Construim înCREDere!

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

AVIZ

asupra proiectului de Lege privind cooperarea polițienească internațională

(proiect aprobat prin Decizia protocolară nr. 34 a Guvernului din 12 august 2026; transpune parțial Regulamentul (UE) 2024/982 – „Prüm II", Decizia 2008/615/JAI a Consiliului și Directiva (UE) 2023/977)

Chișinău, 25 august 2026

I. Obiectul avizului

Mișcarea Civică „Construim Încredere" a analizat proiectul de Lege privind cooperarea polițienească internațională, prin care Republica Moldova instituie cadrul juridic pentru interogarea și schimbul de date polițienești cu statele membre ale Uniunii Europene, cu Europol, INTERPOL și alte state, inclusiv în regim automatizat.

Proiectul vizează categorii deosebit de sensibile de date — profiluri ADN, date dactiloscopice, imagini faciale, date despre vehicule, evidențe ale poliției, documente de călătorie, permise de conducere, precum și date privind persoanele dispărute și cadavrele neidentificate. El marchează trecerea de la o cooperare polițienească bazată preponderent pe cereri și răspunsuri la una în care o parte importantă a verificărilor se poate efectua automatizat și aproape instantaneu.

II. Poziția generală a Mișcării

Mișcarea susține obiectivul proiectului. Alinierea la standardele europene de cooperare polițienească și transpunerea Regulamentului Prüm II reprezintă un pas necesar pe traiectoria de integrare europeană a Republicii Moldova și un instrument legitim de prevenire și combatere a criminalității transfrontaliere.

În același timp, tocmai pentru că mecanismul operează cu cele mai sensibile categorii de date cu caracter personal — biometrice și genetice — nivelul garanțiilor trebuie să fie pe măsura riscurilor. În forma actuală, proiectul reglementează temeinic „ce" date se schimbă și „cu cine", dar lasă insuficient reglementat „cum" se asigură securitatea, controlul accesului și protecția efectivă a cetățeanului. O parte esențială a acestor garanții este amânată către acte normative subsecvente ale Guvernului, ceea ce slăbește previzibilitatea legii și controlul parlamentar și public asupra unor chestiuni ce privesc drepturi fundamentale.

Avizul de față este unul constructiv: recunoaște elementele valoroase ale proiectului, semnalează lacunele de fond și propune soluții concrete de îmbunătățire înainte de adoptare.

III. Elemente pozitive ale proiectului

Proiectul conține garanții importante, care trebuie păstrate și consolidate:

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

- limitarea datelor la categoriile expres prevăzute de lege și distincția pe categorii de persoane — bănuit, învinuit, condamnat, victimă, martor (art. 2 alin. (2));
- principiile schimbului de informații, între care legalitatea, minimizarea, utilizarea în cazuri individuale, responsabilizarea și controlul asupra difuzării ulterioare a datelor (art. 4);
- confirmarea manuală, de către personal calificat, a oricărei concordanțe („hit") înainte de valorificarea ei (art. 11 alin. (7), art. 14 alin. (3), art. 19 alin. (5));
- interdicția utilizării căutării automatizate a imaginilor faciale pentru crearea de profiluri ce pot duce la discriminare (art. 19 alin. (3));
- evaluarea impactului asupra protecției datelor (DPIA) și consultarea CNPDCP înainte de conectarea la Router/EPRIS (art. 46 alin. (6));
- jurnalizarea operațiunilor de acces și schimb de date, precum și controlul de legalitate exercitat de CNPDCP (art. 43, art. 45 alin. (6));
- dreptul persoanei la informare, rectificare, ștergere, plângere și despăgubire (art. 47).

IV. Preocupări de fond

1. Formulări prea largi și previzibilitatea legii

Domeniul de aplicare este definit foarte extins. Pe lângă schimbul de date, proiectul permite cooperarea prin INTERPOL, Europol, echipe comune, ofițeri de legătură, operațiuni comune și „alte forme de cooperare" (art. 1 alin. (2) lit. h), art. 2 alin. (3)). Sunt folosite formulări deschise, de tipul „fără a se limita la acestea" (de exemplu art. 3 pct. 17 și art. 6 alin. (4)). Pentru o lege organică ce autorizează prelucrarea automatizată a datelor biometrice, asemenea formulări reduc previzibilitatea și îngreunează controlul asupra limitelor reale ale mecanismului. Recomandăm circumscrierea expresă a formelor de cooperare și eliminarea ori delimitarea clară a clauzelor deschise.

2. Delegarea excesivă a garanțiilor esențiale către Guvern

Un număr mare de elemente determinante pentru protecția drepturilor sunt lăsate în sarcina actelor normative ale Guvernului: standardele de calitate a datelor (art. 10 alin. (5), art. 13 alin. (2)), structura numărului de referință pentru imaginile faciale (art. 17 alin. (2)), procedurile și cazurile umanitare de căutare (art. 22 alin. (2)), conținutul și termenele cererilor (art. 6 alin. (6)), organizarea punctului unic de contact și a punctelor naționale de contact (art. 6 alin. (7)), regimul de securitate al evidențelor (art. 42 alin. (4)) și altele. Garanțiile care privesc drepturi fundamentale ar trebui să aibă sediu în legea organică, nu în legislația secundară, pentru a asigura previzibilitate, dezbatere parlamentară și control public.

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

3. Lacune de securitate a datelor și de guvernanță a accesului

Deși proiectul menționează recurent „criptarea și alte măsuri tehnice și organizatorice” (art. 10 alin. (4), art. 13 alin. (4), art. 19 alin. (7) și altele), el nu stabilește un standard minim de securitate verificabil. Din analiza tehnico-juridică rezultă următoarele lacune:

a) Nivel minim de securitate (security baseline) nedefinit pentru integrări — lipsesc cerințele tehnice pentru Router, EPRIS, EUCARIS și INTERPOL, standardele de criptare, segmentarea rețelei și cerințele pentru copiile de rezervă / recuperare (backup/DR). Formula „criptare + măsuri tehnice și organizatorice” nu constituie un baseline: fiecare integrator ar implementa „după cum înțelege”.

b) Evaluare de securitate obligatorie înainte de punerea în funcțiune (go-live) — absentă și distinctă de DPIA. Lipsesc modelarea amenințărilor, testarea de vulnerabilități, verificarea go/no-go și aprobarea formală de securitate. DPIA (art. 46 alin. (6)) acoperă protecția datelor, nu maturitatea de securitate; art. 46 alin. (7) atribuie Agenției de Guvernare Electronică „controlul interconectării”, fără o procedură de evaluare.

c) Model insuficient de gestiune a identității și accesului (IAM). Art. 51 alin. (5) lit. d) și art. 45 alin. (2) prevăd drepturi de acces, autentificare, trasabilitate și liste de persoane autorizate, însă proiectul nu consacră: autentificarea multifactor (MFA), rolurile de acces (RBAC), principiul privilegiului minim, separarea sarcinilor (cine inițiază căutarea vs. cine confirmă „hit”-ul), revizuirea periodică a accesului cu termene, dezactivarea accesului la încetarea sau transferul din funcție, accesul de urgență („break-glass”) și desemnarea unui responsabil unic al modelului de acces. Legea permite acces automatizat la ADN, date dactiloscopice, imagini faciale și evidențe penale, dar nu definește cine proiectează, implementează și controlează accesul.

d) Politică unificată de retenție și ștergere — absentă. Termenele sunt fragmentate: 1 an (art. 28 alin. (3)), 3 ani (art. 43 alin. (4), art. 45 alin. (5)), 18 luni (art. 45 alin. (7)), „ștergere imediată” (art. 46 alin. (5)), plus trimiteri la actele Guvernului și la legislația națională. Lipsesc o matrice unică a termenelor pe categorii de date, reguli pentru copiile de rezervă și pentru rezultatele fals-pozitive, precum și corelarea clară între „ștergerea imediată” a datelor și păstrarea jurnalelor.

e) Model operațional de răspuns la incidente (incident response) — inexistent. Art. 9 alin. (6)–(7) prevede doar limitarea efectelor și notificarea partenerilor. Nu sunt reglementate clasificarea incidentelor pe niveluri de severitate, lanțul intern de escaladare, rolul de responsabil de incident, termenele de răspuns și recuperare și analiza post-incident — critice în cazul unei scurgeri de date biometrice.

f) Monitorizare de securitate insuficientă. Jurnalizarea pe 3 ani (art. 43) și verificarea anuală (art. 48) constituie audit trail, nu monitorizare. Lipsesc corelarea centralizată a jurnalelor (SIEM), alertarea în timp real, detectarea anomaliilor (interogări în masă, acces în afara

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

orelor, exporturi anormale) și jurnalele imuabile. Un acces neautorizat masiv poate rămâne nedetectat până la verificarea anuală.

g) Securitatea lanțului de aprovizionare și a terților — neacoperită. Lipsesc cerințele și clauzele de securitate pentru eu-LISA, INTERPOL și serviciile de găzduire, precum și controlul asupra sub-procesatorilor.

h) Managementul vulnerabilităților și al actualizărilor — absent. Lipsesc termenele de aplicare a corecțiilor, periodicitatea scanărilor și testarea de securitate după modificări.

i) Matrice de responsabilitate în materie de securitate — inexistentă. Nu există schema „sistem → proprietar → administrator → auditor → responsabil de incident" și nici un responsabil desemnat pentru postura de securitate a întregului mecanism.

4. Garanții insuficiente pentru cetățean

Deși art. 47 recunoaște drepturile la informare, rectificare, ștergere, plângere și despăgubire, exercitarea lor efectivă depinde de proceduri stabilite ulterior. Într-un mecanism automatizat și transfrontalier, în care o eroare se poate propaga rapid către mai multe state, cetățeanul are nevoie de un remediu clar, accesibil și rapid atunci când o informație transmisă despre el este greșită sau utilizată abuziv. Recomandăm consacrarea în lege a unui mecanism explicit de remediere și a obligației de informare a persoanei, cu termene ferme.

5. Ambiguitate în repartizarea controlului

Proiectul atribuie controlul securității interconectării Agenției de Guvernare Electronică (art. 46 alin. (7)), în timp ce CNPDCP exercită controlul de legalitate a prelucrării (art. 45 alin. (6), art. 46), iar incidentele cibernetice semnificative țin de autoritatea de securitate cibernetică. Coexistența acestor competențe, fără o delimitare clară, poate genera suprapuneri și zone fără responsabil. Recomandăm delimitarea expresă a rolurilor: CNPDCP — legalitatea prelucrării; Agenția de Guvernare Electronică — securitatea tehnică a interconectării; autoritatea de securitate cibernetică — incidentele; punctul unic de contact — guvernanța operațională și modelul de acces.

V. Întrebări adresate autorului proiectului și Parlamentului

1. Care sunt garanțiile concrete pentru protecția datelor persoanelor?
2. Cine controlează și verifică legalitatea schimbului de informații cu autoritățile străine?
3. Ce remediu are cetățeanul dacă informația transmisă despre el este greșită sau este utilizată abuziv?
4. În sarcina cărei instituții din subordinea Ministerului Afacerilor Interne se pune executarea acestui proiect de lege?

Proiectul răspunde parțial la a patra întrebare: executarea revine subdiviziunii specializate în cooperare polițienească internațională din subordinea Inspectoratului General al Poliției —

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

punctul unic de contact, incluzând Biroul Național Central INTERPOL, Punctul Național de Contact EUROPOL și Biroul Național SIRENE (art. 6). Rămâne însă neclar cine poartă răspunderea unică pentru securitatea și guvernanța accesului la nivelul întregului mecanism.

VI. Recomandări

Pentru ca mecanismul să fie deopotrivă eficient, sigur și demn de încrederea cetățenilor, Mișcarea recomandă completarea proiectului, înainte de adoptare, cu:

1. un standard minim de securitate (baseline) obligatoriu pentru toate integrările, consacrat în lege sau prin trimitere la un act normativ verificabil;
2. o evaluare de securitate obligatorie înainte de conectare (go-live), distinctă de DPIA, cu aprobare formală de securitate;
3. un model IAM explicit — MFA, RBAC, privilegiu minim, separarea sarcinilor, revizuirea accesului cu termene, dezactivare la încetarea funcției, acces de urgență și responsabil desemnat;
4. o matrice unică de retenție și ștergere pe categorii de date, cu reguli pentru copiile de rezervă și pentru rezultatele fals-pozitive;
5. un model de răspuns la incidente, cu clasificare, lanț de escaladare, termene și analiză post-incident;
6. monitorizare continuă de securitate — corelarea jurnalelor (SIEM), alertare, detectarea anomaliilor și jurnale imuabile;
7. cerințe de securitate pentru terți și pentru lanțul de aprovizionare, inclusiv clauze contractuale și drept de audit;
8. management al vulnerabilităților și al actualizărilor, cu termene și testare după modificări;
9. o matrice de responsabilitate în materie de securitate și desemnarea unui responsabil unic pentru postura de securitate a mecanismului;
10. delimitarea expresă a competențelor de control între CNPDCP, Agenția de Guvernare Electronică, autoritatea de securitate cibernetică și punctul unic de contact;
11. un mecanism de remediere clar și rapid pentru cetățeanul afectat de date greșite sau utilizate abuziv;
12. ridicarea în legea organică a garanțiilor esențiale delegate în prezent Guvernului.

VII. Concluzie

Mișcarea Civică „Construim Încredere” salută intenția de aliniere a Republicii Moldova la standardele europene de cooperare polițienească și susține adoptarea unui cadru modern în acest domeniu. Solicităm însă ca proiectul să fie completat cu garanțiile de securitate, de guvernanță a accesului și de protecție a cetățeanului enumerate mai sus, astfel încât puterea

Construim înCREDere!

str. M. Kogălniceanu 86, Chișinău
construim.incredere@gmail.com
www.construimincredere.md

sporită de a schimba date sensibile să fie însoțită de un control pe măsură. Numai un mecanism sigur și transparent poate merita încrederea cetățenilor — încredere pe care ne-am asumat să o construim.

Mișcarea Civică „Construim Încredere”
Chișinău, 25 august 2026