Construim înCREDere!

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

OPINION

on the Draft Law on International Police Cooperation

(draft approved by Protocol Decision No. 34 of the Government of 12 August 2026; partially transposing Regulation (EU) 2024/982 — "Prüm II", Council Decision 2008/615/JHA and Directive (EU) 2023/977)

Chișinău, 25 August 2026

I. Subject of the Opinion

The Civic Movement "Building Trust" has analysed the Draft Law on International Police Cooperation, through which the Republic of Moldova establishes the legal framework for querying and exchanging police data with the Member States of the European Union, Europol, INTERPOL and other states, including through automated mechanisms.

The draft concerns particularly sensitive categories of data — DNA profiles, fingerprint data, facial images, vehicle data, police records, travel documents, driving licences, as well as data concerning missing persons and unidentified human remains. It marks a transition from police cooperation based predominantly on requests and responses to a system in which a significant share of checks may be carried out automatically and almost instantaneously.

II. General Position of the Movement

The Movement supports the objective of the draft law. Alignment with European standards on police cooperation and the transposition of the Prüm II Regulation represent a necessary step on the Republic of Moldova's path towards European integration and a legitimate instrument for preventing and combating cross-border crime.

At the same time, precisely because the mechanism involves the most sensitive categories of personal data — biometric and genetic data — the level of safeguards must be commensurate with the risks. In its current form, the draft thoroughly regulates "what" data are exchanged and "with whom", but insufficiently regulates "how" security, access control and the effective protection of citizens are to be ensured. A substantial part of these safeguards is deferred to subsequent secondary legislation adopted by the Government, which

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

weakens the foreseeability of the law and parliamentary and public oversight over matters affecting fundamental rights.

This Opinion is constructive in nature: it acknowledges the valuable elements of the draft, identifies substantive gaps and proposes concrete solutions for improvement prior to adoption.

III. Positive Elements of the Draft

The draft contains important safeguards that should be preserved and strengthened:

● limitation of data to the categories expressly provided for by law and differentiation according to categories of persons — suspect, accused person, convicted person, victim, witness (Article 2(2));

● principles governing the exchange of information, including lawfulness, data minimisation, use in individual cases, accountability and control over further dissemination of data (Article 4);

● manual confirmation, by qualified personnel, of any match (“hit”) before it is acted upon (Article 11(7), Article 14(3), Article 19(5));

● prohibition on the use of automated facial-image searches to create profiles that may lead to discrimination (Article 19(3));

● a Data Protection Impact Assessment (DPIA) and consultation with the National Centre for Personal Data Protection (CNPDCP) before connection to the Router/EPRIS (Article 46(6));

● logging of data-access and data-exchange operations, as well as legality oversight exercised by the CNPDCP (Article 43, Article 45(6));

● the individual’s right to information, rectification, erasure, complaint and compensation (Article 47).

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

IV. Substantive Concerns

1. Overly Broad Wording and Foreseeability of the Law

The scope of application is defined very broadly. In addition to data exchange, the draft allows cooperation through INTERPOL, Europol, joint teams, liaison officers, joint operations and "other forms of cooperation" (Article 1(2)(h), Article 2(3)). Open-ended formulations such as "including but not limited to" are used (for example, Article 3 point 17 and Article 6(4)). For an organic law authorising the automated processing of biometric data, such wording reduces foreseeability and makes it more difficult to exercise oversight over the actual limits of the mechanism. We recommend expressly circumscribing the forms of cooperation and removing or clearly limiting open-ended clauses.

2. Excessive Delegation of Essential Safeguards to the Government

A large number of elements that are decisive for the protection of rights are left to Government regulations: data-quality standards (Article 10(5), Article 13(2)), the structure of the reference number for facial images (Article 17(2)), procedures and humanitarian cases for searches (Article 22(2)), the content and deadlines applicable to requests (Article 6(6)), the organisation of the Single Point of Contact and national contact points (Article 6(7)), the security regime applicable to records (Article 42(4)), among others. Safeguards concerning fundamental rights should be enshrined in the organic law itself rather than in secondary legislation, in order to ensure foreseeability, parliamentary debate and public oversight.

3. Gaps in Data Security and Access Governance

Although the draft repeatedly refers to "encryption and other technical and organisational measures" (Article 10(4), Article 13(4), Article 19(7), among others), it does not establish a verifiable minimum security standard. The technical and legal analysis reveals the following gaps:

a) No defined minimum security baseline for integrations. Technical requirements for Router, EPRIS, EUCARIS and INTERPOL are absent, as are encryption standards, network segmentation requirements and requirements regarding backups/disaster recovery (backup/DR). The formula "encryption + technical and organisational measures" does not constitute a security baseline: each integrator could implement it according to its own interpretation.

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

b) No mandatory security assessment prior to go-live, distinct from the DPIA. Threat modelling, vulnerability testing, go/no-go verification and formal security approval are missing. The DPIA (Article 46(6)) addresses data protection, not security maturity; Article 46(7) assigns the Electronic Governance Agency "control over interconnection", without establishing an assessment procedure.

c) Insufficient identity and access management (IAM) model. Article 51(5)(d) and Article 45(2) provide for access rights, authentication, traceability and lists of authorised persons, but the draft does not establish: multi-factor authentication (MFA), role-based access control (RBAC), the principle of least privilege, segregation of duties (who initiates the search versus who confirms the "hit"), periodic access reviews with defined deadlines, deactivation of access upon termination of employment or transfer to another position, emergency "break-glass" access, or the designation of a single person responsible for the access model. The law allows automated access to DNA profiles, fingerprint data, facial images and criminal records, yet it does not define who designs, implements and oversees access.

d) No unified retention and deletion policy. Retention periods are fragmented: 1 year (Article 28(3)), 3 years (Article 43(4), Article 45(5)), 18 months (Article 45(7)), "immediate deletion" (Article 46(5)), as well as references to Government regulations and national legislation. There is no single retention schedule by data category, no rules for backups and false-positive results, and no clear relationship between "immediate deletion" of data and retention of logs.

e) No operational incident-response model. Article 9(6)–(7) provides only for limiting the effects and notifying partners. There are no rules on classification of incidents by severity level, internal escalation chains, designation of an incident manager, response and recovery deadlines, or post-incident analysis — all of which are critical in the event of a biometric-data breach.

f) Insufficient security monitoring. Three-year logging (Article 43) and annual verification (Article 48) constitute an audit trail, not active monitoring. The draft lacks centralised log correlation through a Security Information and Event Management system (SIEM), real-time alerting, anomaly detection (bulk queries, access outside working hours, abnormal exports) and immutable logs. Large-scale unauthorised access could therefore remain undetected until the annual review.

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

g) Supply-chain and third-party security is not addressed. Security requirements and clauses concerning eu-LISA, INTERPOL and hosting services are absent, as is oversight of sub-processors.

h) Vulnerability and update management is absent. The draft establishes no deadlines for applying security patches, no required frequency for vulnerability scans and no mandatory security testing following system changes.

i) No security responsibility matrix. There is no clear scheme of "system → owner → administrator → auditor → incident manager", nor is there a designated person with overall responsibility for the security posture of the entire mechanism.

4. Insufficient Safeguards for Citizens

Although Article 47 recognises the rights to information, rectification, erasure, complaint and compensation, their effective exercise depends on procedures to be established subsequently. In an automated and cross-border mechanism, where an error can quickly propagate to multiple states, individuals need a clear, accessible and rapid remedy when information transmitted about them is inaccurate or misused. We recommend enshrining in the law an explicit redress mechanism and an obligation to inform the person concerned, subject to firm deadlines.

5. Ambiguity in the Allocation of Oversight Responsibilities

The draft assigns oversight of interconnection security to the Electronic Governance Agency (Article 46(7)), while the CNPDCP exercises oversight over the lawfulness of data processing (Article 45(6), Article 46), and significant cybersecurity incidents fall within the competence of the cybersecurity authority. The coexistence of these competences, without clear delineation, may create both overlaps and accountability gaps. We recommend expressly defining the respective roles: CNPDCP — lawfulness of processing; Electronic Governance Agency — technical security of interconnection; cybersecurity authority — incidents; Single Point of Contact — operational governance and the access model.

V. Questions Addressed to the Author of the Draft and to Parliament

1. What concrete safeguards are in place to protect individuals' personal data?

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

2. Who monitors and verifies the lawfulness of information exchange with foreign authorities?
3. What remedy is available to an individual if information transmitted about them is inaccurate or is used unlawfully?
4. Which institution subordinated to the Ministry of Internal Affairs will be responsible for implementing this draft law?

The draft partially answers the fourth question: implementation falls to the specialised subdivision responsible for international police cooperation within the General Police Inspectorate — the Single Point of Contact, which includes the INTERPOL National Central Bureau, the EUROPOL National Contact Point and the SIRENE National Bureau (Article 6). However, it remains unclear who bears overall responsibility for security and access governance across the entire mechanism.

VI. Recommendations

In order for the mechanism to be effective, secure and worthy of citizens' trust, the Movement recommends supplementing the draft, prior to adoption, with:

1. a mandatory minimum security baseline applicable to all integrations, enshrined in the law or through reference to a verifiable normative act;
2. a mandatory security assessment prior to connection/go-live, separate from the DPIA, including formal security approval;
3. an explicit IAM model — MFA, RBAC, least privilege, segregation of duties, periodic access reviews with defined deadlines, deactivation upon termination of duties, emergency access and a designated responsible person;
4. a unified retention and deletion schedule by category of data, including rules for backups and false-positive results;
5. an incident-response model including classification, escalation chain, deadlines and post-incident analysis;
6. continuous security monitoring — SIEM-based log correlation, alerting, anomaly detection and immutable logs;
7. security requirements for third parties and the supply chain, including contractual clauses and audit rights;
8. vulnerability and update management, with deadlines and mandatory testing following changes;

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

9. a security responsibility matrix and designation of a single person responsible for the overall security posture of the mechanism;
10. express delineation of oversight competences between the CNPDCP, the Electronic Governance Agency, the cybersecurity authority and the Single Point of Contact;
11. a clear and rapid redress mechanism for individuals affected by inaccurate or unlawfully used data;
12. incorporation into the organic law of the essential safeguards currently delegated to the Government.

VII. Conclusion

The Civic Movement "Building Trust" welcomes the intention to align the Republic of Moldova with European standards on police cooperation and supports the adoption of a modern legal framework in this field. However, we call for the draft to be supplemented with the security safeguards, access-governance mechanisms and protections for citizens outlined above, so that the enhanced power to exchange sensitive data is matched by an equally robust level of oversight. Only a secure and transparent mechanism can deserve citizens' trust — the trust we have committed ourselves to building.

Civic Movement "Building Trust"

Chișinău, 25 August 2026