prevederea dată a fost exclusă.
142	Lit. b) liniuta 3: Toate datele aferente calculatorului și asociate cu clientul sunt date cu caracter personal și urmează a fi specificate anterior colectării. De asemenea Legea 133/2011 prevede că datele nu trebuie să fie colectate cu exces și strict în cantitatea necesară pentru îndeplinirea scopului pentru care se colectează. În expunerea condiției date se atestă un exces de date cu privire la client care urmează a fi colectate ceea ce contravine Legii 133/2011, precum și creează dificultăți la colectarea acestora. Se propune a reduce lista datelor colectate la următoarele: - tipul dispozitivului (dacă e posibil marca) - ip adresa (este prevăzută și de Legea 308/2017) - sistemul de operare după necesitate - alte date după necesitate, precum localizarea.	Comentariu: Entitatea va obține datele/informațiile despre dispozitiv pe cele disponibile și posibil a fi obținute. De asemenea, prevederile date au fost introduse în scopul conformării cerințelor tehnologiei informației.

		143	Lit. b) liniuta 5: Considerăm aceste condiții exagerate. Entitatea trebuie să asigure calitate optimă a informației audiovizuale pentru identificarea fără echivoc a persoanei identificare, însă condiționarea parametrilor rezoluției duce la condiționarea dispozitivelor clienților prin care se poate face identificarea, astfel procesul de e-KYC devine unul complicat care va reduce considerabil de numărul utilizatorilor eligibili pentru identificarea la distanță. La moment, procesele de identificare la distanță cu audio sau video nu ar corespunde parametrilor solicitați de Regulament, deși se încadrează în prevederile reglementărilor europene (ex. Ghidului EBA/GL/2022/15). În contextul celor expuse și reieșind din practica și recomandările UE se solicită reformularea cerințelor după cum urmează: ”procesul de verificare video este realizată în condiții de iluminare adecvate și că proprietățile necesare sunt captate cu claritatea necesară pentru a permite verificarea corespunzătoare a identității clientului, astfel încât clientul să poată fi recunoscut fără echivoc și că sunt utilizate sisteme tehnologice fiabile”.	Comentariu: Calitatea informației audiovizuale trebuie să fie de o calitate înaltă astfel încât entitatea să aibă certitudinea că persoana supusă procesului de identificare și verificare a identității este cea reală declarată.
--	--	-----	---	--

		software. Prin urmare, vă solicităm în mod respectuos eliminarea din Proiect a acestei cerințe. Tot art. Art. 24 paragraful b) prevede faptul că: La identificarea video, entitatea se asigură că procesul este înregistrat și corespunde următoarelor: [...] b) este în concordanță cu următoarele condiții: identificarea, verificarea și păstrarea datelor tehnice ale computerului /dispozitivului utilizat de către client (amprenta dispozitivului), IP adresa, localizarea acestuia, date despre calculatorul/dispozitivul utilizat (modelul, numele, parametrii hardware, useragent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea), precum și alte date posibil a fi colectate; Din punct de vedere software, nu este posibil ca informații privind modelul, numele și parametrii hardware ai calculatorului/dispozitivului utilizat de solicitant să fie obținute/citite în mod automat de către soluția software care este folosită la procesul de verificare a identității la distanță. De asemenea, având în vedere suita de elemente care sunt verificate în cadrul procesului, se naște întrebarea legitimă în ce măsură aceste informații sunt relevante pentru a determina identitatea unei persoane. Prin urmare, vă solicităm în mod respectuos eliminarea din Proiect a acestei cerințe.	Comentariu: Entitatea va obține datele/informațiile despre dispozitiv pe cele disponibile și posibil a fi obținute. De asemenea, prevederile date au fost introduse în scopul conformării cerințelor tehnologiei informației.
--	--	--	--

Asociația băncilor din Moldova	145	- lit. a) liniuța 2, propunem a fi exclusă sintagma „data/luna/anul nașterii” – ca fiind excesivă scopului dar și prevederilor art. 4 alin. (1) din Legea nr. 133/2011. Astfel, nu este clară necesitatea colectării acestor categorii de date atât timp cât interacțiunea cu Mconnect sau oricare alt serviciu de consum de date din bazele de date de stat sau private este IDNP. Astfel, aceste date nu sunt necesare și împovărează la propriu procesul de identificare nejustificat. Aceeași situație se referă și la numărul de telefon mobil. Nu este clară necesitatea de a colecta numărul de telefon mobil dar și expedierea SMS prin GSM în situația în care tehnologia utilizată este alta – Internetul. Așadar, datele (actul de identitate și imaginile foto/video/audio vor fi colectate prin intermediul internetului și nu prin GSM.	Nu se acceptă Prevederile punctului este în corespundere cu cerințele de prevenire și combatere a spălării banilor și finanțării terorismului.
--------------------------------	-----	--	--

146	- lit. b) va avea următorul cuprins: „iluminarea este suficientă pentru a capta imaginile foto/video și a declanșa procesul de identificare”. A se menționa că formularea textului din proiect este incertă, ori, nu este clar cum de estimat dacă în încăpere este liniște (nivelul de zgomot redat în decibeli – norme cuantificabile, spre exemplu dacă s-a mai auzit o voce decât cea a clientului procesul trebuie de încetat, sau dacă clientul este în ascensor, automobil, la locul de muncă etc.). Mai mult, în ceea ce privește necesitatea iluminării spațiului clientului la fel nu este clară cerința, or, spațiul în care se află persoana fizică cade sub incidența inviolabilității domiciliului, respectiv este lipsită de necesitate iluminarea spațiului (a întregii camere, sau dacă clientul este afară etc.). Comunicăm că în caz de menținere a textului proiectului fără operarea ajustărilor, procedura de identificare în marea majoritate a cazurilor va fi încetată.	Nu se acceptă Cerință față de entitate este ca această să asigure că la stabilirea relației de afaceri cu clientul prin mijloace electronice procesul de identificare și verificare a identității corespunde unor norme minime pentru care să aibă certitudinea că persoana cu care stabilește relația este cea pretinsă, iar informația/datele colectate să fie sigure. Calitatea habitatului în care se află potențialul client este unul primordial în acest sens, iar entitatea va stabili în politicile interne care trebuie să fie condițiile acceptabile care determină acest fapt (calitatea iluminatului, zgomotul etc.) Stabilirea relației de afaceri este un acord între două părți, în care ambele cad de acord cu anumite condiții fie de stabilire sau de desfășurare a acestei relații, iar entitatea raportoare având obligații de gestionare a anumitor riscuri, urmează să se asigure că are capacitatea de a o face, pe când potențialul client, dacă nu cade de acord cu procesul stabilit, poate să se apropie la ghișeu la bancă pentru a avea o mai bună interacțiune cu entitatea.
147	- lit. b) liniuța 2 propunem a fi exclusă. Nu este argumentată această interdicție, or, ar rezulta că entitatea raportoare va trebui să determine dacă nu sunt și alte persoane în cameră prin solicitarea de a arăta/prezenta împrejurările/ambianța? - lit. b) cuvintele „(amprenta dispozitivului)” urmează a fi exclusă deoarece duce la înțelesul	Se acceptă Comentariu:

			amprentelor digitale și nu la datele tehnice despre dispozitiv. Mai mult, propunem a fi exclus și textul „(modelul, numele, parametrii hardware, user-agent, cookies, fonturi instalate, timpul zonei orare, setări de limbă, dimensiunile ecranului, date despre conexiuni la rețea)” deoarece se creează un înțeles impropriu prin care aceste date devin a fi obligatorii spre colectare, însă din punct de vedere tehnic, clientul ar putea refuza furnizarea acestor date;	Entitatea va obține datele/informațiile despre dispozitiv pe cele disponibile și posibil a fi obținute. De asemenea, prevederile date au fost introduse în scopul conformării cerințelor tehnologiei informației.
		148	- lit. b) liniuța 5, sintagma „, cu o rezoluție de cel puțin 8 mega pixeli sau mai mare FullHD (1920x1080),” urmează a fi modificată deoarece este contradictorie. A se menționa că rezoluția Full HD cu 1920x1080 poate fi asigurată de un senzor nu mai mic de 2 MPx pe când norma vizată determină obligația să fie de cel puțin 8MPx;	Comentariu: Nu este clar de ce sintagma este contradictorie. Considerăm că aceasta stabilește cerința minimă pentru informația audiovizuală care urmează a fi colectată de entitate în anumite condiții de calitate.
Pct. 25: (v2 – pct.22-23) În cazul în care entitatea raportoare utilizează soluții de identificare la distanță neasistate, în care clientul nu interacționează cu un angajat pentru a efectua procesul de verificare, acestea trebuie pe lângă cerințele stipulate supra:	Banca de Finanțe și Comerț S.A.	149	Prin proiect de Regulament nu se regăsește noțiunea ”puternici și fiabili”, ceea ce poate să aducă la tălmăcirea incorectă, subiectivă a acestor noțiuni. <u>Propunerea :</u> De a prezenta cerințe fixe de algoritme sau de a exclude noțiunea ” puternici și fiabili” cu înlocuirea acestora cu descrierea succintă aferente algoritmilor pentru a atinge a scopul final pentru care se face aceasta verificarea	Se acceptă Prevederea dată a fost modificată pentru a reda claritate cu referire la cerința care urmează a fi aplicată de către entitate.

- să se asigure că orice fotografie (fotografii) sau înregistrare video este realizată (sunt realizate) în condiții de iluminare adecvate și că proprietățile necesare sunt captate cu claritatea necesară pentru a permite verificarea corespunzătoare a identității clientului; - să se asigure că orice fotografie (fotografii) sau înregistrare video este realizată (sunt realizate) în momentul în care clientul efectuează procesul de verificare; - să efectueze verificări de detectare a mișcării clientului, care pot include proceduri în cadrul cărora este necesară o acțiune specifică din partea clientului pentru a verifica dacă acesta este prezent la sesiunea de comunicare sau care se pot baza pe analiza datelor primite și nu necesită o acțiune specifică din partea clientului;	A.P. „Camera de Comerț Americană din Moldova”	150	se propune excluderea frazei „pe lângă cerințele stipulate supra” întrucât pct. 24 și pct. 25 descriu două procese diferite de identificare, și anume pct. 24 descrie procesul de identificare prin mijloace video iar pct. 25 pe de altă parte descrie și procesul de identificare foto. Per general, se creează o incertitudine, care cerințe și pentru care proces sunt aplicabile pe întreg parcursul Regulamentului, care ar fi pentru identificarea asistată și care pentru cea neasistată, care sunt pentru identificarea video și care sunt cele pentru identificarea foto. Or, reieșind din norma legală și inclusiv din lit. B cap. IV, soluția expusă presupune două metode distincte de identificare „transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice”. Prin urmare, cerințele aplicabile pentru identificare asistată sau neasistată, foto sau video considerăm că urmează a fi expuse clar și separat. Tot aici, pentru a minimiza riscul de fraude poate fi posibilă o verificare prin doi factori, o verificare biometrică între imaginea captată a feței aplicantului cu actul de identitate și cu poza deținătorului actului de identitate preluată din baza de date pusă la dispoziție de ASP (MConnect). În temeiul celor menționate se propune următoarea redacție a pct. 25, liniuța 5: „-să utilizeze algoritmi puternici și fiabili pentru a verifica dacă fotografia (fotografiile) sau înregistrarea video efectuată (efectuate) corespund fotografiei (fotografiilor) extrase din documentul (documentele) oficiale ale clientului sau fotografiile obținute din surse credibile și independente.	Se acceptă
---	--	------------	--	-------------------

- să utilizeze algoritmi de verificare a corespunderii elementelor actului de identitate prezentat precum ortografia cifrelor, codului de autoritate și a altor înscrisuri existente;				
- să utilizeze algoritmi puternici și fiabili pentru a verifica dacă fotografia (fotografiile) sau înregistrarea video realizată (realizate) corespund fotografiei (fotografiilor) extrase din documentul (documentele) oficiale ale clientului.	BC Comerțbank S.A.	151	se propune excluderea frazei „pe lângă cerințele stipulate supra” întrucât pct. 24 și pct. 25 descriu două procese diferite de identificare, și anume pct. 24 descrie procesul de identificare prin mijloace video iar pct. 25 pe de altă parte descrie și procesul de identificare foto. Per general, se creează o incertitudine, care cerințe și pentru care proces sunt aplicabile pe întreg parcursul Regulamentului, care ar fi pentru identificarea asistată și care pentru cea neasistată, care sunt pentru identificarea video și care sunt cele pentru identificarea foto. Or, reieșind din norma legală și inclusiv din lit. B cap. IV, soluția expusă presupune două metode distincte de identificare „transmiterea în direct a înregistrării video și audio <u>sau</u> a fotografiei cu elementele de verificare a prezenței fizice”. Prin urmare, cerințele aplicabile pentru identificare asistată sau neasistată, foto sau video considerăm că urmează a fi expuse clar și separat. Tot aici, pentru a minimiza riscul de fraude se propune o verificare prin doi factori, o verificare biometrică între imaginea captată a feței applicantului cu actul de identitate și cu poza deținătorului actului de identitate preluată din baza de date pusă la dispoziție de ASP (MConnect).	Se acceptă Punctul dat a fost redactat.

Asociația Businessului European	152	La pct. 25, liniuța 4 propunem a fi exclusă. Cerințele vizate sunt improprii, inclusiv nu este clară necesitatea de a verifica ortografia cifrelor (nu este clar procesul din punct de vedere tehnic), inclusiv în cazul verificării codului de autoritate (actele de identitate nu conțin astfel de coduri) dar și în cazul altor înscrisuri la fel nu este clară cerința din punct de vedere tehnic.	Comentariu: Prevederea dată a fost modificată pentru a reda claritate cu referire la cerința care urmează a fi aplicată de către entitate.

Banca Comercială Română Chișinău S.A.	153	Privitor la pct. 25, liniuța 5, solicităm sa fie furnizate clarificări care algoritme sunt considerate puternice și fiabile față de alte categorii de algoritme care asigură realizarea aceluiași scop (verificarea dacă fotografia (fotografiile) sau înregistrarea video realizată (realizate) corespund fotografiei (fotografiilor) extrase din documentul (documentele) oficiale ale clientului).	Se acceptă Prevederea dată a fost modificată pentru a reda claritate cu referire la cerința care urmează a fi aplicată de către entitate.
„Credimatic Network” SRL	154	Art. 25 prevede faptul că: În cazul în care entitatea raportoare utilizează soluții de identificare la distanță neasistate, în care clientul nu interacționează cu un angajat pentru a efectua procesul de verificare, acestea trebuie pe lângă cerințele stipulate supra: [...] să efectueze verificări de detectare a mișcării clientului, care pot include proceduri în cadrul cărora este necesară o acțiune specifică din partea clientului pentru a verifica dacă acesta este prezent la sesiunea de comunicare sau care se pot baza pe analiza datelor primite și nu necesită o acțiune specifică din partea clientului. Pentru a evita neclarități, considerăm că acest paragraf ar trebui reformulat prin separarea clară a celor două modalități (care să fie îndeplinite în mod alternativ și nu cumulativ). Astfel, paragraful ar putea să menționeze faptul că există obligația de a efectua verificări: (i) de detectare a mișcării clientului, sau (ii) care se pot baza pe analiza datelor primite și nu necesită o acțiune specifică din partea clientului.	Se acceptă Prevederile date au fost modificate pentru a clarifica cerințele specifice pe care entitatea urmează să le aplice.

OCN Microinvest SRL	155	Se propune la pct. 25 din Regulament ca fraza “pe lângă cerințele stipulate supra” să fie eliminată așa cum pct. 24 și pct. 25 descriu două procese diferite de identificare, și anume pct. 24 descrie procesul de identificare prin mijloace video, iar pct. 25 pe de altă parte descrie și procesul de identificare foto. Per general se creează o incertitudine, care cerințe și pentru care proces sunt aplicabile pe întreg parcursul Regulamentului, care ar fi pentru identificarea asistată și care pentru cea neasistată, care sunt pentru identificarea video și care sunt cele pentru identificarea foto. Or, reieșind din norma legală și inclusiv din lit. B cap. IV, soluția expusă presupune două metode distincte de identificare „transmiterea în direct a înregistrării video și audio sau a fotografiei cu elementele de verificare a prezenței fizice”. Prin urmare, cerințele aplicabile pentru identificare asistată sau neasistată, foto sau video considerăm că urmează să fie expuse clar și separat.	Se acceptă Prevederile date au fost modificate.
Banca Comercială Română Chișinău S.A.	156	Privitor la pct. 25 solicităm să se furnizeze clarificări, având în vedere că se face referință la cerințele stipulate în pct. 24 care se referă la identificarea la distanță a clientului prin interacțiunea cu angajatul băncii.	Comentariu: Prevederile date au fost modificate.

	B.C. MAIB S.A.	157	La pct.25 din Regulament, este utilizată noțiunea „soluții de identificare la distanță neasistate”, fiind expusă și semnificația acesteia. Propunem ca noțiunea „soluție de identificare la distanță neasistată” și semnificația acesteia să fie prezentată în pct.4 din Regulament.	Comentariu: Cerințele care urmează a fi aplicate de către entitate au fost ajustate și diferențiate pentru a aduce claritate cu referire la aplicarea cerințelor asistate și neasistate de către un operator uman. Respectiv, considerăm inoportun definirea acestor termeni.
	„Qiw-M” SRL	158	Reieșind din practica și recomandările UE, aceasta ar putea fi inclusă ca o cerință opțională, în dependență de tipul soluției utilizate. Impunerea acestei cerințe ar putea duce la dificultăți de implementare și utilizare a unor soluții alternative mai avansate care nu necesită astfel de tip de verificare pentru a fi conforme legislației aplicabile. Se propune această clauză a fi exclusă sau a fi indicată ca opțională.	Comentariu: Prevederile date au fost modificate.
	Asociația băncilor din Moldova	159	La pct. 25: liniuța 4 propunem a fi exclusă. Cerințele vizate sunt improprii, inclusiv nu este clară necesitatea de a verifica ortografia cifrelor (nu este clar procesul din punct de vedere tehnic), inclusiv în cazul verificării codului de autoritate (actele de identitate nu conțin astfel de coduri) dar și în cazul altor înscrisuri la fel nu este clară cerința din punct de vedere tehnic.	Comentariu: Prevederea dată a fost modificată pentru a reda claritate cu referire la cerința care urmează a fi aplicată de către entitate.
Pct. 27 : (v2 – pct.27) În cadrul identificării video entitatea raportoare verifică actele de identitate	OCN Microinvest SRL	160	Pentru a exclude dublarea prevederilor, se propune excluderea literei d) din pct. 27 din Regulament, deoarece lit. e) din pct. 27 cuprinde elementele minime de securitate a actului de identitate, care par a fi suficiente pentru a atinge obiectivul urmărit.	Se acceptă

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	A.P. „Camera de Comerț Americană din Moldova”	161	se propune excluderea literei d) pentru a nu admite dublarea prevederilor deoarece la lit. e) al aceluiași punct se regăsesc elementele minime de securitate a actului de identitate, care par a fi suficiente pentru a atinge obiectivul urmărit.	Se acceptă S-a exclus lit.e) în scopul evitării dublării prevederii.
	Asociația Businessului European	162	La pct. 27 propunem a fi reformulate cerințele, deoarece procedura de identificare a clientului ar trebuie să conțină cerințe față de stabilirea identității clientului și nu de stabilire a autenticității actului de identitate. Mai simplu spus, din punct de vedere tehnic, pentru determinarea identității persoanei se va utiliza: imaginea facială (biometria punctelor de referință a feței) a imaginii din actul de identitate și a persoanei, iar ulterior, în caz de corespundere, se va face apel la MConnect după IDNP-ul colectat din actul de identitate prezentat, iar ulterior se va face repetat contrapunerea biometriei imaginii foto din Registrul de stat al populației cu fotografia persoanei. Astfel, norma vizată trebuie să conțină descrierea acestui procedeu dar nu verificarea elementelor optice/vizuale/tactile ale actului de identitate.	Nu se acceptă Cerința de verificare a identității clientului este o cerință de bază a legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. Prin urmare, fie stabilirea relației de afaceri la ghișeu sau prin metode electronice, această cerință nu poate fi modificată.
	Banca Comercială Română Chișinău S.A.	163	Privitor la pct. 27 lit. a), d) și e) solicităm prevederile să fie unificate într-o singură prevedere.	Se acceptă parțial Punctul e) a fost exclus pentru a nu dubla cerința cu cea de la lit. d). Cât privește lit.a) menționăm că aceasta diferă ca și conținut și substanță și, prin urmare, nu poate fi exclusă.

care trebuie să fie prezente pe documentul de identitate prezentat de către client cu standardele aplicabile tipului respectiv de acte. e) verificarea corespunderii a cel puțin trei elemente de securitate ale actului de identitate, selectate aleatoriu, cu elementele de securitate proprii tipului respectiv de acte; f) în cazul existenței suspiciunilor privind identitatea persoanei sau autenticitatea documentelor prezentate vor fi adresate întrebări adiționale în scopul verificării identității persoanei și autenticității documentelor.	„Paymaster” SRL	164	La pct. 27 din proiect, opinăm asupra normelor excesive privind stabilirea autenticității unui act de identificare precum și a recunoașterii faciale a clientului de către entitățile raportoare, or entitățile raportoare nu au personal instruit și calificat în acest domeniu. Propunem excluderea acestui punct și expunerea unor detalieri privind pașii necesari a fi întreprinși în cazul unei suspiciuni de prezentare a unui act fals, în speță transmiterea informației privind suspiciunile respective către persoane abilitate, calificate și mandatate acest drept.	Nu se acceptă Cerința de verificare a identității clientului este o cerință de bază a legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului . Prin urmare, fie stabilirea relației de afaceri la ghișeu sau prin metode electronice, această cerință nu poate fi modificată.
	„Qiw-M” SRL	165	Considerăm aceste cerințe dificil de realizat, în special lit. a), d) si e). Sau aceste soluții urmează a fi aplicate la identificare neasistată ? Conform Ghidului EBA asemenea cerințe sunt înaintate entităților care accepta reproducere ale unor documente și nu examinează documentele în original. Propunem excluderea pct. 27 din motivul că este imposibil de realizat în cazul în care se aplică la identificarea video. Este foarte important să preluăm și să transpunem procesele e-KYC la maxim în corespundere cu Ghidul EBA/GL/2022/15, care la moment ia în considerare cele mai bune practici de e-KYC utilizate în UE.	Nu se acceptă Cerința de verificare a identității clientului este o cerință de bază a legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului . Prin urmare, fie stabilirea relației de afaceri la ghișeu sau prin metode electronice, această cerință nu poate fi modificată. De asemenea, menționăm că s-a exclus lit.e) în scopul evitării dublării prevederii.

Asociația băncilor din Moldova	166	- propunem a fi reformulate cerințele, deoarece procedura de identificare a clientului ar trebuie să conțină cerințe față de stabilirea identității clientului și nu de stabilire a autenticității actului de identitate. Mai simplu spus, din punct de vedere tehnic, pentru determinarea identității persoanei se va utiliza: imaginea facială (biometria punctelor de referință a feței) a imaginii din actul de identitate și a persoanei, iar ulterior, în caz de corespundere, se va face apel la MConnect după IDNP-ul colectat din actul de identitate prezentat, iar ulterior se va face repetat contrapunerea biometriei imaginii foto din Registrul de stat al populației cu fotografia persoanei. Astfel, norma vizată trebuie să conțină descrierea acestui procedeu dar nu verificarea elementelor optice/vizuale/tactile ale actului de identitate.	Nu se acceptă Cerința de verificare a identității clientului este o cerință de bază a legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului . Prin urmare, fie stabilirea relației de afaceri la ghișeu sau prin metode electronice, această cerință nu poate fi modificată.
	167	- Prevederile de la lit.d) și e) într-un fel se repetă. Astfel, se propune a unifica aceste două puncte.	Se acceptă S-a exclus lit.e) în scopul evitării dublării prevederii.

Pct. 28: (v2 – pct.28) În scopul verificării și validării datelor/informațiilor obținute de la client în procesul verificării video, entitatea raportoare este: a) obligată să verifice clientul sub aspectul: - implicării în activități teroriste sau de proliferare a armelor de distrugere în masă; - aplicării sancțiunilor internaționale; - aplicării sancțiunilor financiare ale Uniunii Europene; - deținerii calității de persoană expusă politic sau altor factori de risc sporit; - existenței informațiilor care ar putea influența reputația clientului, prin accesarea surselor credibile informaționale și/sau baze de date disponibile, public accesibile și/sau internet, inclusiv deținute de alte instituții publice și entități; - caracteristicilor comportamentale ale persoanei care pot indica un comportament suspect în timpul identificării video;	A.P. „Camera de Comerț Americană din Moldova”	168	Se propune excluderea prevederilor de la lit. a) a pct. 28 întrucât această secțiune este în afara obiectului de reglementare al prezentului Regulament, urmând să reglementeze doar procesul de identificare a clientului. În cadrul procesului de identificare la distanță, în special cel neasistat, aceste cerințe nu vor putea fi satisfăcute, or toate cazurile presupun existența factorului uman care va trebui să consulte toate sursele enumerate, să monitorizeze comportamentul clientului, factori care sunt disproporționați ca și efort, timp și posibilități în raport cu beneficiul urmărit.	Nu se acceptă. Prezentul Regulament are ca 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 în cazul stabilirii relațiilor de afaceri cu aceștia fără prezență fizică. Subsidiar, cerințele menționate urmează a fi coroborate cu cerințele din legislația cu prevenire și prevenirea și combatere a spălării banilor și finanțării terorismului.
	BC Energbank S.A.	169	La pct. 28 lit. a) „În scopul verificării și validării datelor/informațiilor obținute de la client în procesul verificării video, entitatea raportoare este obligată să verifice clientul sub aspectul 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” venim cu propunerea de a se indica ce se va întreprinde în cazul în care informația despre reputația clientului va fi negativă, ce măsuri vor fi aplicate în acest caz.	Comentariu: În cazul în care există factori care indică asupra gradului înalt de risc pe care clientul îl impune entității, aceasta din urmă este obligată să aplice măsuri de precauție sporite, conform cerințelor privind prevenirea și combaterea spălării banilor și finanțării terorismului. Subsidiar, se aplică, după caz, cerințele pct. 10 și/sau 28 din Regulament.
	OCN Microinvest SRL	170	Se propune excluderea alineatului 5 și 6 lit. a) pct. 28 din Regulament, întrucât în cadrul procesului de identificare la distanță, în special cel neasistat aceste cerințe nu vor putea fi satisfăcute, ori în toate cazurile presupune existența factorului uman careva trebui să consulte toate sursele enumerate, să	Nu se acceptă Cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt aplicate deopotrivă cu cerințele de

b) obligată să solicite informații despre natura și scopul relației de afaceri și/sau operațiunii și poate solicita prezentarea fizică la oficiul său, în cazul existenței suspiciunilor și/sau dubiilor în privința viciului de voință/consimțământ (presiuni sau influențe fizice sau psihologice) al clientului din partea terțelor persoane;			monitorizeze comportamentul clientului, factori care sunt disproporționați ca și efort, timp și posibilități în raport cu beneficiul urmărit.	stabilire a relațiilor de afaceri la distanță prin metode electronice.
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;	Asociația Businessului European	171	Pct. 28 propunem a fi exclus deoarece este impropriu obiectului de reglementare a proiectului de Regulament care se referă la cerințe față de identificarea persoanei.	Nu se acceptă Cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt aplicate deopotrivă cu cerințele de stabilire a relațiilor de afaceri la distanță prin metode electronice. În cazul în care există factori care indică asupra gradului înalt de risc pe care clientul îl impune entității, aceasta din urmă este obligată să aplice măsuri de precauție sporite, conform cerințelor privind prevenirea și combaterea spălării banilor și finanțării terorismului. Subsidiar, se aplică, după caz, cerințele pct. 10 și/sau 28 din Regulament.
d) obligată să verifice datele/informațiile primite prin intermediul comunicării electronice în conformitate cu prevederile reglementărilor în	B.C. MAIB S.A.	172	La pct.28 lit.b) din Regulament, propunem ca sintagma „natura și scopul” să fie înlocuită cu sintagma „scopul și natura dorită a”.	Se acceptă

domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.	173	La pct.28 lit.d) din Regulament, se utilizează sintagma „prin intermediul comunicării electronice în conformitate cu prevederile reglementărilor în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului”, fără a fi vreo referință la normele aplicabile ale legislației. Pentru a elimina neclarități, considerăm necesară completarea normei pct.28 lit.d) cu referință la normele aplicabile ale legislației în domeniul PCSBFT, care stabilesc cerințe /reguli privind mijloace de comunicare electronică.	Comentariu: Verificarea informației se face conform cerințelor legislației cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (de ex. pct.35 din Reg. 200/2018).
„Qiw-M” SRL	174	Luând în considerație că măsurile de precauție cu privire la client pe care trebuie să le întreprindă entitatea raportoare sunt prevăzute în Legea 308/2017, considerăm că pct. 28 nu se încadrează în conceptul proiectului Regulamentului cu privire la e-KYC. Cu atât mai mult, cerințele menționate în pct. 28 duc la distorsionarea și neeficientizarea procesului de e-KYC, fiind solicitată efectuarea verificărilor cu listele de sancțiuni, PEP etc. în timpul convorbirii video. Acest lucru va mări timpul convorbirii video, fapt care contravine esenței și scopului în sine a identificării la distanță. Conform bunelor practici verificările trebuie efectuate până la luarea deciziei de a iniția sau continua relația de afaceri cu clientul si nu neapărat în timpul convorbirii video / înregistrării video. În cazul în care nu s-a avut în vedere verificarea, nemijlocit, în timpul convorbirii video, propunem de reformulat textul sau de exclus art. 28.	Comentariu: Prevederile normei nu stabilesc verificarea și validarea datelor despre client în timpul transmisiunii video/foto. Acest exercițiu poate fi efectuat de către entitatea până la inițierea relației de afacere.

„Credimatic Network” SRL	175	Art. 28 paragraful a) prevede faptul că: În scopul verificării și validării datelor/ informațiilor obținute de la client în procesul verificării video, entitatea raportoare este: obligată să verifice clientul sub aspectul: caracteristicilor comportamentale ale persoanei care pot indica un comportament suspect în timpul identificării video. Dorim să menționăm că este imposibil de verificat din punct de vedere tehnic (fie prin soluții automatizate, fie prin soluții asistate de operator uman) a calificării comportamentului persoanei ca fiind suspect sau nu. În plus, sintagma de suspect nu este clar definită, în acest concept putând să fie asimilat orice comportament. Prin urmare, vă solicităm în mod respectuos eliminarea din Proiect a acestei cerințe.	Se acceptă
Asociația băncilor din Moldova	176	Se propune a fi exclus deoarece este impropriu obiectului de reglementare a proiectului de Regulament care se referă la cerințele față de identificarea persoanei. Totodată, prevederea menționată în proiect creează confuzii în privința acțiunilor care trebuie întreprinse de bancă pentru ”validarea datelor obținute”, având în vedere că clientul certifică veridicitatea datelor și informațiilor prezentate, iar banca are obligația de a le verifica.	Nu se acceptă Cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt aplicate deopotrivă cu cerințele de stabilire a relațiilor de afaceri la distanță prin metode electronice. În cazul în care există factori care indică asupra gradului înalt de risc pe care clientul îl impune entității, aceasta din urmă este obligată să aplice măsuri de precauție sporite, conform cerințelor privind prevenirea și combaterea spălării banilor și finanțării terorismului. Subsidiar, se aplică, după caz, cerințele pct. 10 și/sau 28 din Regulament.

Pct. 29: (v2 – pct.30) Entitatea raportoare este obligată să nu intre în relațiile de afaceri cu clientul urmare identificării video în următoarele cazuri: a) procedura de verificare video nu corespunde cerințelor prezentului Regulament; b) există suspiciuni în privința falsificării / nevalabilității semnăturii electronice/digitale, în situația când aceasta se utilizează; c) există suspiciuni privind existența presiunii și/sau influenței fizice/psihologice (viciul de voință) din partea terțelor persoane asupra clientului; d) actul de identitate prezentat este deteriorat; e) există o suspiciune de spălare a banilor sau de finanțare a terorismului;	Banca de Finanțe și Comerț S.A.	177	Proiectul de Regulament, nici Legea nr. 124/2022 nu conține prevederi aferent noțiunii "semnatura digitală" și/sau aplicabilitatea acestora.	Se acceptă
	B.C. MAIB S.A.	178	La pct.29 din Regulament, propunem ca sintagma „să nu intre în relațiile” să fie înlocuită cu sintagma „să nu inițieze relația”.	Se acceptă
	Banca Comercială Română Chișinău S.A.	179	La pct. 29 lit. d) după textul „deteriorat”, solicităm să fie inclusă sintagma “și/sau există suspiciuni sau elemente detectabile de falsificare acestuia”.	Se acceptă

f) există suspiciuni privind veridicitatea, suficiența și precizia datelor de identificare obținute.	„QIWI-M” SRL	180	Luând în considerație că cerințele față de identificarea video sunt exagerate, nerealizabile pe alocuri și nu corespund principiilor proiectului de Regulament cu privire la e-KYC, propunem excluderea pct. 29.	Nu se acceptă. Cerințele de prevenire și combatere a spălării banilor și finanțării terorismului sunt aplicate deopotrivă cu cerințele de stabilire a relațiilor de afaceri la distanță prin metode electronice.
	BC Energbank S.A:	181	Prevederile pct. 29 lit. f) „Entitatea raportoare este obligată să nu intre în relațiile de afaceri cu clientul urmare identificării video în cazul în care există suspiciuni privind veridicitatea, suficiența și precizia datelor de identificare obținute.”, nu se menționează nimic despre informația negativă a clientului.	Comentariu. „Informația negativă” despre client, poate fi luată în calcul la stabilirea nivelului de risc al clientului. Astfel, în cazul în care există factori care indică asupra gradului înalt de risc pe care clientul îl impune entității, aceasta din urmă este obligată să aplice măsuri de precauție sporite, conform cerințelor privind prevenirea și combaterea spălării banilor și finanțării terorismului. Subsidiar, se aplică, după caz, cerințele pct. 10 și/sau 28 din Regulament.
	Asociația băncilor din Moldova	182	Pentru o abordare uniformă de către bănci, considerăm oportun clarificarea calificativului ”deteriorat”, prin specificarea elementelor care să determine atribuirea acestui calificativ sau includerea referinței la vreun act normativ, dacă acesta există. Includerea noțiunii de ”deteriorat” sau specificarea elementelor care să determine atribuirea acestui calificativ, inclusiv cu includerea referinței la vreun act normativ, dacă acesta există.	Comentariu: Deteriorat este un proces de uzură sau stricăciune a unui bun din cauza întrebuințării îndelungate (ca exemplu în cazul BI: ilizibilitate asupra unor elemente sau a fotografiei etc).

	Ministerul Justiției	183	La pct. 29 lit. b), se va exclude textul „/digitale” având în vedere terminologia consacrată în Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere care operează nemijlocit cu noțiunea de „semnătură electronică avansată/calificată”.	Se acceptă
Capitolul V (v2 – cap.V)	Asociația Businessului European	184	Capitolul V propunem a fi exclus. Excluderea acestor prevederi este justificată de lipsa temeiului legal de instituire a unor astfel de cerințe. De menționat că identificarea persoanei la distanță se va realiza nu de angajatul entității raportoare dar de aplicație electronică setată conform unui anumit algoritm care la rândul său trebuie să asigure prin procedee tehnice corespunderea identificării persoanei. Deci, în cazul în care aplicația va fi produsul entității raportoare, atunci anume entitatea raportoare trebuie să dea asigurări că această aplicație este sigură iar în caz de externalizare, această sarcină va fi partajată cu compania vizată.	Nu se acceptă Prevederile cap.V setează cerințe aferente sistemului de control intern în contextul stabilirii relației de afacere la distanță prin metode electronice. Astfel, unele puncte setează cerințe pentru situații de utilizare a metodelor electronice cu implicarea operatorului uman, iar altele în lipsa acestuia.
	Asociația băncilor din Moldova	185	Capitolul V se propune a fi exclus. Rațiunea de excludere este justificată prin lipsa temeiului legal de instituire a unor astfel de cerințe. De menționat că identificarea persoanei la distanță se va realiza nu de angajatul entității raportoare dar de aplicația electronică setată conform unui anumit algoritm, care la rândul său trebuie să asigure prin procedee tehnice corespunderea identificării persoanei. Deci, în cazul în care aplicația va fi produsul entității raportoare, atunci entitatea raportoare trebuie să dea asigurări că această aplicație este sigură iar în caz de externalizare, această sarcină va fi partajată cu compania specializată.	Nu se acceptă Prevederile cap.V setează cerințe aferente sistemului de control intern în contextul stabilirii relației de afacere la distanță prin metode electronice. Astfel, unele puncte setează cerințe pentru situații de utilizare a metodelor electronice cu implicarea operatorului uman, iar altele în lipsa acestuia.

Pct. 30 : (v2 – pct.31) 30. În cazul în care entitatea raportoare externalizează integral sau parțial procesul de identificare la distanță a clienților către un furnizor de servicii externalizate, aceasta va aplica, înaintea și în timpul relației de afaceri cu furnizorul de servicii externalizate, următoarele măsuri, a căror amploare trebuie ajustată în funcție de risc: a) se asigură că furnizorul de servicii externalizate pune în aplicare în mod eficace și respectă politicile și procedurile de identificare la distanță a clienților entității în conformitate cu acordul de externalizare. Acest lucru trebuie realizat prin raportare periodice (cel puțin anuale), monitorizare continuă, vizite la fața locului sau teste prin eșantionare; b) efectuează evaluări pentru a se asigura că furnizorul de servicii externalizate este suficient	OCN Microinvest SRL	186	Se propune ca în tot pct. 30 din Regulament, precum și pe parcursul Regulamentului, termenul de “furnizor de servicii externalizate” să fie substituit cu termenul “prestator de servicii de încredere”, or capitolul respectiv este denumit “Identificarea prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022”, subsecvent și Legea nr. 308/2017 la art. 51 alin. 2), lit. c) se referă anume la prestatorii de servicii de încredere calificați, acreditați. Totodată, și cerințele de mai jos expuse le apreciem ca excesive în raport cu faptul, că, totuși prestatorul contractat este un prestator de servicii de încredere care a trecut toate verificările necesare ale instituțiilor statului și a fost acreditat și se prezumă că este extrem de securizat.	Comentariu: A fost definită noțiunea de „furnizor de servicii externalizate”. Cerințele de externalizare urmează a fi coroborate și cu prevederile art.10 din Legea 308/2017.
b) efectuează evaluări pentru a se asigura că furnizorul de servicii externalizate este suficient	A.P. „Camera de Comerț Americană din Moldova”	187	Se propune excluderea prevederilor de la lit. b) a pct. 30. Activitatea prestatorului de servicii de încredere reprezintă o activitate în domeniul protecției criptografice și tehnice a informației și este supusă licențierii în conformitate cu legislația în domeniul reglementării prin licențiere a activității de întreprinzător. De asemenea, Serviciul de Informații și Securitate al Republicii Moldova, este responsabil de exercitarea controlului în domeniul serviciilor de încredere și efectuează acreditarea prestatorilor de servicii de încredere și retrace statutul respectiv.	Nu se acceptă Prevederile Regulamentului au fost suplinite cu noțiunea de „furnizor de servicii externalizate” pentru a reda claritate asupra termenului utilizat. De asemenea, cerințele de externalizare urmează a fi coroborate și cu prevederile art.10 din Legea 308/2017. În acest context, entitatea urmează să se asigure că relația cu un furnizor de servicii de

de echipat și capabil să efectueze procesul de identificare la distanță a clienților. Evaluările pot include, dar nu se limitează la evaluarea formării personalului, a adecvării tehnologice și a guvernantei datelor la furnizorul de servicii externalizate;			Entitatea raportoare poate decide contractarea unui prestator de servicii de încredere anume din considerentul că nu deține resursele/cunoștințele necesare în domeniu. Tot la pct. 30, precum și pe parcursul textului Regulamentului, se propune ca termenul de „furnizor de servicii externalizate” să fie substituit cu termenul „prestator de servicii de încredere”, or capitolul respectiv este denumit „Identificarea prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022”, subsecvent și Legea nr. 308/2017 la art. 51 alin. 2), lit. c) se referă anume la prestatorii de servicii de încredere calificați, acreditați.	externalizare se desfășoară în condiții de siguranță și nu impune un risc suplimentar de SBFT.
c) în caz de necesitate să solicite un audit complex, aferent procesului de identificare, conform standardelor internaționale în domeniu; d) se asigură că furnizorul de servicii externalizate informează entitatea cu privire la orice propunere de modificare a procesului de identificare la distanță a clienților sau cu privire la orice modificare adusă soluției furnizate de furnizorul de servicii externalizate; e) există mecanisme adecvate de confidențialitate în ceea ce	Asociația Businessului European	188	În cazul în care nu se acceptă excluderea în totalmente a Capitolului V, rugăm operarea următoarelor modificări: Pct. 30 litera b) Rugăm să fie exclus acest punct din următoarele considerente: Activitatea prestatorului de servicii de încredere reprezintă o activitate în domeniul protecției criptografice și tehnice a informației și este supusă licențierii în conformitate cu legislația în domeniul reglementării prin licențiere a activității de întreprinzător. De asemenea, Serviciul de Informații și Securitate al Republicii Moldova, este responsabil de exercitarea controlului în domeniul serviciilor de încredere și efectuează acreditarea prestatorilor de servicii de încredere și retrage statutul respectiv. Entitatea raportoare poate decide contractarea unui prestator de servicii de încredere anume din considerentul că nu deține resursele/cunoștințele necesare în domeniu.	Nu se acceptă Pentru ca entitatea să se asigure că aplicarea cerințelor de către o parte terță corespunde actelor normative în vigoare, inclusiv aferente domeniului PCSBFT și de stabilire a relațiilor la distanță prin metode electronice, aceasta urmează să evalueze modul în care partea terță va fi capabilă să implementeze cerințele care derivă din actele normative. Prin urmare, o altă modalitate de înțelegere a unei părți terțe despre capacitatea acesteia de a aplica cerințele menționate decât printr-un proces de evaluare, momentan, nu este clar cum poate fi determinat.

privește datele și alte informații; f) există o analiză aprofundată, bazată pe riscuri, a funcțiilor, a datelor și a sistemelor asociate care sunt avute în vedere pentru externalizare sau care au fost externalizate și să abordeze riscurile potențiale, în special riscurile operaționale, inclusiv riscurile de natură juridică, TIC, de conformitate și reputațional, precum și limitările de supraveghere aferente țărilor în care sunt sau pot fi furnizate serviciile externalizate și în care datele sunt stocate sau este posibil să fie stocate.	B.C. MAIB S.A.	189	La pct.30 lit. c) din Regulament, considerăm necesară completarea normei cu referința la standardele internaționale în domeniul auditului, care s-au avut în vedere.	Se acceptă Au fost adăugate unele referințe la standardele internaționale pe care un auditor urmează să le utilizeze în eventualitatea organizării unui proces de verificare a procesului de identificare.
	„Qiwi-M” SRL	190	Nu este clar la care standarde internaționale se face referință. Totodată, astfel de cerință este dificil de îndeplinit, fiind solicitat un audit complex conform standardelor internaționale, dar în același timp fiind reglementat la nivel național prin Legea 124/2022. Astfel de cerințe nu pot fi aplicate prestatorilor de servicii de încredere înregistrați conform Legii 124/2022. Se propune a exclude lit. c) al pct. 30	Se acceptă. Au fost adăugate unele referințe la standardele internaționale pe care un auditor urmează să le utilizeze în eventualitatea organizării unui proces de verificare a procesului de identificare.

Pct. 32: (v2 – pct.33) Angajatul entității raportoare responsabil de efectuarea identificării prin mijloace electronice a clientului trebuie să dispună de un nivel de calificare profesională suficientă în domeniul identificării clienților, în vederea prevenirii spălării banilor și combaterii finanțării terorismului, care include: a) cel puțin 5 ani experiență; b) dispune de o instruire specială în scopul identificării prin mijloace electronice a clienților; c) dispune de cunoștințe suficiente despre reglementările aplicabile în materie de prevenirea și combaterea spălării banilor și a finanțării terorismului; d) dispune de cunoștințe suficiente despre aspectele de securitate ale verificării la distanță și care este suficient de instruit pentru	Banca de Finanțe și Comerț S.A.	191	În primul rând necesar de subliniat că acest punct nu este aplicabil pentru entitățile care au ales calea efectuării eKYC automată fără participarea angajatului nemijlocit în procesul verificării identității. În al doilea rând în punctul dat sunt enumerate cerințe aferent nivel de calificare profesională suficientă în domeniul identificării clienților care sunt imposibil de respectat: 1. 5 ani de experiență în circumstanțe că cerința legislativă a apărut 3 luni în urma este imposibil de executat 2. Până la ziua de astăzi nu a fost desfășurată nici o instruire specială în scopul identificării prin mijloace electronice a clienților, dar cele a țărilor vecine nu sunt aplicabile pentru țara noastră din motivul divergențelor în legislația 3. Ariile de prevenirea și combaterea spălării banilor și a finanțării terorismului și cea de riscuri operaționale (nemijlocit legate preveni utilizarea intenționată sau deliberată a tehnicilor de înșelăciune) sunt masive și în practica de aceste se ocup angajații diferiți. Suplimentar, identificarea clientului presupune introducerea datelor în sistem ceea ce prezintă activitatea operațională. Sensul cerințelor față de angajat în califică ca ofițer conformitate, care conform prevederilor Regulamentului 322 p. 204 nu poate fi implicat în activități operaționale Propunerea:	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat. Totodată, entitatea are obligația să-și dezvolte mecanisme, proceduri și procese în scopul minimizării implicării entității în riscuri operaționale, legale, reputaționale, de spălarea a banilor și finanțare a terorismului etc.
--	--	------------	--	--

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.			1. De a concretiza aplicabilitatea acestui punct pentru diferite metode de eKYC 2. De a revizui cerințe aferent angajatului responsabil, divizarea responsabilităților din punct de vedere măsurilor aplicate (identificarea, control, etc).	
	A.P. „Camera de Comerț Americană din Moldova”	192	La pct. 32, urmează a fi specificată expres procedura de identificare electronică la care se face referire, soluția din pct. 24 sau soluția din pct. 25. În conformitate cu prevederile de la Capitolul IV lit. B, pct. 25, în care identificarea se face neasistat, nu are justificare limitarea experienței de 5 ani, prevăzută la pct. 32, lit. a). Pentru soluția din pct. 24, chiar dacă poate fi necesar ca la momentul identificării să fie contactat audio un reprezentant al entității raportoare care are o experiență suficientă, pentru soluția de la pct. 25 de identificare neasistată putem face o analogie dintre o identificare fizică a clientului de către expertul financiar-bancar care efectuează o analiză a clientului și ceea ce vede pe actele de identitate și a raportului din ASP dacă datele din buletin sunt reale și coincid. Atât timp cât prima persoană care efectuează verificarea conform principiului primei linii de apărare/control, care este analogul fizic al expertul financiar bancar/nebancar, iar o altă persoană efectuează o reverificare, drept o a 2-a linie de control - nu considerăm necesar ca persoana care efectuează lucru operațional analogic unui expert financiar bancar/nebancar care poate avea și studii de colegiu/licență pentru a activa, în cazul identificării electronice să aibă nevoie de 5 ani de experiență. În temeiul celor menționate se propune următoarea redacție a pct. 32, a):	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat.

		„cel puțin 1 an experiență, pentru angajații responsabili de control și asigurare a procedurilor interne în domeniul combaterii spălării banilor și finanțării terorismului”.	
A.P. „Camera de Comerț Americană din Moldova”	193	La pct. 32, lit. b) urmează a fi clarificat ce înseamnă o instruire specială și care sunt entitățile care efectuează aceste instruiri speciale. În temeiul celor menționate se propune următoarea redacție a pct. 32, b): <i>„b) dispune de o instruire specială în scopul identificării prin mijloace electronice a clienților, sau a riscurilor de spălare a banilor și finanțare a terorismului;”.</i>	Comentariu: Entitatea raportoare are obligație de a instrui angajații în scopul aplicării eficiente a politicilor și procedurilor interne cu referire la identificarea clienților la distanță prin metode electronice și în scopul implementării cerințelor de prevenire și combatere a spălării banilor și finanțare a terorismului.
OCN Microinvest SRL	194	Se propune includerea la pct. 32 din Regulament, după fraza: “responsabil de efectuarea identificării” a cuvântului “asistată”, or doar în acest caz este implicat un angajat al entității raportoare. Se propune la pct. 32 lit. a) din Regulament, a exclude cerința cu referire la termenul de 5 ani sau cel puțin de a reduce termenul de 5 ani la un an, și excluderea literei b) din pct. 32 din Regulament odată ce litera c) și d) pct.32 înglobează aceste criterii în comun și se prezumă că angajatul dispune de cunoștințele necesare în raport cu și în vederea asigurării scopului urmărit în materie de prevenire și combatere a spălării banilor și prevenirii terorismului.	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat.

BC Comerțbank S.A.	195	Urmează a fi specificată expres procedura de identificare electronică la care se face referire, soluția din pct. 24 sau soluția din pct. 25. În conformitate cu prevederile de la Capitolul IV lit. B, pct. 25, în care identificarea se face neasistat, nu are justificare limitarea experienței de 5 ani, prevăzută la pct. 32, lit. a). Pentru soluția din pct. 24, chiar dacă poate fi necesar ca la momentul identificării să fie contactat audio un reprezentant al entității raportoare care are o experiență suficientă, pentru soluția de la pct. 25 de identificare neasistată putem face o analogie dintre o identificare fizică a clientului de către expertul financiar-bancar care efectuează o analiză a clientului și ceea ce vede pe actele de identitate și a raportului din ASP dacă datele din buletin sunt reale și coincid. Atât timp cât prima persoană care efectuează verificarea conform principiului primei linii de apărare/control, care este analogul fizic al expertul financiar bancar/nebancar, iar o altă persoană efectuează o reverificare, drept o a 2-a linie de control - nu considerăm necesar ca persoana care efectuează lucru operațional analogic unui expert financiar bancar/nebancar care poate avea și studii de colegiu/licență pentru a activa, în cazul identificării electronice să aibă nevoie de 5 ani de experiență. În temeiul celor menționate se propune următoarea redacție a pct. 32, a): <i>„cel puțin 1 an experiență, pentru angajații responsabili de control și asigurare a procedurilor</i>	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat. Totodată, entitatea raportoare are obligația de a instrui angajații în scopul aplicării eficiente a politicilor și procedurilor interne cu referire la identificarea clienților la distanță prin metode electronice și în scopul implementării cerințelor de prevenire și combatere a spălării banilor și finanțare a terorismului.
--------------------	-----	---	---

B.C. „ProCredit Bank” S.A.	196	<i>interne în domeniul combaterii spălării banilor și finanțării terorismului”.</i> La pct. 32, lit. b) urmează a fi clarificat ce înseamnă o instruire specială și care sunt entitățile care efectuează aceste instruiți speciale. În temeiul celor menționate se propune următoarea redacție a pct. 32, b): <i>„b) dispune de o instruire specială în scopul identificării prin mijloace electronice a clienților, sau a riscurilor de spălare a banilor și finanțare a terorismului”.</i> Cu referire la punctul.32, lit.a) din cap.V, solicităm reducerea numărului minim de ani de experiență până la maxim 1 an. Considerăm ca este un termen rezonabil pentru acumularea unui nivel de calificare profesională suficientă, având în vedere și alte mecanisme de control intern impuse de legislația în vigoare și prezentul regulament. De asemenea, cu referire la punctul 32, lit. b), solicităm să fie specificat privind instruirea – dacă se solicită o instruire externă sau internă (organizată de entitatea raportoare) și dacă va fi necesară obținerea unui certificat confirmativ.	
-------------------------------	-----	---	--

Banca Comercială Română Chișinău S.A.	197	La pct. 32 lit. a) solicităm să fie furnizate clarificări privitor la experiența în ce domeniu și/sau zone de deservire ale clienților. Privitor la pct. 32 lit. b) și d) solicităm să fie furnizate clarificări privitor la instruirile speciale și cunoștințele suficiente, care sunt cerințele prin care entitățile raportoare urmează să aprecieze suficiența acestora, fie care sunt condițiile care prezumă și asigură îndeplinirea condiției de instruirile speciale și cunoștințele suficiente Pentru pct. 32 și 36, solicităm să fie elaborate de BNM ghiduri cu îndrumări, clarificări/exemplificări detaliate, pentru asigurarea aplicării uniforme a clauzelor specificate.	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat. Totodată, entitatea raportoare are obligația de a instrui angajații în scopul aplicării eficiente a politicilor și procedurilor interne cu referire la identificarea clienților la distanță prin metode electronice și în scopul implementării cerințelor de prevenire și combatere a spălării banilor și finanțare a terorismului.
Asociația Businessului European	198	La pct. 32 lit. a), textul „5 ani” considerăm necesar a fi substituit cu textul „3 ani”; Micșorarea termenului experienței de muncă la moment este foarte exagerat, și va crea dificultăți la identificarea persoanelor necesare. Considerăm cerința de experiența de munca 5 ani disproporționată, dacă autorii proiectului au avut în vedere că experiența se refera la orice activitate. În situația în care autorii proiectului au avut în vedere că experiența persoanei trebuie să fie pe domeniul AML și identificare e-KYC, atunci această prevedere ar putea aduce un blocaj în implementare pentru că acestea sunt atribuții noi pe piața muncii. Considerăm că termenul de 3 ani experiență generală de muncă sau 1 an AML/identificare e-KYC sunt cerințe suficiente pentru aceste competențe.	Comentariu. Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat.

		Experiență în ce domeniu? Reglementarea identificării prin mijloace electronice abia se elaborează, nu sunt specialiști în acest domeniu cu experiență de 5 ani. Rugăm să fie reglementat cum este necesar de demonstrat această experiență AML/CFT sau cum se va calcula aceasta experiență?! Din momentul angajării, semnării fișei de post sau din considerentul participării la anumite instruirii, training-uri?	
BC Energbank S.A.	199	La pct. 32 lit. a) „Angajatul entității raportoare responsabil de efectuarea identificării prin mijloace electronice a clientului trebuie să dispună de un nivel de calificare profesională suficientă în domeniul identificării clienților, în vederea prevenirii spălării banilor și combaterii finanțării terorismului, care include cel puțin 5 ani experiență”, considerăm relevant indicarea expresă în ce domeniu trebuie să dețină experiență angajatul entității raportoare.	Comentariu: Nivelul de experiență a fost modificat. Cunoștințele și abilitățile pe care trebuie să le posedă angajatul urmează a fi în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului și a parcurgerii procesului de identificare a clienților la distanță prin metode electronice.
B.C. MAIB S.A.	200	La pct.32 din Regulament, propunem completarea expresă, că <i>”angajatul entității raportoare responsabil de efectuarea identificării prin mijloace electronice a clientului”</i> este angajatul din prima linie (adică din subdiviziunea de business) și nu este vorba despre specialistul din domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, întru evitarea interpretării prevederilor și cerințele din pct.32, litera a)-d) sunt aplicabile față de angajatul din prima linie.	Comentariu: Nivelul de experiență a fost modificat. Cunoștințele și abilitățile pe care trebuie să le posedă angajatul urmează a fi în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului și a parcurgerii procesului de identificare a clienților la distanță prin metode electronice. Entitatea raportoare stabilește din care subdiviziune sunt angajații responsabili de procesul de identificare la distanță prin metode electronice, fie din business sau alte subdiviziuni.

„Paymaster” SRL	201	Pct. 32 din proiect, este exagerat și greu realizabil, or piața resurselor umane din R. Moldova este limitată ca număr de persoane care pot un angajate cu cerințele specificate la acest punct.	Comentariu: A fost modificată prevederea dată în scopul micșorării nivelului de experiență necesar unui angajat pentru a putea fi încadrat în procesul de identificare a clienților la distanță prin metode electronice.
„QIWI-M” SRL	202	Conform practicilor și recomandărilor UE , în cazul în care se utilizează soluții de înregistrare la distanță a clienților care beneficiază de asistență, în cadrul cărora clientul interacționează cu un angajat pentru a efectua procesul de verificare, angajatul care participă la identificare trebuie să aibă suficiente cunoștințe despre reglementările aplicabile în materie de combatere a spălării banilor și a finanțării terorismului și 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; De asemenea, în prezent, se aplică și proceduri de control în 4 ochi, unde procesul de verificare și validare este separat. Astfel, considerăm cu certitudine că cerința de experiență de 5 ani a angajatul entității responsabil de e-KYC este excepțional de exagerată, ținând cont de faptul că reglementarea la nivel național a domeniului de identificare la distanță este la etapa incipientă. Astfel de cerințe, de asemenea, contravin principiului de asigurare a unui proces fiabil de	Comentariu: A fost modificată prevederea dată în scopul micșorării nivelului de experiență necesar unui angajat pentru a putea fi încorporat în procesul de identificare a clienților la distanță prin metode electronice.

		înregistrare a clienților la distanță, impunând entităților condiții greu de realizat și care nu asigură continuitatea afacerii și procesului de eKYC.	
„Nova Pay” SRL	203	La pct. 32, urmează a fi specificată expres procedura de identificare electronică la care se face referire, soluția din pct. 24 sau soluția din pct. 25. În conformitate cu prevederile de la Capitolul IV lit. B, pct. 25, în care identificarea se face neasistat, nu are justificare limitarea experienței de 5 ani, prevăzută la pct. 32, lit. a). Pentru soluția din pct. 24, chiar dacă poate fi necesar ca la momentul identificării să fie contactat audio un reprezentant al entității raportoare care are o experiență suficientă, pentru soluția de la pct. 25 de identificare neasistată putem face o analogie dintre o identificare fizică a clientului de către expertul financiar-bancar care efectuează o analiză a clientului și ceea ce vede pe actele de identitate și a raportului din ASP dacă datele din buletin sunt reale și coincid. Atât timp cât prima persoană care efectuează verificarea conform principiului primei linii de apărare/control, care este analogul fizic al expertul financiar bancar/nebancar, iar o altă persoană efectuează o reverificare, drept o a 2-a linie de control - nu considerăm necesar ca persoana care efectuează lucru operațional analogic unui expert financiar bancar/nebancar care poate avea și studii de colegiu/licență pentru a activa, în cazul	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman. De asemenea, nivelul de experiență a fost modificat, la 2 ani.

		identificării electronice să aibă nevoie de 5 ani de experiență. În temeiul celor menționate se propune următoarea redacție a pct. 32, a): „cel puțin 1 an experiență, pentru angajații responsabili de control și asigurare a procedurilor interne în domeniul combaterii spălării banilor și finanțării terorismului”.	
Asociația băncilor din Moldova	204	Pct.32 - lit.a) se solicită reducerea numărului minim de ani de experiență până la maxim 1 an. Considerăm ca este un termen rezonabil pentru acumularea unui nivel de calificare profesională suficientă, având în vedere și alte mecanisme de control intern impuse de legislația în vigoare și prezentul regulament. - lit.b) cerințele incluse pentru angajatul responsabil de efectuarea identificării prin mijloace electronice a clientului par a fi disproporționale (cu excepția metodei specificate la pct.24), ținând cont de: · măsurile de control încorporate și cerințele față de soluțiile de identificare prin mijloace electronice; · cerințele de control intern aplicabile băncilor pe partea de guvernanță generală (modelul celor 3 linii de apărare); · cerințele de control intern în domeniul prevenirii spălării banilor și finanțării terorismului. Astfel, considerăm exagerate/neclare următoarele cerințe: a) cerința de experiență de minim 5 ani – până la implementarea soluției de identificare prin mijloace electronice se efectuează o evaluare a riscurilor cu descrierea și implementarea măsurilor de control a	Comentariu: Nivelul de experiență a fost modificat, la 2 ani. Cunoștințele și abilitățile pe care trebuie să le posede angajatul urmează a fi în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului și a parcurgerii procesului de identificare a clienților la distanță prin metode electronice. Tipul instruirii este stabilit de către entitate, fie cu experții intern sau din exterior.

			acestora. Astfel, dacă măsurile de control sunt suficiente, iar soluția poate fi pusă la dispoziția personalului responsabil de relația cu clienții, atunci această cerință va fi imposibil de respectat, ținând cont inclusiv de situația dificilă cu suficiența personalului în acest domeniu. Astfel, considerăm că experiența de 1 an ar fi suficientă în acest scop; b) cerința de „instruire specială” – în lipsa unor concretizări, considerăm că această cerință ar putea fi asigurată prin instruirea internă obișnuită, doar că dedicată acestui subiect. Se propune ajustarea redacției reieșind din argumentele aduse, pentru o clarificare suficientă și o bună înțelegere a modului de aplicare, ceea ce va determina o abordare uniformă de către bănci. - se solicită să se specifica privind instruirea – dacă se solicită o instruire externă sau internă (organizată de entitatea raportoare) și dacă va fi necesară obținerea unui certificat confirmativ.	
Pct.33 : (v2 – pct.33 lit.b)) 33. Identificarea video a clientului este efectuată într-o încăpere, fizic separată de alte încăperi, în cadrul oficiului entității raportoare, care se află sub control constant și supraveghere video și are acces limitat doar pentru angajații autorizați, și care asigură cel puțin: a) o calitate suficientă a informației audiovizuale,	Banca de Finanțe și Comerț S.A.	205	Acest punct nu este aplicabil pentru entitățile care au ales calea efectuării eKYC automată fără participarea angajatului nemijlocit în procesul verificării identității. <u>Propunerea:</u> De a concretiza aplicabilitatea acestui punct pentru diferite metode de eKYC	Comentariu: Cerințele punctului dat urmează a fi respectate de către entitate la stabilirea relației de afaceri cu clienții la distanță prin metode electronice asistate de operator uman.
	A.P. „Camera de Comerț Americană din Moldova”	206	Obligația entității raportoare prevăzută la pct. 33 se consideră neproportională atât timp cât identificarea clienților se face cu respectarea principiilor de securitate, păstrare a	Se acceptă Prevederea dată a fost modificată.

precum și confidențialitatea acesteia; b) lipsa altor persoane și/sau obiecte în fața camerei video, precum și lipsa oricăror zgomote ce pot compromite calitatea informației.		confidențialității și cu interdicția accesului altor persoane decât angajații entității raportoare la calculatoarele angajaților responsabili de această identificare. Se propune excluderea sintagmei „în cadrul oficiului entității raportoare” precum și cerința de supraveghere video continuă or unul din motivele principale și necesare a identificării prin mijloace electronice a fost și apariția pandemiei Covid19 care practic a sistat activitatea pentru o perioadă determinată de timp. Pe de altă parte, însuși procesul de identificare la distanță, în redacția propusă nu va putea fi externalizat la un furnizor de servicii. Totodată, includerea obligativității deținerii unei încăperi speciale destinate pentru procesul de identificare prin mijloace electronice va presupune costuri semnificative de implementare iar în cazurile în care va apărea necesitatea de a munci de la distanță cum are loc în cazuri de pandemie, boală, greve alte incidente care nu permit prezența fizică la serviciu, această cerință practic va bloca întreaga soluție de identificare la distanță.	
--	--	--	--

BC Comerțbank S.A.	207	Obligația entității raportoare prevăzută la pct. 33 se consideră neproportională atât timp cât identificarea clienților se face cu respectarea principiilor de securitate, păstrare a confidențialității și cu interdicția accesului altor persoane decât angajații entității raportoare la calculatoarele angajaților responsabili de această identificare. Se propune excluderea sintagmei „în cadrul oficiului entității raportoare” precum și cerința de supraveghere video continuă or unul din motivele principale și necesare a identificării prin mijloace electronice a fost și apariția pandemiei Covid19 care practic a sistat activitatea pentru o perioadă determinată de timp. Pe de altă parte, însuși procesul de identificare la distanță, în redacția propusă nu va putea fi externalizat la un furnizor de servicii. Totodată, includerea obligativității deținerii unei încăperi speciale destinate pentru procesul de identificare prin mijloace electronice va presupune costuri semnificative de implementare iar în cazurile în care va apărea necesitatea de a munci de la distanță cum are loc în cazuri de pandemie, boală, greve alte incidente care nu permit prezența fizică la serviciu, această cerință practic va bloca întreaga soluție de identificare la distanță.	Se acceptă Prevederea dată a fost modificată.
--------------------	-----	--	---

--	--	--	--

„Qiwi-M” SRL	208	Considerăm că cerința este exagerată. Luând în considerație că astăzi angajații pot lucra și de la distanță, iar accesul angajatului în sistem este securizat și corespunde cerințelor de securitate aferente TIC (restricționat prin datele de autentificare (login, parola, etc.), iar convorbirea video, în sine, se înregistrează de către sistem – nu sunt necesare astfel de cerințe restrictive față de angajați și mediul în care se face identificarea. Entitatea de sine stătător stabilește scenarii și asigură corespunderea procesului riscurilor identificate. Astfel nu este argumentată cerința de control constant și video, inclusiv cu acces limitat – cu atât mai mult că aceste persoane pot efectua și identificarea față în față la necesitate. Propunem de exclus pct. 33 și de transpus cerințele minime față de tipurile de procese de identificare la distanță prevăzute în Ghidul EBA/GL/2022/15	Se acceptă Prevederea dată a fost modificată.
--------------	-----	---	---

OCN Microinvest SRL	209	Se propune la pct. 33 din Regulament, ca sintagma „în cadrul oficiului entității raportoare” precum și cerința de supraveghere video continuă să fie exclusă, or unul din motivele principale și necesare a identificării prin mijloace electronice a fost și apariția Covid în 2020 care practic a sistat activitatea o perioada determinată de timp. Pe de altă parte, însuși procesul de identificare la distanță, în redacția propusă nu va putea fi externalizat la un furnizor de servicii. Totodată, includerea obligativității deținerii unei încăperi speciale destinate pentru procesul de identificare prin mijloace electronice va presupune costuri semnificative de implementare, iar în cazurile în care va apărea necesitatea de a munci de la distanță cum are loc în cazuri de pandemie, boală, greve alte incidente care nu permit prezența fizică la serviciu, această cerință practic va bloca întreaga soluție de identificare la distanță.	Se acceptă parțial Prevederea dată a fost modificată.
---------------------	-----	--	---

„Nova Pay” SRL	210	Obligația entității raportoare prevăzută la pct. 33 se consideră neproportională atât timp cât identificarea clienților se face cu respectarea principiilor de securitate, păstrare a confidențialității și cu interdicția accesului altor persoane decât angajații entității raportoare la calculatoarele angajaților responsabili de această identificare. Se propune excluderea sintagmei „în cadrul oficiului entității raportoare” precum și cerința de supraveghere video continuă or unul din motivele principale și necesare a identificării prin mijloace electronice a fost și apariția pandemiei Covid19 care practic a sistat activitatea pentru o perioadă determinată de timp. Pe de altă parte, însuși procesul de identificare la distanță, în redacția propusă nu va putea fi externalizat la un furnizor de servicii. Totodată, includerea obligativității deținerii unei încăperi speciale destinate pentru procesul de identificare prin mijloace electronice va presupune costuri semnificative de implementare iar în cazurile în care va apărea necesitatea de a munci de la distanță cum are loc în cazuri de pandemie, boală, greve alte incidente care nu permit prezența fizică la serviciu, această cerință practic va bloca întreaga soluție de identificare la distanță.	Se acceptă Prevederea dată a fost modificată.
----------------	-----	---	---

	Asociația băncilor din Moldova	211	Considerăm că această prevedere nu este aplicabilă soluțiilor de identificare neasistate. Suplimentar, în cazul aplicării metodei specificate la pct.24, aceste cerințe nu sunt aliniate scopului implementării soluțiilor de identificare la distanță, deoarece acestea ar trebui să fie utilizate în perioade de criză care nu permit deplasarea angajaților la locul de muncă și apare necesitatea de a munci de la distanță. Se solicită revizuirea prevederilor pct. 33.	Se acceptă Prevederea dată a fost modificată.
--	--------------------------------	-----	--	---

Capitolul IV, lit. B (v2 – <i>cap.IV secțiunea 1)</i>)	A.P. „Camera de Comerț Americană din Moldova”	212	Considerăm necesară expunerea textului în redacția propunerii de la pct. 15, lit. b). În cazul în care nu va fi modifică redacția acestui punct nu vor putea fi aplicate prevederile Legii nr. 308/2017, art. 5' alin. (2) lit. b).	Comentariu: Au fost redactate prevederile cap.IV și titlurile secțiunilor.
Pct. 34: (v2 – <i>pct.34</i>) Persoana cu funcție de conducere de rang superior trebuie să se asigure că politicile și procedurile de înregistrare la distanță a clienților sunt puse în aplicare în mod eficace, revizuite periodic și modificate, dacă este necesar.	A.P. „Camera de Comerț Americană din Moldova”	213	Propunem următoarea redacție: „Persoana cu funcție de conducere de rang superior trebuie să se asigure că politicile și procedurile de identificare la distanță a clienților sunt puse în aplicare în mod eficace, revizuite periodic și modificate, dacă este necesar”.	Comentariu: Prevederile punctului dat au fost redactate pentru a aduce claritate vis-a-vis de procesul de stabilire a relației de afaceri la distanță.
	BC Comerțbank S.A.	214	„Persoana cu funcție de conducere de rang superior trebuie să se asigure că politicile și procedurile de identificare la distanță a clienților sunt puse în aplicare în mod eficace, revizuite periodic și modificate, dacă este necesar”.	Comentariu: Prevederile punctului dat au fost redactate pentru a aduce claritate vis-a-vis de procesul stabilire a relației de afaceri la distanță.
Pct. 35: (v2 – <i>pct.35</i>) 35. În funcție de riscul de spălare a banilor sau de finanțare a terorismului asociat relației de afaceri sau a altor riscuri asociate, entitatea raportoare va utiliza unul sau mai multe dintre următoarele controale: a) efectuarea primei plăți dintr-un cont de plăți deținut de către client într-o altă entitate raportoare dintr-o jurisdicție în care există cerințe de combatere	A.P. „Camera de Comerț Americană din Moldova” Asociația Businessului European	215	La pct. 35, lit. a) este necesară, pentru claritate, reformularea sintagmei „ <i>nu mai puțin similare</i> ”.	Se acceptă

a) spălării banilor sau a finanțării terorismului nu mai puțin similare decât cele din Republica Moldova; b) trimiterea către client a unui cod de acces generat aleatoriu pentru a confirma prezența acestuia în timpul procesului de verificare la distanță. Codul de acces trebuie să fie un cod de unică folosință și pentru o perioadă limitată de timp; c) colectarea de date biometrice pentru a le compara cu datele colectate din alte surse independente și fiabile; d) efectuarea unei tranzacții dintr-un cont de plăți al clientului deținut într-o altă entitate raportoare, inclusiv prin utilizarea unui instrument de plată; e) contactarea telefonică a clientului; f) corespondență directă (atât electronică, cât și poștală) către client.	B.C. MAIB S.A.	216	La pct.35 lit.a) din Regulament, considerăm necesară modificarea /reformularea prin concretizarea sintagmei „nu mai puțin similare decât cele din Republica Moldova”.	Se acceptă
		217	La pct.35 lit.c) din Regulament, propunem ca sintagma „independente și fiabile” să fie înlocuită cu sintagma „sigure și independente”, analogic terminologiei utilizate în textul Legii nr.308/2017.	Se acceptă
	„QIWI-M” SRL	218	Considerăm cerințele de la lit. a) și d) se suprapun. Se propune revizuirea și reformularea acestora. Un alt moment este faptul, că în lit. c) se face referință la biometrie, însă pe parcursul regulamentului astfel de referință nu se face și nu este definită noțiunea de biometrie. Prin urmare este necesară ajustarea proceselor prevăzute în proiectul Regulamentului, inclusiv prin specificarea modului și tipului de date biometrice colectate.	Se acceptă Se acceptă A fost definită noțiunea de „date biometrice”.

Pct. 36 : (v2 – pct.36 modificat) În cazul în care entitatea raportoare acceptă reproducere ale unui document original și nu examinează documentul original, aceasta va lua măsuri pentru a se asigura că reproducerea este fiabilă. Astfel, entitatea va stabili, cel puțin, următoarele: a) dacă reproducerea include elemente de securitate încorporate în documentul original și dacă specificațiile documentului original care sunt reproduse sunt valabile și acceptabile, în special tipul, dimensiunea caracterelor și structura documentului, prin compararea acestora cu bazele de date oficiale; b) dacă datele cu caracter personal au fost schimbate sau modificate în alt mod sau, după caz, dacă imaginea clientului inclusă în document nu a fost înlocuită; c) dacă se menține integritatea algoritmului	Banca Comercială Română Chișinău S.A.	219	Privitor la pct. 36 lit. c) solicităm furnizarea unor clarificări privitor la “menținerea integrității algoritmului utilizat pentru a genera numărul unic de identificare al documentului original”	Comentariu: Fiecare act de identitate emis identifică o persoană fizică în mod unic, prin crearea unui număr succesiv de litere/cifre care sunt dispuse după o anumită regulă/algoritm. Prevederea Regulamentului este ca în astfel de situații, entitatea să se asigure că această regulă sau algoritm utilizat este integru. Totodată, menționăm că prezentul punct a fost exclus, iar unele cerințe au fost încorporate la pct. 22 și 23.
	A.P. „Camera de Comerț Americană din Moldova”	220	este necesară clarificarea scopului acestei prevederi întrucât în cadrul identificării prin mijloace electronice oricum se examinează o reproducere a actului original și nu actul original prezentat în persoană de client.	Comentariu: Punctul dat a fost exclus, iar unele cerințe au fost încorporate la pct. 22 și 23.
	Asociația Businessului European	221	Pct. 36 litera e) În cadrul identificării prin mijloace electronice oricum se examinează o reproducere a actului original nu actul original prezentat în persoană de client, nu este clar ce presupune litera e) din acest punct. Rugăm să fie exclus.	Comentariu: Punctul dat a fost exclus, iar unele cerințe au fost încorporate la pct. 22 și 23.
	B.C. MAIB S.A.	222	La pct.36 lit.e) din Regulament, nu este clară cerința stabilită, deoarece tot punctul descrie acțiunile entității raportoare în cazul examinării de către aceasta a reproducerii unui document original și nu a documentului original (or în toate cazurile pe ecran va fi afișată o fotografie sau scan-ul de pe documentul de identitate original). Considerăm necesară excluderea din pct.36 a lit.e) sau modificarea textului astfel ca să fie clare acțiunile ce urmează a fi întreprinse de către bancă.	Comentariu: Punctul dat a fost exclus, iar unele cerințe au fost încorporate la pct. 22 și 23.

utilizat pentru a genera numărul unic de identificare al documentului original, în cazul în care documentul oficial a fost eliberat cu o zonă de citire optică (machine-readable zone – MRZ); d) dacă reproducerea furnizată este de o calitate și o rezoluție suficiente pentru a se asigura că informațiile relevante sunt lipsite de ambiguitate; e) că reproducerea furnizată nu a fost afișată pe un ecran pe baza unei fotografii sau a unei scanări a documentului de identitate original.				
Pct. 40 : (v2 – pct.39) Identificarea prin mijloace electronice nu poate fi efectuată în raport cu clientul dacă acesta:	A.P. „Camera de Comerț Americană din Moldova”	223	La pct. 40, lit. b) din proiect urmează a fi clarificat dacă se permite identificarea prin mijloace electronice a rezidentului altei jurisdicții, care nu intră în categoria cu risc sport, or conform pct. 13 identificarea și verificarea se efectuează doar în raport cu cetățenii Republicii Moldova.	Comentariu: Se permite identificarea prin mijloace electronice a unei persoane rezidente a altei jurisdicții, dar care este cetățean al R. Moldova.

a) a fost anterior clasificat ca fiind din categoria de risc sporit de spălare a banilor și/sau de finanțare a terorismului în baza analizei riscului entității raportoare; b) este rezident, inclusiv temporar al unei jurisdicții cu risc sporit; c) este o persoană care gestionează bunurile aflate sub administrare fiduciară (trust, fond de investiții etc.).	B.C. „ProCredit Bank” S.A.	224	Privind punctul 40, lit. c), considerăm oportun a se specifica dacă restricția se referă la identificarea persoanei juridice, și anume a fiduciilor sau construcțiilor juridice similare, sau restricția dată se aplică și în cazul în care o persoană fizică care gestionează bunurile aflate sub administrare fiduciară dorește să deschidă cont personal.	Comentariu: Restricția se referă atât la persoana juridică (trust, fond de investiții etc), cât și la persoana fizică care gestionează bunurile aflate sub administrare fiduciară.
	B.C. MAIB S.A.	225	La pct.40 lit.a) din Regulament, nu este clar sensul restricției propuse. Având în vedere formularea utilizată – „a fost anterior clasificat la fiind din categoria de risc sporit” – sub norma lit.a) cad clienții existenți ai băncii, în privința cărora banca deține deja documentele de cunoaștere și cărora anterior li-a fost atribuit gradul de risc sporit (înalt). Solicităm excluderea din pct.40 a lit.a), ca pentru clienții existenți cu risc înalt să fie accesibilă utilizarea soluției de identificare la distanță în scopul actualizării periodice a informațiilor. Suplimentar menționăm că atât Legea nr.308/2017, cât și alte documente de referință (Directiva (UE) 2015/849, Ghidul EBA nr.EBA/GL/2022/15) nu conțin asemenea restricții.	Comentariu: Prevederea dată setează limitări la stabilirea relației de afaceri la distanță sau actualizarea datelor despre clienți în anume circumstanțe, considerate cu un grad de risc sporit. Comentariu:

			La pct.40 lit.b) din Regulament, nu este clar sensul restricției, având în vedere regula generală din art.5/1 al Legii nr.308/2017 și pct.13 lit.a) al Regulamentului, privind posibilitatea aplicării soluțiilor informatice de identificare la distanță doar în privința cetățenilor Republicii Moldova și persoanelor juridice rezidente. În cazul în care se intenționează a restricționa utilizarea soluției pentru identificarea la distanță a cetățenilor Republicii Moldova, aflate temporar în alte jurisdicții, considerăm necesară completarea normei, la final, cu sintagma „desemnate /monitorizate de Grupul de Acțiune Financiară Internațională (GAFI)”, conform art.8/2 din Legea nr.308/2017. Suplimentar menționăm că atât Legea nr.308/2017, cât și alte documente de referință (Directiva (UE) 2015/849, Ghidul EBA nr.EBA/GL/2022/15) nu conțin asemenea restricții.	Se permite identificarea prin mijloace electronice a unei persoane rezidente a altei jurisdicții, dar care este cetățean al R. Moldova.
	Asociația băncilor din Moldova	226	Pct. 40 - se specifică conform proiectului că, identificarea prin mijloace electronice nu poate fi efectuată în raport cu clientul dacă acesta: a) a fost anterior clasificat ca fiind din categoria de risc sporit de spălare a banilor și/sau de finanțare a terorismului în baza analizei riscului entității raportoare; Prin clasificarea anterioară în categoria de risc sporit, se are în vedere nivelul de risc atribuit clientului la momentul solicitării actualizării datelor, sau dacă istoric clientul a deținut nivel de risc sporit, cu retrogradarea ulterioară a acestuia?	Comentariu: Prevederea dată setează limitări la stabilirea relației de afaceri la distanță sau actualizarea datelor despre clienți în anume circumstanțe, considerate cu un grad de risc sporit.

227	- lit.b) ținând cont de faptul că măsurile și metodele de identificare influențează măsurile de precauție doar în sensul sporirii acestora și nu diminuează măsurile de precauție aplicate în raport cu tranzacțiile/activitățile clienților, considerăm exagerată interzicerea identificării persoanelor care anterior au fost clasificate în categoria de risc sporit (de exemplu PEP).	Comentariu: Se permite identificarea prin mijloace electronice a unei persoane rezidente a altei jurisdicții, dar care este cetățean al R. Moldova.
228	- conform pct.13 din proiect: “Entitatea raportoare va efectua identificarea și verificarea clienților prin mijloace electronice, în raport cu: a) persoana fizică, cetățean al Republicii Moldova; b) persoana juridică rezidentă, ai căror reprezentanți, fondatori, administratori și beneficiari efectivi sunt cetățeni ai Republicii Moldova.” Prevederile pct.13 se contrazic cu prevederile pct.40 lit.b). Din prevederile pct.40 lit.b) poate fi trasă concluzia că în cazul în care persoana este rezident al unei jurisdicții căreia nu i se atribuie un grad de risc sporit, acesta poate fi identificat și verificat prin intermediul mijloacelor electronice. Astfel, se propune de a reformula prevederea din pct.40 lit.b) în așa fel, încât să nu inducă în eroare în privința rezidenților a unei jurisdicții căreia nu i se atribuie un grad de risc sporit.	Comentariu: Prevederea dată setează limitări la stabilirea relației de afaceri la distanță sau actualizarea datelor despre clienți în anume circumstanțe, considerate cu un grad de risc sporit.

		229	- lit. c) considerăm oportun a se specifica dacă restricția se referă la identificarea persoanei juridice, și anume a fiduciilor sau construcțiilor juridice similare, sau restricția dată se aplică și în cazul în care o persoană fizică care gestionează bunurile aflate sub administrare fiduciară dorește să deschidă cont personal.	Comentariu: Restricția se referă atât la persoana juridică (trust, fond de investiții etc), cât și la persoana fizică care gestionează bunurile aflate sub administrare fiduciară.
		230	- se propune excluderea sau detalierea limitării stipulate la lit.a).	Comentariu: Prevederea dată setează limitări la stabilirea relației de afaceri la distanță sau actualizarea datelor despre clienți în anume circumstanțe, considerate cu un grad de risc sporit.

Pct. 43 : (v2 – pct.43 modificat) Entitatea raportoare va oferi un punct de acces securizat pentru începerea procesului de identificare la distanță a clienților pe baza certificatelor calificate pentru sigiliile electronice în conformitate cu Legea nr. 124/2022. De asemenea, clientul trebuie să fie informat cu privire la măsurile de securitate aplicabile care trebuie luate pentru a garanta utilizarea securizată a sistemului.	A.P. „Camera de Comerț Americană din Moldova”	231	Solicităm oferirea unor clarificări, or certificatele calificate pentru sigiliile electronice nu se emit de entitățile raportoare și nu se pun la dispoziție de către acestea clienților. Prestatorii de servicii de încredere sunt cei care emit și pun la dispoziția cetățenilor certificatele electronice.	Comentariu: Prevederile punctului dat au fost redactate pentru a aduce claritate entităților.
Pct. 46: (v2 – pct.46) În scopul identificării electronice a clientului, entitatea raportoare realizează prelucrarea datelor, dar și asigură protecția datelor cu caracter personal obținute în procesul de implementare a prevederilor și cerințelor prezentului Regulament, precum și confidențialitatea acestor date, în conformitate cu reglementările actelor		232	La pct. 46, considerăm oportună substituirea cuvintelor „reglementările actelor normative naționale” cu cuvintele „actele normative”, potrivit uzanțelor de redactare a normelor juridice.	Se acceptă

normative naționale cu privire la protecția datelor cu caracter personal și prezentului Regulament.				
Pct. 47: (v2 – pct.47) Entitatea raportoare păstrează toate documentele și informațiile despre clienți, inclusiv înregistrările video, audio, foto, capturile de ecran, obținute în cadrul identificării electronice, inclusiv copiile documentelor de identificare, arhiva, amprenta digitală aferentă computerului /dispozitivului utilizat, adresa IP, documentele, orice alte informații, pe perioada activă a relației de afaceri și pe o perioadă de 5 ani după terminarea acesteia.	A.P. „Camera de Comerț Americană din Moldova”	233	Se propune completarea după cuvântul „informațiile” cu cuvântul „obținute” or nu toate metodele de identificare prin mijloace electronice presupun concomitent obținerea tuturor datelor menționate în pct. 47. În acest caz, cuvântul „inclusiv” se propune de a fi substituit cu cuvântul „precum”.	Se acceptă
	B.C. „ProCredit Bank” S.A.	234	La punctul 47 din cap.VII se menționează că entitatea raportoare păstrează toate documentele și informațiile despre clienți. În acest sens, rugăm a se adăuga unde sunt specificate condițiile sau parametrii tehnici pentru arhivare și păstrare.	Comentariu: Entitatea va stabili individual, la necesitate, condițiile sau parametrii tehnici pentru arhivare și păstrare a datelor și informațiilor obținute prin mijloace electronice de la clienți. Important ca aceasta să asigure că datele arhivate sunt păstrate cu asigurarea integrității și disponibilității acestora.
	OCN Microinvest SRL	235	La pct. 47 din Regulament se propune după cuvântul “informațiile” să fie inclus cuvântul „obținute”, or nu toate metodele de identificare prin mijloace electronice presupun concomitent obținerea tuturor datelor menționate în pct. 47. În acest caz, cuvântul „inclusiv” se propune de a fi substituit cu cuvântul „precum”.	Se acceptă

Asociația Businessului European	236	Pct. 47 propunem a fi exclus deoarece este impropriu obiectului de reglementare a proiectului de Regulament care se referă la cerințe față de identificarea persoanei și nu față de accesul la datele colectate de către alte autorități.	Nu se acceptă Cerința de păstrare a documentelor /informațiilor obținute la stabilirea relației de afaceri și desfășurarea acesteia într-o anumită perioadă este o cerință esențială prevăzută de către standardele internaționale în materie de PCSBFT.
B.C. MAIB S.A.	237	La pct.47 din Regulament, propunem de exclus cuvântul „, inclusiv”, în ambele cazuri, deoarece o entitate raportoare poate să nu dispună de toate categoriile de documente și informații enumerate în textul normei (de exemplu, poate să nu aplice metoda de identificare prin înregistrare video, audio). Or, utilizarea cuvântului „inclusiv” presupune existența concomitentă a tuturor informațiilor și datelor menționate.	Se acceptă
	238	De asemenea, la pct.47 din Regulament propunem înlocuirea cuvântului „terminarea” cu cuvântul „încetarea”.	Se acceptă
Asociația băncilor din Moldova	239	Propunem a fi exclus deoarece este impropriu obiectului de reglementare a proiectului de reglementare care se referă la cerințe față de identificarea persoanei și nu față de accesul la datele colectate de către alte autorități. Suplimentar, proiectul stabilește ca entitatea raportoare păstrează toate documentele și informațiile despre clienți, condițiile tehnice și/sau specificațiile și sursa acestora nefiind menționate.	Nu se acceptă Cerința de păstrare a documentelor /informațiilor obținute la stabilirea relației de afaceri și desfășurarea acesteia într-o anumită perioadă este o cerință esențială prevăzută de către standardele internaționale în materie de PCSBFT.

Pct. 49 (v2 – pct.49)	Asociația băncilor din Moldova	240	Nu este clar ce presupune o „activitate suspectă” despre care entitatea raportoare trebuie să informeze BNM. În lipsa unor precizări în privința noțiunii respective, poate fi interpretat că activitățile suspecte raportate SPCSB conform pct.38 din proiect și art.11 (1) din Legea nr.308/22.12.2017 urmează a fi raportate și BNM. Totodată, nu este clar termenul și modul/ canalul de informare a BNM. Se propune completarea pct.49 cu prevederi privind termenul și modul/ canalul de informare a BNM, și de precizat în privința căror activități suspecte urmează a fi informată BNM.	Comentariu: Entitatea raportoare are obligația să informeze despre activitățile suspecte și incidentele de fraudă care prezintă riscuri pentru siguranța, buna funcționare sau reputația entității, printr-o scrisoare de informare.
Pct. 50 : (v2 – pct.50) Entitatea raportoare, anterior demarării procedurii de identificare prin mijloace electronice a clienților, este obligată să informeze Banca Națională a Moldovei cu privire la corespunderea cu următoarele cerințe:	Asociația Businessului European	241	La pct. 50, se necesită a fi completat cu prevederi specifice cu privire la finalitatea procesului de notificare a BNM. Astfel, se necesită a determina perioada de timp în care BNM examinează informațiile și emite actul administrativ prin care constată/acceptă utilizarea acestui procedeu.	Comentariu: BNM prin prevederile date implementează un mecanism de notificare, prin care exclude obligația de evaluare și răspuns. Totuși, în situația în care BNM va identifica anumite lacune conceptuale în politici, proceduri și în mecanismul de implementare a procesului de identificare la distanță a clienților, va informa entitatea în decurs de 30 zile.
a) dovada că entitatea raportoare dispune de politici și proceduri interne corespunzătoare, care vor pune în aplicare cerințele din prezentul Regulament. b) dovada că entitatea raportoare a efectuat evaluarea preimplementare a soluției	OCN Microinvest SRL	242	Având în vedere prevederile pct. 50-52 din Regulament, se propune includerea unei reglementări care va stabili o normă derogatorie pentru cazurile în care entitățile au aprobate deja la nivel intern unele prevederi/cerințe ce țin de procesul de identificare a clienților la distanță. Astfel, se propune includerea unui nou pct. 55 în Regulament, după cum urmează: “În vederea asigurării implementării treptate a prevederilor Regulamentului și asigurarea unui termen rezonabil pentru ajustarea proceselor în vederea conformării cu cerințele prevăzute de prezentul Regulament,	Se acceptă Hotărârea BNM prin care se aprobă Regulamentul prevede că entitățile raportoare care au implementate soluții informatice pentru stabilirea relației de afaceri la distanță a clienților la data intrării în vigoare a hotărârii BNM se vor conforma noilor cerințe în decurs de 6 luni.

de identificare la distanță a clienților în conformitate cu pct.6 din prezentul Regulament;			entitățile raportoare care au aprobat procese interne ce țin de identificare la distanță și/sau implementat soluții active de identificare la distanță în termen de 6 luni de la data intrării în vigoare a prezentului Regulament, vor informa Banca Națională a Moldovei cu prezentarea informațiilor prevăzute la pct. 50-52.”	
c) dovada că angajații entității raportoare responsabili de identificarea video sunt instruiți în conformitate cu pct. 32 din prezentul Regulament;	A.P. „Camera de Comerț Americană din Moldova”	243	La pct. 50, lit. c) din proiect propunem următoarea redacție în corespundere cu comentariul adresat la pct. 32 din proiectul Regulamentului: <i>„c) dovada că angajații entității raportoare responsabili de identificarea video sunt instruiți în conformitate cu pct. 32 din prezentul Regulament, în cazurile identificării electronice asistate”.</i>	Se acceptă
d) dovada că entitatea raportoare dispune de spațiu corespunzător pentru efectuarea procedurii de identificare video, în conformitate cu pct. 33 din prezentul Regulament;	A.P. „Camera de Comerț Americană din Moldova”	244	La pct. 50, lit. d) din proiect propunem următoarea redacție în corespundere cu comentariul adresat la pct. 33 din proiectul Regulamentului: <i>„d) dovada că entitatea raportoare dispune de spațiu corespunzător pentru efectuarea procedurii de identificare video, în conformitate cu pct. 33 din prezentul Regulament, în cazurile identificării electronice asistate”.</i>	Se acceptă
e) dovada că entitatea raportoare dispune de mijloace tehnice corespunzătoare, în conformitate cu cerințele cap. IV din prezentul Regulament.	Asociația băncilor din Moldova	245	- se impune a fi completat cu prevederi specifice privind finalitatea procesului de notificare a BNM. Astfel, se impune a determina perioada de timp în care BNM examinează informațiile și emite actul administrativ prin care constată/acceptă utilizarea acestui procedeu.	Comentariu: BNM prin prevederile date implementează un mecanism de notificare, prin care exclude obligația de evaluare și răspuns. Totuși, în situația în care BNM va identifica anumite lacune conceptuale în politici, proceduri și în mecanismul de implementare a procesului de identificare la distanță a clienților, va informa entitatea în decurs de 30 zile.

		246	- lit.c) se propune a se ține cont de comentariul/propunerea aferentă pct.32 lit. b)	Se acceptă
	Ministerul Justiției	247	La pct. 50 lit. b) - e) , se va lua în considerare că „În cazul în care se face trimitere la o normă juridică care este stabilită în același act normativ, pentru evitarea reproducerii acesteia, se face trimitere la elementul structural sau constitutiv respectiv, fără a se indica că elementul respectiv face parte din același act normativ.”, în conformitate cu art. 55 alin. (4) din Legea nr. 100/2017 cu privire la actele normative (obiecție valabilă și pentru pct. 51).	Se acceptă
Pct. 51: (v2 – pct.51) Procedura stabilită la pct. 50 din prezentul Regulament este efectuată o singură dată, înainte ca entitatea raportoare să pună în aplicare prevederile prezentului Regulament și se efectuează în scopul evidenței și verificării corespunderii criteriilor stabilite la lit. a) – e) din pct. 50.	A.P. „Camera de Comerț Americană din Moldova”	248	La pct. 51 din proiect considerăm util de a prevedea limita de timp (de ex. 10 zile) în care BNM revine cu o decizie de accept / refuz asupra soluției prezentate pentru ca entitățile raportoare să fie pregătite inclusiv din punctul de vedere de identificare urgentă a unei alte soluții. De asemenea, urmează a fi clarificat modul de tratare a entităților raportoare care au implementat o soluție adecvată și în conformitate, inclusiv, cu prevederile prezentului regulament dar înainte ca BNM să reglementeze acest domeniu. Până în acest moment nu a existat nici o interdicție de a folosi o asemenea soluție cu respectarea principiilor recunoscute la nivel european și bunele standarde în materie KYC/AML.	Comentariu: BNM prin prevederile date implementează un mecanism de notificare, prin care exclude obligația de evaluare și răspuns. Totuși, în situația în care BNM va identifica anumite lacune conceptuale în politici, proceduri și mecanismul de implementare a procesului de identificare la distanță a clienților, va informa entitatea în decurs de 30 zile.
	„Paymaster” SRL	249	Pct. 51 lit c) din proiect, propunem să fie exclusă prin prisma argumentului expus la pct. 15 din acest aviz.	Comentariu: Prevederea dată a fost modificată pentru a reda claritate.
	Asociația băncilor din Moldova	250	Nu este clar dacă BNM va reveni cu comentarii, decizie de acceptare sau refuz în urma informării de către entitatea raportoare a BNM conform pct.50 din prezentul proiect. Totodată, nu este clar modul / canalul de informare a BNM de către entitatea raportoare. Astfel, se propune de completat:	Comentariu: BNM prin prevederile date implementează un mecanism de notificare, prin care exclude obligația de evaluare și răspuns. Totuși, în situația în care BNM va identifica anumite lacune conceptuale în politici, proceduri și în

			- pct.51 cu o prevedere aferentă acțiunilor BNM după prezentarea de către entitatea raportoare a informațiilor conform pct.50 din prezentul proiect; - pct.50 cu prevederi privind modul / canalul de informare.	mecanismul de implementare a procesului de identificare la distanță a clienților, va informa entitatea în decurs de 30 zile.
Pct. 52: (v2 – pct.52) Entitatea raportoare, anterior demarării procesului de externalizare integrală sau parțială a procesului de identificare la distanță a clienților, informează Banca Națională a Moldovei, cel puțin, asupra următoarelor : a) numele furnizorului de servicii, numărul de înregistrare al companiei, codul de identificare (dacă este disponibil), adresa și alte date de contact relevante (dacă este cazul); b) o descriere succintă a funcțiilor externalizate, inclusiv a datelor care sunt externalizate și dacă au fost transferate sau nu date cu caracter personal sau dacă prelucrarea lor este externalizată către un furnizor de servicii;	SPCSB	251	Observăm că exclusiv în conținutul pct. 52 din proiect, se utilizează noțiunea de „funcție externalizată”, fapt care considerăm că face dificilă interpretarea și eventuala aplicare corectă a normei, considerente din care se propune definirea conceptului juridic și completarea pct. 4 cu noțiunea corespunzătoare.	Se acceptă A fost definită noțiunea „furnizor de servicii externalizate”.
	A.P. „Camera de Comerț Americană din Moldova”	252	La pct. 52, lit. d) din proiect urmează a specifica criteriile de apreciere după care putem concluziona că externalizarea este sau nu este de importanță critică.	Comentariu: Prevederea dată a fost exclusă. Procesul de identificare la distanță a clienților se consideră critic.
		253	La pct. 52, lit. e) și lit. f) din proiect se propune includerea cerințelor specifice de bază a evaluării pe care entitatea raportoare este obligată să le efectueze și să le ia în considerare.	Comentariu. Prevederea lit.e) a fost exclusă. Procesul de identificare la distanță a clienților se consideră critic. Cu referire la lit.f), entitatea va prezenta ultima evaluare a soluției care se dorește a fi implementată și furnizată de o parte terță , în special, cu referire la riscurile descrise în Regulament (fraudă, identitate pretinsă, dovezile de identitate, spălarea banilor și finanțarea terorismului etc.).
	OCN Microinvest SRL	254	La lit. e) și lit. f) pct. 52 din Regulament se propune includerea cerințelor specifice de bază a evaluării pe care entitatea raportoare este obligată să efectueze și să le ia în considerare.	Comentariu: Prevederea lit.e) a fost exclusă. Procesul de identificare la distanță a clienților se consideră critic.

c) țara sau țările în care serviciul urmează să fie prestat, inclusiv locația datelor (și anume, țara sau regiunea); d) dacă funcția externalizată este considerată sau nu critică sau importantă, inclusiv, dacă este cazul, un rezumat succint al motivelor pentru care funcția externalizată este considerată critică sau importantă; e) data celei mai recente evaluări a caracterului critic sau a importanței funcției externalizate. f) data celei mai recente evaluări a riscurilor și un rezumat succint al principalelor rezultate; g) în cazul externalizării către un furnizor de servicii de tip cloud, serviciile de tip cloud și modelele de implementare, și anume publice/private/hibride/co munitare, precum și natura specifică a datelor care				Cu referire la lit.f), entitatea va prezenta ultima evaluare a soluției care se dorește a fi implementată și furnizată de o parte terță , în special, cu referire la riscurile descrise în Regulament (fraudă, identitate pretinsă, dovezile de identitate, spălarea banilor și finanțarea terorismului etc.).
	Asociația băncilor din Moldova	255	Nu este clar: - dacă BNM va reveni cu decizie de acceptare sau refuz în urma informării de către entitatea raportoare a BNM conform pct.52 din proiect. - modul / canalul de informare a BNM de către entitatea raportoare. Suplimentar, referitor la lit. g), considerăm oportun concordarea normei cu prevederile Regulamentului privind cerințe minime pentru gestiunea riscurilor TIC și de Securitate a Informației, deoarece nu s-a observat o viziune clară a supraveghetorului privind utilizarea soluțiilor de tip "cloud" în sistemul bancar. Astfel, se propune de completat: - cu prevederi privind acțiunile BNM urmare a informării de către entitatea raportoare conform pct.52 din proiect; - pct.52 cu prevederi privind modul / canalul de informare. Totodată, se propune de concretizat dacă obligația cu privire la informarea BNM menționată în pct.52 se aplică suplimentar la obligația de informare și după caz, obținere a aprobării prealabile a BNM, care revin conform Regulamentului privind externalizarea activităților și operațiunilor băncii nr.46 din 26.02.2020. Complementar se impune a specifica termenul examinării de către BNM.	Comentariu: BNM prin prevederile date implementează un mecanism de notificare, prin care exclude obligația de evaluare și răspuns. Totuși, în situația în care BNM va identifica anumite lacune conceptuale în politici, proceduri și în mecanismul de implementare a procesului de identificare la distanță a clienților, va informa entitatea în decurs de 30 zile. Cerințele care derivă din prezentul Regulament și Regulamentul nr.46/2020 sunt separate.

urmează să fie deținute și locațiile (și anume, țări sau regiuni) unde datele respective sunt stocate;				
Pct. 54: (v2 – pct.54) BNM poate solicita, după caz, un raport de audit, efectuat conform standardelor internaționale de audit în domeniul sistemelor informaționale.	A.P. „Camera de Comerț Americană din Moldova”	256	La pct. 54 din proiect se propune indicarea situațiilor în care BNM va putea solicita un raport de audit în domeniul sistemelor informaționale, precum și periodicitatea cu care acestea vor putea fi solicitate pentru mai multă transparență și previziune.	Comentariu: BNM va solicita un raport de audit în domeniul sistemelor informaționale în cazul în care BNM va identifica în cadrul procesului de supraveghere anumite lacune/deficiențe în politici, proceduri și în mecanismul de implementare a procesului de identificare la distanță a clienților prin mijloace electronice (de ex. incidente de securitate, încălcarea cerințelor de protecție a datelor cu caracter personal, fraude etc.).
	OCN Microinvest SRL	257	La pct. 54 din Regulament se propune indicarea situațiilor când BNM va putea solicita un raport de audit în domeniul sistemelor informaționale, precum și periodicitatea cu care acestea vor putea fi solicitate pentru mai multă transparență și previziune.	Comentariu: BNM va solicita un raport de audit în domeniul sistemelor informaționale în cazul în care BNM va identifica în cadrul procesului de supraveghere anumite lacune/deficiențe în politici, proceduri și în mecanismul de implementare a procesului de identificare la distanță a clienților prin mijloace electronice (de ex. incidente de securitate, încălcarea cerințelor de protecție a datelor cu caracter personal, fraude etc.).

	Banca Comercială Română Chișinău S.A.		La pct. 54 solicităm să fie revizuit astfel încât să fie clar ca raportul de audit solicitat se referă la soluția informatică ce urmează să fie implementată de entitățile de raportare pentru identificarea clienților la distanță.	Comentariu: Raportul de audit solicitat se referă la soluția informatică ce urmează să fie implementată de entitățile de raportare pentru identificarea clienților la distanță prin mijloace electronice.
Pct. 50-52 (v2 – pct.50-52)	A.P. „Camera de Comerț Americană din Moldova” OCN Microinvest SRL	258	Având în vedere prevederile pct. 50-52 din proiectul Regulamentului, ar fi utilă includerea unei reglementări care va stabili o normă derogatorie pentru cazurile în care entitățile au aprobat deja la nivel intern unele prevederi/cerințe ce țin de procesul de identificare a clienților la distanță. Astfel, se propune includerea unui nou pct. 55 în Regulament, în următoarea redacție: <i>„În vederea asigurării implementării treptate a prevederilor Regulamentului și asigurarea unui termen rezonabil pentru ajustarea proceselor în vederea conformării cu cerințele prevăzute de prezentul Regulament, entitățile raportare care au aprobat procese interne ce țin de identificare la distanță și/sau implementat soluții active de identificare la distanță în termen de 6 luni de la data intrării în vigoare a prezentului Regulament, vor informa Banca Națională a Moldovei cu prezentarea informațiilor prevăzute la pct. 50-52”.</i>	Se acceptă Hotărârea BNM prin care se aprobă Regulamentul prevede că entitățile raportare care au implementat soluții informatice pentru stabilirea relației de afaceri la distanță a clienților la data intrării în vigoare a hotărârii BNM se vor conforma noilor cerințe în decurs de 6 luni.
Propunere de completare a cap. A – Politici și Proceduri (v2 – cap. II secțiunea 1)	„Qiwi-M” SRL	259	Luând în considerație că fiecare entitate va utiliza soluții de identificare diferite se propune a completa proiectul Regulamentului BNM cu privire la e-KYC cu următoarea cerință: „Pe lângă elementele prezentate la pct. 5, Entitatea raportare trebuie să prevadă în politicile și procedurile lor informațiile necesare pentru identificarea clientului, tipurile de documente, date sau informații pe care instituția le va utiliza pentru a verifica identitatea clientului și modul în care vor fi verificate aceste informații”.	Nu se acceptă Cerințele de precauție aferente clienților sunt prevăzute în actele normative aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului. Pct. 2 prevede acest aspect.

Propunere de completare a cap.III (v2 – cap.III)	„Qiwi-M” SRL	260	Considerăm oportun stabilirea și specificarea în proiectul Regulamentului a cerințelor minime față de soluția de identificare la distanță. În acest sens propunem completarea Capitolului III cu un punct suplimentar cu următorul conținut: „Entitatea raportoare trebuie să se asigure că: a) informațiile obținute prin intermediul soluției de înregistrare la distanță a clienților sunt actualizate și adecvate pentru a respecta cerințele de precauție stabilite de Legea 308/2017; b) toate imaginile, înregistrările video, înregistrările audio și datele sunt captate într-un format lizibil și de o calitate suficientă, astfel încât clientul să poată fi recunoscut fără echivoc; c) procesul de identificare nu continuă dacă sunt detectate deficiențe tehnice sau întreruperi neașteptate ale conexiunii”.	Nu se acceptă Cerințele de precauție aferente clienților sunt prevăzute în actele normative aferente domeniului prevenirii și combaterii spălării banilor și finanțării terorismului. Pct. 2 prevede acest aspect. Cât privește cerințele asociate soluției de identificare la distanță prin mijloace electronice, acestea sunt deja prevăzute de Regulament.
Propunere de completare cap. C Identificarea prin alte mijloace electronice oferite de către un prestator de servicii de încredere calificat, acreditat în condițiile Legii nr.124/2022. (v2 – cap.IV secțiunea 1)	„Qiwi-M” SRL	261	Luând în considerare că acest capitol se referă la externalizarea procesului de identificare la distanță, propunem redenumirea capitolului, de exemplu “Dependența de terți și externalizarea”. De asemenea, propunem completarea politicilor și procedurilor interne cu specificații care să stabilească funcțiile și activitățile de înregistrare la distanță a clienților care vor fi efectuate sau desfășurate de instituția de credit și financiară, de terți sau de alt furnizor de servicii externalizate.	Comentariu: Cerințele vis-a-vis de externalizarea procesului de stabilire a relației de afaceri la distanță prin mijloace electronice au fost ajustate și separate într-o secțiune dedicată.
	BC EuroCredit Bank S.A. Î.S. ”Poșta Moldovei”	262	Lipsa propunerilor și obiecțiilor	