Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din _____
Chișinău

privind aprobarea procedurii de identificare a persoanei la distanță utilizând mijloace digitale

---

În temeiul art. 10 alin. (2) pct. 4) lit. d) din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere (Monitorul Oficial al Republicii Moldova, 2022, nr. 170-176, art. 317), Guvernul HOTĂRĂȘTE:

1. Se aprobă procedura de identificare a persoanei la distanță utilizând mijloace digitale, conform anexei.
2. Prezenta hotărâre intră în vigoare în termen de 3 luni de la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării economice și digitalizării **Dumitru ALAIBA**

Aprobată
prin Hotărârea Guvernului nr.____

Procedura
de identificare a persoanei la distanță utilizând mijloace digitale

I. DISPOZIȚII GENERALE

1. Prezenta procedură stabilește regulile și, cerințele minime tehnice și de securitate pentru realizarea identificării și verificării la distanță a persoanei utilizând mijloace digitale.

2. În înțelesul prezentei proceduri, termenii, expresiile și abrevierile de mai jos au următoarele semnificații:

atribute de identitate - subset al datelor de identificare trimise de serviciul de identificare a persoanei la distanță către serviciul client;

beneficiar al unui serviciu de identificare a persoanei la distanță – persoană fizică sau juridică, posesor al unui serviciu client care utilizează serviciul de identificare a persoanei la distanță pentru a identifica persoane fizice în vederea înregistrării a acestora în calitate de clienți sau pentru a le presta servicii;

detectarea biometrică a vieții (Biometric Liveness Detection) - tehnică utilizată pentru a detecta o tentativă de falsificare prin determinarea dacă sursa unei probe biometrice este o ființă umană vie sau o reprezentare falsă. Acest lucru se realizează prin algoritmi care analizează datele colectate de la senzorii biometrici pentru a determina dacă sursa este în direct sau reprodusă;

componenta de securitate – componenta electronică a unui act de identitate electronic, utilizat ca suport de stocare securizat pentru datele de identificare și fotografia deținătorului legitim al actului;

consimțământ - orice indicare liberă, specifică, informată și neechivocă a dorințelor solicitantului prin care acesta, printr-o declarație sau printr-o acțiune afirmativă clară, indică acordul cu privire la prelucrarea datelor cu caracter personal care îl privesc;

date biometrice – date cu caracter personal rezultate în urma prelucrărilor tehnice specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acesteia;

date de identificare – set de date cu caracter personal, inclusiv date biometrice, colectate și verificate de către serviciul de identificare a persoanei la distanță în vederea verificării identității unei persoane fizice;

dispozitivul solicitantului – orice dispozitiv aflat în posesia solicitantului, care este compatibil cu sistemul informatic pentru identificarea persoanei la distanță;

dosar electronic de evidență – element reținut de furnizorul de servicii de identificare care colectează datele relevante ce urmează să fie păstrate pentru soluționarea litigiilor sau în cazul unei investigații și în special în vederea furnizării de probe în instanță;

furnizor de servicii de identificare a persoanei la distanță utilizând mijloace digitale - persoană juridică de drept public sau privat, inclusiv prestatorii de servicii de încredere calificați, care identifică persoana la distanță prin mijloace digitale în

scopurile precizate de prezenta procedură, denumit în continuare furnizor de servicii de identificare;

furt de identitate - fapta de a utiliza în mod fraudulos datele de identificare ale altei persoane sau modificarea identității implicând utilizarea unor date de identificare frauduloase care nu aparțin unei persoane existente;

identitate electronică – datele de identificare a persoanelor în format electronic reprezentând în mod unic o persoană fizică;

identificarea persoanei la distanță prin mijloace digitale - procesul de identificare și verificare a identității persoanei fizice, în baza actelor de identitate prezentate, măsurătorilor semnalmentelor biometrice faciale, comparării de imagini și a informațiilor comunicate de persoana fizică și/sau preluate din surse de date externe, utilizând mijloace digitale;

mijloace digitale - mijloace care utilizează tehnologii digitale inovatoare care folosesc, printre altele, mijloace video, inteligența artificială și/sau procese de învățare automată (machine learning), cum ar fi aplicațiile care realizează identificarea unei persoane și/sau verificări ale actelor de identitate (prin capturi de imagini digitale, măsurători ale semnalmentelor biometrice faciale, comparare de imagini), tehnologia NFC (comunicare în câmp apropiat) încorporată în actele de identitate electronice;

mijloace video - mijloace de identificare la distanță ce utilizează tehnologii care presupun fie transmiterea audiovideo de succesiuni de imagini în mișcare, în timp real, în cadrul unei videoconferințe cu prezența unui operator uman, fie transmiterea de succesiuni de imagini în mișcare reprezentând capturi video cu persoana fizică, fără prezența unui operator uman, cu verificarea acestora cu sau fără implicarea unui operator uman;

MRZ (Machine Readable Zone) - zonă a unui act de identitate, care conține informații personale ale titularului și este concepută pentru a fi citită automat de către dispozitivele sau sistemele de recunoaștere optică a caracterelor (OCR);

NFC (Near Field Communication) - tehnologie de comunicare wireless pe distanțe scurte, care permite schimbul de date între dispozitive compatibile, aflate la o distanță până la câțiva centimetric;

prestator de servicii de încredere calificat – astfel cum este definit conform prevederilor Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere;

rezultatul verificării identității de la distanță – toate informațiile trimise de serviciul de identificare a persoanei la distanță către serviciul client, inclusiv verdictul (reușit sau nereușit) al verificării identității la distanță, motivul eșecului, dacă există, atributele de identitate legate de solicitant cerute de serviciul client și verificate de către furnizorul de servicii de identificare și orice date suplimentare solicitate de serviciul client;

serviciu client – serviciu sau grup de servicii la care solicitantul dorește să se identifice, utilizând serviciul de identificare a persoanei la distanță;

serviciu de identificare a persoanei la distanță – serviciul electronic acoperit de acest set de reguli, responsabil de colectarea și verificarea datelor de identificare a solicitanților în vederea identificării acestora, crearea dosarului electronic de evidență și transmiterea rezultatului verificării identității la distanță către servicii client;

sistem informatic pentru identificarea persoanei la distanță - ansamblul de elemente tehnologice implicate în procesul de identificare a persoanei la distanță prin mijloace digitale, prin care se transmit datele, imaginile capturate/încărcate și/sau informațiile comunicate de solicitant, denumit în continuare sistem informatic;

solicitant – persoană fizică a cărei identitate este verificată de către serviciul de identificare a persoanei la distanță;

surse externe de date – sisteme informaționale și registre de stat sau private;

verdictul de verificare a identității de la distanță – verdict binar („reușit" sau „nereușit") generat de serviciul de identificare a persoanei la distanță după etapele de colectare și verificare a datelor de identificare. Verdictul este „reușit" dacă serviciul de identificare a persoanei la distanță concluzionează că actul de identitate prezentat de solicitant este autentic și că solicitantul este deținătorul legitim al actului de identitate, în caz contrar verdictul este „nereușit".

3. Procedura este obligatorie pentru prestatorul de servicii de încredere calificat acreditat în condițiile Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere, pentru situația în care acesta utilizează mijloace digitale pentru verificarea identității persoanei căreia urmează să-i fie emis un certificat calificat și poate fi aplicată opțional de către alți prestatori de servicii.

4. Prestatorul de servicii de încredere calificat poate realiza identificarea persoanei la distanță utilizând mijloace digitale fie în vederea eliberării de certificate calificate, în conformitate cu prevederile art. 10 alin. (2) pct. 4) lit. d) din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, fie în calitate de furnizor de servicii de identificare, în conformitate cu prevederile prezentei proceduri.

5. Prestatorul de servicii de încredere calificat care intenționează să realizeze identificarea persoanei la distanță utilizând mijloace digitale, în scopul emiterii certificatelor calificate conform Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere și/sau în calitate de furnizor de servicii de identificare, are obligația de a notifica Serviciul de Informații și Securitate, în calitate de organ de supraveghere și control, cu 30 de zile înainte de utilizarea mijloacelor digitale pentru identificarea persoanei la distanță.

6. Notificarea prevăzută la pct. 5 va fi însoțită de următoarele documente:

1) descrierea sistemului informatic și a echipamentelor utilizate în procesul de identificare a persoanei la distanță utilizând mijloace digitale;

2) raportul de evaluare a conformității emis de un organism independent de evaluare, care să ateste inclusiv îndeplinirea cerințelor prevăzute în prezenta procedură;

3) declarația reprezentantului legal că prestatorul de servicii de încredere calificat dispune de politici de identificare și diminuare a riscului asociat metodei de identificare, inclusiv personal calificat;

4) declarația pe propria răspundere a reprezentantului legal că prestatorul de servicii de încredere calificat a adoptat și implementat proceduri privind protecția datelor cu caracter personal în procesul de identificare a persoanei la distanță utilizând mijloace digitale, în concordanță cu legislația în domeniu.

7. Notificarea prevăzută la pct. 5 are caracter informativ și nu necesită aprobare pentru inițierea de către prestatorul de servicii de încredere a utilizării mijloacelor digitale pentru identificarea persoanei la distanță.

Capitolul II. ACTIVITĂȚILE SERVICIULUI DE IDENTIFICARE A PERSOANEI LA DISTANȚĂ

8. Identificarea la distanță utilizând mijloace digitale poate fi realizată prin mijloace de verificare automatizate, fără operator uman, sau prin mijloace de verificare cu operator uman.

9. Identificarea la distanță utilizând mijloace digitale realizată cu operator uman poate fi efectuată doar de personal instruit.

10. Persoanele care au atribuții și responsabilități în procesul de identificare a persoanei la distanță utilizând mijloace digitale vor beneficia sau vor fi obligate să urmeze cursuri de pregătire profesională sau programe de instruire anuale, organizate extern sau intern.

11. Identificarea la distanță utilizând mijloace digitale realizată prin mijloace de verificare automatizate, fără operator uman, va utiliza mijloace digitale în conformitate cu standardele în vigoare.

12. Un serviciu de identificare a persoanei la distanță efectuează succesiv următorii pași:

1) colectarea datelor de identificare;
2) verificarea datelor de identificare;
3) constituirea dosarului electronic de evidență;
4) transmiterea rezultatului verificării identității la distanță.

13. La inițierea procedurii de identificare a persoanei la distanță utilizând mijloace digitale, după prezentarea de către solicitant a actului de identitate, acesta trebuie să își dea consimțământul în vederea parcurgerii procesului de identificare și asupra scopului identificării, precum și acordul cu privire prelucrarea datelor cu caracter personal, inclusiv la realizarea de fotografii și/sau capturi de imagini ale sale și ale actului de identitate. Exprimarea consimțământului va fi păstrată împreună cu probele colectate în procesul de identificare.

14. Colectarea datelor de identificare se poate efectua simultan sau succesiv, în orice ordine. În procesul de colectare a datelor de identificare sunt furnizate sau preluate din surse externe de date cel puțin datele referitoare la solicitant:

1) numele și prenumele solicitantului;
2) numărul de identificare de stat al persoanei fizice;
3) data și locul nașterii solicitantului;
4) numărul unic al actului de identitate;
5) data emiterii actului de identitate;
6) data de expirare a actului de identitate;
7) înregistrări foto și video a feței solicitantului;
8) înregistrări foto și video ale actului de identitate a solicitantului - în cazul verificării manuale;
9) datele și semnătura datelor din componenta de securitate a actul de identitate preluată prin NFC;
10) datele de contact (telefon, adresa poștei electronice (e-mail) etc.).

15. Când autenticitatea actului de identitate este verificată criptografic folosind componenta de securitate, datele de identificare ale solicitantului (inclusiv fotografia solicitantului) stocate pe componenta de securitate a actului de identitate sunt

preluate în mod securizat și utilizate în procesul de identificare și verificare a identității la distanță.

16. Serviciul de identificare a persoanei la distanță protejează confidențialitatea și integritatea datelor de identificare ale solicitantului pe măsură ce acestea sunt preluate de serviciu prin intermediul dispozitivului solicitantului.

17. Suplimentar, datelor preluate conform pct. 14, pot fi furnizate date de către solicitant sau preluate din surse externe de date.

18. Pe baza datelor de identificare colectate, prin intermediul prelucrării automatizate, după caz cu implicarea operatorilor, se realizează verificarea autenticității actului de identitate prezentat și că solicitantul este deținătorul legitim al acestuia. Autenticitatea actului de identitate prezentat de solicitant poate fi verificată criptografic folosind tehnologia NFC pentru citirea componentei de securitate a acestuia. De asemenea, verificarea autenticității actului de identitate prezentat, a statutului acestuia (nedeclarat pierdut sau furat) și a datelor pe care le conține, precum și a datelor furnizate de solicitant, se realizează prin compararea cu datele din surse externe de date, inclusiv Registrul de stat al populației.

19. Pentru identificarea solicitantului și verificarea identității acestuia se realizează în mod automatizat conversia în date a imaginilor preluate (crearea amprentei faciale) și compararea acestora cu cele din Registrul de stat al populației. Verificarea identității solicitantului este efectuată pe baza potrivirii semnalmentelor biometrice faciale și a detectării biometrice a vieții printr-un algoritm de învățare profundă. În timpul sesiunii de verificare a identității, pentru a determina vivacitatea semnalmentelor biometrice faciale ale solicitantului se face o comparație între un instantaneu luat dintr-un flux video selfie cu imaginea persoanei citită de pe componenta de securitate a actului de identitate, după caz, preluată din Registrul de stat al populației.

20. În procesul de identificare a persoanei la distanță utilizând mijloace digitale sunt permise numai actele de identitate identificabile în mod clar, aflate în termenul de valabilitate și emise de o autoritate publică competentă.

21. Serviciul de identificare a persoanei la distanță trebuie să implementeze cerințele tehnice și de securitate care permit verificarea autenticității, validității și integrității actelor de identitate utilizate în procesul de identificare utilizând mijloace digitale, în concordanță cu standardele în domeniu.

22. Pentru verificarea identității persoanei la distanță se utilizează atât acte de identitate, a căror imagine este capturată prin mijloace video sau sunt verificate criptografic folosind tehnologia NFC pentru citirea componentei de securitate a acestuia, cât și date sau informații obținute din surse credibile și independente, în măsura în care sunt disponibile, inclusiv pe bază de acorduri/parteneriate încheiate între instituții publice sau private și furnizorii de servicii de identificare.

23. La etapa de verificare a datelor de identificare pentru sporirea nivelului de asigurare, suplimentar măsurilor prevăzute la pct.18 și 19 se pot aplica următoarele măsuri:

1) efectuarea de către solicitant a unei tranzacții cu sumă zero cu propriul card bancar pentru validarea numelui și prenumelui acestuia;

2) verificarea numărului de telefon și adresa de e-mail a solicitantului prin verificarea codului cu o singură utilizare (OTP-One Time Password);

3) geolocalizarea dispozitivului solicitantului și preluarea datelor despre acesta.

24. La verificarea identității solicitantului fața, capul și umerii acestuia trebuie să fie vizibile și încadrate. Fața trebuie să fie liberă de umbre și descoperită și să se distingă clar de fundal și alte obiecte și să fie recunoscută.

25. Serviciul de identificare a persoanei la distanță, după caz operatorul, poate îndruma solicitantul să-și schimbe poziția corpului și să se introducă pe sine, după caz și actul de identitate în cadru pentru a face posibilă identificarea persoanei și verificarea identității persoanei.

26. Serviciul de identificare a persoanei la distanță, după caz operatorul, poate cere îndepărtarea obiectelor care acoperă capul sau fața și ochelarii.

27. La verificarea identității solicitantului se au în vedere următoarele aspecte, dar fără a se limita la acestea:

1) să se asigure că fotografia și elementele înscrise pe actul de identitate corespund solicitantului care parcurge procedura de identificare a persoanei la distanță utilizând mijloace digitale;

2) să se asigure că informațiile conținute în actul de identitate sunt corecte și valabile, în raport cu solicitantul care parcurge procedura de identificare a persoanei la distanță utilizând mijloace digitale;

3) să se asigure că informațiile furnizate de solicitantul care parcurge procedura de identificare a persoanei la distanță utilizând mijloace digitale sunt corecte;

4) în cazul în care identificarea solicitantului la distanță prin metode digitale se realizează în mod automatizat, solicitările sau secvențele video trebuie să conțină un element aleatoriu pentru a preveni riscul de preînregistrare a procesului de identificare la distanță prin mijloace digitale;

5) să se efectueze verificarea încrucișată a informațiilor furnizate de solicitant care parcurge procedura de identificare a persoanei la distanță utilizând mijloace digitale și a informațiilor rezultate din calculul automat al citirii caracterelor MRZ, atunci când este posibil;

6) să se solicite, dacă este cazul, alte documente și/sau informații prin care să se verifice identitatea.

28. Cerințele tehnice și organizatorice în procesul de identificare a solicitantului la distanță utilizând mijloace digitale sunt următoarele:

1) identificarea persoanei la distanță prin mijloace digitale este efectuată în timp real, într-o sesiune unică și fără întreruperi/pauze, iar în cazul necesității validării suplimentare a probelor colectate de către un operator, transmiterea rezultatului verificării identității la distanță se va realiza într-un termen de maxim 24 de ore din momentul finalizării sesiunii;

2) integritatea și confidențialitatea comunicării trebuie asigurată în mod corespunzător prin utilizarea unui canal criptat;

3) înregistrarea trebuie să prevadă în mod clar data și ora, fie în cuprinsul acesteia, fie în metadate;

4) calitatea comunicării trebuie să fie adecvată pentru a permite identificarea clară a caracteristicilor feței solicitantului și, după caz, a elementelor de securitate ale actelor de identitate;

5) furnizorul de servicii de identificare trebuie să pună la dispoziția publicului lista completă a actelor de identificare acceptate în scopurile prevăzute de prezenta procedură.

29. Dacă nu sunt îndeplinite condițiile tehnice necesare desfășurării corespunzătoare a procesului de verificare a identității, de exemplu: în cazuri de calitate slabă a imaginii, condiții slabe de lumină sau sunet ori întreruperi în transmisia video, procesul de identificare a persoanei la distanță utilizând mijloace digitale trebuie întrerupt, urmând a se relua.

30. Ori de câte ori actul de identitate prezentat în timpul procesului de identificare a persoanei la distanță utilizând mijloace digitale oferă îndoieli cu privire la conținutul său în ceea ce privește autenticitatea, actualitatea și exactitatea informațiilor oferite, procesul de identificare a persoanei la distanță prin mijloace digitale se va întrerupe, caz în care furnizorul de servicii de identificare va documenta motivele întreruperii pentru evidențe interne și pentru controale/audituri externe viitoare.

31. Ori de câte ori, în timpul identificării utilizând mijloace digitale, există suspiciuni cu privire la veridicitatea elementelor de identificare, procesul de identificare nu produce efectele dovedirii elementelor de identificare pentru care este destinat, acesta va fi întrerupt, caz în care furnizorul de servicii de identificare va documenta motivele întreruperii pentru evidențe interne și pentru controale/audituri externe viitoare.

32. Datele colectate în procesul identificare și verificare a identității solicitantului, indiferent de sursa acestora, împreună cu constatările și rezultatul verificării se păstrează în dosarul electronic de evidență pentru o perioadă de 15 ani.

33. Serviciul de identificare și verificare a identității la distanță protejează confidențialitatea și integritatea dosarului electronic de evidență.

34. După verificarea identității solicitantului, serviciul de identificare a persoanei la distanță comunică în regim automatizat serviciului client rezultatul procesului de verificare a identității, inclusiv verdictul (reușit sau nereușit), motivul eșecului, dacă este cazul, atributele de identitate referitoare la solicitantul verificat și orice alte date suplimentare solicitate de către serviciul client care nu sunt parte a procesului identificare și verificare a identității la distanță, dar care sunt utilizate de către serviciul client pentru înregistrarea în calitate de client a solicitantului sau pentru prestarea unui serviciu.

35. Identificarea persoanei la distanță cu ajutorul mijloacelor digitale este considerată nereușită dacă:

1) solicitantul a transmis în mod intenționat date care nu corespund datelor de identificare colectate din surse externe de date;

2) sesiunea expiră sau este întreruptă în timpul identificării unei persoane, a interviului, ori fluxul de informații nu asigură transmiterea de sunet și imagini sincronizate, clare, înregistrabile și reproductibile, care trebuie să fie suficiente pentru a înțelege fără ambiguitate și încredere că conținutul transmis este sigur;

3) solicitantul refuză să respecte instrucțiunile serviciului de verificare a identității sau a operatorului specificate la pct. 24-26.

36. Se interzice utilizarea datelor obținute de către furnizorii de servicii de identificare în procesul de identificare a persoanei la distanță prin mijloace digitale

din diverse surse în alte scopuri, fără consimțământul persoanei sau alte prevederi legale în acest sens.

37. Furnizorul de servicii de identificare este responsabil pentru luarea tuturor măsurilor care să asigure confidențialitatea datelor de identificare ale persoanei, securitatea transmisiei, autenticitatea, integritatea și conservarea înregistrării.

III. CERINȚE PENTRU REALIZAREA PROCEDURII DE IDENTIFICARE A PERSOANEI LA DISTANȚĂ UTILIZÂND MIJLOACE DIGITALE

Secțiunea 1
Cerințe generale

38. Identificarea persoanei la distanță utilizând mijloace video se realizează cu ajutorul unui sistem informatic.

39. La identificarea persoanei la distanță se utilizează mijloace digitale de înaltă încredere, care garantează identificarea veridică a unei persoane și permite prevenirea modificării sau utilizării abuzive a datelor transmise.

40. Fluxul de informații care conține imaginea și/sau sunetul este înregistrat în așa fel încât să permită reproducerea acestuia cu o calitate egală cu transmisia inițială a sunetului și imaginii sincronizate.

41. Fluxul de informații care conține imagine și/sau sunet trebuie înregistrat cu marca temporală, adresa IP a solicitantului, numărul de identificare de stat al persoanei fizice care urmează să fie identificată. Marca temporală trebuie să fie legată de datele care o privesc astfel încât să poată fi identificate orice modificare ulterioară a datelor, persoana care a făcut modificările, data, ora, modul și motivul acestora.

42. Furnizorul de servicii de identificare trebuie:

1) să elaboreze și să mențină o descriere detaliată a arhitecturii sistemului informatic a serviciului de identificare a persoanei la distanță;

2) să elaboreze și să mențină un plan de reziliență pentru a se asigura că informațiile relevante rămân accesibile, pentru o perioadă adecvată de timp, în scopul furnizării de dovezi legale și al continuității activității;

3) să înregistreze toate prelucrările de date și acțiunile automatizate efectuate de operatori în cadrul unei verificări a identității la distanță;

4) să se asigure că informațiile furnizate nu sunt false sau înșelătoare;

5) să furnizeze serviciul în mod imparțial, cu bună-credință și cu respect pentru solicitanți, beneficiarii serviciului, personalul și infrastructura acestora;

6) să furnizeze suficiente dovezi că modul în care funcționează, nu este de natură să-și compromită imparțialitatea și calitatea serviciului său către client sau să dea naștere unor conflicte de interese;

7) să aibă licențe valabile pentru instrumentele (software sau hardware) utilizate pentru furnizarea serviciului;

8) să solicite clientului să-l informeze cu privire la orice cerințe legale și de reglementare specifice cărora le sunt supuși, în special cele referitoare la sectorul său de activitate.

43. Dacă serviciul necesită instalarea unei anumite aplicații pe dispozitivul solicitantului, furnizorul de servicii de identificare asigură disponibilitatea aplicației

mobile prin publicarea pe principalele platforme/magazine online de aplicații mobile.

44. Furnizorul de servicii de identificare după publicarea aplicațiilor monitorizează platformele/magazinele online de aplicații mobile pentru a detecta disponibilitatea aplicațiilor frauduloase menite să înlocuiască aplicația legitimă a serviciului.

Secțiunea a 2-a
Evaluarea și managementul riscurilor

45. Furnizorul de servicii de identificare asigură realizarea și revizuirea cel puțin o dată pe an a unei evaluări a riscurilor legate de furtul de identitate și a unei evaluări a riscurilor legate de securitatea sistemelor informatice.

46. În evaluarea riscurilor legate de furtul de identitate, furnizorul de servicii de identificare identifică scenariile de risc legate de:

1) contrafacerea și falsificarea actelor de identitate prin mijloace fizice, inclusiv cel puțin următoarele:

a) utilizarea unui act de identitate contrafăcut pentru a crea o identitate falsă;

b) utilizarea unui act de identitate contrafăcut pentru a sustrage identitatea unei persoane existente;

c) utilizarea unui act de identitate falsificat pentru a crea o identitate falsă;

d) utilizarea unui act de identitate falsificat pentru a sustrage identitatea unei persoane existente.

2) contrafacerea și falsificarea actelor de identitate prin mijloace digitale, inclusiv cel puțin următoarele:

a) prezentarea unui act de identitate „virtual” (de exemplu modelarea unei imagini de transpus pe videoclipul actului de identitate) pentru a crea o identitate falsă - atunci când autenticitatea actului de identitate nu este verificată criptografic folosind componenta de securitate;

b) inserarea de date frauduloase (fotografie, date de identitate etc.) în locul datelor prezente pe actul de identitate pentru a crea o identitate falsă - atunci când autenticitatea actului de identitate nu este verificată criptografic folosind componenta de securitate;

c) compromiterea secretelor criptografice sau exploatarea unei vulnerabilități în protocolul criptografic pentru modificarea datelor de identificare extrase din actul de identitate - atunci când autenticitatea actului de identitate este verificată criptografic folosind componenta de securitate.

3) modificarea aspectului solicitantului prin mijloace fizice, inclusiv cel puțin următoarele:

a) folosirea unei măști „fizice” (de exemplu din latex) care seamănă cu o persoană existentă pentru a-i fura identitatea;

b) folosirea machiajului pentru a se face să arate ca o persoană existentă pentru a-i fura identitatea.

4) modificarea aspectului solicitantului prin mijloace digitale, inclusiv cel puțin următoarele:

a) utilizarea unei măști „virtuale” (de exemplu, modelarea unei măști virtuale din videoclipuri sau fotografii) care seamănă cu o persoană existentă pentru a-i fura identitatea;

b) înserarea de fotografii sau videoclipuri frauduloase ale feței unei persoane existente pentru a înlocui datele furnizate la etapa de colectare pentru a-i sustrage identitatea;

c) utilizarea tehnologiilor „deep-fake” pentru a genera imaginea și/sau vocea unei persoane existente în fluxul video și/sau audio.

5) asemănarea solicitantului cu o persoană existentă pentru a fura identitatea acelei persoane (sosie, geamăn etc.).

6) furtul identității prin reluarea fluxurilor video și/sau audio a unei sesiuni de înregistrare anterioare.

7) influența asupra comportamentului solicitanților, inclusiv cel puțin următoarele:

a) generarea unei constrângeri asupra solicitantului care îl obligă să se identifice de la distanță (ex. amenințare fizică, șantaj etc.);

b) atragerea solicitantului prin invitarea acestuia să se identifice de la distanță la un alt serviciu decât cel pe care crede că îl accesează, pentru a-și colecta datele de identificare.

47. Furnizorul de servicii de identificare revizuie evaluarea riscurilor legate de furtul de identitate ori de câte ori se modifică politica de verificare a identității la distanță sau în dependență de evoluțiile tehnologice.

48. În evaluarea riscurilor legate de securitatea sistemelor informatice, furnizorul de servicii de identificare identifică scenarii de risc legate de:

1) scurgere de date cu caracter personal;

2) scurgerea de informații sensibile referitoare la procesele de detectare a fraudelor.

49. Furnizorul de servicii de identificare revizuie evaluarea riscurilor legate de securitatea sistemelor informatice în cazul oricăror modificări structurale ale sistemului informatic al serviciului de identificare a persoanei la distanță, inclusiv modificări ale găzduirii, infrastructurii sau arhitecturii acestuia sau modificări ale politicii de verificare a identității.

50. Furnizorul de servicii de identificare trebuie să elaboreze un plan de management al riscului care să acopere întreaga sferă a serviciului de verificare a identității electronice și să fie asociat cu toate evaluările de risc identificate în pct. 46.

51. De asemenea, furnizorul de servicii de identificare elaborează și menține un plan pentru a testa capacitatea efectivă a serviciului de a detecta tentativele de furt de identitate:

1) pentru autenticitatea actului de identitate:

a) testarea eficacității măsurilor aplicate în cadrul planului de gestionare a riscurilor pentru a reduce riscurile legate de contrafacerea și falsificarea actelor de identitate prin mijloace fizice sau digitale identificate în evaluarea riscuri legate de furtul de identitate - atunci când autenticitatea actului de identitate nu este verificată criptografic folosind componenta de securitate;

b) măsurarea ratelor de fals respingere (FRR) și fals acceptare (FAR) realizate efectiv de serviciu în contextul detectării riscurilor legate de contrafacerea și falsificarea actelor de identitate prin mijloace fizice sau digitale identificate în evaluarea riscurilor legate de furtul de identitate - atunci când autenticitatea actului de identitate nu este verificată criptografic folosind componenta de securitate.

2) pentru detectarea biometrică a vieții:

a) testarea eficacității măsurilor aplicate în cadrul planului de management al riscurilor pentru reducerea riscurilor legate de modificarea aspectului solicitantului prin mijloace fizice sau digitale identificate în evaluarea riscurilor legate de furtul de identitate;

b) măsurarea ratelor de fals respingere (FRR) și fals acceptare (FAR) realizate efectiv de serviciu în detectarea riscurilor legate de modificarea aspectului solicitantului prin mijloace fizice sau digitale identificate în evaluarea riscurilor legate de furtul de identitate.

3) pentru compararea semnalmentelor biometrice faciale ale solicitantului:

a) testarea eficacității măsurilor aplicate în cadrul planului de gestionare a riscurilor pentru a reduce riscurile legate de asemănarea firească a solicitantului cu o altă persoană (sosie, geamăn etc.);

b) măsurarea ratelor de fals respingere (FRR) și fals acceptare (FAR) realizate efectiv de serviciu prin compararea semnalmentelor biometrice faciale ale solicitantului cu fotografia din actul de identitate, după din Registrul de stat al populației.

4) pentru riscurile legate de influențarea comportamentului solicitantului - testarea eficacității măsurilor aplicate în cadrul planului de management al riscurilor pentru a reduce riscurile legate de influențarea comportamentului solicitanților identificate în evaluarea riscurilor privind furtul de identitate.

52. Furnizorul de servicii de identificare trebuie să execute planul de testare anual și ori de câte ori are loc o modificare structurală a serviciului, o actualizare a evaluărilor riscurilor sau a planului de management al riscului.

Secțiunea a 3-a
Politica de verificare a identității de la distanță

53. Furnizorul de servicii de identificare trebuie să elaboreze și să mențină o politică de verificare a identității la distanță.

54. Furnizorul de servicii de identificare se asigură că solicitanții și clienții au acces ușor, direct și permanent la politica de verificare a identității la distanță.

55. Politica de verificare a identității la distanță trebuie:

1) să identifice dacă serviciul de identificare a persoanei la distanță operează cu mijloace de verificare automatizate fără operator uman sau prin mijloace de verificare cu operator uman;

2) să identifice atributele actului de identitate care caracterizează unicitatea identității unei persoane fizice;

3) să precizeze că furnizorul de servicii respectă principiul minimizării datelor colectate și păstrate;

4) să identifice toate datele personale referitoare la solicitanți prelucrate de serviciul de identificare a persoanei la distanță;

5) să identifice care dintre datele personale ale solicitantului prelucrate de serviciu pot face obiectul prelucrării biometrice;

6) să interzică corectarea sau ștergerea de către solicitant a dosarului electronic de evidență și a rezultatelor verificării la distanță a identității transmise serviciului client, precum și a tuturor informațiilor necesare stabilirii rezultatului;

7) să interzică accesul solicitantului la datele care au făcut obiectul unei prelucrări automate sau manuale, a căror dezvăluire poate oferi informații despre natura verificărilor efectuate de serviciu și referitoare la detectarea furtului de identitate;

8) să identifice toate limbile acceptate de serviciul de identificare a persoanei la distanță și să indice că serviciul acceptă cel puțin limba română;

9) să precizeze că serviciul, înainte de a obține date de identificare, trebuie să ceară solicitantului limba pe care dorește să o folosească, atunci când serviciul acceptă una sau mai multe limbi, altele decât româna;

10) să identifice cerințele care pot fi făcute de către serviciu către solicitant pentru colectarea corectă a datelor din actul de identitate (luminozitate, focalizare, strălucire etc.);

11) să descrie solicitările care pot fi făcute de către serviciu solicitantului în procesul de colectare și verificare a datelor de identificare (ex. luminozitate, focalizare, îndepărtarea ochelarilor solicitantului etc.);

12) să identifice actele de identitate acceptate de serviciul de identificare a persoanei la distanță;

13) să indice că numai actele de identitate neexpirate sunt acceptate de către serviciu;

14) să precizeze că, dacă se efectuează o verificare a valabilității actului de identitate, iar verificarea validității concluzionează că actul de identitate este invalid, atunci verdictul verificării identității la distanță este întotdeauna „nereușit”;

15) atunci când autenticitatea actului de identitate nu este verificată criptografic folosind componenta de securitate:

a) să descrie modul în care sunt verificate actele de identitate modificate fizic (acte de identitate rupte sau deteriorate etc.);

b) să precizeze rezoluția minimă post-compresie a actului de identitate video acceptat de serviciu. Această rezoluție minimă nu poate fi mai mică de 720p: 1280 × 720 la 25 de cadre pe secundă;

16) atunci când autenticitatea actului de identitate este verificată criptografic folosind componenta de securitate:

a) să precizeze că verdictul dat de serviciu este automat „nereușit”, fără intervenția operatorului, dacă procesele automatizate de verificare a autenticității a actului de identitate concluzionează că actul nu este autentic;

b) să menționeze că fotografia folosită pentru efectuarea comparației faciale este cea extrasă din componenta de securitate sau, după caz, preluată din Registrul de stat al populației;

17) să precizeze că autenticitatea actului de identitate este verificată criptografic folosind componenta de securitate a documentului respectiv. Dacă din punct de vedere tehnic sau juridic este imposibil să se utilizeze componenta de securitate a actului de identitate, sau dacă actul de identitate nu are componentă de securitate, actul de identitate nu poate fi acceptat;

18) să precizeze că, pentru fiecare act de identitate acceptat, valabilitatea actului de identitate este verificată sistematic prin intermediul unui serviciu furnizat de autoritatea emitentă a actului de identitate. Dacă acest serviciu nu există sau este indisponibil, actul de identitate nu poate fi acceptat;

19) să specifice rezoluția minimă după comprimare acceptată de serviciu pentru videoclipul feței solicitantului. Această rezoluție nu poate fi mai mică de 720p: 1280 × 720 la 25 de cadre pe secundă;

20) să precizeze că trebuie creat un dosar de dovezi pentru fiecare verificare a identității, indiferent de verdict („reușit” sau „nereușit”);

21) să identifice componentele dosarului electronic de evidență. Aceste elemente trebuie să ofere informațiile necesare soluționării litigiilor;

22) să specifice metodele de gestionare a cheii de decriptare a dosarului de dovezi și în special să permită accesul la această cheie numai celor care au nevoie să știe;

23) trebuie să prevadă că solicitanții își pot exercita dreptul de acces la datele cu caracter personal deținute de furnizorul de servicii în dosarul de evidență, dar nu pot exercita dreptul la rectificarea acelui fișier;

24) să precizeze că rezultatul verificării identității la distanță este transmis sistematic către serviciul client, indiferent de verdict (reușit sau nereușit);

25) trebuie să indice că rezultatul verificării identității la distanță constă din verdictul (reușit sau nereușit) al verificării și atributele de identitate ale solicitantului (de exemplu: nume, prenume, sex, data nașterii, locul nașterii, numărul de identificare de stat al persoanei fizice, numărul actului de identitate, o fotografie a feței solicitantului luată din videoclipul feței solicitantului sau o sursă autentică, etc.), precum și orice date suplimentare solicitate de serviciul client;

26) să precizeze că videoclipurile cu actul de identitate și fața solicitantului nu sunt trimise în niciun fel către serviciul client, nici integral, nici parțial;

27) să precizeze întârzierea maximă dintre începerea colectării datelor de identificare ale solicitantului și notificarea rezultatului verificării identității către serviciul client.

56. În politica de verificare a identității la distanță se specifică expres că dosarul electronic de evidență conține cel puțin următoarele elemente:

1) datele de identificare:

a) videoclipul actului de identitate - atunci cînd autenticitatea actului de identitate nu este verificata criptografic folosind componenta de securitate;

b) fotografia solicitantului extrasă din componenta de securitate a actului de identitate - atunci cînd autenticitatea actului de identitate este verificata criptografic folosind componenta de securitate;

c) videoclipul sau o serie de poze ce includ fața solicitantului;

2) data colectării fiecărei date de identificare;

3) o listă a tuturor verificărilor efectuate asupra datelor de identificare și pentru fiecare verificare:

a) data verificării;

b) activitatea asociată verificării, în special:

- verificarea autenticității actului de identitate;
- detectarea vivacității semnalmentelor biometrice faciale a solicitantului;
- compararea semnalmentelor biometrice faciale ale solicitantului;

c) tipul verificării: automată sau manual;

d) identitatea operatorului care a efectuat verificarea, dacă a fost efectuată manual;

e) versiunea și configurația, dacă există, a instrumentelor care au efectuat verificarea, dacă au fost efectuate automat;

f) constatarea intermediară returnată de prelucrarea automatizată, operatorului în urma verificării, dacă este necesară o validare manuală;

4) verdictul verificării identității la distanță (reușit sau nereușit);
5) motivele care au generat verdictul „nereușit”;
6) identitatea operatorului care a emis verdictul, în cazul verificării manuale;
7) data la care a fost emis verdictul;
8) numele și prenumele solicitantului;
9) numărul de identificare de stat al persoanei fizice;
10) data nașterii solicitantului;
11) numărul unic al actului de identitate;
12) data emiterii actului de identitate;
13) data de expirare a actului de identitate;
14) rezultatul verificării identității la distanță trimisă serviciului client.

NOTA INFORMATIVĂ
la proiectul hotărârii Guvernului privind aprobarea procedurii de identificare a persoanei la distanță utilizând mijloace digitale

1. Denumirea autorului proiectului

Proiectul hotărârii Guvernului este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, cu participarea Agenției de Guvernare Electronică, Consiliului Economic pe lângă PM și suportul UK-GGF.

2. Condițiile ce au impus elaborarea proiectului și finalitățile urmărite

Transformarea digitală este un obiectiv cheie asumat de către Guvern. Un factor cheie în transformarea digitală a unei societăți îl constituie identitatea și semnătura electronică – componentă esențială a infrastructurii pe care se va construi viitorul sistemelor de e-guvernare și de e-servicii private. Posibilitatea identificării electronice a cetățeanului, de rând cu semnătura electronică, oferă instrumentarul necesar pentru a face acțiuni obligatorii, din punct de vedere legal și în regim online – oriunde și oricând – ce reprezintă un avantaj imens, atât pentru cetățeni, companii, cât și pentru Guvern.

Ecosistemul de identitate și semnătură electronică este o parte esențială a strategiei digitale a oricărui guvern, către procese digitalizate, sigure, fără hârtie, durabile și cooperarea transfrontalieră sau inter-instituțională. Cererea de semnături electronice apare de fiecare dată când este nevoie de a lega o decizie sau o tranzacție de o anumită persoană sau entitate și de a asigura integritatea datelor. Posibilitatea de a conduce toate afacerile și interacțiunile din domeniul digital, a devenit mai presantă, deoarece contactul fizic în contextul actual este adesea limitat sau costisitor.

În Republica Moldova, serviciile electronice există în majoritatea sectoarelor guvernamentale și reprezintă un canal de livrare mai ușor și mai convenabil, decât canalele tradiționale de prestare a serviciilor publice.

În anul 2022, Parlamentul a adoptat Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere, scopul căreia este armonizarea parțială a legislației naționale cu 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.

Legea nr. 124/2022, prin care s-a transpus parțial Regulamentul (UE) nr. 910/2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă, introduce prevederi pentru identificarea electronică, ca fiind o pârghie cheie pentru dezvoltarea unei piețe exclusiv digitale. Identificarea electronică constituie o soluție digitală care oferă dovada identității cetățenilor, pentru a accesa servicii online sau pentru a efectua tranzacții online. Mai exact, în conformitate cu articolul 10, alineatul (4) litera d) din lege, se permit aplicarea mijloacelor alternative la prezența fizică pentru verificarea identității, în contextul eliberării de certificate calificate și deschide calea pentru verificarea

identității de la distanță utilizând metode alternative de identificare de la distanță a persoanei stabilite de către Guvern.

Prin modificările operate la Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Legea nr. 66/2023 cu privire modificarea unor acte normative), legiuitorul a reglementat și posibilitatea entităților raportoare (bănci, societăți de investiții, asiguratori, organizații de creditare nebancare etc.) de a aplica un set de mijloace electronice pentru identificarea și verificarea identității clienților.

Mai mult ca atât, prin promovarea Pachetului legislativ de digitalizare 1.0 (Legea175/2021) și Pachetul legislativ pentru dezvoltarea afacerilor la distanță în Republica Moldova (Legea 126/2023), Guvernul a realizat pași consecvenți spre digitalizarea afacerilor din țară, atât pentru antreprenorii locali, cât și pentru investitorii de peste hotare (fie din diasporă, sau cetățeni străini) – proces în care sunt indispensabile implementarea instrumentelor de identificare la distanță și de oferire a accesului la serviciile de semnătură electronică.

Transformarea digitală a societății a creat necesitatea de a putea identifica de la distanță persoanele care doresc să acceseze servicii online publice sau private, atunci când nu au o identitate digitală recunoscută de aceste servicii.

Pentru a garanta fiabilitatea acestor procese, procedura stabilește o serie de reguli, precum și cerințe de ordin tehnic și de securitate, pe care furnizorii de servicii de identificare a persoanei la distanță utilizând mijloace digitale, trebuie să le implementeze. Un serviciu de identificare a persoanei la distanță are același scop ca și verificarea față în față a identității, și anume – comunicarea directă, verificarea autenticității actului de identitate prezentat de solicitant și că acesta este deținătorul legitim al actului respectiv. Obiectivul principal al persoanelor rău intenționate față de un serviciu de identificare a persoanei la distanță este același ca și în cazul verificării față în față a identității, și anume - furtul sau modificarea identității unei persoane, doar că în cazul procedurilor electronice sunt anumite riscuri suplimentare, dar si instrumente mai variate de contracarare a acestor fraude. Procedura propusă stabilește o serie de cerințe aplicabile pentru serviciile de identificare a persoanei la distanță pentru a oferi un nivel de asigurare bazat pe riscurile și profilurile atacatorilor și are scopul de a reduce substanțial riscul de furt sau modificare a identității unei persoane. Procedura nu impune prin sine nici-o arhitectură pentru sistemul informatic al serviciului de identificare a persoanei la distanță, astfel încât la etapa dezvoltărilor pot fi luate în considerare de către prestatorii de servicii de încredere mai multe implementări. De asemenea, Procedura nu impune restricții referitoare la tipologia sau organizarea furnizorilor de servicii de verificare a identității la distanță, care pot fi instituții publice sau private.

Digitalizarea procedurii standard de identificare și înregistrare la distanță a clientului va contribui, la reducerea costurilor operațiunilor de desfășurare a afacerilor, accesarea serviciilor publice și comerciale, economisirea timpului și resurselor pentru comerțul transfrontalier, precum și îmbunătățirea securității datelor, reducerea costurilor administrative și a riscurilor de corupție prezente în cazul proceselor bazate pe interacțiunea fizică, sprijinind în același timp strategia mai amplă de digitalizare a Guvernului Moldovei și eforturile de guvernare

electronică. Capacitatea de verificare a identificării de la distanță promovează și crește posibilitatea tranzacțiilor electronice, asigurând totodată valabilitatea identității părților implicate în tranzacție.

Digitalizarea procedurii standard de identificare și înregistrare la distanță a clientului va contribui, de asemenea la diversificarea în regim online a posibilităților de eliminare a fraudelor, reducerea timpului și economisirea resurselor pentru comerțul transfrontalier, precum și îmbunătățirea securității datelor, reducerea costurile administrative și a riscurilor de corupție prezente în cazul proceselor bazate pe interacțiunea fizică.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul nu conține norme de armonizare a legislației naționale cu legislația Uniunii Europene, dar deschide oportunități pentru aplicarea bunelor practici europene în acest sens.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul cuprinde norme care au ca obiectiv reglementarea procesului de identificare a persoanei la distanță utilizând mijloace digitale. Procedura stabilește regulile și cerințele minime tehnice și de securitate pentru realizarea identificării și verificării la distanță a persoanei, utilizând mijloace digitale. De asemenea, procedura impune o serie de cerințe și responsabilității pentru furnizorii de servicii de identificare a persoanei la distanță utilizând mijloace digitale.

5. Fundamentarea economico-financiară

Pentru implementarea prevederilor proiectului nu este necesară alocarea resurselor financiare de la bugetul de stat.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Proiectul de hotărâre a Guvernului se integrează organic în cadrul normativ în vigoare și se întemeiază pe competențele Guvernului stabilite în art. 10 alin. (2) pct. 4) lit. d) din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere.

7. Avizarea și consultarea publică a proiectului

În conformitate cu procedurile stabilite pentru transparența în procesul decizional şi în vederea elaborării actelor normative, anunțul de inițiere a procesului de elaborare a proiectului de hotărâre a Guvernului a fost plasat pe portalul guvernamental particip.gov.md - https://particip.gov.md/ro/document/stages/anunt-de-initiere-a-procesului-de-elaborare-a-proiectului-de-hotarare-a-guvernului-privind-aprobarea-procedurii-de-identificare-a-persoanei-la-distanta-utilizand-mijloace-digitale/10956

8. Constatările altor expertize

Proiectul nu cade sub incidența altor expertize necesare de a fi efectuate în condițiile Legii nr.100/2017 cu privire la actele normative, dat fiind faptul că nu reglementează activitatea de întreprinzător, nu conține reglementări cu impact asupra bugetului public național sau a unor componente din cadrul acestuia și nu prevede reorganizări și reforme structurale sau instituționale ale autorităților ori ale instituțiilor publice. Prin urmare, proiectul nu cade sub incidența Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr.23/2019.

Secretar de stat **Mihai LUPAȘCU**